

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту Web-сайту компа-
нії»

Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Євгеній Єзюкинський

Керівник професор кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

Рецензент доцент кафедри КІ та КБ, к.т.н., доцент

 Юрій Бродський

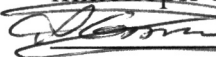
Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Єзюкинський Євгеній Олексійович

Тема роботи: «Проект підсистеми захисту Web-сайту компанії»

затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 29 червня 2023 р.

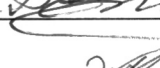
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

є проєкт підсистеми захисту веб-сайту компанії;

Обладнання та програмне забезпечення:

1. Windows 10
2. VisualStudio Code
3. Postman

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Воротніков В.В	1.03.23 	 01.03.2023
2	Воротніков В.В	1.03.23 	 01.03.2023
3	Пірог О.В.	1.03.23 	 01.03.2023

Студент  Євгеній Єзюкинський
Керівник  Володимир Воротніков

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір теми кваліфікаційної роботи	14.02.2023 06.03.2023	
2	Аналіз теоретичних основ проектування веб-сайту	07.03.2023 11.03.2023	
3	Аналіз теоретичних основ розробки веб-сайту	15.03.2023 – 25.03.2023	
4	Аналіз теоретичних основ захисту веб-сайту	27.03.2023 05.04.2023	
5	Створення та налаштування бази даних	08.04.2023 17.04.2023	
6	Розробка Back частини веб-сайту	19.04.2023 30.04.2023	
7	Розробка Front частини веб-сайту	3.05.2023 8.05.2023	
8	Налагодження захисту веб-сайту	10.05.2023 25.05.2023	
9	Тестування працездатності системи	30.05.2023 31.05.2023	
10	Написання пояснювальної записки	01.06.2023 19.06.2023	
11	Захист	29.06.2023	

Студент  Євгеній Єзюкинський

Керівник  Володимир Воротніков

АНОТАЦІЯ

Текстова частина викладена на 55 сторінках друкованого тексту.

Пояснювальна записка не має додатків. Список використаних джерел містить 13 найменувань та займає 2 сторінки. В роботі наведено 39 рисунки. Загальний обсяг роботи – 56 сторінок.

Мета кваліфікаційної роботи полягає у розробці проекту підсистеми захисту Web-сайту компанії. У кваліфікаційній роботі досліджено основні концепції та методи захисту веб-сайту. Розглянуто процес розробки та захисту сайту. Після розробки було проведено тестування безпеки ручним методом. Ключові слова: ЗАХИСТ, ВЕБ-САЙТ, CSRF, FIREWALL, BCrypt, ТЕСТУВАННЯ.

КІК.КР.Б – 125 – 04 – ПЗ

Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Єзюкинський Є.О.		23.06.19	Літ.	Арк.	Аркушів
Керівник		Воротніков В.В.		23.06.19		1	45
Реценз.		Бродський Ю.Б.		23.06.19	ФІКТ гр. КБ-19-1		
Н. контр.							
Затвердив		Єфіменко. А.А.		23.06.19			

Проект підсистеми захисту
Web-сайту компанії

ANNOTATION

The textual part of the work is presented in 55 pages of printed text. The explanatory note does not include any appendices. The list of used sources contains 13 references and spans 2 pages. The work includes 39 figures. The total volume of the work is 46 pages. The objective of this qualification work is to develop a project for the web site protection subsystem of the company. The qualification work explores the fundamental concepts and methods of web site protection. The process of web site development and protection is discussed. After the development, manual security testing was conducted. Keywords: PROTECTION, WEB SITE, CSRF, FIREWALL, BCrypt, TESTING.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		2

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	4
ВСТУП:	5
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ СТВОРЕННЯ ТА ЗАХИСТУ ВЕБ-САЙТУ	6
1.1 Основні принципи створення веб-сайту.....	6
1.2 Загрози безпеці веб-сайту	9
1.3 Заходи захисту веб-сайту	11
1.4 Тестування та аудит безпеки веб-сайту.....	15
Висновки до першого розділу	20
РОЗДІЛ 2 РОЗРОБКА ТА ЗАХИСТ ВЕБ-САЙТУ	22
2.1 Аналіз вимог	22
2.2 Проектування ERP системи	22
2.3 Розробка та захист функціональності веб-сайту	31
Висновок до другого розділу	42
РОЗДІЛ 3. ТЕСТУВАННЯ ВЕБ-САЙТУ	43
3.1 Розробка плану тестування	43
3.2 Результати тестування додатку	45
Висновки до 3 розділу	50
ВИСНОВКИ.....	52
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	54

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ERP – Планування ресурсів підприємства

БД – База даних

ПЗ – Програмне забезпечення

XSS – Міжсайтовий скриптинг

CSRF – Підробка міжсайтових запитів

BCRYPT – Адаптивна криптографічна хеш-функція формування ключа

SEO – Оптимізація під пошукові системи

SQL – Мова структурованих запитів

URL – Єдиний вказівник на ресурс

TLS – Протокол захисту на транспортному рівні

CSS – Спеціальна мова, що використовується для запису оформлення сторінок, написаних мовами розмітки даних

HTML – Мова розмітки гіпертексту

JavaScript – динамічна, об'єктно-орієнтована прототипна мова програмування

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		4

ВСТУП:

Актуальність теми. З поширенням інтернет-технологій та зростанням кількості веб-сайтів, захист інформації, що знаходиться на цих сайтах, стає надзвичайно важливою задачею для компаній. Захист веб-сайту компанії від різних видів кібератак є актуальною темою, оскільки втрати даних або доступ до важливої інформації можуть призвести до серйозних фінансових, репутаційних та правових проблем.

Метою кваліфікаційної роботи є розробка та реалізація проєкту підсистеми захисту веб-сайту компанії. Головним завданням цього проєкту є забезпечення високого рівня безпеки веб-сайту, захист його від різних видів атак, таких як вторгнення, кросс-сайтовий скриптинг, впровадження шкідливого програмного забезпечення тощо. Крім того, метою є також забезпечення контролю доступу до веб-сайту та захист основних ресурсів компанії, що знаходяться на ньому.

Об'єктом дослідження є проєкт підсистеми захисту веб-сайту компанії. У рамках даної роботи буде проведений аналіз загроз, що можуть впливати на веб-сайт компанії, визначені важливі ресурси, які потребують захисту, та розроблені технічні рішення для забезпечення безпеки веб-сайту.

Предметом дослідження є процес розробки та реалізації підсистеми захисту веб-сайту компанії. Дослідження буде орієнтоване на вивчення сучасних методів і технологій захисту веб-сайтів, розробку архітектури та функціональності підсистеми, а також на впровадження та тестування її ефективності. Основними аспектами дослідження будуть ідентифікація загроз, визначення вразливостей веб-сайту, розробка та впровадження заходів захисту, а також оцінка ефективності цих заходів.

Ця кваліфікаційна робота має на меті вирішення проблем безпеки веб-сайтів компаній, що є важливим кроком у підвищенні рівня захищеності інформації та забезпеченні безперебійної роботи бізнесу. Результати дослідження та розробки проєкту підсистеми захисту будуть корисними для компаній, які прагнуть забезпечити безпеку своїх веб-сайтів та уникнути потенційних загроз

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		5

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ СТВОРЕННЯ ТА ЗАХИСТУ ВЕБ-САЙТУ

1.1 Основні принципи створення веб-сайту

Розробка веб-сайту включає кілька ключових етапів, які допомагають забезпечити успішну реалізацію проекту. Основні етапи розробки веб-сайту включають:[7]

- Планування та аналіз: На цьому етапі визначаються цілі та вимоги проекту, проводиться дослідження цільової аудиторії, аналіз конкурентів та визначення ключових функціональних та дизайнерських вимог.
- Проектування інформаційної структури: На цьому етапі створюється структура веб-сайту, його інформаційна архітектура та навігація. Розробляється схема сторінок, меню та логіка взаємодії користувача з сайтом.
- Веб-дизайн та інтерфейс: На цьому етапі створюється дизайн веб-сайту, включаючи вибір кольорової палітри, шрифтів, графічних елементів та компонентів. Розробляється інтерфейс користувача з урахуванням зручності використання та естетичних принципів.
- Розробка функціональності: На цьому етапі програмісти реалізують функціональність веб-сайту. Використовуються веб-технології та мови програмування, такі як HTML, CSS, JavaScript, а також фреймворки та бібліотеки для розробки конкретних функцій.
- Тестування та налагодження: На цьому етапі проводиться випробування різних аспектів веб-сайту, включаючи перевірку функціональності, сумісності з різними пристроями та браузерами, а також оптимізацію продуктивності. Виявлені помилки виправляються та вносяться необхідні зміни.
- Розгортання та підтримка: Після успішного тестування веб-сайт готується до розгортання на веб-сервері, доменному хостингу або іншій інфраструктурі. Після розгортання проводиться постійна підтримка, оновлення та виправлення помилок для забезпечення безперебійної роботи сайту.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		6

Одним з ключових аспектів створення веб-сайту є вибір технологічного стеку, який визначає набір інструментів та технологій, що використовуються під час розробки. У даному розділі ми розглянемо технологічний стек, який складається з NEXT.js, PostgreSQL та Nest.js

NEXT.js є потужним фреймворком розробки веб-додатків, який базується на популярній JavaScript бібліотеці React. Він надає можливість створювати швидкі та ефективні веб-сайти з використанням серверного рендерингу (SSR) та статичного генерування (SSG). NEXT.js забезпечує високу продуктивність, швидке завантаження сторінок та розширені можливості для SEO оптимізації. Крім того, він надає зручні інструменти для роботи з маршрутизацією, стилізацією та управлінням станом додатку.

PostgreSQL є потужною та надійною системою керування базами даних, яка використовує реляційну модель даних. Вона володіє великим набором функцій та можливостей, таких як підтримка транзакцій, оптимізація запитів, реплікація даних та висока масштабованість. PostgreSQL забезпечує безпеку даних та надійність, що є важливими аспектами для захисту веб-сайту компанії.

Nest.js є фреймворком для створення ефективних та масштабованих серверних додатків з використанням TypeScript. Він базується на принципах модульності, розширюваності та реактивного програмування. Nest.js надає зручний спосіб організації коду, підтримує різні типи розробки (монолітні, мікросервісні архітектури) та надає багато інструментів для розробки API та взаємодії з базою даних.

Використання NEXT.js, PostgreSQL та Nest.js у технологічному стеці дозволяє створювати веб-сайти з високою продуктивністю, швидким завантаженням сторінок та потужним функціоналом. Вони підтримують модульну архітектуру, що дозволяє зручно розширювати та підтримувати код. Крім того, цей технологічний стек забезпечує високий рівень безпеки та надійності, що є критичними факторами при захисті веб-сайту компанії.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		7

Використання сучасних стандартів та протоколів веб-розробки є важливим для ефективної та стабільної реалізації веб-проектів. Ось декілька причин, чому використання таких стандартів має велику вагу:

Сумісність: Сучасні стандарти веб-розробки, такі як HTML5, CSS3, та JavaScript ES6, є прийнятими і розповсюдженими стандартами, які підтримуються більшістю сучасних браузерів. Використання цих стандартів забезпечує сумісність веб-сайту на різних платформах та забезпечує однаковий вигляд і поведінку незалежно від використововуваного браузера чи пристрою.

Покращена продуктивність: Сучасні стандарти та протоколи веб-розробки дозволяють розробникам створювати більш продуктивні та швидкі веб-сайти. Нові можливості HTML5 та CSS3 дозволяють ефективно використовувати ресурси пристрою, зменшуючи завантаження сторінок та покращуючи час відгуку. Протоколи, такі як HTTP/2, дозволяють знижувати час завантаження сторінок шляхом одночасної передачі багатьох ресурсів.

Мобільна адаптація: З ростом використання мобільних пристроїв для доступу до Інтернету, важливо мати веб-сайт, який адаптується до різних екранних розмірів та можливостей мобільних пристроїв. Сучасні стандарти та протоколи веб-розробки дозволяють створювати адаптивні та мобільно-дружні дизайни, які забезпечують оптимальний користувацький досвід на будь-якому пристрої.

Безпека: Стандарти та протоколи веб-розробки також включають набір рекомендацій та заходів безпеки, які допомагають зменшити ризики для веб-сайту. Наприклад, використання HTTPS забезпечує шифрування даних, що передаються між сервером та клієнтом, тим самим захищаючи конфіденційну інформацію. Крім того, сучасні стандарти дозволяють використовувати механізми аутентифікації та авторизації для забезпечення безпеки доступу до веб-ресурсів.

Підтримка розширення та масштабованості: Використання сучасних стандартів та протоколів спрощує підтримку та розширення веб-сайту у майбутньому. Це означає, що ви можете легко додавати нові функції, модулі та покращувати функціональність вашого веб-сайту, зберігаючи сумісність зі стандартами та найкращими практиками розробки.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Використання сучасних стандартів та протоколів веб-розробки є ключовим фактором у створенні ефективних, безпечних та сумісних веб-сайтів. Вони дозволяють розробникам максимально використовувати можливості сучасних технологій та забезпечують зручний користувацький досвід на будь-яких пристроях та платформах.

Висновок до підрозділу 1.2

1.2 Загрози безпеці веб-сайту

Сучасні веб-сайти стикаються з різноманітними видами кібератак, які можуть негативно вплинути на їх безпеку та надійність. Ось кілька основних видів кібератак, з якими веб-сайти можуть зіткнутися:

DDoS-атаки (розподілене заподіювання відмови в обслуговуванні): У цьому типі атак зловмисники намагаються перевантажити сервер веб-сайту, надсилаючи велику кількість запитів одночасно. Це може призвести до перебоїв у роботі сайту та недоступності для користувачів.

SQL-ін'єкції: Ця атака полягає в використанні недостатньо захищених запитів до бази даних. Зловмисник вставляє зловісний SQL-код у вхідні дані, що може призвести до некоректної обробки запиту та витоку чутливої інформації.

Кросс-сайтові скрипти (XSS): У цьому типі атак зловмисник вставляє зловісний скрипт у веб-сторінку, який виконується у браузері користувача. Це може призвести до крадіжки конфіденційних даних, перенаправлення на шахрайські сайти або зловживання правами користувача.

Крадіжка сесій: Зловмисник, шляхом підкрадання сесійного ідентифікатора користувача, може набути несанкціонований доступ до облікового запису і пов'язаної з ним інформації. Це може призвести до викрадення особистих даних, зміни інформації або навіть виконання дій в ім'я користувача.

Зловмисники часто використовують вразливості в програмному забезпеченні веб-сайтів для здійснення атак. Основні вразливості включають:

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		9

Недостатня перевірка введення: Веб-сайти повинні правильно перевіряти вхідні дані від користувачів, щоб запобігти вводу шкідливих символів або коду. Недостатня перевірка введення може призвести до вразливостей, таких як SQL-ін'єкції або XSS-атаки.

Відсутність або слабкі паролі: Використання недостатньо складних або легко вгадуваних паролів робить веб-сайт більш вразливим до атак перебору паролів.

Застаріле програмне забезпечення: Недостатнє оновлення програмного забезпечення може призвести до наявності вразливостей, які використовуються зловмисниками. Регулярні оновлення та патчі важливі для забезпечення безпеки веб-сайту.

Соціальний інжиніринг є методом атаки, який залучає маніпуляцію людьми з метою отримання несанкціонованого доступу до веб-сайту. Наприклад, це може бути фішингова атака, де зловмисник видаватиметься за довірену особу або організацію, намагаючись отримати від користувачів конфіденційну інформацію, таку як паролі або особисті дані. Соціальний інжиніринг вимагає від учасників веб-сайту бути пильними та обережними, щоб уникнути попадання в пастку зловмисників.

Загрози, пов'язані з порушенням аутентифікації та авторизації

Аутентифікація та авторизація є важливими компонентами безпеки веб-сайту. Однак, недостатня аутентифікація та авторизація можуть призвести до наступних загроз:

Підбір пароля: Зловмисники можуть намагатися вгадати або підібрати паролі користувачів, щоб отримати несанкціонований доступ до їх облікових записів.

Крадіжка сесій: Зловмисники можуть намагатися викрасти сесійні ідентифікатори користувачів, щоб отримати несанкціонований доступ до їх облікових записів.

Перехоплення токенів: У випадку використання токенів для авторизації, зловмисники можуть намагатися перехопити токени та використовувати їх для отримання доступу до ресурсів, на які вони не мають права.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Для запобігання цим загрозам рекомендується використовувати надійні методи аутентифікації та авторизації, а також регулярно оновлювати заходи безпеки, щоб забезпечити безпечну роботу веб-сайту.

1.3 Заходи захисту веб-сайту

Захист веб-сайту є важливим аспектом забезпечення безпеки для його користувачів і збереження цілісності та доступності даних. Цей розділ розглядає різноманітні заходи захисту, які можуть бути використані для забезпечення безпеки веб-сайту.

Встановлення Firewall

Встановлення Firewall є важливим етапом у забезпеченні безпеки веб-сайту. Ці заходи допомагають виявляти та блокувати небажану мережеву активність, включаючи потенційно шкідливі атаки та недозволений доступ до системи. Вони забезпечують захист на рівні мережі, контролюючи вхідний та вихідний мережевий трафік.

Основною функцією Firewall є моніторинг мережевого трафіку та виявлення потенційно шкідливої активності. Вони аналізують пакети даних, що переходять через мережу, і порівнюють їх з набором правил і правил безпеки. Якщо виявляється підозріла активність або відбувається спроба несанкціонованого доступу, Firewall приймає відповідні заходи, наприклад, блокування зловмисного трафіку або сповіщення адміністратора системи про потенційну загрозу. Одним з важливих компонентів Firewall є мережеві фільтри. Вони встановлюються на рівні мережевого обладнання, такого як маршрутизатори або фایрволи, і контролюють трафік, що проходить через мережу. Мережеві фільтри дозволяють встановлювати правила, які визначають, який тип трафіку допускається або блокується. Наприклад, можуть бути встановлені правила для блокування певних портів, протоколів чи IP-адрес. Додатковою функцією Firewall може бути виявлення та захист від різних видів атак, таких як DDoS-атаки (розподілені атаки перевантаження), атаки на вразливості мережевих протоколів чи атаки на рівні застосунків. Вони можуть використовувати різні методи, включаючи аналіз пакетів

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				11
Змн.	Арк.	№ докум.	Підпис	Дата		

даних, інтелектуальний аналіз поведінки, фільтрацію за виявленими сигнатурами атак та інші методи для виявлення та запобігання атакам.

Загалом, встановлення Firewall є важливим етапом у захисті веб-сайту. Вони допомагають забезпечити безпеку мережі, виявляти та блокувати потенційно шкідливу активність та захищати веб-сайт від небажаного доступу та атак.

Використання SSL-шифрування для захисту передачі даних

SSL (Secure Sockets Layer) або його більш безпечна версія TLS (Transport Layer Security) є широко використовуваними протоколами шифрування, які дозволяють забезпечити безпеку передачі даних між веб-сервером і клієнтом. Використання SSL-шифрування дозволяє забезпечити конфіденційність та цілісність передачі даних, запобігаючи їх перехопленню або зміні зловмисниками. Це особливо важливо для передачі чутливої інформації, такої як особисті дані або фінансова інформація.

Застосування механізмів аутентифікації та авторизації

Застосування механізмів аутентифікації та авторизації є ключовими аспектами забезпечення безпеки веб-сайту. Ці механізми дозволяють ідентифікувати користувачів, перевіряти їх правомочності та керувати рівнями доступу до ресурсів сайту. Основна мета полягає у запобіганні несанкціонованому доступу до конфіденційної інформації та дій на веб-сайті.

Нижче наведені деякі важливі механізми аутентифікації та авторизації:

Користувальницькі облікові записи: Веб-сайт повинен вимагати від користувачів створення облікових записів з унікальними ідентифікаторами та безпечними паролями. Для забезпечення безпеки, рекомендується використовувати механізми перевірки паролів, такі як хешування та використання солі, щоб унеможливити зловмисникам отримання паролів у разі скомпрометування бази даних.

Багаторівнева аутентифікація: Для підвищення рівня безпеки можна використовувати механізми багаторівневої аутентифікації. Наприклад, можна вимагати введення додаткових факторів аутентифікації, таких як одноразові паролі через SMS або електронну пошту, біометричні дані або апаратні токени.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Управління правами доступу: Веб-сайт повинен мати систему управління правами доступу, яка дозволяє адміністраторам надавати різні рівні доступу користувачам в залежності від їх ролі і обов'язків. Це забезпечує контроль над тим, які ресурси мають доступність для кожного користувача і запобігає несанкціонованому доступу до конфіденційної інформації.

Часове обмеження сесій: Для запобігання атакам на перехоплення сесій, веб-сайт може встановлювати обмеження на тривалість сесій. Після певного періоду неактивності користувача або вийдів з системи сесія автоматично завершується, що допомагає зменшити ризик несанкціонованого доступу до облікових записів.

Моніторинг та журналювання: Веб-сайт повинен мати механізми моніторингу та журналювання, які дозволяють виявляти підозрілу активність, неуспішні спроби входу та інші можливі загрози. Регулярний аналіз журналів допомагає виявляти вразливості та негайно реагувати на можливі атаки.

Використання двофакторної автентифікації (2FA): Для підвищення рівня безпеки можна використовувати двофакторну автентифікацію. Це передбачає введення додаткового фактора підтвердження, такого як одноразовий код, отриманий з мобільного пристрою або за допомогою аутентифікатора, разом зі звичайним логіном і паролем.

Застосування механізмів аутентифікації та авторизації дозволяє зменшити ризик несанкціонованого доступу до веб-сайту та його ресурсів. Важливо розробити імплементацію, що відповідає конкретним потребам і характеристикам веб-сайту, а також постійно оновлювати та покращувати ці механізми для забезпечення безпеки.

Впровадження системи моніторингу та виявлення вторгнень (IDS/IPS)

Впровадження системи моніторингу та виявлення вторгнень (IDS/IPS) є ще одним важливим заходом для захисту веб-сайту. IDS (система виявлення вторгнень) та IPS (система запобігання вторгнень) використовуються для виявлення, моніторингу та запобігання небажаним або зловмисним діям в мережі та на сервері. IDS використовується для моніторингу мережевого трафіку та ідентифікації

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		13

підозрілої або ворожої активності. Він аналізує пакети даних, що переходять через мережу, та порівнює їх з базою правил або виявляє аномальні патерни, які можуть свідчити про потенційну атаку. IDS може сповіщати адміністратора системи про виявлені загрози, а також записувати журнали подій для подальшого аналізу.

IPS, у свою чергу, не тільки виявляє небажану активність, але й приймає активні заходи для її запобігання. Він може автоматично блокувати або відхиляти пакети даних, які відповідають певним критеріям вторгнення. Це дозволяє реагувати на потенційні загрози в реальному часі та зменшує ризик успішного вторгнення.

IDS/IPS можуть мати різні методи виявлення вторгнень, включаючи сигнатурний аналіз, що використовує відомі сценарії атак, та аналіз поведінки, що виявляє незвичайні або відхиляються дії. Деякі системи IDS/IPS також використовують машинне навчання або штучний інтелект для виявлення нових, раніше невідомих атак.

Впровадження IDS/IPS дозволяє забезпечити постійний моніторинг безпеки веб-сайту та реагувати на потенційні загрози в реальному часі. Вони можуть виявляти і блокувати атаки, такі як вторгнення в мережу, веб-додатки, DDoS атаки та інші небажані дії. Подальший аналіз журналів подій IDS/IPS також може допомогти виявити слабкі місця в системі та прийняти відповідні заходи для їх усунення.

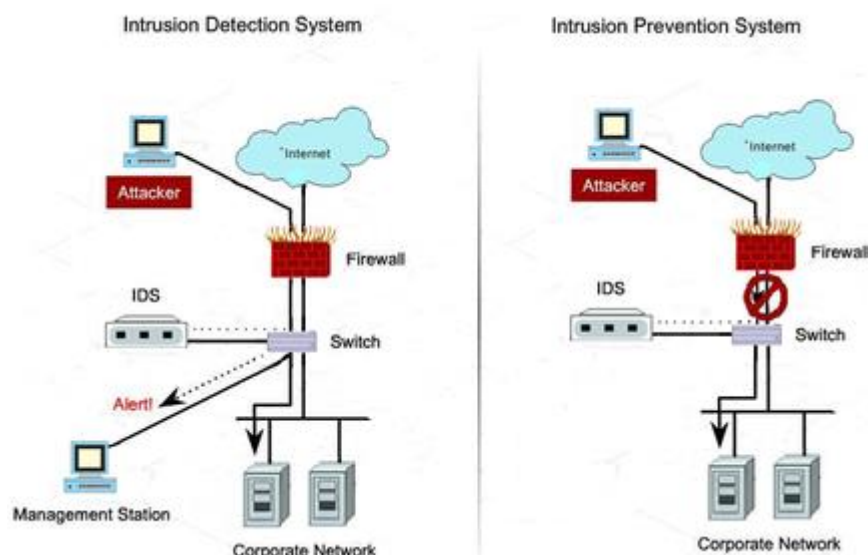


Рис.1.1 Зліва поведінка IDS, справа поведінка IPS

Захист від вразливостей, таких як кросс-сайтовий скриптинг та інші атаки

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Забезпечення захисту від вразливостей є необхідним кроком для запобігання різним типам атак, включаючи кросс-сайтовий скриптинг (XSS) та інші вразливості. Для цього можуть застосовуватись різні підходи, такі як регулярні оновлення веб-сервера та веб-додатків, використання безпечних програмних бібліотек, перевірка та валідація вхідних даних, обмеження прав доступу до файлів та ресурсів, а також проведення тестування на проникнення. Ці заходи допомагають знизити ризик вразливостей і підвищують загальний рівень безпеки веб-сайту.

В цьому розділі було розглянуто кілька основних заходів захисту веб-сайту, включаючи встановлення Firewall, використання SSL-шифрування для захисту передачі даних, застосування механізмів аутентифікації та авторизації, впровадження системи моніторингу та виявлення вторгнень, а також захист від вразливостей. Використання цих заходів допомагає підвищити безпеку веб-сайту та забезпечити захист користувачів та їхніх даних.

1.4 Тестування та аудит безпеки веб-сайту

Тестування та аудит безпеки веб-сайту є важливими етапами процесу забезпечення безпеки. Огляд основних методів тестування безпеки веб-сайту включає ряд підходів та інструментів, які допомагають ідентифікувати потенційні вразливості та проблеми безпеки. Нижче наведено деякі з цих методів:

Сканування вразливостей: Цей метод використовується для автоматичного виявлення вразливостей веб-сайту. Зазвичай використовуються спеціалізовані програми, відомі як сканери вразливостей, які аналізують веб-сайт з метою виявлення популярних вразливостей, таких як незахищені URL-адреси, недостатньо захищені параметри безпеки, слабкі налаштування сервера та інші.

Тестування на проникнення: Цей метод полягає в спробі активного проникнення в систему з метою виявлення слабких місць та вразливостей. Тестування на проникнення включає різні техніки, такі як спроби зламу паролів,

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				15
Змн.	Арк.	№ докум.	Підпис	Дата		

атаки на вразливості програмного забезпечення, соціально-інженерні атаки та інші методи, що можуть використовувати зловмисники.

Аналіз коду: Цей метод передбачає перевірку програмного коду веб-сайту з метою виявлення потенційних вразливостей. Розглядаються різні аспекти коду, такі як можливість вразливостей кросс-сайтового скриптингу, SQL-ін'єкції, недостатня валідація введених даних та інші проблеми, які можуть бути використані зловмисниками.

Соціальний інженерінг: Цей метод зосереджений на оцінці вразливостей, пов'язаних з людським фактором. Він передбачає проведення контрольованих атак або тестів, які використовують соціальні методи для отримання несанкціонованого доступу до системи. Прикладами можуть бути спроби фішингу, імітація атаки "чоловік посередині" та інші методи маніпулювання користувачами з метою отримання незаконного доступу.

Аудит конфігурації та журналів: Цей метод включає перевірку конфігурації сервера, веб-сайту та системних параметрів з метою виявлення слабких налаштувань, незахищених точок входу або неадекватного журналювання подій. Аудит конфігурації та журналів може допомогти виявити можливі проблеми та встановити належні налаштування безпеки.

Ці методи тестування та аудиту безпеки веб-сайту можуть використовуватися окремо або комбіновано для забезпечення повноцінного та всебічного аналізу безпеки веб-сайту. Важливо зауважити, що тестування безпеки має бути проведене регулярно, оскільки загрози та вразливості можуть змінюватися з часом.

Також можна застосовувати автоматизовані інструменти для виявлення вразливостей. Ці інструменти допомагають автоматично сканувати веб-сайт з метою виявлення потенційних вразливостей, що можуть бути використані зловмисниками для несанкціонованого доступу або атак на систему. Нижче перераховані деякі популярні автоматизовані інструменти для виявлення вразливостей веб-сайтів:

OpenVAS: Це відкрите програмне забезпечення для сканування вразливостей, яке використовується для виявлення широкого спектру проблем

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				16
Змн.	Арк.	№ докум.	Підпис	Дата		

безпеки. OpenVAS включає в себе базу даних відомих вразливостей, а також здатний виявляти нові вразливості шляхом сканування системи.

Nessus: Це комерційний інструмент сканування вразливостей, який забезпечує широкий спектр функцій для виявлення і аналізу потенційних проблем безпеки. Nessus використовує велику базу даних вразливостей та дозволяє автоматично сканувати веб-сайти з метою ідентифікації вразливих точок.

Burp Suite: Це популярний набір інструментів для тестування безпеки веб-додатків, який включає в себе функціонал для сканування вразливостей. Burp Suite може виявляти вразливості, такі як кросс-сайтовий скриптинг, SQL-ін'єкції, переповнення буфера та інші, шляхом автоматичного перебору та аналізу вхідних параметрів.

Acunetix: Це інструмент для автоматизованого сканування вразливостей веб-додатків. Він виявляє різноманітні вразливості, включаючи вразливості на рівні кодування, недостатню перевірку вхідних даних, недостатню авторизацію та багато інших.

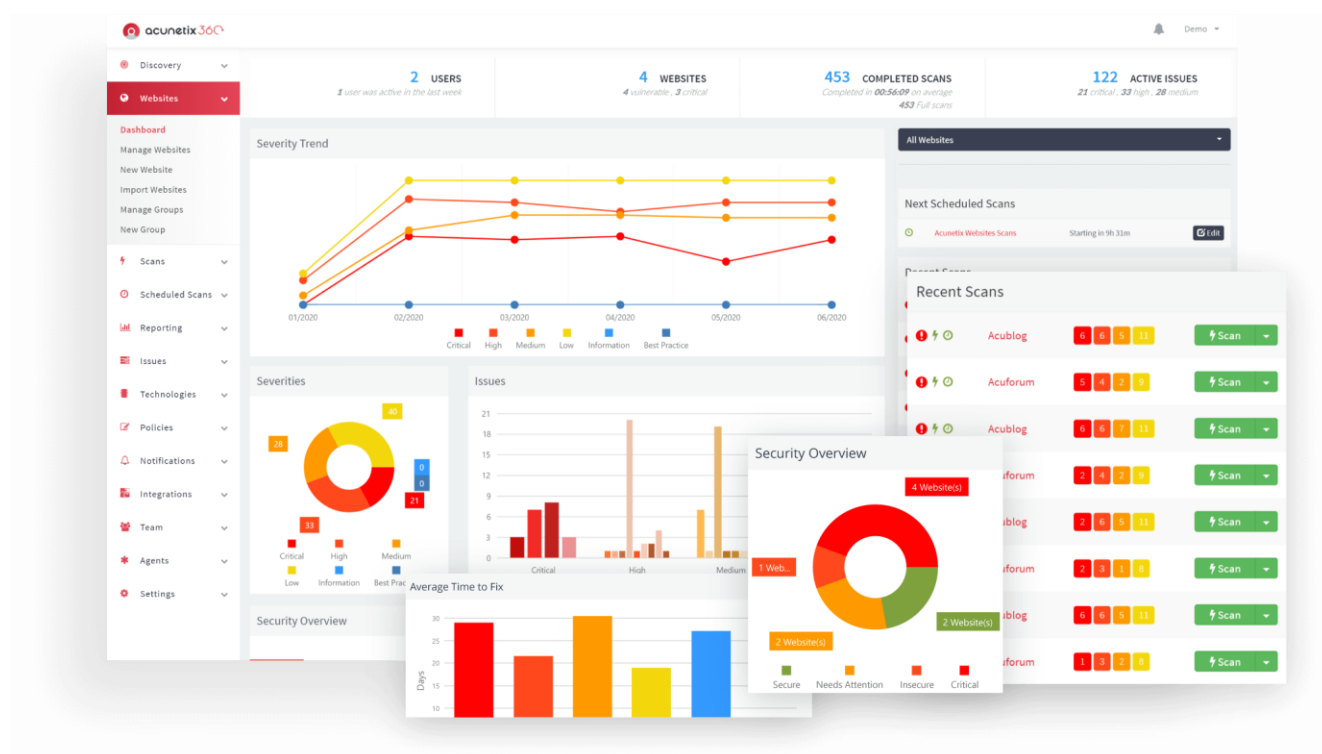


Рис.1.2 Головне меню Acunetix

Ці автоматизовані інструменти дозволяють здійснювати швидке та ефективне сканування веб-сайту для виявлення вразливостей. Важливо зауважити,

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				17
Змн.	Арк.	№ докум.	Підпис	Дата		

що хоча ці інструменти здатні виявляти багато вразливостей, вони не замінюють необхідність проведення ручного аудиту безпеки веб-сайту, який може виявити контекстуальні або складні проблеми безпеки, що не завжди виявляються автоматичними інструментами.

Використання тестування на проникнення (penetration testing) є важливою складовою процесу оцінки рівня захищеності веб-сайту. Цей вид тестування включає спробу проникнення в систему з боку потенційного зловмисника з метою виявлення потенційних вразливостей та визначення ризиків, пов'язаних з безпекою.

Тестування на проникнення зазвичай виконується командою експертів з безпеки, які відтворюють дії потенційного зловмисника, спробуючи проникнути в систему або отримати несанкціонований доступ до конфіденційної інформації. Основна мета тестування на проникнення полягає в ідентифікації слабких місць у системі та розробці рекомендацій щодо поліпшення безпеки.

Під час тестування на проникнення можуть бути використані різні методи та техніки, такі як активне сканування портів, використання вразливостей, перехоплення трафіку, атаки на аутентифікацію та авторизацію, імітація соціального інжинірингу та інше. Цей процес дозволяє виявити потенційні проблеми безпеки та оцінити їх вплив на систему.

Після завершення тестування на проникнення експерти з безпеки підготовляють детальний звіт, який включає опис виявлених вразливостей, їх потенційний вплив на систему та рекомендації щодо запобігання та виправлення проблем безпеки. Цей звіт надає команді розробників та адміністраторів веб-сайту важливу інформацію для вдосконалення захисту системи та підвищення її безпеки. Використання тестування на проникнення допомагає виявити слабкі місця веб-сайту, що можуть бути використані зловмисниками для несанкціонованого доступу або атак. Це дозволяє забезпечити веб-сайт ефективними заходами безпеки та зменшити ризик інцидентів, пов'язаних з безпекою.

Проведення аудиту безпеки веб-сайту є необхідним кроком для забезпечення надійності та захищеності системи. Цей процес включає докладний аналіз різних аспектів веб-сайту з метою виявлення потенційних проблем, вразливостей та

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		18

слабких місць, які можуть бути використані зловмисниками для несанкціонованого доступу чи атак на систему.

Аудит безпеки веб-сайту зазвичай починається з інвентаризації ресурсів, тобто виявлення всіх компонентів, що становлять веб-сайт та його інфраструктуру. Це включає перелік серверів, баз даних, веб-додатків, систем керування контентом та інших складових частин. Після цього проводиться оцінка потенційних загроз і ризиків, пов'язаних з кожним з цих компонентів.

Далі аудитор зосереджується на перевірці веб-додатків на наявність вразливостей та потенційних проблем безпеки. Це включає аналіз коду, перевірку на наявність кросс-сайтового скриптингу (XSS), SQL-ін'єкцій, недостатній валідації введених даних та інших вразливостей, які можуть бути використані для атак на систему. Для цього можуть використовуватись автоматизовані інструменти тестування безпеки, а також ручна перевірка веб-додатків з боку експерта з безпеки.

Окрім веб-додатків, аудитор також звертає увагу на мережеву інфраструктуру та конфігурацію серверів. Він перевіряє налаштування фаєрволу, використання безпечних протоколів, наявність необхідних патчів та оновлень, правильну конфігурацію доступу до системи та інші аспекти, що впливають на безпеку веб-сайту.

Після проведення всіх необхідних перевірок, аудитор складає детальний звіт, в якому фіксуються виявлені проблеми безпеки, їх потенційні наслідки та рекомендації щодо усунення проблем. Цей звіт стає цінним документом для власників веб-сайту та адміністраторів системи, оскільки він надає зрозумілу картину щодо поточного стану безпеки та вказує на можливі шляхи поліпшення захисту.

Важливим аспектом проведення аудиту безпеки є його регулярність. Оскільки загрози та вразливості постійно еволюціонують, важливо проводити аудит безпеки на регулярній основі, зазвичай один або два рази на рік, або при внесенні значних змін до веб-сайту чи його інфраструктури.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Узагальнюючи, проведення аудиту безпеки веб-сайту є необхідною складовою частиною процесу забезпечення безпеки. Він дозволяє виявити потенційні проблеми та вразливості, які можуть бути використані зловмисниками, і встановити необхідні заходи для запобігання атакам та забезпечення надійності системи. Результатом аудиту є детальний звіт, який вказує на виявлені проблеми та надає рекомендації щодо їх усунення. Регулярне проведення аудиту є важливою практикою для підтримки безпеки веб-сайту на високому рівні.

Висновки до першого розділу

У цьому розділі було розглянуто теоретичні основи створення та захисту веб-сайту. Були представлені основні етапи процесу розробки веб-сайту, включаючи аналіз вимог, проектування і реалізацію. Також були розглянуті ключові аспекти безпеки веб-сайту, включаючи заходи захисту і методи виявлення потенційних загроз.

Захист веб-сайту є важливою задачею, оскільки веб-сервери і додатки постійно піддаються ризику атак зловмисників. Встановлення Firewall фільтрів, використання SSL-шифрування, застосування механізмів аутентифікації та авторизації, впровадження системи моніторингу та виявлення вторгнень - це лише декілька засобів, які можна використовувати для забезпечення безпеки веб-сайту. Крім того, було розглянуто методи тестування безпеки веб-сайту, такі як використання автоматизованих інструментів для виявлення вразливостей та тестування на проникнення. Ці методи допомагають ідентифікувати потенційні проблеми та вразливості, що дозволяє розробникам прийняти відповідні заходи для виправлення та підвищення рівня захищеності системи.

Аудит безпеки веб-сайту є ще одним важливим етапом, що дозволяє оцінити поточний рівень захищеності системи та виявити потенційні проблеми. Цей процес включає перевірку конфігурацій, перевірку вразливостей та аналіз журналів подій, що допомагає виявити слабкі місця та вжити відповідних заходів для поліпшення безпеки.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Узагалі, знання теоретичних основ створення та захисту веб-сайту є ключовим для забезпечення безпеки в цифровому середовищі. Розуміння основних концепцій та застосування відповідних заходів безпеки дозволяє розробникам створювати надійні та безпечні веб-сайти, що мінімізує ризики атак та зловмисного використання інформації.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		21

РОЗДІЛ 2 РОЗРОБКА ТА ЗАХИСТ ВЕБ-САЙТУ

2.1 Аналіз вимог

У рамках дипломної роботи на тему "Захист веб-сайту компанії" було обрано створення та захист ERP системи для будівельної компанії під назвою "ТЕРМОУНІВЕРСАЛ". Для успішної розробки та ефективного захисту системи необхідно провести аналіз вимог, який включає визначення основних функціональних та нефункціональних вимог до веб-сайту.

Під час визначення функціональних вимог до ERP системи "ТЕРМОУНІВЕРСАЛ" необхідно врахувати потреби будівельної компанії щодо управління проектами, розкладу робіт, обліку ресурсів та звітності. Функціональні вимоги повинні охоплювати можливості системи з планування та керування будівельними проектами, відстеження робіт та прогресу, обліку матеріалів і ресурсів, а також генерації звітів і аналітичних даних. Крім того, необхідно врахувати вимоги до інтерфейсу користувача, забезпечуючи зручну навігацію, інтуїтивно зрозумілу структуру та зручність використання системи.

Нефункціональні вимоги передбачають встановлення вимог щодо безпеки, надійності, продуктивності, масштабованості та інших аспектів системи. Для ERP системи "ТЕРМОУНІВЕРСАЛ" необхідно встановити вимоги до безпеки даних, забезпечення захисту від несанкціонованого доступу, забезпечення конфіденційності і цілісності інформації. Також вимагається надійність системи, що означає стабільну та безперебійну роботу, враховуючи можливість обробки великого обсягу даних та підтримку багатьох користувачів одночасно. Крім того, вимоги до продуктивності системи передбачають швидкий відгук інтерфейсу та ефективне виконання різноманітних операцій.

2.2 Проектування ERP системи

На цьому етапі буде визначена структура веб-сайту та його інтерфейс. Визначення структури включає розподіл функцій та модулів системи на різні сторінки та розділи, що забезпечують зручну навігацію для користувачів. Розробка

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				22
Змн.	Арк.	№ докум.	Підпис	Дата		

інтерфейсу веб-сайту передбачає вибір кольорової схеми, типографіки, розташування елементів, створення зручного інтерактивного дизайну та інших аспектів, що забезпечують зручність використання та приємний зовнішній вигляд системи.

Основна структура сайту виглядає таким чином:

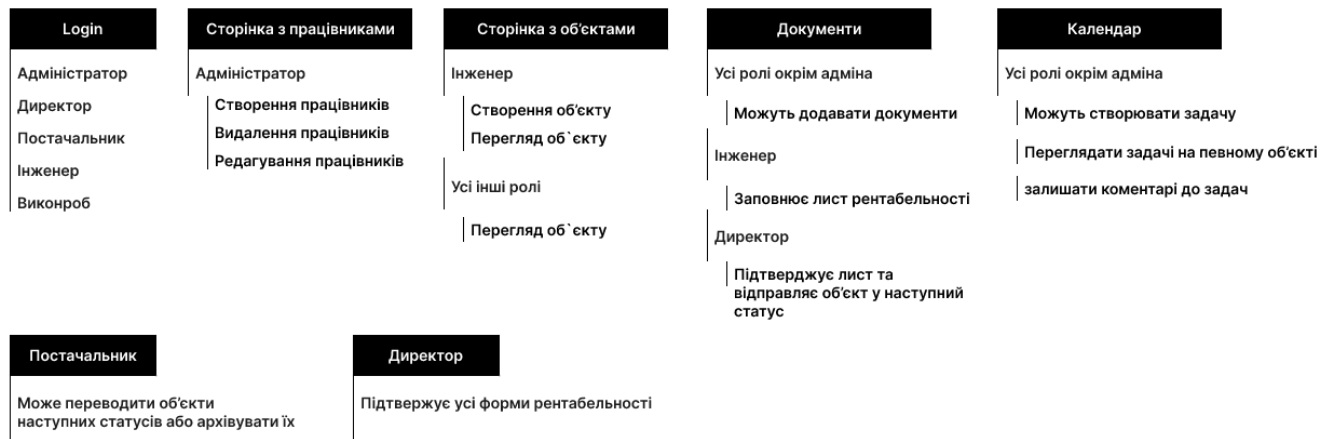


Рис.2.1 Загальна структура ERP системи



Рис.2.2 Модель процесу

Ми маємо 5 ролей: Адміністратор, директор, постачальник та виконроб. Адміністратор має доступ до створення, видалення та редагування нових працівників. Після авторизації (не адміністратор)

Ми потрапляємо на головну сторінку з таблицею усіх об'єктів де інженер може створити нові об'єкти. Усі ж інші ролі можуть тільки їх переглянути.

Після натиску на об'єкт ми бачимо інформацію про нього та форму для додавання документів та листа рентабельності. Інженер заповнює цей лист. Директор його підтвержує. І об'єкт переходить в наступний статус «Підготовка до робіт». У цьому статусі ми можемо повторно заповнити лист рентабельності завантажити «Проект робіт», «Кошторис», «Договір». Директор повинен усе це підтвердити та Постачальник перевести у наступний статус «У роботі». Це основний статус робіт у якому ми можемо додавати задачі у календарі, робити фото звіти з самих робіт, добавляти зарплати, оплати від замовника та непередбачувані витрати. Після того як усі роботи по об'єкту завершилися, Постачальник завершує об'єкт та відправляє його у архів.

Розробка інтерфейсу веб-сайту передбачає вибір кольорової схеми, типографіки, розташування елементів, створення зручного інтерактивного дизайну та інших аспектів, що забезпечують зручність використання та приємний зовнішній вигляд системи.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		24

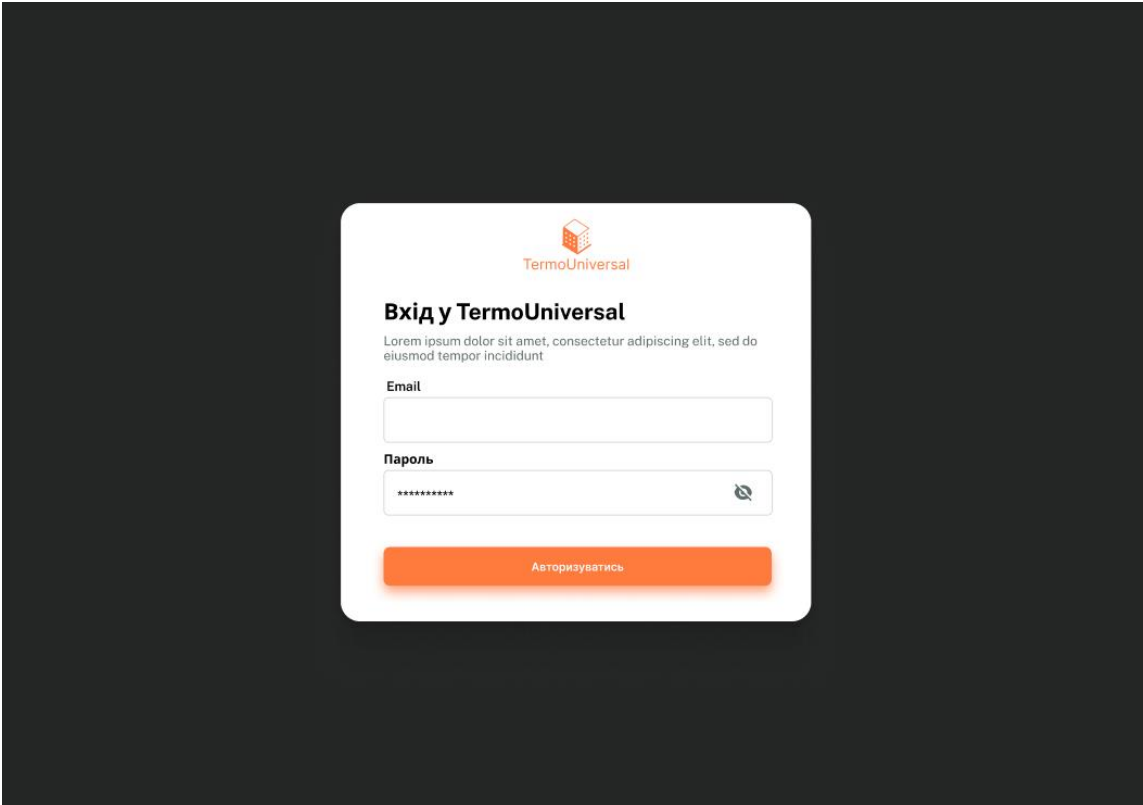


Рис.2.3 Дизайн авторизації

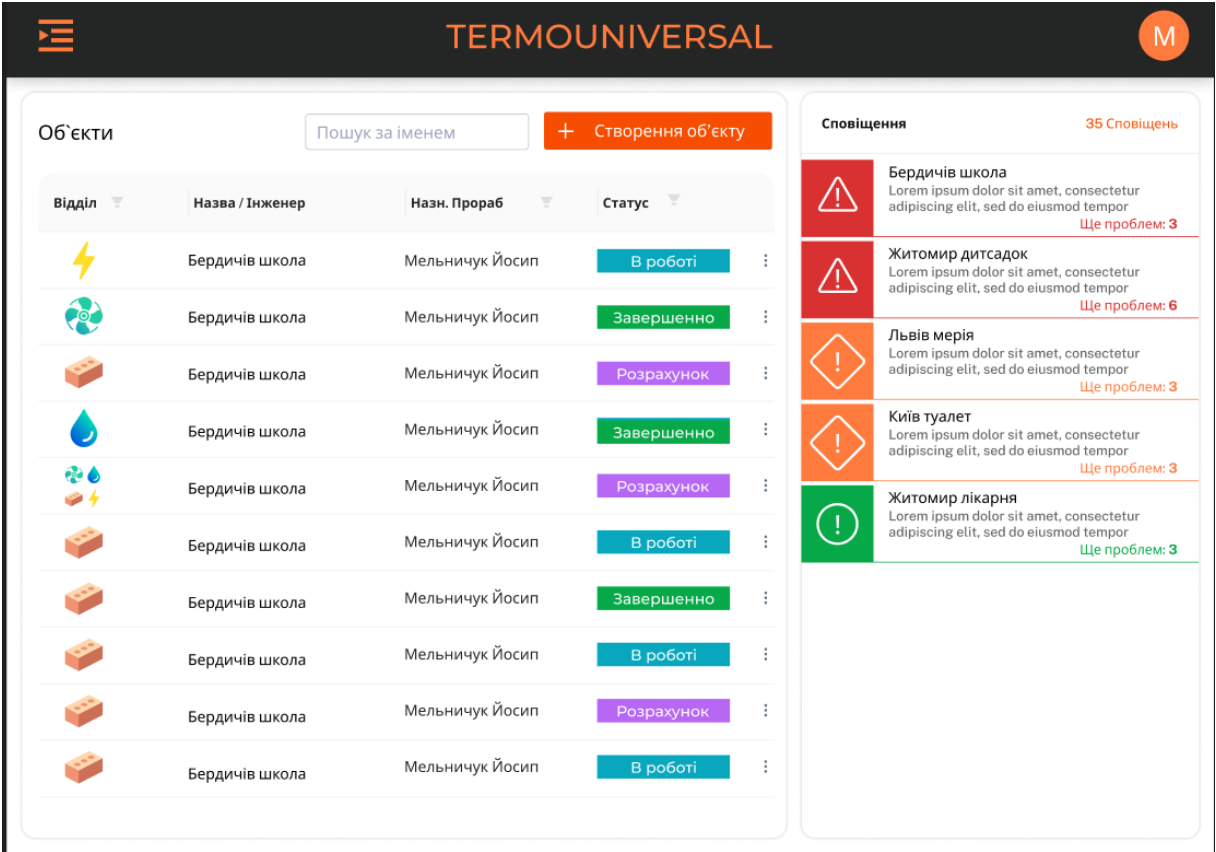


Рис.2.4 Сторінка з об'єктами

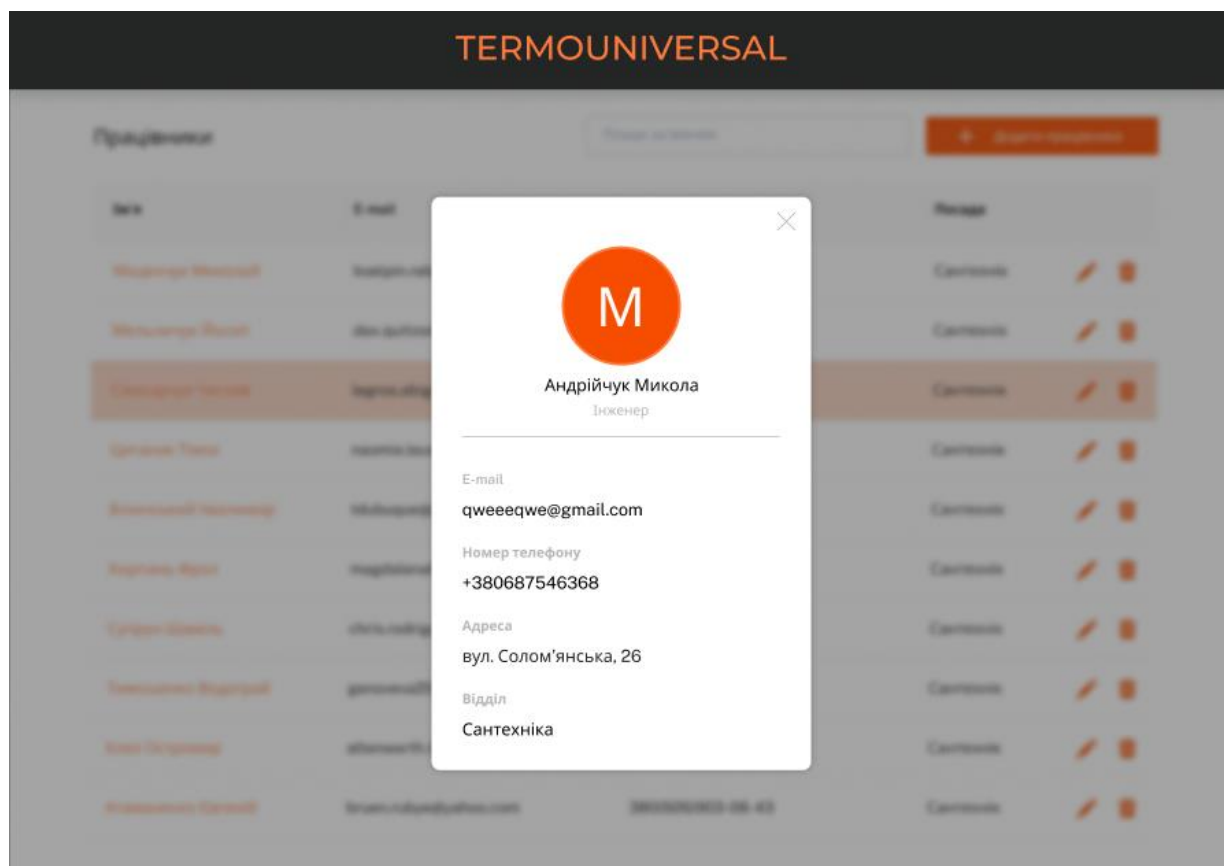


Рис.2.5 Інформація про працівника

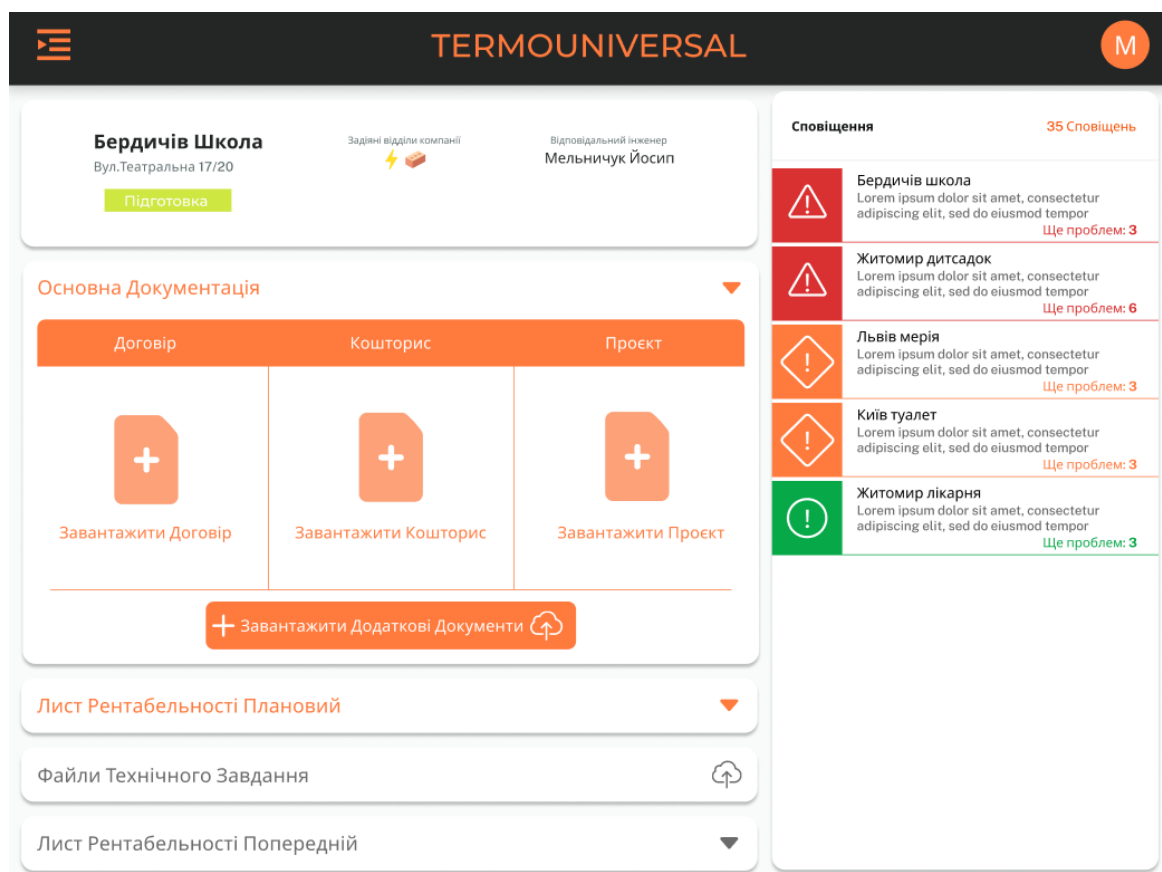


Рис.2.6 Сторінка з документами

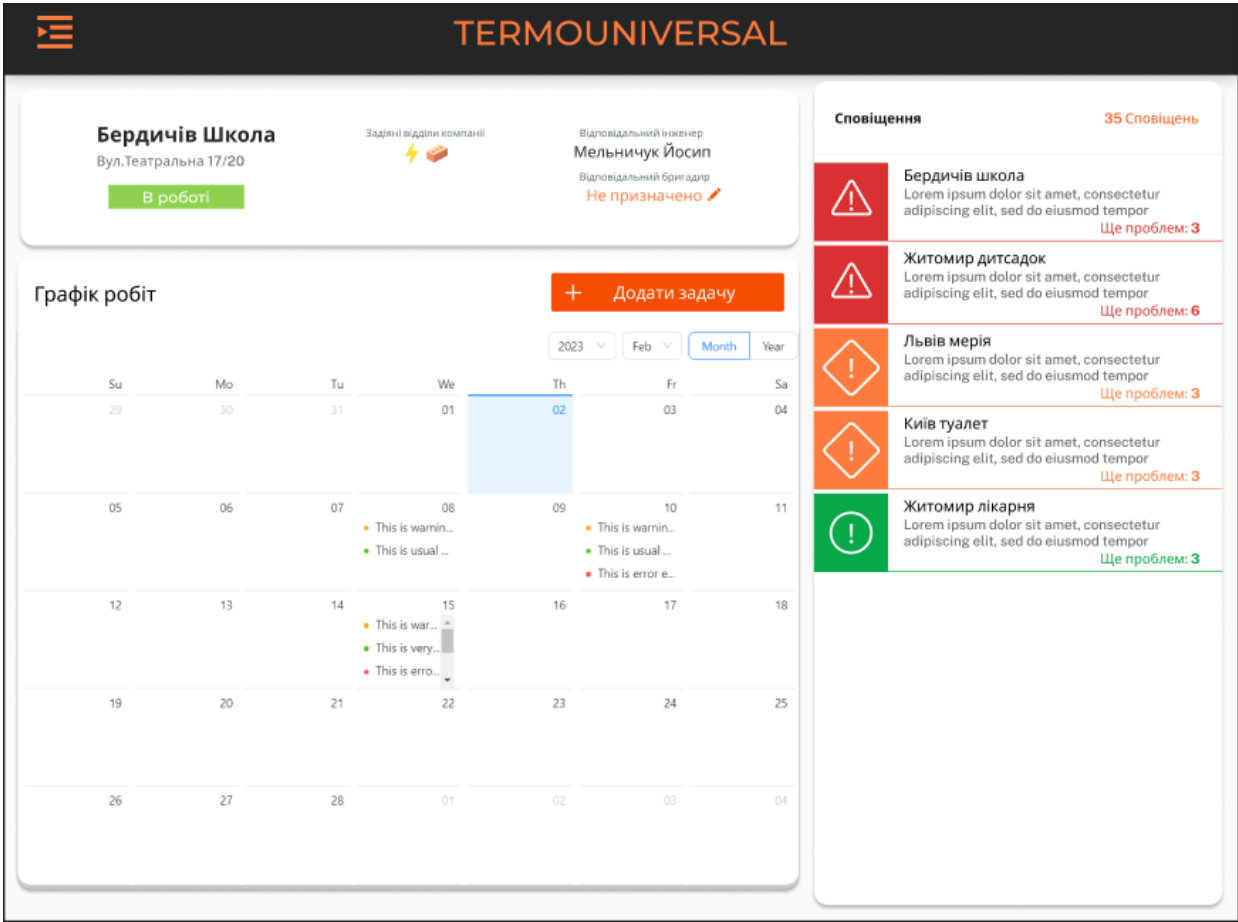


Рис.2.7 Сторінка з календарем та задачами

Працівники				Пошук за іменем		+ Додати працівника
Ім'я	E-mail	Моб.Телефон	Посада			
Мищенко Миколай	koelpin.rebeka@hotmail.com	380(069)312-09-16	Сантехнік			
Мельничук Йосип	dax.quitzon@yahoo.com	380(90)086-39-48	Сантехнік			
Слюсарчук Чеслав	legros.abigayle@gmail.com	380(54)477-62-73	Сантехнік			
Циганик Тімох	naomie.leuschke@hotmail.com	380(66)973-04-70	Сантехнік			
Білинський Хвалимир	tdubuque@gmail.com	380(503)337-25-26	Сантехнік			
Кирпань Фрол	magdalena03@yahoo.com	380(742)797-06-43	Сантехнік			
Супрун Шаміль	chris.rodriquez@hotmail.com	380(275)561-06-43	Сантехнік			
Тимошенко Водограй	genoveva20@hotmail.com	380(70)330-70-59	Сантехнік			

Рис.2.8 Сторінка адміністратора

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Вибір конкретного стеку технологій для розробки ERP системи "ТЕРМОУНІВЕРСАЛ" для будівельної компанії є важливим кроком у процесі забезпечення ефективності, надійності та захищеності веб-сайту. Комбінація NEXT.JS, NEST.JS та PostgreSQL виявилася оптимальною, оскільки кожна з цих технологій вносить свої унікальні переваги і сприяє досягненню успішного результату.

Next.js є одним з ключових компонентів вибраного стеку технологій для розробки та захисту ERP системи "ТЕРМОУНІВЕРСАЛ". Наступні причини були вирішальними при виборі Next.js:

Реактивний підхід: Next.js базується на React, що дозволяє побудувати веб-сайт з високим рівнем динамічності та інтерактивності. Реактивність дозволяє швидко оновлювати вміст сторінки без перезавантаження, що покращує взаємодію з користувачем.

Серверний рендеринг: Next.js надає можливість використовувати серверний рендеринг, що забезпечує швидке відображення вмісту на стороні сервера перед відправкою до клієнта. Це покращує швидкодію та SEO-оптимізацію веб-сайту.

Універсальність: Next.js підтримує як статичні, так і динамічні веб-сайти. Це дозволяє створювати різноманітні розділи та функціональні компоненти, що задовольняють потреби будівельної компанії в ефективному управлінні проектами, персоналом та клієнтами.

Підтримка серверних функцій: Next.js надає можливість використовувати серверні функції, що дозволяє забезпечити обробку запитів на серверному рівні та виконання потрібних дій. Це дозволяє використовувати комплексні бізнес-логіки та забезпечує безпеку веб-додатку.

Розширюваність: Next.js забезпечує гнучку архітектуру, що дозволяє легко розширювати функціональність веб-сайту і додавати нові модулі або компоненти. Це важливо для компанії, яка може швидко реагувати на зміни в бізнес-потребах та вимогах користувачів.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Активна спільнота: Next.js має велику та активну спільноту розробників, яка постійно вносить покращення та забезпечує підтримку. Це забезпечує наявність документації, статей, плагінів та різноманітних ресурсів, що спрощують розробку та захист веб-сайту.

Обираючи Next.js, отримуємо потужну інструментальну базу для створення та захисту ERP системи "ТЕРМОУНІВЕРСАЛ" для будівельної компанії.

Одним з ключових компонентів вибраного стеку технологій для розробки та захисту ERP системи "ТЕРМОУНІВЕРСАЛ" є Nest.js. Наступні переваги сприяли вибору Nest.js:

Модульність та організація коду: Nest.js використовує концепцію модулів, що дозволяє організовувати код в окремі, повторно використовувані блоки. Це сприяє чистоті коду, полегшує його розширення та підтримку, а також сприяє використанню кращих практик розробки.

Підтримка TypeScript: Nest.js базується на мові програмування TypeScript, що дозволяє використовувати сильну типізацію, покращує надійність та стабільність коду. TypeScript надає переваги під час розробки, такі як підказки про типи, рефакторинг та виявлення помилок на етапі компіляції.

Масштабованість: Nest.js забезпечує потужність та гнучкість для створення масштабованих додатків. Він пропонує модульний підхід до розробки, що дозволяє легко розширювати функціональність та додавати нові модулі без необхідності змінювати вже наявний код.

Підтримка HTTP протоколу та API розробки: Nest.js надає зручні інструменти для розробки API, що дозволяють створювати потужні та гнучкі веб-сервіси. Він підтримує різні види маршрутизації, обробку HTTP запитів, аутентифікацію та авторизацію.

Вбудована безпека: Nest.js надає різні механізми та інструменти для забезпечення безпеки веб-додатків. Він має вбудовану підтримку валідації даних, обробки запитів, захисту від атак, включаючи вразливості, такі як SQL-ін'єкції, кросс-сайтовий скриптинг тощо.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				29
Змн.	Арк.	№ докум.	Підпис	Дата		

У стеку технологій для розробки та захисту ERP системи "ТЕРМОУНІВЕРСАЛ" була обрана **PostgreSQL** як база даних. Вибір PostgreSQL зумовлений наступними перевагами:

Надійність та стабільність: PostgreSQL відомий своєю надійністю та стабільністю, що робить його чудовим вибором для критичних застосунків. Він має потужну систему контролю цілісності даних, транзакційну безпеку та механізми відновлення після збоїв, що дозволяє забезпечити цілісність та доступність даних.

Розширені можливості: PostgreSQL підтримує широкий спектр функцій та можливостей, що дозволяють розробникам ефективно працювати з базою даних. Він підтримує реляційну модель даних, індексування, тригери, функції та багато інших розширень, що спрощують розробку та оптимізацію запитів.

Масштабованість: PostgreSQL може ефективно масштабуватись для обробки великих обсягів даних. Він підтримує паралельну обробку, розподілені запити та реплікацію, що дозволяє розподіляти навантаження та забезпечувати високу продуктивність системи.

Безпека: PostgreSQL має вбудовану систему безпеки, що дозволяє захищати дані від несанкціонованого доступу та зловживання. Він підтримує різні рівні автентифікації, шифрування даних та механізми контролю доступу, що дозволяє забезпечити конфіденційність та цілісність даних.

Спільнота та підтримка: PostgreSQL має велику та активну спільноту розробників, яка забезпечує регулярні оновлення, виправлення помилок та надає підтримку користувачам. Це забезпечує надійну підтримку та актуальність технології.

Обираючи PostgreSQL як базу даних для ERP системи "ТЕРМОУНІВЕРСАЛ", ми отримуємо потужний та надійний інструмент для зберігання, керування та захисту даних будівельної компанії. Таким чином, обрані технології NEXT.JS, NEST.JS та PostgreSQL виявилися оптимальним варіантом для розробки та захисту ERP системи "ТЕРМОУНІВЕРСАЛ" для будівельної компанії. Вони поєднують в собі простоту розробки, швидкодію, масштабованість та надійність, що є необхідними вимогами для успішної реалізації проекту. Обрані

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				30
Змн.	Арк.	№ докум.	Підпис	Дата		

технології дозволять створити потужну та функціональну ERP систему, яка відповідатиме потребам та очікуванням користувачів та бізнесу будівельної компанії.

2.3 Розробка та захист функціональності веб-сайту

У підрозділі "Розробка функціональності веб-сайту" буде здійснена реалізація основних функцій та модулів, які відповідають вимогам проекту ERP системи "ТЕРМОУНІВЕРСАЛ" для будівельної компанії. Цей етап розробки має на меті створення функціональності, яка задовольняє потреби користувачів та бізнесу.

Реалізація основних функцій та модулів веб-сайту передбачає розробку таких функцій, як управління проектами, облік замовлень, управління ресурсами, фінансовий облік та звітність, управління клієнтами та контактами, а також інші необхідні функції відповідно до вимог компанії.

Розробка функціональності веб-сайту є важливим етапом у створенні ERP системи "ТЕРМОУНІВЕРСАЛ" для будівельної компанії. Цей етап дозволить реалізувати основні функції, необхідні для ефективної роботи компанії, і забезпечить приємний користувацький досвід завдяки стильному дизайну та зручному інтерфейсу.

База даних - упорядкований набір логічно пов'язаних даних, які є спільними та призначеними для задоволення інформаційних потреб користувачів. Основне завдання бази даних - гарантувати зберігання великих обсягів[10]

Розроблена модель бази даних "Термоуніверсал" представлена на рис. 2.3.1.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Авторизація веб-сайту визначає, які ресурси та функціональні можливості доступні користувачу після успішної аутентифікації. Це означає, що система повинна мати механізми контролю доступу, які встановлюють права та обмеження для кожного типу користувача. Наприклад, адміністратор системи має повний доступ до всіх функцій і може керувати іншими користувачами, тоді як звичайний співробітник має обмежений доступ до певних модулів та функцій. Це забезпечує безпеку та конфіденційність даних, контролюючи, хто має право на доступ до яких ресурсів.

Авторизація здійснюється за допомоги паролю та e-mail.(рис.2.10)[3]

Рис.2.10 Форма авторизації

При успішній авторизації backend вертає access та refresh токени. Далі access токен записується в headers для подальшої взаємодії з backend.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		33



```

1  export const baseQuery = fetchBaseQuery({
2    baseUrl: process.env.NEXT_PUBLIC_BACKEND_URL,
3    credentials: 'same-origin',
4    prepareHeaders(headers, { getState }) {
5      const token = (getState() as RootState).auth.accessToken;
6      if (token) {
7        headers.set('Authorization', `Bearer ${token}`);
8      }
9      return headers;
10   },
11 });

```

Рис.2.11 Запис токена в header



```

1  export const validateField = (name: string) => {
2    const required: Rule = {
3      required: true,
4      message: "Поле обов'язкове!",
5    };
6    const email: Rule = {
7      type: 'email',
8      message: 'Введіть правильну електронну адресу!',
9    };
10   const passwordLogin: Rule = {
11     min: 8,
12     message: 'Введіть правильний пароль!',
13   };
14   const passwordNewUser: Rule = {
15     min: 8,
16     message: 'Пароль має складатися не менш як 8 символів!',
17   };

```

Рис.2.12Валідація полів авторизації

Важливим аспектом є також збереження конфіденційності та безпеки інформації під час процесів авторизації та аутентифікації. Для цього можуть використовуватися шифрування, хешування паролів, застосування захищених протоколів передачі даних (наприклад, SSL/TLS), забезпечення безпеки збереження облікових записів користувачів та інших заходів.

Bcrypt є одним з найпопулярніших алгоритмів хешування паролів, який широко використовується для забезпечення безпеки при зберіганні облікових записів користувачів. Він є особливо ефективним у випадку, коли потрібно зберегти паролі таким чином, щоб вони не могли бути легко відновлені або зламані в разі витоку даних.

Одним з головних переваг bcrypt є використання солі. Сіль - це додатковий випадковий рядок, який додається до пароля перед хешуванням. Це додає додатковий рівень безпеки, оскільки навіть для однакових паролів хеші будуть відрізнятися через унікальну сіль. Це ускладнює атаки на паролі, таким як атаки методом перебору.

Крім того, bcrypt має вбудовану механіку повільного хешування. Він використовує ітеративний процес, який дозволяє витратити значну кількість обчислювальних ресурсів на кожне хешування пароля. Це ускладнює атаки на паролі шляхом уповільнення швидкості перебору.

Однак, варто враховувати, що bcrypt може бути дещо повільним в порівнянні з іншими алгоритмами хешування, що може вплинути на продуктивність системи в разі великого обсягу авторизаційних запитів. Тому важливо знайти баланс між безпекою та продуктивністю при виборі алгоритму хешування паролів.

Загалом, використання bcrypt є розумним вибором для забезпечення безпеки паролів веб-сайту ERP системи "ТЕРМОУНІВЕРСАЛ". Він забезпечує міцний захист від атак на паролі і забезпечує безпеку облікових записів користувачів. При належному використанні та врахуванні рекомендацій щодо безпеки паролів, bcrypt допоможе зробити систему доступу до веб-сайту компанії безпечною та надійною.[1]

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		35

```
const hashPassword = await bcrypt.hash(userDto.password, 5);
```

Рис.2.13 Хешування паролю за допомогою bcrypt при реєстрації користувача

```
const passwordEquals = await bcrypt.compare(
```

Рис.2.14 Перевірка паролю при авторизації

```
1  const resetLogoutTimer = (): void => {
2    clearTimeout(logoutTimer);
3    logoutTimer = setTimeout(onLogout, 15 * 60 * 1000);
4  }
5
6  const onLogout = async () => {
7    await logout()
8      .unwrap()
9      .then(() => {
10       dispatch(unSetCredentials())
11       message.success('Вихід через неактивність!')
12     })
13     .then(() => push(AppRoutes.HOME))
14     .catch(e => message.error(`Помилка виходу з профілю! ${e?.data.message}`))
15  }
```

Рис.2.15 Логіка завершення сесії через неактивність

Далі було розроблено основний функціонал ERP системи який складається з

- Сторінка Працівників, на якій адміністратор може створювати, видаляти, та редагувати всю інформацію про працівників.
- Список Об'єктів, на який є таблиця з усіма об'єктами, створення об'єкта для інженера, пошук об'єкта за назвою, фільтрація за відділом та статусом роботи.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				36
Змн.	Арк.	№ докум.	Підпис	Дата		

Об'єкти				
Пошук за назвою		+ Створення об'єкта		
Відділ	Назва	Район	Інженер	Статус
⚡	Житомир політех	Житомирський	Євгеній	Обчислення
⚡	test	test	Євгеній	Обчислення

Рис.2.16 Розроблена сторінка списку об'єктів

- Сторінка Об'єкта, на якому є уся інформація про об'єкт та доступне меню в якому є пункти Графік роботи, Документи, Рахунки, Фото, Витрати та зарплати.

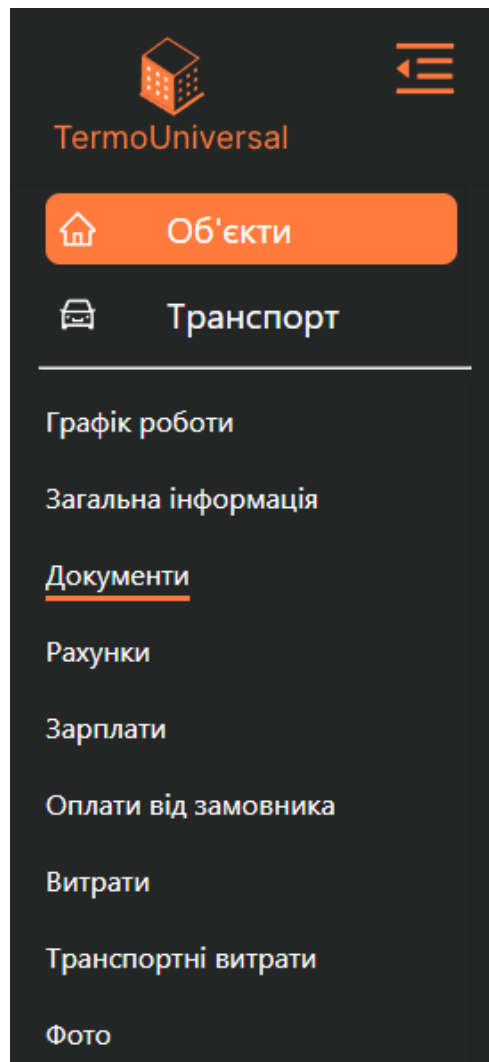


Рис.2.17 Розроблене меню

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				37
Змн.	Арк.	№ докум.	Підпис	Дата		

Рис.2.18 Розроблена сторінка об'єкта

- Сторінка Графік роботи, на якій зображений календар та усі завдання по проекту які можна добавляти.

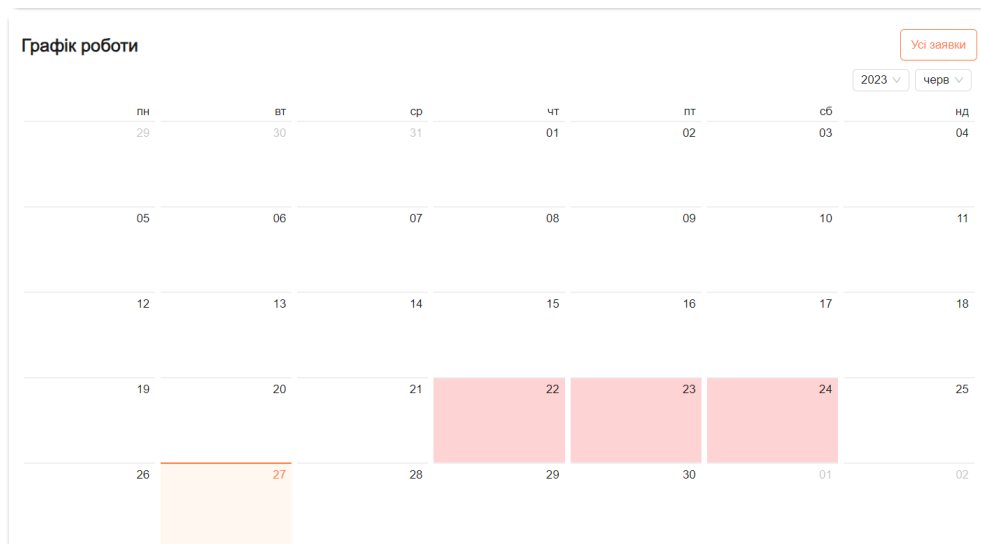


Рис.2.19 Розроблена сторінка Графік роботи

- Сторінка Документи, на якій зображені усі документи та листи рентабельності.
- Сторінка Зарплат, є таблиця з усіми зарплатами та формою додавання зарплат

TERMOUNIVERSAL

TestObj
qwe

Завершений

Задіяні відділи компанії

Відповідальний інженер
Mykola Birzhamemou
Відповідальний виконавець
не призначено

Список зарплат

Пошук за іменем

+ Додати

ПІБ	Сумма виплати	Дата виплати
name	12 345 грн	2023-06-15
Всього: 12 345 грн		

Рис.2.20 Розроблена сторінка Список зарплат

- Сторінка Витрат, є таблиця з усіма витратами та формою додавання витрат

TERMOUNIVERSAL

TestObj
qwe

Завершений

Задіяні відділи компанії

Відповідальний інженер
Mykola Birzhamemou
Відповідальний виконавець
не призначено

Витрати

+ Додати

Готівкова

Безготівкова

Назва	Сумма виплати	Дата виплати	Коментар
Даних немає			
Всього: 0 грн			

Рис.2.21 Розроблена сторінка витрат

- Сторінка Фото,форма завантаження фотозвіту та доступні усі фото до перегляду

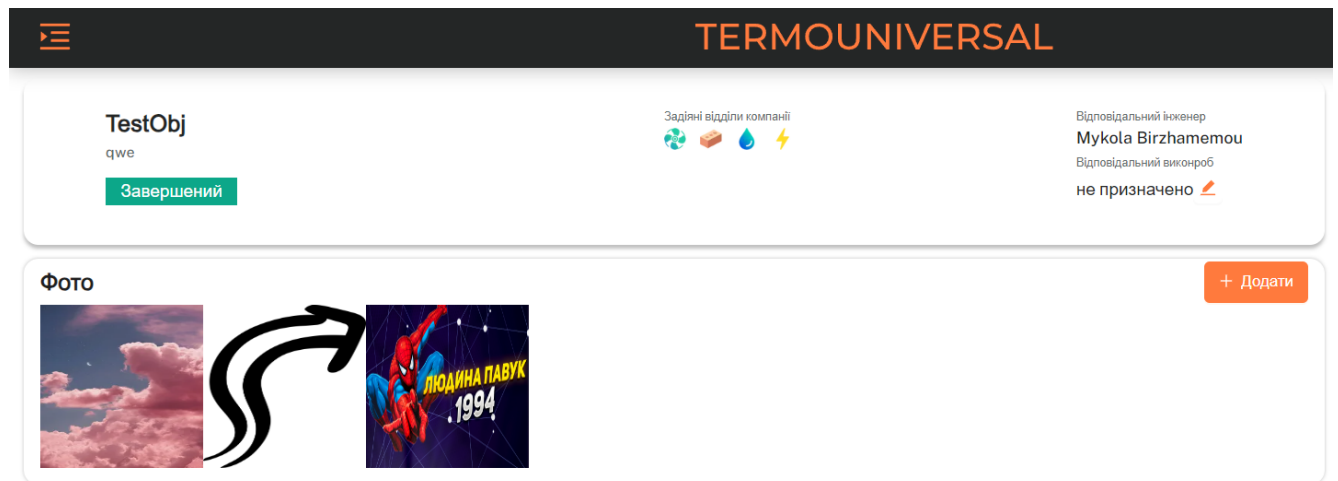


Рис.2.22 Розроблена сторінка Фото

Далі було налаштовано CSRF – токен для захисту веб-сайту від атак, які використовують Cross-Site Request Forgery (CSRF). Атаки CSRF полягають у виконанні небажаних дій на веб-сайті від імені автентифікованого користувача, коли він відвідує зловмисний сайт або натискає на шкідливе посилання.

CSRF токен є одним з методів захисту від цих атак. Він використовується для перевірки автентичності запиту та переконання, що запит на веб-сайт надійно походить від автентифікованого користувача, а не від зловмисника.

Механізм використання CSRF токена полягає в тому, що при завантаженні сторінки, яка містить форму або виклик API, генерується унікальний токен. Цей токен передається разом зі заявкою на сервер. При отриманні запиту сервер перевіряє, чи співпадає CSRF токен з тим, що зберігається на сервері для даного користувача. Якщо токени збігаються, запит вважається довіреним і обробляється; у протилежному випадку, запит може бути відхилено.

CSRF токен допомагає забезпечити, що лише дії, які ініціює сам користувач, будуть прийняті на сервері. Він додає додатковий рівень безпеки, надаючи захист від атак, які намагаються зловживати авторизацією користувача.[2]

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				40
Змн.	Арк.	№ докум.	Підпис	Дата		



```
1 import { Injectable, NestMiddleware } from '@nestjs/common';
2 import { Request, Response } from 'express';
3
4
5 @Injectable()
6 export class CsrfMiddleware implements NestMiddleware {
7   use(req: Request, res: Response, next: Function) {
8     const csrfToken = generateCsrfToken();
9     req.session.csrfToken = csrfToken;
10    next();
11  }
12 }
13
14
```

Рис.2.23 Створення проміжного ПЗ CSRF



```
1 import { doubleCsrf } from "csrf-csrf";
2
3 export const doubleCsrfUtilities = doubleCsrf({
4   getSecret: () => "Secret",
5   cookieName: "__Host-psifi.x-csrf-token",
6   cookieOptions: {
7     httpOnly : true,
8     sameSite : "lax",
9     path : "/",
10    secure : true,
11    //@ts-ignore
12    ...remainingCookieOptions
13  },
14   size: 64,
15   ignoredMethods: ["GET", "HEAD", "OPTIONS"],
16   getTokenFromRequest: (req) => req.headers["x-csrf-token"],
17 });
```

Рис.2.24 Налаштування параметрів CSRF

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновок до другого розділу

У другому розділі нашої дипломної роботи ми зосередилися на розробці та захисті веб-сайту для будівельної компанії "ТЕРМОУНІВЕРСАЛ". Під час розробки, ми використали широкий набір технологій та методів, зокрема bcrypt і CSRF, щоб забезпечити надійний рівень безпеки.

Bcrypt був використаний для захисту паролів користувачів. Хеш функція з додаванням солі забезпечує безпечне зберігання паролів, що зменшує ризик викриття конфіденційної інформації у випадку скомпрометування бази даних. Застосування bcrypt підвищує надійність автентифікації користувачів та забезпечує їх конфіденційність.

Одним з ключових аспектів захисту веб-сайту було використання CSRF-токенів. Цей механізм дозволяє перевірити, що запити, які надходять на сервер, походять від автентифікованого користувача і не є результатом атаки. Це запобігає зловмисникам виконувати несанкціоновані дії від імені користувачів і забезпечує безпеку взаємодії між клієнтом і сервером.

Окрім заходів безпеки, під час виконання роботи було зроблено веб-сайт "ТЕРМОУНІВЕРСАЛ" з урахуванням основних функціональних та нефункціональних вимог. Ми створили структуру веб-сайту та його інтерфейс, вибрали відповідні технології та платформу розробки, а також розробили архітектуру бази даних. Всі ці елементи спільно працюють для забезпечення ефективної роботи системи та задоволення потреб користувачів та бізнесу.

Загалом, застосування bcrypt і CSRF, а також розробка самого сайту "ТЕРМОУНІВЕРСАЛ", дозволяють забезпечити надійний рівень безпеки, ефективну роботу системи та задоволення потреб користувачів. Результатом даної роботи є розробка функціональної і захищеної ERP-системи для будівельної компанії, яка готова до використання та відповідає вимогам сучасного ринку.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				42
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ТЕСТУВАННЯ ВЕБ-САЙТУ

3.1 Розробка плану тестування

На першому етапі планується проведення автоматичного тестування розробленого додатку за допомогою інструмента Burp Suite.

На другому етапі планується проведення ручного тестування розробленого додатку за визначеним планом тестування. Необхідно виконати всі пункти плану тестування і отримати очікувані результати. Вказаний план ручного тестування приведений у таблиці 3.1.[12]

Таблиця 3.1.

План тестування додатку

№ з/п	Початкові умови	Порядок дій	Очікуваний результат
1	Анонімний користувач /admin	Відкрити URL сторінок адміністрування	HTTP Status 302 – редірект на сторінку авторизації /login
2	Авторизований користувач /admin	Відкрити URL сторінок адміністрування	Редірект на сторінку 404
3	Авторизований адміністратор /admin	Відкрити URL сторінок адміністрування	Доступ відкритий
4	Анонімний користувач /objects /objects/3 / objects /3/calendar / objects /3/salaries	Відкрити URL сторінок користувача	редірект на сторінку авторизації /login

5	Авторизований користувач /objects /objects/3 /settings/3/calendar /settings/3/salaries	Відкрити URL сторінок користувача	Доступ відкритий
6	Авторизований користувач з рівнем допуску CEO /objects	Відкрити URL сторінок користувача.	Користувач не має доступу до створення нового об'єкту
8	Авторизований користувач з рівнем допуску CEO /objects/3	Завершення або перевод об'єкту у інший статус	Доступ відкритий
9	Авторизований адміністратор	Реєстрація користувача з паролем довжиною менше 8 символів.	Пароль повинен містити мінімум вісім символів.
10	Будь-який користувач	Відкрити будь-яку сторінку адміністратора або користувача з формою Ввести в будь-яке текстове поле (крім пароля) символи: XSS')"> Виконати submit форми	

Таким чином розроблено план тестування розробленого додатку на вразливості контролю доступу, логіки авторизації, XSS, використання слабо захищених паролів, розкриття інформації

3.2 Результати тестування додатку

На першому етапі планувалося проведення автоматичного тестування розробленого додатку за допомогою інструмента Burp Suite. Але у зв'язку з відсутністю можливостей проведення автоматичного тестування у безкоштовному наборі Burp Suite Community Edition даний вид тестування не проводився.

На наступному етапі було проведено тестування додатку за розробленим планом ручного тестування. Було протестовано систему контролю доступу до закритих частин сайту (адміністративна, для авторизованих користувачів, а саме посилання на каталоги: /objects, /objects/3, /objects/3/calendar, /objects/3/salaries, /admin). Система не дає змоги завантажити вказані сторінки. Після звернення до вказаних сторінок спрацьовує переадресація на сторінку авторизації (Див. рис. 3.1).

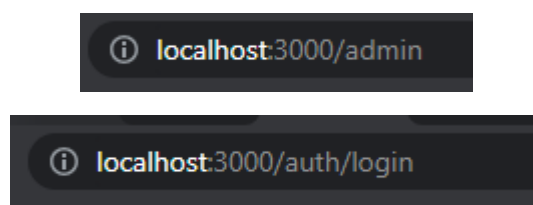


Рисунок 3.1 Переадресація на сторінку авторизації при зверненні до закритих частин сайту

Авторизований користувач не може відвідати сторінки адміністратора

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		45



404
Something is going wrong...

Рисунок 3.2 Переадресація на сторінку 404 при зверненні до адмін частини сайту



Рисунок 3.3 Сторінка переліку працівників в акаунті адміністратора

Анонімний користувач не має доступу до будь яких сторінок, відразу іде редірект на сторінку логіну

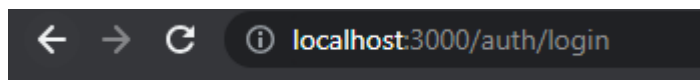


Рисунок 3.4 Редірект на логін

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				46
Змн.	Арк.	№ докум.	Підпис	Дата		

Авторизований користувач має доступ до усіх сторінок які йому дозволені

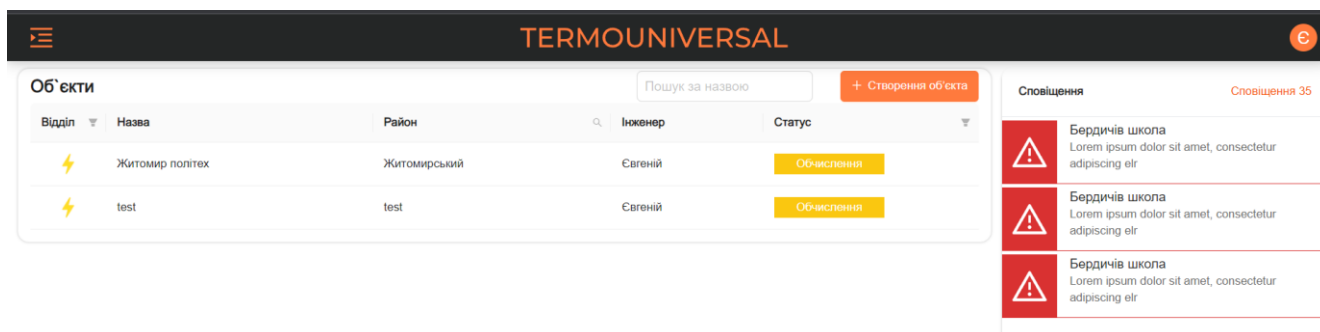


Рисунок 3.5 Доступ до сторінки /objects

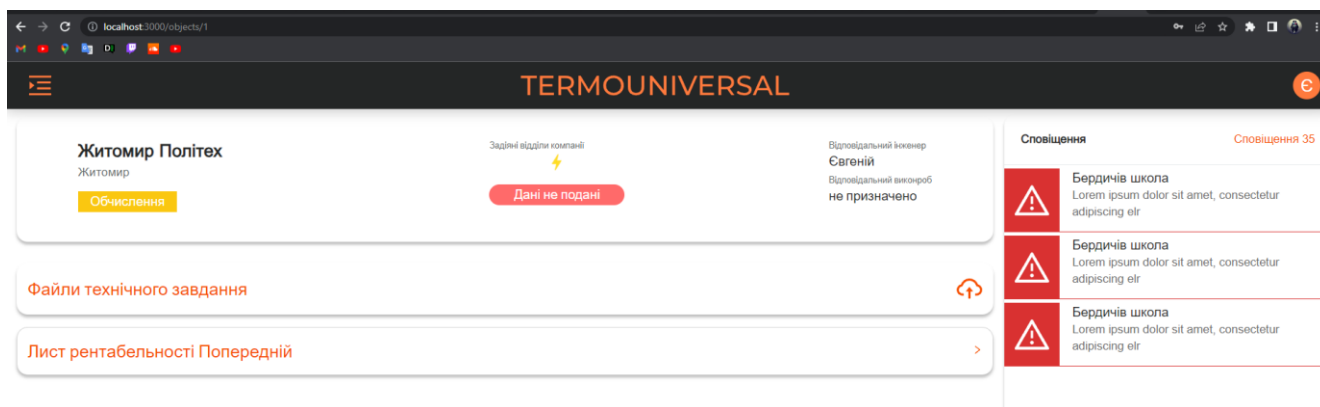


Рисунок 3.6 Доступ до сторінки /objects/1

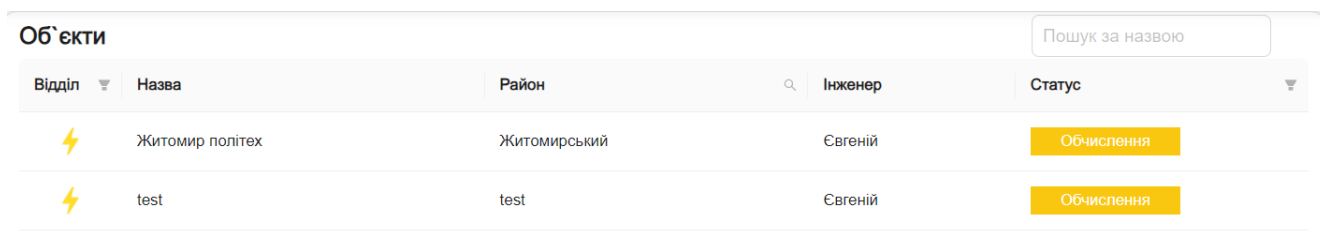


Рисунок 3.7 Користувач з рівнем доступу CEO на має кнопки та доступу до створення об'єкту

Користувач з рівнем допуску CEO має змогу завершити або перевести об'єкт у інший статус

Житомир Політех

Житомирська

В роботі

Задімі відділи компанії

⚡

Відповідальний інженер

Вася Васювич

Відповідальний виконавець не призначено

Сповіщення

Сповіщення 35

⚠ Бердичів школа

⚠ Бердичів школа

⚠ Бердичів школа

Завершити об'єкт та перевести його до архіву

Ні

Так

Основна документація

>

Лист рентабельності Плановий

Підтвердили SEO 2/2

>

Файли технічного завдання

⬆

Лист рентабельності Попередній

>

Рисунок 3.8 Перевод об’єкту у статус завершений для SEO

Пароль повинен містити мінімум вісім символів. Тому у відповідь на пропозицію пароля з 5 символів система його не прийняла та видала повідомлення: «Пароль має містити не менш, ніж 8 символів».

Пошук за іменем

Додавання нового працівника

×

Інформація про працівника

ПІБ працівника

E-mail

admin@gmail.co

Номер телефону

+380

Адреса

Посада

▼

Відділ

Електричний ▼

Створення паролю

Пароль

..

👁

Пароль має містити не менш, ніж 8 символів

Підтвердження паролю

👁

Створити випадковий пароль

Додати

Рисунок 3.9 Пароль повинен мати не менше ніж 8 символів

Було протестовано додаток на вразливість XSS, в поле назви документа було внесено наступний код: . Після реєстрації документа назва вказаного документа видається як простий текст, а не виконується як код(Див. рис. 3.9-3.10)

Рисунок 3.10 Заповнення форми

Рисунок 3.11 Видача небезпечного коду як простий текст,
а не як виконуваний код

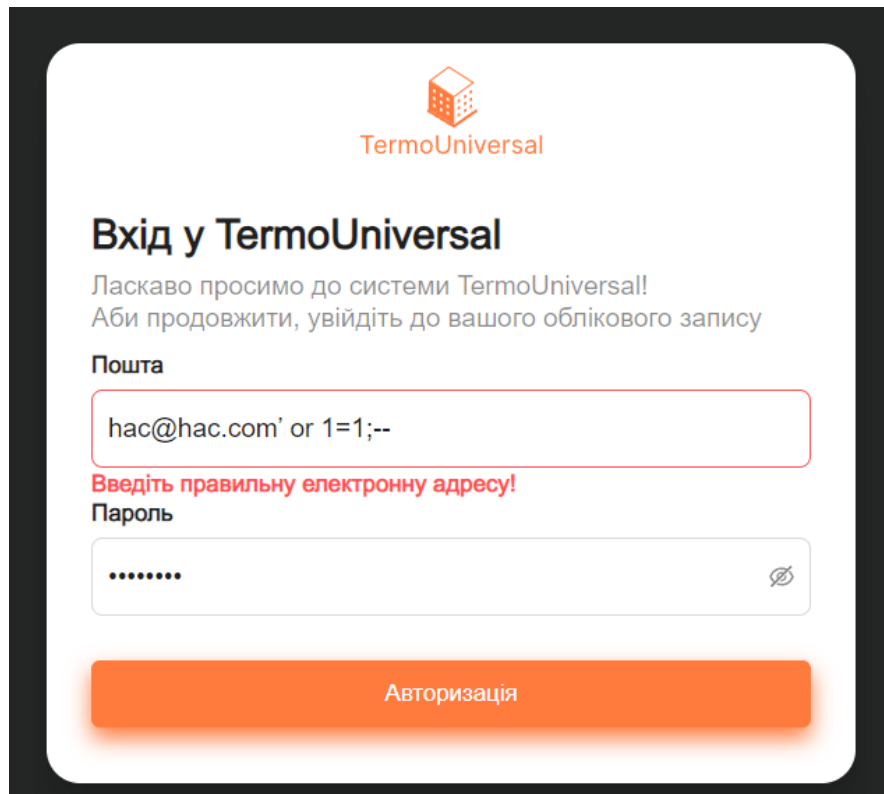
Проведено тестування логіки авторизації. В поле логіну було введено код:
has@has.com' or 1=1;--

А в поле паролю – будь яке значення (наприклад any).

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Цей код розраховано на спрацювання логіки, що 1 завжди дорівнює 1, і за таких обставин логічна операція АБО в даному випадку буде виконана як TRUE навіть якщо введено неправильний логін.

Система видає повідомлення: «Введіть правильну адресу» (Див. рис. 3.10)



The screenshot shows the login interface of the TermoUniversal system. At the top is the TermoUniversal logo. Below it, the title 'Вхід у TermoUniversal' is displayed. A message in Ukrainian asks the user to log in to continue. There are two input fields: 'Пошта' (Email) and 'Пароль' (Password). The email field contains the text 'hac@hac.com' or 1=1;--', which is highlighted with a red border. Below the email field, a red error message reads 'Введіть правильну електронну адресу!' (Enter a correct email address!). The password field is masked with dots. At the bottom is an orange button labeled 'Авторизація' (Authorize).

Рисунок 3.12 Результат спроби злому логіки у формі авторизації

Висновки до 3 розділу

Під час виконання третього розділу було:

1. Розроблено план тестування розробленого додатку на:

- вразливості контролю доступу,
- логіки авторизації,
- XSS,
- використання слабо захищених паролів,
- захищеність від brute-force атак,
- розкриття інформації,

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				50
Змн.	Арк.	№ докум.	Підпис	Дата		

2. Під час тестування системи отримані очікувані результати. Таким чином нами не було виявлено вразливостей додатку та підтверджено його захищеність

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		51

ВИСНОВКИ

У рамках даної дипломної роботи було розглянуто теоретичні основи створення та захисту веб-сайту. Були представлені основні етапи процесу розробки веб-сайту, включаючи аналіз вимог, проектування і реалізацію. Також були розглянуті ключові аспекти безпеки веб-сайту, включаючи заходи захисту і методи виявлення потенційних загроз.

Також було розроблено веб-сайт для будівельної компанії "ТЕРМОУНІВЕРСАЛ" та систему його захисту. Під час розробки, використано широкий набір технологій та методів, зокрема використання bcrypt і CSRF-токенів, щоб забезпечити надійний рівень безпеки.

Bcrypt був використаний для захисту паролів користувачів. Хеш функція з використанням солі забезпечує безпечне зберігання паролів, що зменшує ризик викриття конфіденційної інформації у випадку скомпрометування бази даних. Застосування bcrypt підвищує надійність автентифікації користувачів та забезпечує їх конфіденційність.

Одним з ключових аспектів захисту веб-сайту було використання CSRF-токенів. Цей механізм дозволяє перевірити, що запити, які надходять на сервер, походять від автентифікованого користувача і не є результатом атаки. Це запобігає зловмисникам виконувати несанкціоновані дії від імені користувачів і забезпечує безпеку взаємодії між клієнтом і сервером.

Було розроблено веб-сайт "ТЕРМОУНІВЕРСАЛ" з урахуванням основних функціональних та нефункціональних вимог. Створено структуру веб-сайту та його інтерфейс, вибрано відповідні технології та платформу розробки, а також розроблено архітектуру бази даних.

Загалом, застосування bcrypt і CSRF-токенів, а також розробка самого сайту "ТЕРМОУНІВЕРСАЛ", дозволяють забезпечити надійний рівень безпеки, ефективну роботу системи та задоволення потреб користувачів. Результатом даної роботи є розробка функціональної і захищеної ERP-системи для будівельної компанії, яка готова до використання та відповідає вимогам сучасного ринку.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Також було розроблено план тестування розробленого додатку на:

- використання слабо захищених паролів,
- вразливості контролю доступу,
- розкриття інформації,
- логіки авторизації,
- XSS,
- захищеність від brute-force атак,

Під час тестування системи отримані очікувані результати. Таким чином нами не було виявлено вразливостей додатку та підтверджено його захищеність.

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		53

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Приклади налаштування Bcrypt: [Електронний ресурс].
<https://www.npmjs.com/package/bcrypt>
2. Приклади використання CSRF токenu: [Електронний ресурс]
<https://blog.logrocket.com/protecting-next-js-apps-csrf-attacks/>
3. Інформація про аутентифікацію: [Електронний ресурс]
<https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F>
4. Основи створення баз даних: [Електронний ресурс]
<https://step.org.ua/konspekt/base/tema1>
5. Офіційна документація Next.js : [Електронний ресурс]
<https://nextjs.org/docs>
6. Офіційна документація Nest.js: [Електронний ресурс] <https://docs.nestjs.com/>
7. Етапи створення веб сайтів: [Електронний ресурс]
<https://webtune.com.ua/statti/web-rozrobka/etapy-stvorenniya-veb-sajtiv/>
8. Як захистити сайт від злому: [Електронний ресурс]
<https://fondy.ua/uk/blog/how-to-protect-website/>
9. 5 найпоширеніших атак на веб-сайти: [Електронний ресурс]
<https://www.websiterating.com/uk/online-security/most-common-website-attacks-how-to-defend-against-them/>
10. Офіційна документація postgresQL: [Електронний ресурс]
<https://www.postgresql.org/docs/>
11. Що таке Фаєрвол: [Електронний ресурс]
<https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/>
12. Тестування веб-проектів: [Електронний ресурс] <https://qalight.ua/baza-znaniy/testuvannya-veb-proektiv-osnovni-etapi-ta-poradi/>

13.Ручне та автоматизоване тестування: [Електронний ресурс]

<https://qalight.ua/baza-znaniy/ruchne-ta-avtomatizovane-testuvannya/>

14.Eloquent JavaScript Written by Marijn Haverbeke Chapter 20 Node.js

		Єзюкинський Є.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Воротніков В.В				
Змн.	Арк.	№ докум.	Підпис	Дата		55