

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

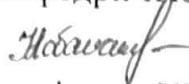
до випускної кваліфікаційної роботи магістра
на тему: «Захист веб-орієнтованої системи
електронного документообігу на основі
блокчейн технологій»

Виконав студент 2-го курсу групи КБм-21-1
спеціальності 125 «Кібербезпека»



Олександр Пірог

Керівник доцент кафедри ІІЗ, к.т.н.



Надія Лобанчикова

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



Володимир Воротніков

Житомир – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Факультет Інформаційно-комп'ютерних технологій
Кафедра Комп'ютерної інженерії та кібербезпеки
Освітній рівень бакалавр
Спеціальність 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри комп'ютерної інженерії та кібербезпеки

 Андрій Єфіменко
“ 25 ” 10 20 22 року

З А В Д А Н Н Я

ДО ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ МАГІСТРА СТУДЕНТУ

Пірогу Олександрові Вікторовичу

1. Тема проекту:

Захист веб-орієнтованої системи електронного документообігу на основі блокчейн технологій

Керівник проекту

Надія Лобанчикова к.т.н., доцент кафедри інженерії програмного забезпечення.

2. Строк подання студентом проекту (роботи) **29 грудня 2022 року**.

3. Вихідні дані до проекту (роботи):

- Розробити веб-додаток реєстрації документів.
- Захистити його від основних вразливостей.
- Розробити розвинену систему контролю доступу.
- На основі блокчейн технологій захистити систему від підробки зареєстрованих документів.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз стану захисту систем електронного документообігу.
2. Розробка ТЗ та реалізація веб-додатку.
3. Тестування веб-додатку.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 27 жовтня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	27.10.2022 р.	
2	Аналіз літературних джерел	31.10.2022 р.	
3	Аналіз об'єкта дослідження	02.11.2022 р.	
4	Постановка задачі дослідження	07.11.2022 р.	
5	Структурування інформації	09.11.2022 р.	
6	Аналіз загроз та розробка технічного завдання	11.11.2022 р.	
7	Вибір системи управління доступом та розробка структури БД	14.11.2022 р.	
8	Розробка коду елементів захисту	16.11.2022 р.	
9	Розробка плану тестування додатку	22.11.2022 р.	
10	Тестування додатку	28.11.2022 р.	
11	Висновки	04.12.2022 р.	
12	Оформлення пояснювальної записки	08.12.2022 р.	
13	Оформлення презентації	11.12.2022 р.	
	Захист	Згідно розкладу	

Студент

Олександр Пірог

Керівник проекту

Надія Лобанчикова

ЗМІСТ

ЗАВДАННЯ	2
КАЛЕНДАРНИЙ ПЛАН	3
ВСТУП.....	6
РОЗДІЛ 1. АНАЛІЗ СТАНУ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ	9
1.1 Обґрунтування актуальності теми роботи.....	9
1.2 Аналіз сучасного стану захисту веб-орієнтованих систем електронного документообігу.....	11
1.3 Розробка вимог до захисту системи електронного документообігу	21
Висновки до першого розділу	24
РОЗДІЛ 2. РОЗРОБКА ТЕХНІЧНИХ ВИМОГ ТА РЕАЛІЗАЦІЯ ВЕБ-ДОДАТКУ	26
2.1 Аналіз загроз та розробка технічних вимог до завдання.....	26
2.2 Вибір системи управління доступом та розробка структури БД	28
2.3 Розробка коду елементів захисту	31
Висновки до другого розділу	43
РОЗДІЛ 3. ТЕСТУВАННЯ ВЕБ-ДОДАТКУ	44
3.1 Розробка плану тестування додатку	44
3.2 Результати тестування додатку	48
Висновки до третього розділу	56
ВИСНОВКИ	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	61

КІК.КР.Б – 125 – 12 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата
		Пірог О.В.	<i>[Підпис]</i>	13.12.22
		Лобанчикова Н.М.	<i>[Підпис]</i>	19.12.22
		Єфіменко А.А.	<i>[Підпис]</i>	15.12.22

ЗАХИСТ ВЕБ-ОРІЄНТОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА ОСНОВІ БЛОКЧЕЙН ТЕХНОЛОГІЙ

Лім.	Арк.	Аркушіє

ФІКТ, Гр. КБм-21-1

ЗМІСТ

З А В Д А Н Н Я	2
КАЛЕНДАРНИЙ ПЛАН	3
ВСТУП.....	6
РОЗДІЛ 1. АНАЛІЗ СТАНУ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ	9
1.1 Обґрунтування актуальності теми роботи.....	9
1.2 Аналіз сучасного стану захисту веб-орієнтованих систем електронного документообігу	11
1.3 Розробка вимог до захисту системи електронного документообігу	21
Висновки до першого розділу	24
РОЗДІЛ 2. РОЗРОБКА ТЗ ТА РЕАЛІЗАЦІЯ ВЕБ-ДОДАТКУ	26
2.1 Аналіз загроз та розробка технічних вимог до завдання.....	26
2.2 Вибір системи управління доступом та розробка структури БД	28
Рисунок 2.2.1 Діаграма прецедентів Use-case diagram	29
2.3 Розробка коду елементів захисту	31
Висновки до другого розділу	43
РОЗДІЛ 3. ТЕСТУВАННЯ ВЕБ-ДОДАТКУ	44
3.1 Розробка плану тестування додатку	44
3.2 Результати тестування додатку	48
Висновки до третього розділу	56
ВИСНОВКИ	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	61

					КІК.КР.Б – 125 – 12 – ПЗ			
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	ЗАХИСТ ВЕБ-ОРІЄНТОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА ОСНОВІ БЛОКЧЕЙН ТЕХНОЛОГІЙ	<i>Літ.</i>	<i>Арк.</i>	<i>Аркушів</i>
Розроб.		<i>Пірог О.В.</i>						
Керівник		<i>Лобанчикова Н.М.</i>						
Реценз.		.				ФІКТ, Гр. КБм-21-1		
Н. контр.								
Затверд.		<i>Єфіменко А.А.</i>						

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД – База даних

ЕЦП – Електронний цифровий підпис

СЕД – Система електронного документообігу

СЕТАМ – Системи електронних торгів заарештованим майном

СУБД – Система управління базами даних

API – Application Programming Interface

CCPA – California Consumer Privacy Act

CRM – Customer Relationship Management

CSRF – Cross-Site Request Forgery

DOM – Document Object Model

FINRA – Financial Industry Regulatory Authority

GDPR – General Data Protection Regulation

GLBA – Gramm–Leach–Bliley Act

HIPAA – Health Insurance Portability and Accountability Act

HSM – Hierarchical Storage Management

HTTP – HyperText Transfer Protocol

MVC – ModelViewController

NFT –Non-Fungible Token

ORM – Object Relational Mapper

PHP – Personal Home Page Tools

PKI – Public Key Infrastructure

RBAC – Role Based Access Control

SEC – Securities and Exchange Commission

SEO – Search Engine Optimization

SQL – Structured Query Language

SQLi – SQL Injection

URL – Uniform Resource Locator

XSS – Cross-Site Scripting

		Пірог О.В.			KIK.KP.B – 125 – 12 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми роботи. Система електронного документообігу (СЕД) – дуже важлива частина інформаційного ландшафту сучасної організації. Електронний документообіг у сьогоднішній час широко впроваджується у таких захищених законом сферах як: медицина, судова діяльність, освіта, фінанси, державні послуги (Дія). СЕД також призначена для вирішення критично важливих бізнес-завдань, пов'язаних з управлінням, зберіганням та інтеграцією документів, різних файлів та іншої важливої інформації, що міститься в інформаційних системах та бізнес-додатках. Для нормальної роботи електронного документообігу необхідний безпечний та надійний процес обробки та зберігання інформації. Захищений електронний документообіг – одне з найважливіших завдань забезпечення спільної безпеки в організації, якій необхідно приділяти дуже велике значення та пильну увагу. Для забезпечення інформаційної безпеки використовуються сучасні криптографічні засоби захисту та шифрування інформації для однозначного розмежування доступу до неї, а одним з новітніх методів є застосування технології блокчейн для збереження даних і виключення їх фальсифікації, що особливо актуально в період переходу людства до використання INDUSTRY 4.0.

Метою кваліфікаційної роботи магістра є розробка та тестування веб-орієнтованої системи електронного документообігу на основі блокчейн технологій.

Встановлена мета обумовлює наступні наукові завдання:

- аналіз методик захисту системи електронного документообігу;
- аналіз технологій захисту системи електронного документообігу на основі блокчейн технологій;
- аналіз існуючих веб-орієнтованих систем документообігу;
- розробка захисту веб-орієнтованої системи електронного документообігу на основі блокчейн технологій;
- тестування розробленої системи.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						6
Змн.	Арк.	№ докум.	Підпис	Дата		

Об'єктом дослідження є процеси побудови веб-орієнтованої системи електронного документообігу на основі блокчейн технологій.

Предметом дослідження є моделі, методи, засоби та технології побудови та захисту веб-орієнтованої системи електронного документообігу на основі блокчейн технологій.

Методологія роботи –Під час дослідження було використано загальнонаукові та емпіричні наукові методи, що ґрунтуються на системному підході, такі як абстрагування, аналіз, синтез, порівняння, узагальнення, систематизація, методи об'єктно-орієнтованого проектування та моделювання, блокчейн технології.

Наукова новизна дослідження. До найбільш вагомих наукових результатів слід віднести:

- аналіз методик захисту системи електронного документообігу;
- аналіз технологій захисту системи електронного документообігу на основі блокчейн технологій;
- аналіз існуючих веб-орієнтованих систем документообігу;
- вимоги до розробки системи документообігу;
- технічне завдання на розробку системи документообігу;
- модель загроз та модель порушників системи документообігу;
- аналіз сервісів розробки та захисту системи документообігу;
- розроблений додаток електронної системи документообігу;
- план та результати тестування розробленого додатку системи документообігу.

Особистий внесок здобувача. Усі результати роботи отримані автором самостійно.

За результатами дослідження було опубліковано:

1. Пірог О.В. Аналіз сучасного стану захисту web-орієнтованих систем електронного документообігу. Тези V Всеукраїнської науково-технічної конференція «Комп'ютерні технології: інновації, проблеми, рішення». Житомир: Державний університет «Житомирська політехніка», 2022.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

2. Пірог О.В. Рецепти безпечної розробки веб-додатків від OWASP щодо запобігання вразливості міжсайтового скриптингу (XSS). Тези IV Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення». Житомир: Державний університет «Житомирська політехніка», 2021. С. 21.

3. Пірог О. В. Моделювання комплексної системи захисту інформації. Тези Всеукраїнської науково-практичної on-line конференції здобувачів вищої освіти і молодих учених, присвяченої Дню науки. Житомир: Державний університет «Житомирська політехніка», 2021. С. 135-136.

4. Пірог О. В. Способи «соління» таблиці паролів користувачів web-серверу. Тези III Всеукраїнської конференція «Комп'ютерні технології: інновації, проблеми, рішення». Житомир: Державний університет «Житомирська політехніка», 2020. С. 35.

Апробація результатів дослідження. Основні результати роботи були оприлюднені на Всеукраїнській науково-практичній on-line конференції здобувачів вищої освіти і молодих учених, присвяченої Дню науки (15-17 травня 2019 р., м. Житомир).

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних літературних джерел та додатку.

Основний зміст роботи викладено на 66 сторінках друкованого тексту. Робота містить 1 таблицю та 40 рисунків. Список використаної літератури налічує 49 джерел, що викладені на 3 сторінках. Робота містить 1 електронний додаток.

		Пірог О.В.			KIK.KP.B – 125 – 12 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ СТАНУ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1.1 Обґрунтування актуальності теми роботи

Останнім часом у зв'язку з реформуванням та розвитком всіх сфер української держави, а саме медичної реформи, судової та правоохоронної реформи, розвитком електронної держави та так званої «діджиталізації» держави та в умовах триваючої кібервійни з державою агресором постають нові виклики щодо захисту інформації, що обробляється в державних та комерційних телекомунікаційних системах. Такі сфери як медицина, державне управління, збереження персональної інформації громадян захищено низкою законів: «Про інформацію», «Про нотаріат», «Про захист персональних даних», «Про адвокатуру та адвокатська діяльність», «Про телекомунікації», «Про оперативно-розшукову діяльність», «Про Національну поліцію», «Про банки и банківську діяльність», «Основи законодавства України про охорону здоров'я» [1]. Кримінальний кодекс України містить до прикладу наступні статті:

- Ст. 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю;
- Ст. 232. Розголошення комерційної або банківської таємниці;
- Ст. 132. Розголошення відомостей про проведення медичного огляду...;
- Ст. 145. Незаконне розголошення лікарської таємниці т.ін.

Також віхою останнього часу є створення та введення в дію електронного сервісу державних послуг «Дія».

Інтерес до блокчейну продовжує зростати: багато банків, бірж та фінтех-компаній оголосили про запуск власних проектів з розвитку цієї технології. Блокчейн залишається однією з найгарячіших тем у сфері фінансових послуг та на фондових ринках, і є всі підстави очікувати зростання швидкості його розповсюдження. Згідно з доповіддю, представленою на Світовому економічному форумі за три останні роки у вивчення блокчейна та можливостей його

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

застосування в індустрії фінансових послуг було вкладено понад 1,4 мільярда доларів [20].

Консалтингова компанія Booz Allen Hamilton представила огляд можливих шляхів вирішення бюрократичних проблем у держорганах за допомогою блокчейн-технологій.

Завдяки прозорій та децентралізованій системі перевірка даних може здійснюватись будь-яким учасником, що дозволить зміцнити довіругромадян до держорганів. Крім того, використання блокчейну для деяких послуг дозволить проводити незалежну перевірку скарг.

Іншою потенційною перевагою є захист конфіденційних даних, таких як номери соціального страхування, дати народження, адреси та номери прав водія. Державні службовці є основними цілями хакерів. Але кібератаки можна зменшити або запобігти при розгортанні блокчейн-технологій.

Третя можлива перевага – зниження витрат та підвищення ефективності. Використання блокчейна може знизити надмірність даних, спростити процеси, зменшити навантаження на аудит, підвищити безпеку та забезпечити цілісність даних.

Урядові установи, безумовно, зацікавлені у перспективі використання блокчейну. Приклади використання блокчейну в держорганах включають голосування, автоматизовану реєстрацію даних, ведення обліку, транзакції та звірку рахунків, соціальну та гуманітарну допомогу, ринки активів та надання окремим особам контролю за своїми конфіденційними даними та медичними записами.

Блокчейн може підвищити ефективність децентралізованих процесів. Наприклад, застосування блокчейн-технологій здатне прискорити збирання документації від кількох державних структур, які не мають спільних систем або тісних організаційних відносин. Подібне використання може вирішити проблему таких процесів як видача дозволів та реєстрація.

Обмін інформацією між державними організаціями та приватним сектором щодо надання допомоги у надзвичайних ситуаціях, страхових претензіях,

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

медичних позовах та інших багатосторонніх угодах може покращити узгодженість роботи цих структур та значно покращити ставлення громадян до них.

Крім бюрократії, поширеною урядовою проблемою є корупція, і тут блокчейн також може зіграти роль у боротьбі з нею. Використання блокчейну може бути використано для обмеження корупції, шахрайства, крадіжок та нецільового використання державних ресурсів як самим урядом, так і громадянами.

Блокчейн-технології здатні не лише боротися з бюрократією та корупцією, а й загалом змінити спосіб надання державних послуг громадянам. Можливості практично безмежні: блокчейн-технології надають громадянам та підприємствам можливість керувати та ділитися інформацією, знижують проблеми при оцінці інтелектуальної власності та виплати роялті, забезпечують цифрові ідентифікаційні документи та економічну свободу.

Незважаючи на бурний розвиток блокчейн все ще залишається експериментальною технологією – вона постійно знаходиться у розвитку, з'являються все нові способи її використання.

1.2 Аналіз сучасного стану захисту веб-орієнтованих систем електронного документообігу

Блокчейн – розподілена база даних, яка зберігає інформацію про всі транзакції учасників системи у вигляді «ланцюжка блоків» (саме так з англ. перекладається Blockchain). Доступ до реєстру є у всіх користувачів блокчейна, що виступають як колективний нотаріус, який підтверджує істинність інформації в базі даних. Блокчейн може застосовуватися для фінансових операцій, ідентифікації користувачів, створення технологій кібербезпеки та ін.

Блокчейн виник як технології для запуску в обіг біткойна, і спочатку використовувався виключно для управління криптовалютами. Проте з його появи, сфера застосування істотно розширилася. А зараз у найрізноманітніших статтях, на форумах і конференціях обговорюються нові варіанти використання

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

технології, у тому числі в комплаєнсі (запобігання фінансовим злочинам, боротьбі з шахрайством).

Унікальність блокчейна полягає у незмінності чи незворотності, яку гарантує криптографічна система захисту. Наприклад, коли транзакції з реєстру згруповані в блоки та записуються в базу даних, запис передують криптографічна верифікація, внаслідок чого змінити стан реєстру шляхом будь-яких махінацій практично неможливо. На користь довіри до блокчейну говорить і те, що будь-які зміни даних у ланцюжку блоків можливі тільки якщо учасники мережі підтверджують легітимність транзакції відповідно до загальних правил і протоколів.

У середині 2021 року журнал Forbes розповів про основні тренди використання блокчейну, які охоплюють численні сфери діяльності [11].

Блокчейн для відстеження та розповсюдження вакцин.Цілком імовірно, що блокчейн буде використовуватися для відстеження доставки вакцин від місця виробництва до пацієнта. На кожному етапі шляху блокчейн дозволяє створювати постійні, такі що не піддаються фальшуванню, записи про місцезнаходження кожної партії. Лідером у розгортанні вирішення цих проблем на основі блокчейну є IBM, яка вже веде переговори з фармацевтичними компаніями з метою запуску пілотного проекту.

Зростання корпоративного блокчейну.Корпоративний блокчейн має на увазі контроль централізованого «власника»— зазвичай це компанія, яка надала блокчейн-платформу. Відповідні банківські та фінансові послуги стануть лідерами у своїй галузі завдяки зручності ведення бухгалтерського обліку. Крім того, додатки корпоративного блокчейну все частіше використовуватимуться в охороні здоров'я, виробництві та сфері професійних послуг.

Зростання застосування NFT.Незалежні токени (NFT, non-fungible token) по суті є цифровими активами (зображеннями, музикою, кодом, контрактами), цінність яких обґрунтована їх унікальністю. Деякі називають їх «цифровими предметами колекціонування», тому що, на відміну більшості цифрових файлів, ці активи не можна просто дублювати і копіювати.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

NFT надають власникам цифрових активів можливість підтверджувати своє право власності. Крім унікальних творів мистецтва, NFT можуть використовуватися для відстеження прав власності на землю та майно, що нині часто вимагає трудомісткого та дорогого пошуку у реєстрах, або для відстеження уживаних транспортних засобів, коли дані про попереднє власника можуть вплинути на ціну.

Блокчейн як послуга. Така модель поширення дозволила швидко запровадити низку технологічних інновацій, зокрема хмарні обчислення, Інтернет речей, штучний інтелект. Amazon, IBM і Microsoft вже почали розробляти інструменти та платформи, що дозволяють підприємствам використовувати технологію блокчейну як послугу, тобто без попередніх вкладень в інфраструктуру та навчання спеціальним навичкам. Хмарні платформи зроблять цю технологію доступною для багатьох організацій.

На аналітики Gartner опублікували список рекомендацій про те, в яких сферах урядовим органам потрібно впроваджувати блокчейн [27].

За прогнозами дослідників, до 2025 блокчейн-технології стануть основою для глобальної децентралізованої системи ідентифікації. Перед урядовими чиновниками, які розглядають можливість використання блокчейну, вже стоїть низка перспективних і практичних варіантів використання цієї технології.

1. Вибори.

Використання блокчейну на виборах становить інтерес для багатьох урядів, хоча лише деякі використовують цю технологію на національному рівні. Різні стартапи вже провели пілотні проекти у США, Україні та Сьєрра-Леоне. Загалом, жоден з пілотних проектів поки що не зміг уявити безпечний варіант автентифікації виборців або вирішити серйозніші проблеми, пов'язані з шахрайством та залякуванням.

2. Гуманітарні та соціальні послуги.

Ще одним приводом для впровадження блокчейну може стати покращення послуг, які надаються населенню, що потребує, без документів.

3. Ринки цифрових активів.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

Уряди зацікавлені у використанні блокчейна для торгівлі чисто цифровими активами або цифровими уявленнями матеріальних активів.

4. Підвищення ефективності.

Ініціативи підвищення ефективності ґрунтуються на ідеї, що система транзакцій може бути оптимізована за допомогою блокчейну. Це може стати в нагоді урядам, які повинні забезпечувати взаємодії та угоди між різними урядовими організаціями або за участю великих державних/приватних екосистем.

5. Діловодство.

Уряди деяких країн оголосили про створення систем управління документацією на основі блокчейну. Існуючі блокчейн-рішення оптимізовані під управління «токенами», що являють собою різноманітні активи, і не годяться для зберігання документів, оскільки самі документи в блокчейн не поміщаються (інакше через стрімке наростання обсягів було б вкрай проблематично підтримувати копії реєстру на численних відносно слабких комп'ютерах). У блокчейні у разі зберігаються лише хеші документів чи документованої інформації, тобто блокчейн-решення виконує роль довіреної системи позначок часу, функціонуючої без використання традиційної інфраструктури відкритих ключів (PKI).

В Естонії підтримуваний довіреною третьою стороною інтерфейс з блокчейн-системою був підключений до базової системи міжвідомчої взаємодії X-Road, що дозволяє будь-якому державному органу скористатися цим сервісом для необхідних йому цілей. Головне завдання, яке при цьому вирішувалося, – забезпечити надійний контроль цілісності та автентичності інформації в державних системах через можливі кібератаки. Внаслідок цього блокчейн-система де-факто виконує функції довіреного постачальника послуг позначок часу. Тим самим забезпечується додатковий рівень контролю цілісності та автентичності документів та інформації. Самі документи, однак, у блокчейн-рішення не розміщуються. Зокрема блокчейн використовується для документування відомостей про те, хто мав доступ до документів про здоров'я громадян країни.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

Грузія багато в чому спирається на досвід Естонії, і в даний час найбільш амбітним є проект захисту транзакцій у земельному кадастрі за допомогою рішення на платформі Біткойн. Для цього він використовується рішення компанії BitFury.

Нині низка експертів вважає Україну однією з провідних країн з питань функціонування технології блокчейн та криптовалют. Доказом цього може стати те, що Кабінет Міністрів України схвалив впровадження блокчейну в роботу держреєстру речових прав на нерухоме майно та Системи електронних торгів заарештованим майном (CETAM), а Міністерство юстиції розробляє один із перших у світі державних проєктів, пов'язаних із цією технологією. Поряд із цим, простежується посилення тиску силових структур України на майнерів та власників криптовалют, а також заяви про необхідність держрегулювання цього сегменту ринку.

Розглянемо основні веб-сервіси, що в даний час використовуються для управління документами (Див.рис. 1.1).

Найбільш відомими та вживаними є Google Drive, Dropbox та OneDrive. Google Drive допомагає користувачам зберігати дані компанії в одному місці. Користувачі можуть отримувати доступ до файлів з настільних та мобільних пристроїв та контролювати, як члени команди обмінюються цими файлами. Платформа надає центральну панель адміністратора, захист від втрати даних та сховище для диска, щоб забезпечити відповідність та обмін файлами між користувачами. Google Drive пропонує інструменти для спільної роботи, такі як Документи, Таблиці та Слайди.

Команди можуть створювати нові документи та ділитися ними з учасниками. Вони також можуть брати участь у редагуванні документів у режимі реального часу та залишати коментарі, щоб повідомляти учасників про зміни. Він включає технологію машинного навчання, що допомагає користувачам прогнозувати майбутні потреби. Google Drive надає такі функції, як пошук природною мовою та оптичне розпізнавання символів (OCR). Google Drive інтегрується зі сторонніми програмами, включаючи DocuSign для електронних

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

підписів, CloudLock для додаткових рівнів безпеки та LucidCharts для макетів. Користувачі можуть відкривати різні типи файлів, такі як PDF та MPEG4, та працювати з файлами Microsoft Word прямо з диска [21].



Рисунок 1.1 Основні веб-сервіси управління документами

Примітка: Складено за [39]

Dropbox – це хмарна система обміну файлами, яка підходить для приватних осіб та компаній будь-якого розміру. Це рішення дозволяє користувачам обмінюватися файлами та надсилати запити на файли людям, навіть якщо у них немає облікового запису Dropbox. Декілька користувачів можуть залишати коментарі до файлів і співпрацювати з Microsoft Office. Рішення може відновлювати видалені файли та підтримує історію версій на випадок, якщо

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

користувачі захочуть відновити старі версії файлів. Він також відстежує всі дії, які виконуються з певними файлами. Розширений спільний доступ дозволяє лише вибраним користувачам бачити важливі файли, а файли можна видалено стерти, якщо конфіденційні дані будуть скомпрометовані. Dropbox також може створювати резервні копії всіх фотографій у міру їхнього додавання. Dropbox також надає панель адміністратора для централізованого керування файлами. Ліцензії користувача, контент та права доступу можуть передаватися від одного користувача до іншого [17].

OneDrive – це хмарне рішення для керування контентом, яке надає організаціям платформу для спільної роботи, спільного використання та зберігання документів. Ця система забезпечує міжплатформну синхронізацію та запобігає втраті даних. OneDrive дозволяє користувачам спільно працювати та обмінюватися документами в режимі реального часу з членами команди та клієнтами, а менеджери можуть отримувати доступ, переглядати та редагувати. Він допомагає користувачам в керуванні файлами, обмежуючи доступ до файлів усередині команд та організацій. Крім того, система ділиться повідомленнями в реальному часі, коли файл переглядається або редагується. OneDrive автоматично позначає фотографії, виявляючи зображення, збережені у хмарі, що спрощує їх пошук та впорядкування. Крім того, рішення дозволяє користувачам обмінюватися файлами та отримувати до них доступ 24/7 з будь-якого мобільного пристрою. OneDrive надає безкоштовне сховище обсягом до 5 ГБ та доступне на пристроях Windows, Android та iOS [35].

MODX – це система управління контентом, яка допомагає підприємствам будь-якого розміру оптимізувати операції, пов'язані зі створенням контенту, управлінням ресурсами, контролем дозволів та автоматичною обробкою відмовостійкості серед інших процесів. Він дозволяє співробітникам створювати блоги, каталоги, цільові сторінки, PDF-файли та форми з полями, меню, макетами і шаблонами. Модуль управління ресурсами MODX дозволяє співробітникам створювати деревоподібні меню для обробки та відстеження цифрових активів на кількох платформах. Адміністратори можуть налаштовувати щоденне резервне

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

копіювання даних та налаштовувати елементи керування доступом на основі атрибутів для забезпечення безпеки контенту. Це дозволяє членам команди створювати шаблони HTML для декількох елементів, таких як панель навігації, нижній колонтитул, заголовки та перегляд. Крім того, функції моментальних знімків та проміжного зберігання дозволяють співробітникам клонувати сайти та проміжний вміст. MODX поставляється з інтерфейсом прикладного програмування (API), що дозволяє підприємствам інтегрувати платформу з кількома сторонніми рішеннями[30].

Tresorit – це хмарне рішення для синхронізації та обміну файлами із наскрізним шифруванням. Він призначений для різних галузевих вертикалей, таких як юриспруденція, охорона здоров'я, фінанси та технологічний бізнес. Він пропонує віддалене очищення пристрою, відновлення файлів (після атаки програм-вимагачів), брендинг, історію файлів і двофакторну автентифікацію, що налаштовується. Редагування та обмін файлами можна відстежувати на стіні активності. Tresorit доступний на настільних комп'ютерах та мобільних телефонах (Android, iOS). Користувачі можуть встановлювати права доступу на основі ролей для перегляду даних та обміну файлами з колегами та партнерами за межами організації, використовуючи захищені паролем посилання. Користувачі також можуть встановити дату закінчення терміну дії та ліміт відкриття для кожного спільного посилання. Відкриття посилань можна відстежувати. Рішення відповідає GDPR та HIPAA, сертифіковано за ISO 27001 та є членом Trusted Cloud та Cloud Security Alliance. Підтримка доступна через телефон або через базу знань [44].

FileCloud – це захищена платформа для спільної роботи з вмістом, яка підтримує мільйони користувачів у всьому світі, включаючи підприємства, навчальні заклади, державні організації та постачальників керованих послуг. Інноваційні рішення FileCloud для відповідності, детального контролю спільного доступу, управління та збереження, захисту від витоку даних та керування цифровими правами повністю інтегровані в загальнодоступні, приватні або гібридні хмарні моделі [19].

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

SmartVault – це програмне забезпечення для керування документами, яке дає змогу підприємствам обробляти та зберігати документи в централізованому сховищі. Організації можуть створити персоналізований портал із власними логотипами, щоб створити ідентичність бренду для клієнтів. SmartVault включає спеціальні робочі процеси, які дозволяють підприємствам автоматизувати завантаження, сканування та розповсюдження документів із внутрішніми та зовнішніми зацікавленими сторонами. Він пропонує численні функції, такі як двофакторна аутентифікація, можливості перетягування, керування версіями файлів, обробка платежів, повнотекстовий пошук, керування спільною роботою, фіксація електронного підпису тощо. Крім того, адміністратори можуть забезпечити відповідність вимогам CCPA, GDPR, SEC, GLBA, FINRA та іншим юридичним та промисловим стандартам. SmartVault полегшує інтеграцію з різними програмами сторонніх розробників, такими як Salesforce, Hubdoc, TaxCalc, Xero, FreshBooks, Method CRM, Microsoft Outlook тощо [38].

iDOC – це інструмент документообігу, система контролю та адаптивна мобільна версія. Система адаптується під усі пристрої, є можливість ставити та контролювати задачі, швидко підписати документи та онлайн-контракти з клієнтами за допомогою ЕЦП [5].

CleverForms – забезпечує створення, реєстрацію, збереження електронних документів та сканованих оригіналів документів, підписання електронних документів ЕЦП згідно ДСТУ 4145-2002, створення документів за шаблоном, пошук документів за контекстом, архівування документів, формування, створення та збереження історії опрацювання документу, формування та контроль виконання завдань, передачу електронних документів користувачам системи та зовнішнім адресатам. Система містить вбудований редактор для створення та редагування довідників, форм та шаблонів документів, відповідає вимогам чинних державних стандартів України на програмну продукцію, відповідає вимогам Закону України «Про електронні документи та електронний документообіг», Закону України «Про електронні довірчі послуги» [5].

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

Megapolis.DocNet – це бізнес інструмент, що охоплює всі етапи життєвого циклу документів: від підготовки проектів документів до організації архівного зберігання з забезпеченням електронного архіву та електронного підпису. Система побудована на платформі UnityBase, що дозволяє різні типи аутентифікації: Basic, Digest, на основі IP адреси клієнта, Negotiate (Kerberos, NTLM), на основі відкритих / закритих ключів RSA / ДСТУ, OpenIDConnect. Щоб запобігти атакам людина в середині, нападкам CSRF кожен запит супроводжується унікальним підписом у заголовку авторизації. Забезпечує контроль доступу на основі ролей. Має журнал аудиту [29].

Різні приватні платформи (наприклад, IBM Hyperledger Fabric, Corda [15], Waves Enterprise [45]) дозволяють забезпечити конфіденційний обмін даними всередині блокчейн-мережі різними способами, в основному за рахунок взаємодії приватних баз даних поза блокчейн-мережею, зі зберіганням хеш-сум цих даних у блокчейні. Такий підхід до зберігання самих даних поза блокчейном (англ. off-chain) може бути додатково актуальним через те, що розмір блоку обмежений і не підходить для зберігання великих обсягів даних.

Corda – це блокчейн-платформа з відкритим вихідним кодом, яка спрощує управління юридичними контрактами та іншою спільною інформацією між сторонами, які взаємно довіряють. Спочатку Corda була розроблена для застосування у фінансових установах. Існує також його комерційне видання – Corda Enterprise. Corda Enterprise розширює видання Corda і підтримує додаткові функції, включаючи підтримку комерційних баз даних (Oracle, MSSql), HSM, підвищення продуктивності (виконання паралельного потоку), налаштування вузлів високої доступності та інструменти для розгортання мережі Corda.

Hyperledger Fabric – це фреймворк блокчейну з відкритим кодом, який дозволяє розробляти продукти, рішення та додатки на основі блокчейну. Він має модульну архітектуру (підключи і працюй).

Waves Enterprise – це гібридна корпоративна блокчейн-платформа, яка об'єднує публічні та приватні мережні підходи. Платформа забезпечує

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

конфіденційність даних, простоту розгортання й керування, а також високу доступність і пропускну здатність транзакцій.

Таким чином існують багато пропозицій он-лайн систем управління документами в корпоративному верхньому ціновому сегменті навіть з використанням технологій блокчейну. В нижньому ціновому сегменті пропозиції захисту документів можливі або за додаткову ціну, або з використанням сторонніх інструментів, підключених або розроблених самостійно.

1.3 Розробка вимог до захисту системи електронного документообігу

Учасники блокчейн-мережі не є рівноправними: майже в будь-якій реалізації цієї технології введено такий розподіл ролей:

- валідатори;
- учасники, що пишуть транзакції в журнал;
- аудитори;
- учасники, які не записують транзакції, а лише перевіряють їхню правильність;
- легкі клієнти;
- учасники, які не зберігають повні копії блокчейну, а взаємодіють із мережею через інші вузли.

Однією з найбільш перспективних є технологія захищеного документообігу, який може стати набагато безпечнішим – насамперед за рахунок ведення децентралізованого реєстру документів, який неможливо змінити чи підправити. Користувачі зможуть працювати з документами, маючи повну впевненість у їхньому авторстві та справжності. Таким чином, вирішується безліч проблем, пов'язаних із недосконалістю бюрократичного апарату, небезпекою махінацій та підробки документів. На даний момент у світі вже існує безліч реалізацій подібної технології, наприклад, сервіс BlockSign, розроблений компанією Basno, що є загальнодоступним реєстром, в якому зберігаються, підписані електронним способом, документи [12].

Класифікація блокчейн-технологій.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		21

Виділяють 3 типи блокчейну:

- 1) Публічні блокчейни з відкритим доступом (Public blockchains)
- 2) Приватні блокчейни з відкритим доступом (Consortium blockchains)
- 3) Приватні блокчейни із закритим доступом (Fully private blockchains)

Розберемо кожен із них детальніше.

1. Публічні блокчейн з відкритим доступом Найпоширенішим на даний момент є саме цей тип, що використовується в таких криптовалютах як Біткоїн, Ефіріум, Ріпл та ін.

- 1) Повна відкритість блоків всім користувачів.
- 2) Користувачам не потрібно довіряти один одному.
- 3) Повна децентралізація та незалежність від третіх осіб.
- 4) Захищеність мережі за рахунок криптографічних алгоритмів та застосування великої кількості комп'ютерних систем.

Він насамперед добре підходить для застосування у фінансовій сфері, де потрібна повна незалежність від третьої особи, прозорість операцій та висока надійність системи.

2. Приватні блокчейни з відкритим доступом.

Тут право завіряти транзакції, вести аудит безпеки, вносити зміни до програмного забезпечення та змінювати бази даних мають лише привілейовані користувачі, решта отримують доступ до файлів для читання. Відповідно, така система вже не є повністю децентралізованою та залежить від певного кола осіб.

Їх основні властивості:

- 1) Наявність перевірених валідаторів.
- 2) Висока швидкість підтвердження транзакцій.
- 3) Неможливість проведення атаки 51% (коли у розпорядженні атакуючого перебувають потужності більше, ніж у решти мережі).
- 4) Можливість видалення записів із ланцюга чи його зміни.
- 5) Нижча вартість транзакцій за рахунок відсутності необхідності застосування великих обчислювальних потужностей.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

Враховуючи перелічені властивості, можна зробити висновок, що дана система може добре підійти для державних структур (наприклад, охорона здоров'я: привілейованими користувачами в такому разі можуть бути медустанови, які будуть вносити в ланцюжок дані історії хворих, а користувачі зможуть завжди відкрити свою історію).

3. Приватні блокчейни із закритим доступом.

Блокчейн цього виду має ті ж властивості, що й попередні, але за умови, що прості користувачі не можуть стати учасниками мережі без підтвердження валідаторів, а також не завжди мають доступ до читання файлів ланцюга. Таким чином, дана система повністю перестає бути відкритою та незалежною від третіх осіб.

Властивості даної системи:

- 1) Закритість даних від непривілейованих користувачів мережі.
- 2) Повна закритість мережі від неавторизованих користувачів.
- 3) Неможливість проведення атаки 51%.
- 4) Повна залежність від кола привілейованих користувачів.
- 5) Висока надійність та стійкість мережі за умови довіри до валідаторів.

Цей блокчейн вже більше схожий на класичні централізовані мережі, проте, володіючи властивістю ведення ланцюга взаємопов'язаних блоків, може вдало застосовуватися для внутрішніх закритих приватних мереж та системах захищеного документообігу на підприємствах або державних структурах, де необхідно зберігання службової інформації.

Найбільш поширеними є моделі «Доказ роботою» (Prof of Work – PoW), «Доказ часток» (Prof of Stake – PoS), «Делегований доказ часток» (Delegated proof of stake), Гібридна система Prof of Work/Prof of Stake, Система «Доказ активністю» (Prof of Activity), «Доказ спалювання» (Prof of burn), «Доказ ємністю» (Proof of Capacity), «Доказ зберігання» (Proof of Storage) [31].

На підставі проведеного аналізу було сформульовано такі вимоги до розробки:

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

- Кожен авторизований користувач системи повинен мати доступ до документів.
- Несанкціонований доступ до документів має бути неможливим.
- Змінювати, підробляти чи видаляти документи з реєстру не повинно бути можливо.
- Кожен документ повинен мати автора та бути підписаний.

Виходячи з вимог, що пред'являються до системи, було визнано доцільним використовувати наступний тип блокчейну: приватний закритого доступу, так як блокчейн цього виду має умову, що прості користувачі не можуть стати учасниками мережі без підтвердження валідаторів, а також не завжди мають доступ до читання файлів ланцюга.

Як алгоритм досягнення консенсусу була обрана гібридна система доказу часток і доказу роботою – «Proof of Activity», оскільки вона включає всі переваги цих двох алгоритмів.

Висновки до першого розділу

В результаті проведеного дослідження були отримані наступні висновки:

1. Інтерес до блокчейн технологій продовжує зростати з реформуванням та розвитком всіх сфер української держави, а саме медичної реформи, судової та правоохоронної реформи, розвитком електронної держави та так званої «діджиталізації» держави та в умовах триваючої кібервійни з державою агресором.

2. Використання блокчейн технологій може вирішити багато проблем пов'язаних з бюрократією, корупцією, крадіжками та шахрайствами у таких процесах як видача дозволів та реєстрацій.

3. Незважаючи на бурний розвиток блокчейн все ще залишається експериментальною технологією – вона постійно знаходиться у розвитку, з'являються все нові способи її використання.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		24

4. Серед основних трендів в сфері використання блокчейн технологій є: його використання для відстеження вакцин, корпоративний блокчейн, застосування NFT та розвиток блокчейну як послуги.

5. В сфері державного управління прогнозується використання технологій блокчейну для організації виборів, гуманітарних та соціальних послуг, захисту цифрових активів, підвищенні ефективності договірних відносин та у діловодстві.

6. Україна наряду з Естонією та Грузією є одними з провідних країн щодо впровадження технологій блокчейну.

7. На ринку існують багато пропозицій он-лайн систем управління документами в корпоративному верхньому ціновому сегменті навіть з використанням технологій блокчейну. В нижньому ціновому сегменті пропозиції захисту документів можливі або за додаткову ціну, або з використанням сторонніх інструментів, підключених або розроблених самостійно.

8. На підставі проведеного аналізу було сформульовано такі вимоги до розробки:

- Кожен авторизований користувач системи повинен мати доступ до документів.
- Несанкціонований доступ до документів має бути неможливим.
- Змінювати, підробляти чи видаляти документи з реєстру не повинно бути можливо.
- Кожен документ повинен мати автора та бути підписаний.

9. Виходячи з вимог, що пред'являються до системи, було визнано доцільним використовувати наступний тип блокчейну: приватний закритого доступу, так як блокчейн цього виду має умову, що прості користувачі не можуть стати учасниками мережі без підтвердження валідаторів, а також не завжди мають доступ до читання файлів ланцюга.

10. Як алгоритм досягнення консенсусу була обрана гібридна система доказу часток і доказу роботою – «Proof of Activity», оскільки вона включає всі переваги цих двох алгоритмів.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		25

РОЗДІЛ 2. РОЗРОБКА ТЗ ТА РЕАЛІЗАЦІЯ ВЕБ-ДОДАТКУ

2.1 Аналіз загрози розробка технічних вимог до завдання

Під час розробки технічного завдання до проекту, стояли наступні цілі:

1. Створити он-лайн сервіс реєструвати документів.
2. Забезпечити безпеку користувацьких даних.
3. Забезпечити безпечну авторизацію.
4. Створити зручний веб-інтерфейс.
5. Створити можливість верифікувати документ та валідувати його на спробу модифікації за реєстраційним номером та самим електронним документом (чи дійсно саме цей документ був зареєстрований за цим номером та не був змінений).
6. Створення децентралізованого сховища зареєстрованих документів.
7. Запобігання можливості внесення змін в реєстраційні дані за рахунок атак.
8. Шифрування ключів доступу користувачів та реєстраційних ключів документів.
9. Запобігання найбільш поширеним веб-атакам.

Аналіз моделі загроз (Див. Модель загроз, рис.2.1) вказує, що основними порушниками в нашому випадку є:

1. Порушник Інсайдер. Він має доступ до адміністрування додатку реєстрації документів або до адміністрування бази даних додатку, що несе в собі загрозу зміни ним цих даних.

2. Порушник Хакер. Це зовнішній порушник, що може використовувати основні вразливості web-додатків, такі як SQL-ін'єкції, CSRF, XSS атаки, атаки грубого перебору реєстраційних даних, задля розвідки, отримання адміністративних прав доступу та внесення змін в реєстраційні дані.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

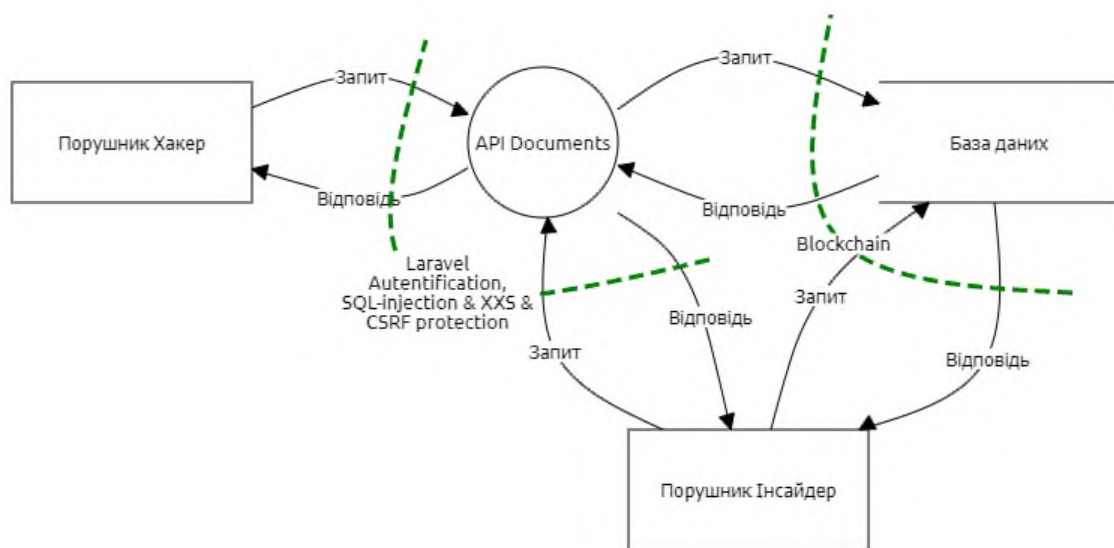


Рисунок 2.1 Модель загроз

Використання технології Blockchain при побудові додатку виключає можливість зміни даних реєстрації Інсайдером без загрози бути викритим, а також перешкоджає можливості непомітної зміна реєстраційних даних зовнішнім порушником Хакером. Також використання при цьому хешування та зберігання цих перевірочних кодів дозволяє підтверджувати цілісність та незмінність зареєстрованих електронних документів.

Фреймворк Laravel включає функції, необхідні для створення сучасних, підтримуваних, розподілених веб-додатків. Завдяки кешуванню, оптимізації фронтенду та правильному поділу коду на компоненти вдається забезпечувати справді швидкий доступ до даних. У фреймвоці добре розроблені механізми аутентифікації. Laravel пропонує ряд вбудованих функцій безпеки: захист від SQL-ін'єкцій, захист від підробки міжсайтових запитів (CSRF), захист від XSS атак та ін. Фреймворк захищає за замовчуванням, унеможливорює нелегітимні SQL-запити за рахунок нормалізації всіх параметрів під час побудови, а також екранування заборонених html-тегів і виведення його як текстових даних без можливості виконання.

Тому у сервісі будуть використані наступні технології: фреймворк Laravel, реляційна база даних MySQL, децентралізоване сховище даних blockchain (Див. Діаграма сервісів та додатків, рис.2.2).

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

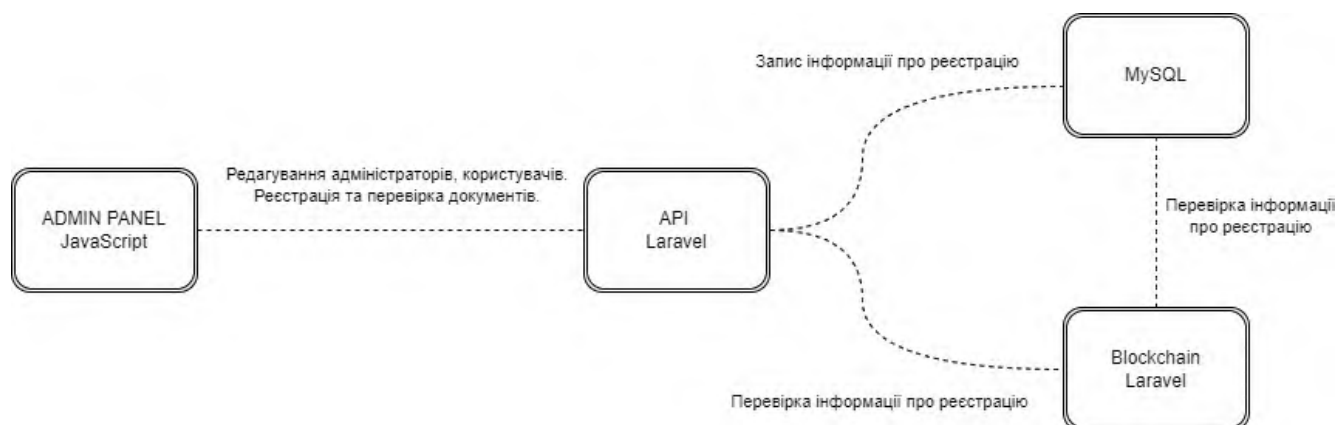


Рисунок 2.2 Діаграма сервісів та додатків

Таким чином розроблено та проаналізовано технічні вимоги до проекту, модель загроз та моделі порушників для додатку. Виходячи з цього вибрано сервіси розробки та захисту додатку, що розробляється, а саме фреймворк Laravel, реляційна база даних MySQL, децентралізоване сховище даних blockchain.

2.2 Вибір системи управління доступом та розробка структури БД

В системі будуть створені наступні ролі:

- Користувач. Він буде мати права на реєстрацію документів, перегляд зареєстрованих документів, до яких він має доступ згідно його рівня доступу (від 1 до 4) та перевірку дійсності (автентичності та цілісності) документів.
- Адміністратор. Може все те, що й Користувач та на додачу ще має можливість додавати (видавати атрибути доступу в систему) та видаляти користувачів.
- Супер Адміністратор. Може все те, що й Адміністратор та ще має права додавання та видалення Адміністраторів.

У цій схемі є Супер Адміністратор, що створює локальних Адміністраторів у відокремлених (територіально та/або адміністративно) підрозділах установи чи підприємства.

(Див. Діаграма прецедентів Use-casediagram, рис.2.3).

		Пірог О.В.			KIK.KP.B – 125 – 12 – ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		

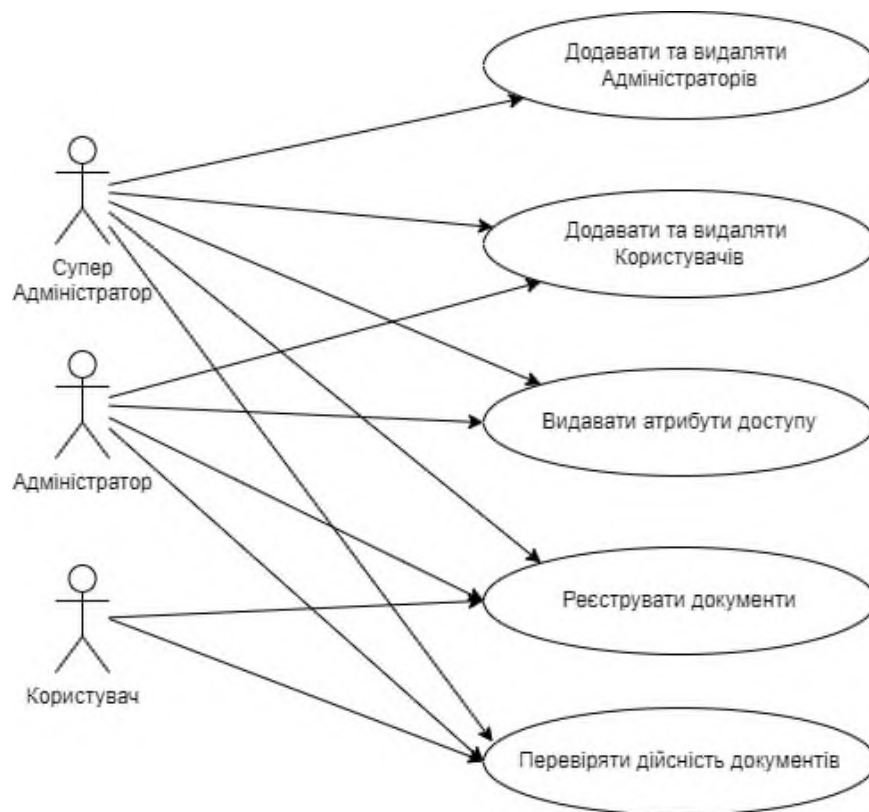


Рисунок 2.3 Діаграма прецедентів Use-casediagram

Виходячи з цілей проекту пропонується створення двох баз даних:

1. Документи (Documents) з наступними полями:

- Номер документа (DocumentID) – ключове поле цієї бази даних, надає реєстраційний номер документу в системі. Також буде використовуватися під час верифікації документа.

- ID виконавця (реєстранта) (UserID) – визначає користувача, що виконав або зареєстрував цей документ.

- Дата та час реєстрації (SigningDate&Time).

- Назва документа (Document'sName).

- Рівень доступу до документу (Access level) – має значення 1, 2, 3, 4 та не дає можливість доступу до даних документа користувачам з нищим рівнем доступу.

- Код перевірки (Verificationcode) – Хешоване значення на основі самого документа, та коду перевірки попереднього документа. Вираховується за формулою:

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

$$VC_i = SHA(SHA(DocFile) + VC_{i-1}) \quad (1)$$

Де

VC – Код перевірки (Verificationcode),

DocFile – файл, що перевіряється,

SHA – функція хешування SHA 256.

2. Користувачи (Users) з наступними полями:

- Ідентифікатор користувача (UserID) – ключове поле цієї бази даних.
 - ПІБ користувача (Fullname).
 - Рівень доступу до документу (Access level) – має значення 1, 2, 3, 4 та не дає можливість доступу до даних документа користувачам з нижчим рівнем доступу.
 - Роль (Role) – роль користувача в системі (Супер Адміністратор, Адміністратор, Користувач)
 - Ключ доступу (Key) – пароль входу в систему, може розповсюджуватися на пристроях (Flesh).
- (Див. Діаграма баз даних, рис.2.4).

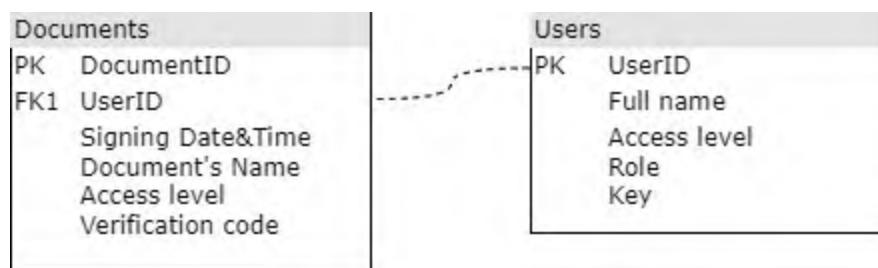


Рисунок 2.4 Діаграма баз даних

Таким чином розроблена діаграма прецедентів та ролі, що використовуються в додатку. Виходячи з цього розроблена діаграма баз даних.

2.3 Розробка коду елементів захисту

Структура розробленого проекту виглядає наступним чином(Див. рис. 2.5):



Рисунок 2.5 Структура розробленого проекту

Функція save(Див. Фрагмент коду збереження даних реєстрації, рис.2.6)використовується для збереження реєстраційної інформації під час реєстрації нових документів в системі. Дані передаються із форми та зберігаються в базі даних. Значення hashвираховується за формулою 1.

```

ocuf| _row.blade.php x | Route.php x | manage.blade.php — documents x | DocumentsRepository.php x | UsersRepository.php

/**
 * @param array $data
 * @return Documents
 */
public function save(array $data) : Documents
{
    $data['hash'] = hash_file('sha256', $data['path']->path());
    $lastDocument = $this->documents->orderBy('created_at', 'desc')->first();
    if($lastDocument){
        $data['hash'] .= $lastDocument->hash;
    }
    $data['hash'] = hash('sha256', $data['hash']);
    $document = $this->documents->updateOrCreate(['id' => $data['id'] ?? 0], $data);
    $fileName = $document->id.'.'.$data['path']->extension();
    $this->_storage->putFileAs('documents', $data['path'], $fileName);
    $document->path = $fileName;
    $document->save();
    return $document;
}

```

Рисунок 2.6 Фрагмент коду збереження даних реєстрації

Розроблений додаток має функцію перевірки реєстраційних данихcheck(Див. Фрагмент коду перевірки даних реєстрації, рис.2.7) за переданими у форму номером документа та самим документом, що перевіряється. Значення hash_varifдокумента, що завантажується та перевіряється, розраховується за формулою 1, а потім звіряється із значенням hash, що збережено в базі даних для документа із вказаним реєстраційним номером.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ge.blade.php — users × DocumentsController.php × UsersController.php × UsersService.php × DocumentsService.php × _row.blade
public function check(Request $request) : Application|Factory|View|RedirectResponse
{
    if($request->isMethod('post')){
        $request->validate([
            'id' => 'required',
            'path' => 'required'
        ], $this->validationFields);
        $id = $request->get('id');
        $id1 = $id - 1;
        $file = $request->file('path');
        $document = $this->documentsService->findById($id);
        $document1 = $this->documentsService->findById($id1);
        if(!$document){
            return back()->with('error', 'Відсутній документ за №: '.$id);
        }
        $hash_varif = hash_file('sha256', $file->path());
        if($document1){
            $hash_varif .= $document1->hash;
        }
        $hash_varif = hash('sha256', $hash_varif);
        if($document->hash !== $hash_varif){
            return back()->with('error', 'Документ було змінено');
        }
        return back()->with('success', 'Назва документа '.$document->name.', файл не було змінено, видано й зареєстровано в системі за №'.$document->id.', Дата та час підписання '.$document->subscribed_at.', Автор '.$document->user->name);
    }

    return view('documents.check');
}

```

Рисунок 2.7 Фрагмент коду перевірки даних реєстрації

Для протидії грубому перебору реєстраційних даних bruteforceфреймворк має можливість обмежити кількість спроб аутентифікації з одного IP (Див. Фрагмент коду налаштування кількості спроб аутентифікації, рис.2.8)

```

DocumentsController.php × UsersController.php × User.php × ThrottlesLogins.php × manage.blade.php — d
/**
 * Get the maximum number of attempts to allow.
 *
 * @return int
 */
public function maxAttempts()
{
    return property_exists($this, 'maxAttempts') ? $this->maxAttempts : 5;
}

```

Рисунок 2.8 Фрагмент коду налаштування кількості спроб аутентифікації

		Пирог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		33

Після вичерпання обмеженої кількості спроб аутентифікації є можливість визначити тривалість тайм-ауту.(Див. Фрагмент коду налаштування тайм-ауту у зв'язку з перевищенням кількості спроб аутентифікації, рис.2.9)

```

app.blade.php x auth.php x UsersRepository.php x 2014_10_12_000000_create_users_table.php x User.php
-----
Password Confirmation Timeout
-----

Here you may define the amount of seconds before a password confirmation
times out and the user is prompted to re-enter their password via the
confirmation screen. By default, the timeout lasts for three hours.

*/

'password_timeout' => 10800,
  
```

Рисунок 2.9 Фрагмент коду налаштування тайм-ауту у зв'язку з перевищенням кількості спроб аутентифікації

Для протидії використання паролів у випадку їх викрадення з БД, де вони зберігаються на сервері, паролі зберігаються в хешованому вигляді.(Див. Фрагмент коду створення даних аккаунту, рис.2.10, Фрагмент коду збереження даних аккаунту, рис.2.11)

```

DocumentsController.php x RegisterController.php x manage.blade.php — documents
/**
 * Create a new user instance after a valid registration.
 *
 * @param array $data
 * @return \App\Models\User
 */
protected function create(array $data)
{
    return User::create([
        'name' => $data['name'],
        'email' => $data['email'],
        'password' => Hash::make($data['password']),
    ]);
}
  
```

Рисунок 2.10 Фрагмент коду створення даних аккаунту

```

/**
 * @param array $data
 * @return User
 */
public function save(array $data) : User
{
    !$data['password'] ? : $data['password'] = Hash::make($data['password']);
    if(!$data['password']){
        unset($data['password']);
    }
}

```

Рисунок 2.11 Фрагмент коду збереження даних аккаунту

Задля збереження конфіденційної та комерційної таємниці в установі у додатку впроваджено розмежування доступу до інформації, що в ньому збережено.

Наприклад тільки Супер Адміністратор може дивитися дані інших Адміністраторів.(Див. Фрагмент коду управління виводом інформації в залежності від вибраної ролі користувача, рис.2.12)

```

protected function manage($compact)
{
    $parent = parent::manage($compact);
    $compact = $parent->getData();

    $compact['userRole'] = $compact['model']->roles->first();
    $compact['roles'] = $this->rolesService->all()->pluck('name', 'id')->toArray();

    if($compact['userRole'] !== 'Super Admin'){
        $compact['roles'] = $this->rolesService->getByName('User')->pluck('name', 'id')->toArray();
    }

    return view($compact['modelName'].'.manage', $compact);
}

```

Рисунок 2.12 Фрагмент коду управління виводом інформації в залежності від вибраної ролі користувача

Також назви зареєстрованих документів можуть побачити тільки користувачі з рівнем доступу не нижче рівня доступу цього документу.(Див.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

Фрагмент коду управління виводом інформації в залежності від призначеного рівня доступу до інформації, рис.2.13)



```

public function scopeAllowedLvl(Builder $query): Builder
{
    $user = Auth::user();

    if(!$user){
        return $query;
    }

    $userRole = $user->getRoleNames()->first();
    return $userRole === 'User' ? $query->where('allowed_lvl', '>=', $user->
        allowed_lvl) : $query;
}

```

Рисунок 2.13 Фрагмент коду управління виводом інформації в залежності від призначеного рівня доступу до інформації

Laravel включає конструктор запитів, який допомагає у запитах до бази даних, використовуючи різні прості методи ланцюга. Він забезпечує ORM (ObjectRelationalMapper) та реалізацію ActiveRecord, що називається Eloquent. Це запобігає впровадженню SQL ін'єкцій. Eloquent працює, вдосконалюючи методи управління записами, автоматично перетворює стовпці таблиці у властивості класу PHP. Таким чином, можна оновлювати, видаляти та додавати нові дані до бази даних без використання SQL запитів. (Див. Фрагмент коду визначення методу Eloquent доступу до БД, рис.2.14, Фрагмент коду управління записами БД, що перетворено на властивості класу PHP, рис.2.15)

Задля протидії XSS атакам та деяким іншим розповсюдженим атакам необхідно проводити валідацію вхідних даних отриманих з ненадійних джерел та фільтрацію виводу вихідних даних, що було отримано з ненадійних джерел.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

```

auth.php x UsersRepository.php x 2014_10_12_000000_create_users_table.php x User.php x Throttles
|-----|
| User Providers |
|-----|
| All authentication drivers have a user provider. This defines how the |
| users are actually retrieved out of your database or other storage |
| mechanisms used by this application to persist your user's data. |
| |
| If you have multiple user tables or models you may configure multiple |
| sources which represent each model / table. These sources may then |
| be assigned to any extra authentication guards you have defined. |
| |
| Supported: "database", "eloquent" |
| |
| */ |
| |
| 'providers' => [ |
|     'users' => [ |
|         'driver' => 'eloquent', |
|         'model' => App\Models\User::class, |
|     ], |
| ]

```

Рисунок 2.14 Фрагмент коду визначення методу Eloquent доступу до БД

```

2014_10_12_000000_create_users_table.php x User.php x ThrottlesLogins.php x Do
* Run the migrations.
*
* @return void
*/
public function up()
{
    Schema::create('users', function (Blueprint $table) {
        $table->id();
        $table->string('name');
        $table->string('email')->unique();
        $table->timestamp('email_verified_at')->nullable();
        $table->string('password');
        $table->rememberToken();
        $table->timestamps();
    });
}

```

Рисунок 2.15 Фрагмент коду управління записами БД, що перетворено на властивості класу PHP

На наступному фрагменті коду представлена валідаціїреєстраційних даних користувача. Як можна побачити відбувається валідація вхідних даних за форматом (string)та довжиною (max:255). Також задля того, щоб забезпечити достатню захищеність пароллю обмежена його довжина (min:8)(Див. Фрагмент коду валідаціїреєстраційних даних користувача, рис.2.16, Фрагмент коду валідаціїзбереження даних користувача, рис.2.17, Фрагмент коду

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

валідації коригування даних користувача, рис.2.18, Фрагмент коду валідації вхідних даних збереження даних користувача, рис.2.19)



```

/**
 * Get a validator for an incoming registration request.
 *
 * @param array $data
 * @return \Illuminate\Contracts\Validation\Validator
 */
protected function validator(array $data)
{
    return Validator::make($data, [
        'name' => ['required', 'string', 'max:255'],
        'email' => ['required', 'string', 'email', 'max:255', 'unique:users'],
        'password' => ['required', 'string', 'min:8', 'confirmed'],
    ]);
}

```

Рисунок 2.16 Фрагмент коду валідації реєстраційних даних користувача

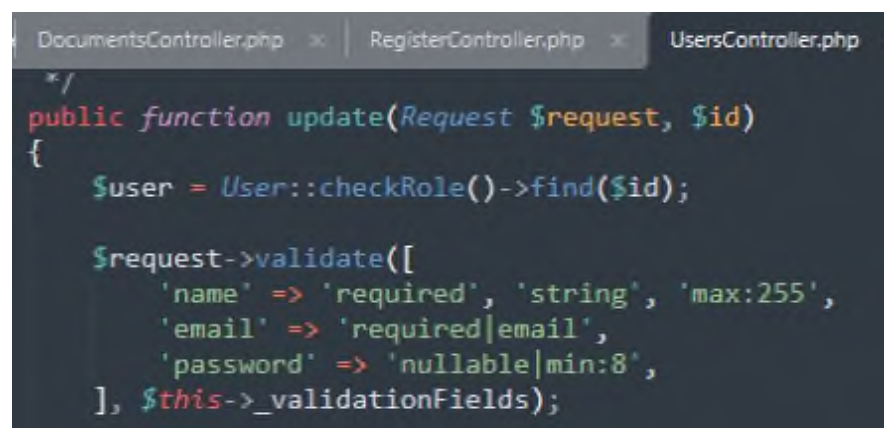


```

public function store(Request $request)
{
    $request->validate([
        'name' => 'required', 'string', 'max:255',
        'email' => 'required|email|unique:users',
        'password' => 'required|min:8',
    ], $this->_validationFields);
}

```

Рисунок 2.17 Фрагмент коду валідації збереження даних користувача



```

/**
 *
 */
public function update(Request $request, $id)
{
    $user = User::checkRole()->find($id);

    $request->validate([
        'name' => 'required', 'string', 'max:255',
        'email' => 'required|email',
        'password' => 'nullable|min:8',
    ], $this->_validationFields);
}

```

Рисунок 2.18 Фрагмент коду валідації коригування даних користувача

```

public function settings(Request $request)
{
    $title = 'Налаштування';

    $user = auth()->user();

    if($request->isMethod('post')){
        $request->validate([
            'name' => 'required', 'string', 'max:255',
            'email' => 'required|email',
            'password' => 'nullable|min:8'
        ], $this->_validationFields);
    }
}

```

Рисунок 2.19 Фрагмент коду валідації вхідних даних збереження даних користувача

Якщо вхідні дані не проходять валідацію, то видається попередження. (Див. Фрагмент коду виводу коментарів до помилок під час валідації даних користувача, рис.2.20, Фрагмент коду виводу коментарів до помилок під час валідації даних документів, що реєструються, рис.2.21)

```

protected $_validationFields = [
    'name.required' => 'ПІБ не введено',
    'name.max' => 'ПІБ занадто довгий',
    'email.required' => 'Емейл не введено',
    'email.email' => 'Емейл не валіден',
    'email.unique' => 'Користувач з даним емейлом вже є',
    'role.required' => 'Роль не вибрана',
    'password.required' => 'Пароль не вказано',
    'password.min' => 'Пароль занадто короткий'
];

```

Рисунок 2.20 Фрагмент коду виводу коментарів до помилок під час валідації даних користувача

Також необхідним заходом для запобігання XSS атак є фільтрація при виводі вихідних даних отриманих з ненадійних джерел. За замовчуванням оператори Blade `{{...}}` автоматично надсилаються через функцію PHP `htmlspecialchars`, що виконує екранування вихідних даних.

```

DocumentsController.php x RegisterController.php x UsersController.php x VerificationContro
protected $_validationRules = [
    'name' => 'required', 'string', 'max:255',
    'allowed_lvl' => 'required',
    'path' => 'required',
    'subscribed_at' => 'required'
];

protected $_validationFields = [
    'id.required' => '№ документа не було введено',
    'name.required' => 'Назву документа не було введено',
    'allowed_lvl.required' => 'Рівень доступу не було вказано',
    'path.required' => 'Файл не було прикріплено',
    'subscribed_at.required' => 'Дата підписання не було вказано'
];

```

Рисунок 2.21 Фрагмент коду виводу коментарів до помилок підчас валідації даних документів, що реєструються

Таким чином у додатку підчас виводу даних, що було отримано з ненадійних джерел використовується вказаний оператор. Наприклад підчас виводу введеного користувачем та збереженого ПІБ користувача використано вказаний оператор. (Див. Фрагмент коду виводу коментарів до помилок підчас валідації поля ПІБ, рис.2.22)

```

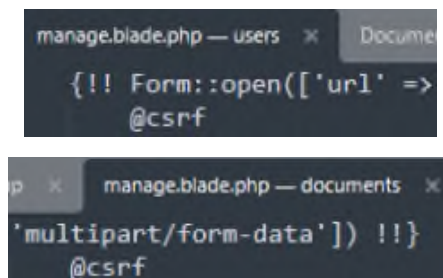
manage.blade.php — documents x app.blade.php x User.php x ThrottlesLogins.php
<label>Назва</label>
{!! Form::text('name', old('name') ?? $model->name, [
    'placeholder' => 'Назва',
    'class' => 'form-control'
]) !!}
@if ($errors->has('name'))
    <span class="text-danger">{{ __($errors->first('name'))
    }}</span>
@endif

```

Рисунок 2.22 Фрагмент коду виводу коментарів до помилок підчас валідації поля ПІБ

Laravel включає вбудований плагін CSRF, який генерує токени для кожного активного сеансу користувача. Ці токени перевіряють, чи надсилаються операції чи запиту відповідним аутентифікованим користувачем. Тому в додатку використовується цей токен підчас передавання даних з вхідних форм та

використання переданих даних (Див. Фрагмент коду вставки CSRF токену до даних, що передаються формою, рис.2.23, Фрагмент коду використання CSRF токену, рис.2.24)

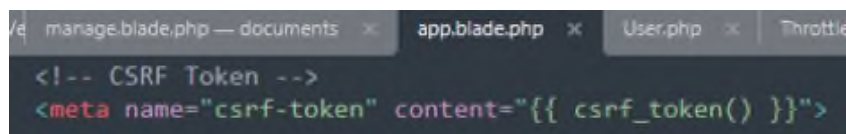


```

manage.blade.php — users × Documente
{!! Form::open(['url' =>
    @csrf

p × manage.blade.php — documents ×
'multipart/form-data']) !!}
    @csrf
  
```

Рисунок 2.23 Фрагмент коду вставки CSRF токену до даних, що передаються формою



```

/e manage.blade.php — documents × app.blade.php × User.php × Throttli
<!-- CSRF Token -->
<meta name="csrf-token" content="{{ csrf_token() }}">
  
```

Рисунок 2.24 Фрагмент коду використання CSRF токену

Також для підтримання сесії фреймворк генерує персональний токен. (Див. Фрагмент коду управління записами БД персональних токенів, рис.2.25, Фрагмент коду зберігання персональних токенів, рис.2.26)



```

app.blade.php × 2019_12_14_000001_create_personal_access_tokens_table.php × UsersRepository.php × 0_create_u
.../
public function up()
{
    Schema::create('personal_access_tokens', function (Blueprint $table) {
        $table->id();
        $table->morphs('tokenable');
        $table->string('name');
        $table->string('token', 64)->unique();
        $table->text('abilities')->nullable();
        $table->timestamp('last_used_at')->nullable();
        $table->timestamps();
    });
}
  
```

Рисунок 2.25 Фрагмент коду управління записами БД персональних токенів

```

014_10_12_000000_create_users_table.pl User.php
"/
protected $hidden = [
    'password',
    'remember_token',
];

```

Рисунок 2.26 Фрагмент коду зберігання персональних токенів

Таким чином розроблено додаток, що реалізує визначені механізми захисту:

- Використання технології Blockchain для неможливості непомітної зміни реєстраційних даних зареєстрованих документів.
- Збереження хеш-суми зареєстрованих документів та верифікація зареєстрованих документів.
- Захист від bruteforceатак за рахунок обмеження кількість спроб аутентифікації та влаштування таймауту у зв'язку з перевищенням кількості спроб, а також перевірки вибору достатньо безпечного паролю.
- Захист від викрадення паролів за рахунок зберігання в хешованому вигляді.
- Налаштування розмежування доступу для збереження конфіденційної та комерційної таємниці в установі.
- Захист від впровадженню SQL ін'єкцій за рахунок використання методів управління записами БД Eloquent.
- Захист від XSSта деяких інших атакза рахунок валідації вхідних даних та фільтрації виводу вихідних даних, що було отримано з ненадійних джерел.
- Захист від CSRF атак за рахунок використання токенів CSRF.
- Захист сесій за рахунок використання персональних токенів.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до другого розділу

1. Розроблено технічні вимоги до проекту, що розробляється.
2. Розроблено та проаналізовано модель загроз для додатку, що розробляється.
3. Розроблено та проаналізовано моделі порушників для додатку, що розробляється.
4. Виходячи з цього вибрано сервіси розробки та захисту додатку, що розробляється, а саме фреймворк Laravel, реляційна база даних MySQL, децентралізоване сховище даних blockchain.
5. Розроблена діаграма прецедентів та ролі, що використовуються в додатку.
6. Виходячи з цього розроблена діаграма баз даних.
7. Розроблено додаток, що реалізує визначені механізми захисту:
 - Використання технології Blockchain для неможливості непомітної зміни реєстраційних даних зареєстрованих документів.
 - Збереження хеш-суми зареєстрованих документів та верифікація зареєстрованих документів.
 - Захист від bruteforce атак за рахунок обмеження кількості спроб аутентифікації та влаштування таймауту у зв'язку з перевищенням кількості спроб, а також перевірки вибору достатньо безпечного паролю.
 - Захист від викрадення паролів за рахунок зберігання в хешованому вигляді.
 - Налаштування розмежування доступу для збереження конфіденційної та комерційної таємниці в установі.
 - Захист від впровадженню SQL ін'єкцій за рахунок використання методів управління записами БД Eloquent.
 - Захист від XSS та деяких інших атак за рахунок валідації вхідних даних та фільтрації виводу вихідних даних, що було отримано з ненадійних джерел.
 - Захист від CSRF атак за рахунок використання токенів CSRF.
 - Захист сесій за рахунок використання персональних токенів.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						43
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ТЕСТУВАННЯ ВЕБ-ДОДАТКУ

3.1 Розробка плану тестування додатку

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

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.

Таблиця 3.1.

План тестування додатку

№ з/п	Початкові умови	Порядок дій	Очікуваний результат
1	Анонімний користувач /documents /documents-check /users /settings	Відкрити URL сторінок адміністрування	HTTP Status 302 – редірект на сторінку авторизації /login
2	Авторизований користувач /users	Відкрити URL сторінок адміністрування	HTTP Status 403 – USER DOES NOT HAVE THE RIGHT PERMISSIONS.
3	Авторизований адміністратор /documents /documents-check /users /settings	Відкрити URL сторінок адміністрування	Доступ відкритий

№ з/п	Початкові умови	Порядок дій	Очікуваний результат
4	Анонімний користувач /documents /documents-check /settings	Відкрити URL сторінок користувача	HTTP Status 302 - редірект на сторінку авторизації /login
5	Авторизований користувач /documents /documents-check /settings	Відкрити URL сторінок користувача	Доступ відкритий
6	Авторизований користувач з рівнем допуску 2	Відкрити URL сторінок користувача.	Користувач не має доступу до розділу адміністрування користувачів та не бачить записи с рівнем доступу 1
7	Будь-який користувач	Відкрити будь-яку сторінку адміністратора або користувача з формою Ввести в будь-яке текстове поле (крім пароля) символи: Виконати submit форми	Дія повинна бути відхилена сервером Alert не виконується.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

№ з/п	Початкові умови	Порядок дій	Очікуваний результат
8	Розробник вносить в текстові поля БД інформацію виду 	Відкрити сторінки, на яких відображаються підготовлені дані	Дія повинна бути відхилена сервером Alert не виконується.
9	Авторизований адміністратор	Реєстрація користувача з паролем довжиною менше 8 символів.	Пароль повинен містити мінімум вісім символів.
10	Анонімний користувач	Авторизація. Організація bruteforce атаки на модуль авторизації за допомогою інструмента BurpSuite	Після п'яти невдалих спроб авторизації можливість авторизації блокується на визначений тайм-аут (11 секунд).
11	Анонімний користувач	Відновлення паролю по email	Після сабміта форми користувач повинен отримати повідомлення, яке не дозволяє визначити, чи правильно введено email. Посилання на

№ з/п	Початкові умови	Порядок дій	Очікуваний результат
			скидання пароля повинні бути валідні не більше двох годин.
12	Авторизований користувач	Доступ до перегляду документів вищого рівня доступу ніж рівень допуску користувача	Записи щодо реєстрації документів вищого рівня допуску не відтворюються у списку зареєстрованих документів
13	Анонімний користувач	Спроба UNION SQL-ін'єкції у модулі авторизації за допомогою інструмента BurpSuite	Невдала.
14	Анонімний користувач	Тестування логіки авторизації Login: hac@hac.com' or 1=1;-- Parol: any	Видається повідомлення про помилку.
15	Авторизований користувач	Реєстрація документа в системі та наступна перевірка цього документа в системі на справжність.	Успіх. Видача реквізитів справжнього документа.
16	Авторизований користувач	Реєстрація документа в системі, зміна його змісту та наступна перевірка цього документа в системі	Помилка. Документ було змінено. Реквізити документа не

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

№ з/п	Початкові умови	Порядок дій	Очікуваний результат
		на справжність.	видаються.
17	robots.txt sitemap	Перевірити спеціальні файли SEO	Посилання на адміністративну (захищену) зону, на update не повинні бути вказані в robots.txt або sitemap. Сама зона закривається в файлі .htaccess

Таким чином розроблено план тестування розробленого додатку на вразливості контролю доступу, логіки авторизації, XSS, SQL ін'єкції, використання слабо захищених паролів, захищеність від Brute-force атак, розкриття інформації, а також блокчейн системи перевірки зареєстрованих документів на дійсність.

3.2 Результати тестування додатку

На першому етапі планувалося проведення автоматичного тестування розробленого додатку за допомогою інструмента BurpSuite. Але у зв'язку з відсутністю можливостей проведення автоматичного тестування у безкоштовному наборі BurpSuiteCommunityEdition 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: /documents, /documents/create, /documents-check, /users, /users/create, /settings). Система не дає змоги завантажити вказані сторінки. Після

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						48
Змн.	Арк.	№ докум.	Підпис	Дата		

звернення до вказаних сторінок спрацьовує переадресація на сторінку авторизації (Див. рис. 3.1).

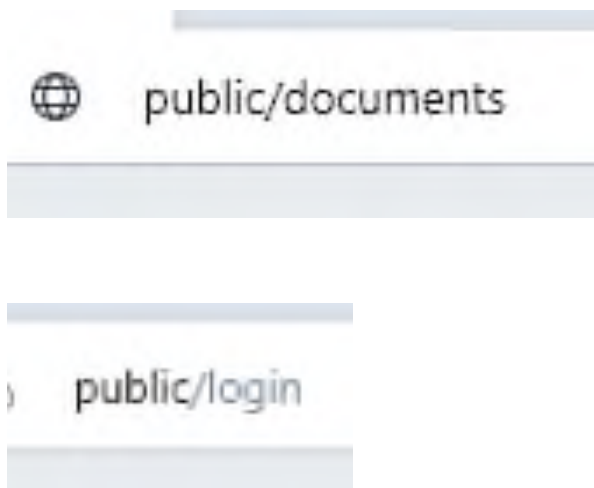


Рисунок 3.1 Переадресація на сторінку авторизації при зверненні до закритих частин сайту

Після реєстрації як адміністратор користувач може відвідувати вказані вище сторінки (Див. рис. 3.2, 3.3, 3.4, 3.5).

Документи

Додати

Перелік

✓

Перевірка документа

Користувачи

НАЛАШТУВАННЯ ПРОФІЛЮ

Профіль

Перелік документів

№	Назва	Автор	Рівень доступа	Дата підписання	Дата створення
4	Хеш 1	Admin	1	2022-07-30 13:42:56	2022-07-30 12:48:04
3	Тест 2	Admin	1	2022-08-16 13:24:55	2022-07-18 13:25:58
2	Test	Admin	1	2022-07-18 03:03:35	2022-07-18 00:05:35

Рисунок 3.2 Сторінка переліку зареєстрованих документів в акаунті адміністратора

Документи

Додати

Перелік

✓

Повірка документа

Користувачи

НАЛАШТУВАННЯ ПРОФІЛЮ

Профіль

Створення документа

Створення документа

Назва

Назва

Рівень доступу

1

Дата підписання

Файл

Виберіть файл

Browse

Підтвердити

Рисунок 3.3Сторінка реєстрації документа в аккаунті адміністратора або користувача

Documents

Документи

Користувачи

Додати

Перелік

НАЛАШТУВАННЯ ПРОФІЛЮ

Профіль

Admin

Перелік користувачів

ID	ПІБ	Email	Дата створення	
9	Адміністратор 4	admin4@admin.com	30.07.2022 14:50	
8	Адміністратор 3	admin3@admin.com	27.07.2022 12:29	
7	test admin	test11@admin.com	19.07.2022 06:57	
6	Пользователь 3	user3@admin.com	16.07.2022 16:18	
5	Администратор 1	admin1@admin.com	16.07.2022 16:16	

Рисунок 3.4Сторінка редагування користувачів в аккаунті адміністратора

Створення користувача

Створення користувача

ПІБ

ПІБ

Пошта

Пошта

Рівень доступу

1

Роль

Адміністратор

Пароль

Пароль

Рисунок 3.5 Сторінка додавання користувачів в аккаунті адміністратора

Було проведено перевірку контролю доступу для різних груп користувачів. Раніше було вказано до чого має доступ користувач, що авторизований як адміністратор з рівнем допуску 1 (Див. рис. 3.2, 3.4). Він має доступ до розділу адміністрування користувачів та до записів про реєстрацію документів з рівнями доступу 1, 2, 3, 4. Після авторизації в системі як користувач з рівнем допуску 2 користувач не має доступу до розділу адміністрування користувачів та не бачить записи с рівнем доступу 1 (Див. рис. 3.6)

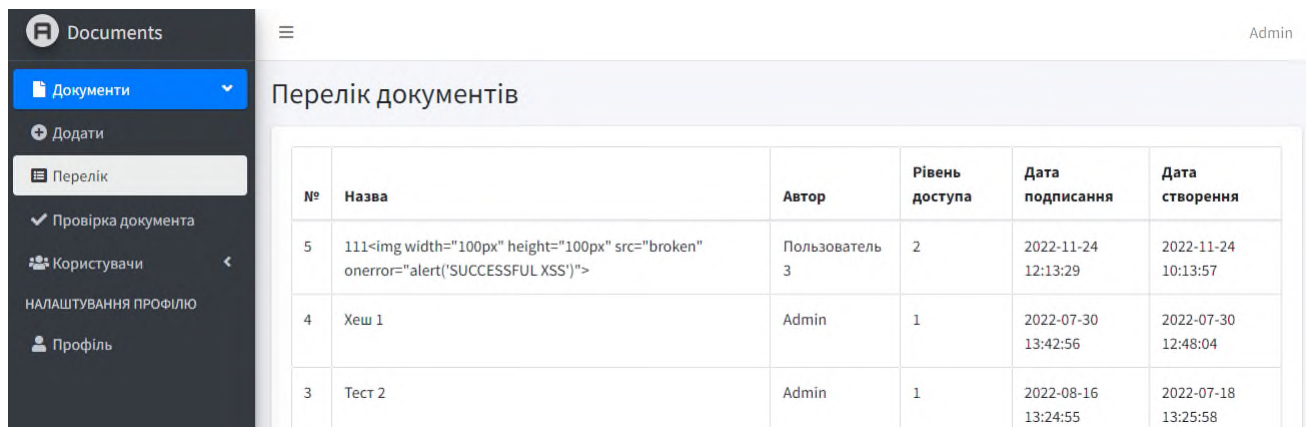
Documents Пользователь 3

Перелік документів

№	Назва	Автор	Рівень доступу	Дата підписання	Дата створення
5	111	Пользователь 3	2	2022-11-24 12:13:29	2022-11-24 10:13:57

Рисунок 3.6 Сторінка переліку зареєстрованих документів в аккаунті користувача з рівнем доступу 2

Було протестовано додаток на вразливість XSS, в поле назви документа було внесено наступний код: `<imgwidth="100px" height="100px" src="broken"onerror="alert('SUCCESSFUL XSS')">`. Після реєстрації документа назва вказаного документа видається як простий текст, а не виконується як код (Див. рис. 3.7).



№	Назва	Автор	Рівень доступу	Дата підписання	Дата створення
5	111	Пользователь 3	2	2022-11-24 12:13:29	2022-11-24 10:13:57
4	Хеш 1	Admin	1	2022-07-30 13:42:56	2022-07-30 12:48:04
3	Тест 2	Admin	1	2022-08-16 13:24:55	2022-07-18 13:25:58

Рисунок 3.7Видача небезпечного коду як простий текст,
а не як виконуваний код

Було протестовано процес створення паролля перевірка його довжини (Див. рис. 3.8)

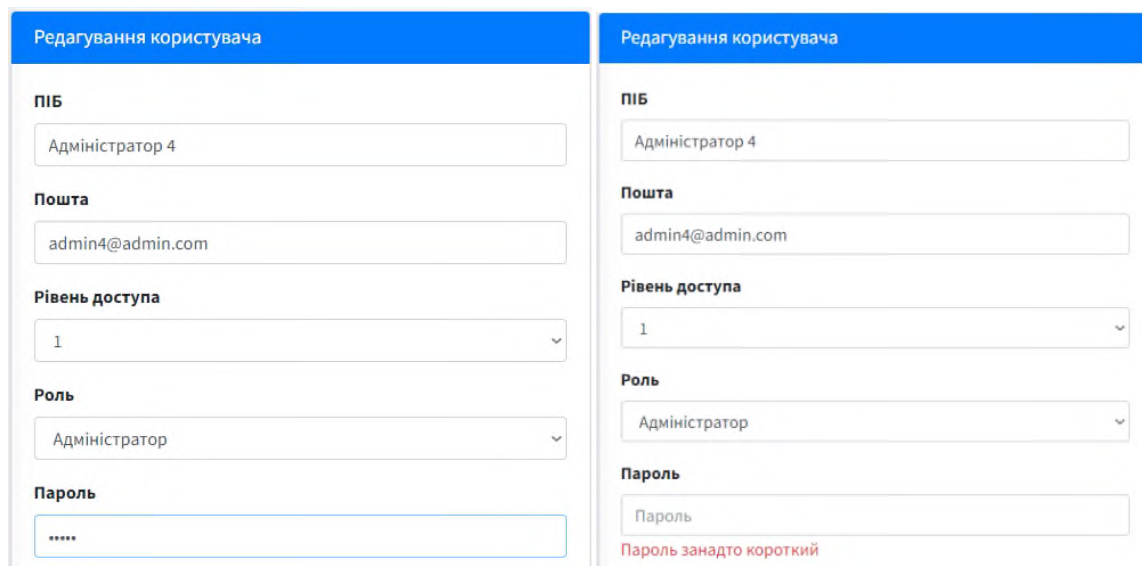


Рисунок 3.8Перевірка довжини введеного пароллю

Пароль повинен містити мінімум вісім символів. Тому у відповідь на пропозицію пароля з 5 символів система його не прийняла та видала повідомлення: «Пароль занадто короткий».

Було проведено імітацію bruteforce атаки на модуль авторизації за допомогою інструмента BurpSuite. Після п'яти невдалих спроб процес авторизації блокується на визначений тайм-аут (11 секунд), про що видається відповідне повідомлення (Див. рис. 3.9)

Рисунок 3.9 Видача повідомлення про тайм-аут

Проведено тестування логіки авторизації. В поле логіну було введено код:

hac@hac.com' or 1=1;-- (2)

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

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: «These credentials do not match our records» (Див. рис. 3.10)

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

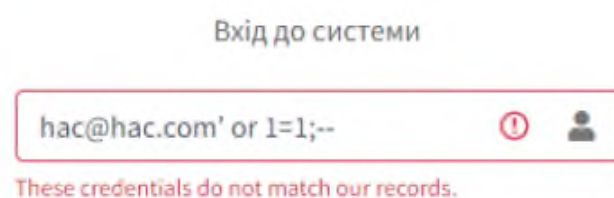


Рисунок 3.10 Результат спроби злому логіки у формі авторизації

Було зареєстровано документ з назвою Хеш 1 за № 4. Потім проводилася перевірка цього документа на справжність в системі. Було вказано № документа (4) та завантажено сам документ, що перевіряється (Див. рис. 3.11)

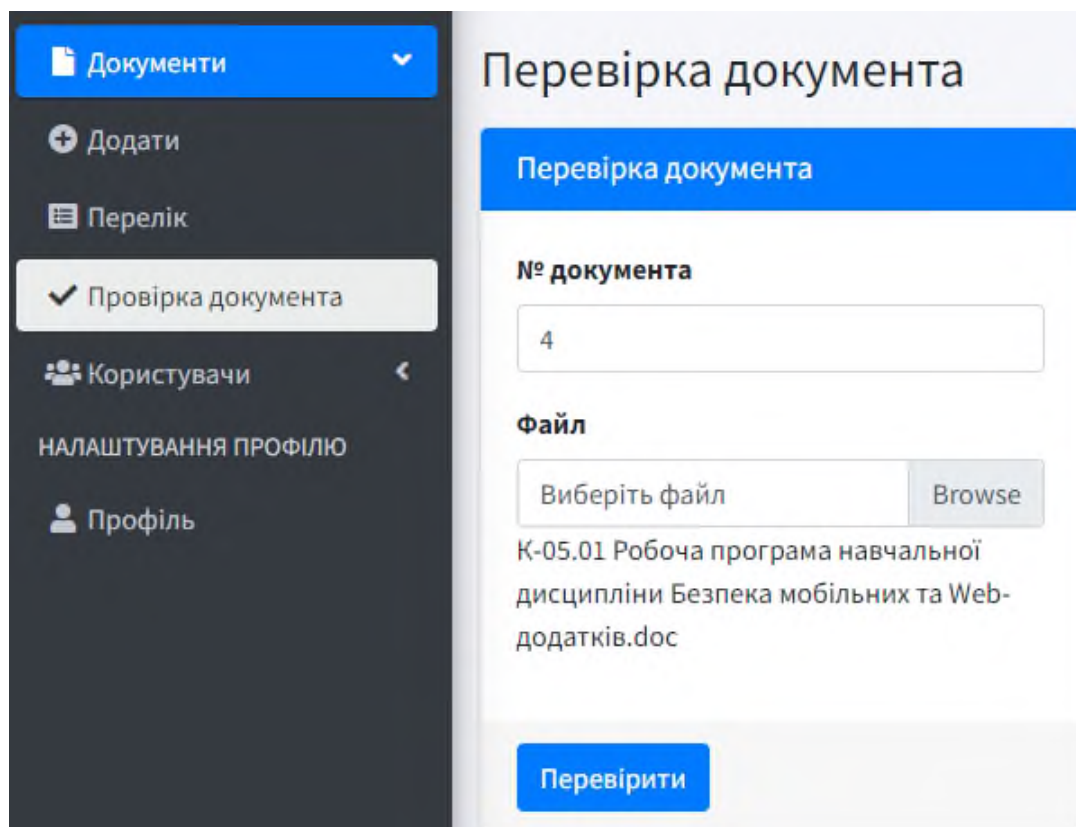


Рисунок 3.11 Завантаження на перевірку документа, що перевіряється

В результаті перевірки система видає повідомлення про справжність перевіряемого документа, що саме його було зареєстровано в системі за № 4 (Див. рис. 3.12).

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		54

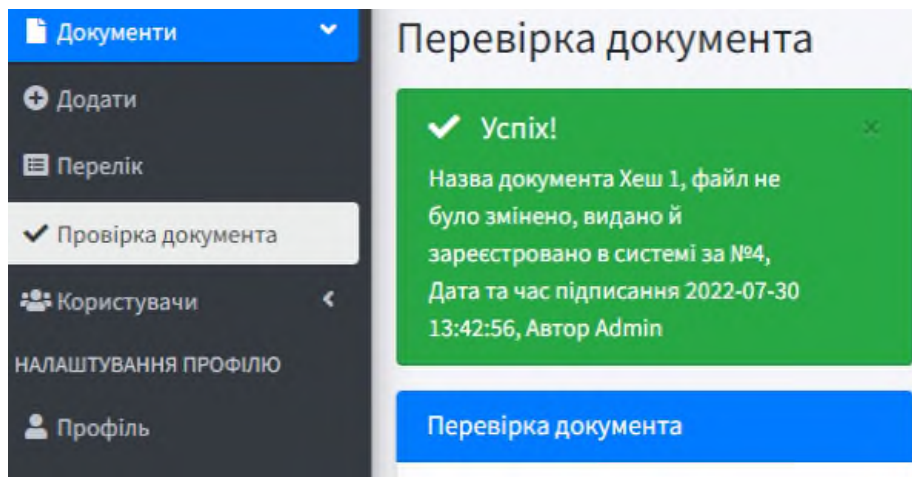


Рисунок 3.12 Позитивний результат перевірки документа

Потім у файл документа, що перевіряється, було внесено невеличкі зміни та процес перевірки було здійснено повторно, вже з новим (зміненим) файлом. Як й очікувалося система підтвердила, що цей, змінений, документ не відповідає первинно зареєстрованому документу (Див. рис. 3.13).

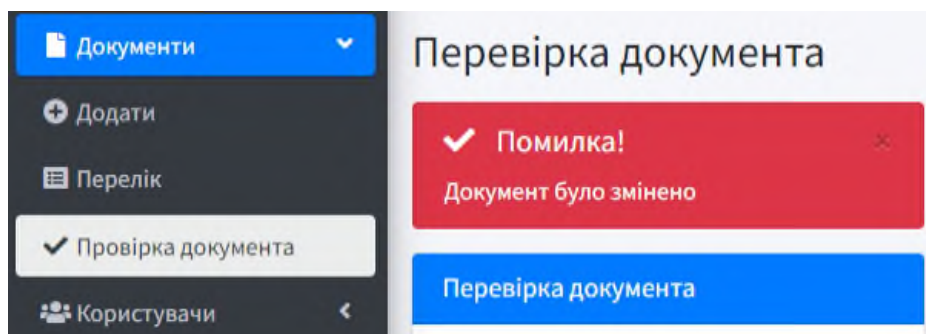


Рисунок 3.13 Негативний результат перевірки документа

Цей результат очікуваний, тому що навіть у наслідок незначних змін у файлі його хеш сума значно змінюється і вихідний перевірочний код таким чином змінюється.

Блокчейн логіка запобігає спробам зловмисників, якщо вони зможуть отримати доступ до бази даних системи, змінити перевірочний код даного документа, тому що цей код використовується в підрахунку перевірочного коду наступних зареєстрованих документів, що призведе до його невідповідності та буде виявлено під час перевірки наступного документа. Змінити перевірочні коди

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		55

всіх зареєстрованих пізніше документів, щоб приховати зміну зареєстрованого документа, не виявляється можливим, тому що самі документи не зберігаються в системі й вирахувати їх хеш суми неможливо.

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

Висновки до третього розділу

Під час виконання третього розділу було:

1. Розроблено план тестування розробленого додатку на:

- вразливості контролю доступу,
- логіки авторизації,
- XSS,
- SQL ін'єкції,
- використання слабо захищених паролів,
- захищеність від brute-force атак,
- розкриття інформації,
- а також блокчейн системи перевірки зареєстрованих документів на дійсність.

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

3. Блокчейн логіка запобігає спробам зловмисників, якщо вони зможуть отримати доступ до бази даних системи, змінити перевірочний код даного документа, тому що цей код використовується в підрахунку перевірочного коду наступних зареєстрованих документів, що призведе до його невідповідності та буде виявлено під час перевірки наступного документа. Змінити перевірочні коди всіх зареєстрованих пізніше документів, щоб приховати зміну зареєстрованого документа, не виявляється можливим тому що самі документи не зберігаються в системі й вирахувати їх хеш суми неможливо.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В результаті проведеного дослідження були отримані наступні висновки:

1. Інтерес до блокчейн технологій продовжує зростати з реформуванням та розвитком всіх сфер української держави, а саме медичної реформи, судової та правоохоронної реформи, розвитком електронної держави та так званої «діджиталізації» держави та в умовах триваючої кібервійни з державою агресором.
2. Використання блокчейн технологій може вирішити багато проблем пов'язаних з бюрократією, корупцією, крадіжками та шахрайствами у таких процесах як видача дозволів та реєстрацій.
3. Незважаючи на бурний розвиток блокчейн все ще залишається експериментальною технологією – вона постійно знаходиться у розвитку, з'являються все нові способи її використання.
4. Серед основних трендів в сфері використання блокчейн технологій є: його використання для відстеження вакцин, корпоративний блокчейн, застосування NFT та розвиток блокчейну як послуги.
5. В сфері державного управління прогнозується використання технологій блокчейну для організації виборів, гуманітарних та соціальних послуг, захисту цифрових активів, підвищенні ефективності договірних відносин та у діловодстві.
6. Україна наряду з Естонією та Грузією є одними з провідних країн щодо впровадження технологій блокчейну.
7. На ринку існують багато пропозицій он-лайн систем управління документами в корпоративному верхньому ціновому сегменті навіть з використанням технологій блокчейну. В нижньому ціновому сегменті пропозиції захисту документів можливі або за додаткову ціну, або з використанням сторонніх інструментів, підключених або розроблених самостійно.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

8. На підставі проведеного аналізу було сформульовано такі вимоги до розробки:

- Кожен авторизований користувач системи повинен мати доступ до документів.
- Несанкціонований доступ до документів має бути неможливим.
- Змінювати, підробляти чи видаляти документи з реєстру не повинно бути можливо.
- Кожен документ повинен мати автора та бути підписаний.

9. Виходячи з вимог, що пред'являються до системи, було визнано доцільним використовувати наступний тип блокчейну: приватний закритого доступу, так як блокчейн цього виду має умову, що прості користувачі не можуть стати учасниками мережі без підтвердження валідаторів, а також не завжди мають доступ до читання файлів ланцюга.

10. Як алгоритм досягнення консенсусу була обрана гібридна система доказу часток і доказу роботою – «Proof of Activity», оскільки вона включає всі переваги цих двох алгоритмів.

11. Розроблено технічні вимоги до проекту, що розробляється.

12. Розроблено та проаналізовано модель загроз для додатку, що розробляється.

13. Розроблено та проаналізовано моделі порушників для додатку, що розробляється.

14. Виходячи з цього вибрано сервіси розробки та захисту додатку, що розробляється, а саме: фреймворк Laravel, реляційна база даних MySQL, децентралізоване сховище даних blockchain.

15. Розроблена діаграма прецедентів та ролі, що використовуються в додатку.

16. Виходячи з цього розроблена діаграма баз даних.

17. Розроблено додаток, що реалізує визначені механізми захисту:

- Використання технології Blockchain для неможливості непомітної зміни реєстраційних даних зареєстрованих документів.
- Збереження хеш-суми зареєстрованих документів та верифікація зареєстрованих документів.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

- Захист від bruteforceатак за рахунок обмеження кількості спроб аутентифікації та влаштування тайм-ауту у зв'язку з перевищенням кількості спроб, а також перевірки вибору достатньо безпечного паролю.
- Захист від викрадення паролів за рахунок зберігання в хешованому вигляді.
- Налаштування розмежування доступу для збереження конфіденційної та комерційної таємниці в установі.
- Захист від впровадженню SQL ін'єкцій за рахунок використання методів управління записами БД Eloquen.
- Захист від XSSта деяких інших атакза рахунок валідації вхідних даних та фільтрації виводу вихідних даних, що було отримано з ненадійних джерел.
- Захист від CSRF атак за рахунок використання токенів CSRF.
- Захист сесій за рахунок використання персональних токенів.

18.Розроблено план тестування розробленого додатку на:

- вразливості контролю доступу,
- логіки авторизації,
- XSS,
- SQL ін'єкції,
- використання слабо захищених паролів,
- захищеність від Brute-force атак,
- розкриття інформації,
- а також блокчейн системи перевірки зареєстрованих документів на дійсність.

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

20.Блокчейн логіка запобігає спробам зловмисників, якщо вони зможуть отримати доступ до бази даних системи, змінити перевірочний код даного

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						59
Змн.	Арк.	№ докум.	Підпис	Дата		

документа, тому що цей код використовується в підрахунку перевірного коду наступних зареєстрованих документів, що призведе до його невідповідності та буде виявлено під час перевірки наступного документа. Змінити перевірочні коди всіх зареєстрованих пізніше документів, щоб приховати зміну зареєстрованого документа, не виявляється можливим тому що самі документи не зберігаються в системі й вирахувати їх хеш суми неможливо.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		60

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Законодавство України: Верховна рада України. – URL: <https://zakon.rada.gov.ua/laws/>
2. Посібник з web-безпеки. – URL: <http://websecurity.com.ua/security/>
3. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. – URL: <https://zakon.rada.gov.ua/laws/show/2155-19>
4. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. – URL: <https://zakon.rada.gov.ua/laws/show/851-15>
5. CleverForms – платформа для управління бізнесом. – URL: <https://clever-forms.com/>
6. iDoc – комплекс управління організацією. – URL: <https://www.icore.com.ua/>
7. An Overview of the Best Laravel Security Practices – 2021. – URL: <https://www.cloudways.com/blog/laravel-security/#laravel-authentication>.
8. Andre A. Professional Pen Testing for Web Applications, Indianapolis: Wiley Publishing Inc., 2006, 502 p.
9. Bell L. Agile Application Security, 2018, 448 p.
10. Bellare M. Introduction to Modern Cryptography URL: <https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf>
11. Bernard M. The 5 Biggest Blockchain Trends In 2022 // Forbes URL: <https://www.forbes.com/sites/bernardmarr/2021/11/19/the-5-biggest-blockchain-trends-in-2022/>
12. BlockSigh: How it all works URL: <https://blocksign.com>
13. Blokdyk G. OWASP: Third Edition, Brendale: The Art of Service, 2018, 124 p.
14. Burp Suite – URL: <https://portswigger.net/burp>
15. Corda. – URL: <https://corda.net/>

		Пірог О.В.			<i>КІК.КР.Б – 125 – 12 – ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		61

- 16.CRLF URL: <https://cryptoworld.su/chto-takoe-crlf-inekciya-primery-ispolzovaniya-uroki-xakinga-glava-4/>
- 17.Dropbox. – URL: <https://www.dropbox.com/>
- 18.Dwork C. Pricing via Processing or Combatting Junk Mail // The Weizmann Institute of Science URL: <https://wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf>
- 19.FileCloud. – URL: <https://filecloud.com/>
- 20.FINRA_Blockchain_Report: Distributed Ledger Technology: Implications of Blockchain for the Securities Industry URL: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf
- 21.Google Drive. – URL: <https://www.google.com/intl/ua/drive/>
- 22.Hoffman A. Web Application Security Exploitation and Countermeasures for Modern Web Application 2021, 328 p.
- 23.ISO 27034 Information technology - Security techniques – Application security.
- 24.Jakobsson M. Proofs of Work and Bread Pudding Protocols // Hashcash. URL: <https://hashcash.org/papers/bread-pudding.pdf>.
- 25.Kosseff J. Cybersecurity Law / J.Kosseff.– 2020.– 768 p.
- 26.Laravel Documentation – 2022. URL: <https://laravel.com>
- 27.Leaders must determine the suitability of blockchain and set the right expectations // Gartner URL: <https://www.gartner.com/en/articles/how-governments-can-successfully-embark-on-any-blockchain-project>
- 28.McDonald M. Web Security for Developers: Real Threats, Practical Defense / M. McDonald., 2020. – 216 p.
- 29.Megapolis.DocNet. – URL: <https://megapolis.inbase.com.ua/>
- 30.MODX. – URL: <https://modx.com/>
- 31.Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System URL: <https://bitcoin.org/bitcoin.pdf>.
- 32.NIST 800-144 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		62

33. NIST 800-218 Secure Software Development Framework (SSDF).
34. NIST 800-95 Guide to Secure Web Services.
35. OneDrive. – URL: <https://www.microsoft.com/uk-ua/microsoft-365/onedrive/online-cloud-storage>
36. REST API URL: <https://webdevblog.ru/kak-obespechit-bezopasnost-rest-api/>
37. Sinha S. Bug Bounty Hunting for Web Security, 2019, 228 p.
38. SmartVault. – URL: <https://smartvault.com/>
39. Software Advice URL: <https://www.softwareadvice.com/>
40. Staffer M. Laravel Up & Running: A Framework for Building Modern PHP Apps / M. Staffer. – 512 p.
41. Stewart R. Laravel: The Ultimate Beginner's Guide to Learn Laravel Step by Step/ R. Stewart., 2020.
42. The Open Web Application Security Project® (OWASP). – URL: <https://owasp.org/>
43. The Web Security Academy. – URL: <https://portswigger.net/web-security>
44. Tresorit. – URL: <https://tresorit.com/>
45. Waves Enterprise. – URL: <https://wavesenterprise.com/>
46. Web Backend Security Risks to Consider in Development – 2020. – URL: <https://geekflare.com/web-backend-security-risk/>
47. Why Laravel is the Recommended Framework for Secure, Mission-Critical Applications– 2018. URL: <https://auth0.com/blog/why-laravel-is-the-recommended-framework-for-secure-mission-critical-applications/>
48. XSS URL: <https://school38vrn.ru/uk/zashchita-ot-xss-atak-easy-hack-kak-dobyt-dannye-cherez-cross-site-scripting-inclusion.html>
49. Zeldovich N. Computer Systems Security. – URL: <https://css.csail.mit.edu/6.858/2020/>

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		63

Електронний архів розробленого додатку системи електронного документообігу
та його бази даних, флеш носій додається.

		Пірог О.В.			КІК.КР.Б – 125 – 12 – ПЗ	Арк.
						64
Змн.	Арк.	№ докум.	Підпис	Дата		