

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

КУРДУПОВ ОЛЕКСІЙ ЛЕОНІДОВИЧ

Допускається до захисту:
в. о. завідувача кафедри
інформаційних технологій,
канд. техн. наук, доцент
_____ О. В. ЗЕЛІНСЬКА
«_____» _____ 2024 р.

**МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ МЕДИЧНОГО
ЗАКЛАДУ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН**

Спеціальність 122 «Комп'ютерні науки»

Кваліфікаційна (магістерська) робота

Науковий керівник:
Антонов Ю.С., кан. фіз.-мат. наук,
доцент, доцент кафедри
інформаційних технологій

Оцінка: _____ / _____ / _____
(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця 2024

АНОТАЦІЯ

Курдупов О.Л. Моделювання інформаційної системи медичного закладу на основі технології блокчейн. Спеціальність 122 «Комп'ютерні науки», Освітня програма «Комп'ютерні технології обробки даних», Донецький національний університет імені Василя Стуса, Вінниця, 2024.

У роботі проведено дослідження методів та інструментів розробки інформаційної системи для медичних закладів на основі технології блокчейн. Розглянуто алгоритмічні моделі для забезпечення захисту даних пацієнтів. Результатом роботи є створення інформаційної системи з надійним механізмом контролю за змінами медичних записів, незмінність збережених даних, їх захищеність. Висновком є підтвердження необхідності використання технології блокчейну в медичній галузі для забезпечення безпеки та прозорості обробки даних, що значно підвищить ефективність системи. Подальші етапи розвитку включають розширення функціоналу та пошук інноваційних підходів для покращення масштабованості при зростанні обсягу даних.

Ключові слова: інформаційна система, блокчейн-технології, база даних, децентралізація, захист даних, масштабованість, смарт-контракти.

Р. 77 с., 19 рис., 1 табл., 40 джерел, 4 додатки.

ANNOTATION

Kurdupov O.L. Modeling the Information System of a Medical Institution Based on Blockchain Technology. Specialty 122 "Computer Science," Educational Program "Computer technologies of data processing," Vasyl' Stus Donetsk National University, Vinnytsia, 2024.

This work explores the methods and tools for developing an information system for medical institutions using blockchain technology. Algorithmic models were examined to ensure the protection of patient data. The result of the work is the creation of an information system with a reliable mechanism for controlling changes in medical

records, ensuring the immutability and security of stored data. The findings confirm the need for blockchain technology in the medical sector to guarantee data security and transparency, which significantly increases system efficiency. Future development stages include expanding functionality and exploring innovative approaches to improve scalability as data volumes grow.

Keywords: information system, blockchain technologies, database, decentralization, data protection, scalability, smart contracts.

P. 77, Fig. 19,1 tabl., Sources 40, Annex 4.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1 ОГЛЯД ІСНУЮЧИХ СИСТЕМ ТА АНАЛІЗ ЗАГАЛЬНИХ ТЕНДЕНЦІЙ	11
1.1 Огляд існуючих інформаційних систем у медицині	11
1.1.1 Опис основних функціональних можливостей.....	11
1.1.2 Переваги та недоліки.....	17
1.2 Аналіз тенденцій використання блокчейн технологій у медичних інформаційних системах	20
1.2.1 Переваги блокчейну для медичних даних	20
1.2.2 Проблеми та обмеження.....	21
1.3 Порівняльний аналіз систем управління базами даних (СУБД)	24
1.3.1 Традиційні СУБД проти блокчейн-орієнтованих СУБД.....	24
1.3.2 Критерії порівняння: безпека, швидкість обробки даних, масштабованість та інше	26
1.4 Аналіз наукових робіт у галузі застосування блокчейн у медицині.....	28
РОЗДІЛ 2 ПОСТАНОВКА ЗАДАЧІ ТА ТЕОРЕТИЧНА ОСНОВА ДЛЯ РОЗРОБКИ МЕДИЧНОЇ СИСТЕМИ.....	31
2.1 Визначення проблеми та аналіз потреб медичного закладу	31
2.1.1 Огляд сучасних проблем управління медичними даними.....	31
2.1.2 Аналіз поточних потреб медичних закладів	32
2.1.3 Проблеми взаємодії між різними медичними установами	33
2.1.4 Потреби в покращенні безпеки та приватності.....	33
2.1.5 Постановка задачі	35
2.2 Архітектура інформаційної системи.....	36
2.2.1 Вибір платформи блокчейн	36
2.2.2 Схема взаємодії компонентів системи.....	39
2.3 Опис технологій та інструментів розробки.....	41
2.3.1 Блокчейн технології.....	41
2.4 Вимоги до системи	43
2.4.1 Функціональні вимоги	43
2.4.2 Нефункціональні вимоги.....	44
2.4.3 Інтеграційні вимоги	46
2.4.4 Заходи забезпечення безпеки та приватності.....	47
РОЗДІЛ 3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ.....	50
3.1. Розробка системи.....	50
3.1.1. Вибір та конфігурація інструментів	50
3.1.2. Створення архітектури бази даних.....	53
3.1.3 Програмування функціоналу.....	57

	5
3.2 Тестування системи	59
3.2.1 Методи та інструменти тестування	59
3.2.2 Оцінка продуктивності та безпеки	62
3.3 Демонстрація роботи системи.....	63
3.3.1 Сценарії використання	63
3.3.2 Інтерфейс користувача та управління даними	64
3.4 Оцінка ефективності та можливості масштабування системи	66
ВИСНОВКИ	69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	71
ДОДАТОК А.....	78
ДОДАТОК Б.....	79
ДОДАТОК В.....	82

ВСТУП

Актуальність теми. Технологія блокчейну, вперше запропонована на початку 90-х років минулого століття у контексті розробки цифрових валют, відтоді пройшла значний шлях розвитку і трансформації. Нині блокчейн застосовується у напрямках, де важливі безпека, відкритість та незмінність інформації.

З огляду на збільшення застосування блокчейну в різних галузях, його інтеграція в медичну сферу виглядає особливо перспективною. Технологія може внести вагомий вклад у забезпечення конфіденційності пацієнтів, ефективності лікувальних процесів та управління медичними даними, що робить дану тему важливою та актуальною для дослідження.

З огляду на глобальні кризи у сфері охорони здоров'я, такі як пандемія COVID-19 і війна, зростаючий інтерес та потреба в інноваційних рішеннях у медичних закладах стають особливо актуальними. Відповідь на цю кризу вимагає інтеграції новітніх технологій, здатних оптимізувати медичні процеси, підвищити ефективність лікування та забезпечити безперебійну взаємодію між медичними закладами. Інновації, такі як блокчейн, можуть грати ключову роль у цьому процесі, надаючи рішення для безпечного та ефективного управління медичними даними.

Блокчейн технологія може внести значний вклад у вдосконалення системи розподілу медичних ресурсів, забезпечення прозорості і слідування нормативним вимогам, що стало нагальною потребою під час пандемії та війни. Вона дозволяє створити надійну платформу для обміну даними між лікарнями, лабораторіями і страховими компаніями, мінімізуючи ризик помилок і зловживань.

Таким чином, зростаючий інтерес до новітніх технологічних рішень у медичних закладах є відповіддю на потребу підвищення ефективності та безпеки медичного сервісу, особливо у кризові періоди, такі як пандемія COVID-19, що змушує світ шукати нові шляхи для оптимізації охорони здоров'я.

Цілі та задачі дослідження. Основна ціль дипломної роботи: розробка моделі та прототипу інформаційної системи для медичного закладу, яка базується на використанні блокчейн технології. Ця система покликана підвищити ефективність управління медичними даними, забезпечити їхню безпеку та доступність, а також оптимізувати різні внутрішні процеси медичного закладу.

Для досягнення поставленої мети передбачається вирішення наступних задач:

1. Аналіз існуючих систем управління медичними даними:
 - Вивчення та оцінка сучасних інформаційних систем в охороні здоров'я.
 - Ідентифікація основних проблем та недоліків цих систем, які можуть бути усунуті за допомогою блокчейн технології.
2. Розробка технічного проекту системи:
 - Визначення вимог до системи, включаючи функціональні та невимушені вимоги.
 - Проектування архітектури інформаційної системи з використанням блокчейн технології.
 - Вибір інструментів та технологій для реалізації системи.
3. Імплементация прототипу системи:
 - Розробка програмного забезпечення для прототипу згідно з проектом.
 - Інтеграція блокчейн модулів для забезпечення безпеки, незмінності та прозорості даних.
4. Тестування та валідація системи:
 - Проведення комплексних тестів для перевірки функціональності, надійності та ефективності системи.
 - Аналіз отриманих результатів та внесення необхідних коректив.
5. Оцінка впливу системи на медичний заклад:
 - Аналіз переваг використання блокчейн технології у контексті зберігання та обміну медичними даними.
 - Визначення можливостей для масштабування системи та її адаптації в інших медичних закладах.

Виконання цих задач дозволить не тільки розробити ефективну інформаційну систему для медичного закладу, але й глибше зрозуміти потенціал та обмеження блокчейн технології в медицині, а також її вплив на якість медичного обслуговування.

Методологія та структура роботи. Дослідження базується на інтеграції різноманітних методів та підходів, які охоплюють як теоретичні так і практичні аспекти розробки інформаційних систем на основі блокчейн технологій. Важливими компонентами дослідження є:

1. Літературний огляд: передбачається провести детальний аналіз академічних робіт, наукових статей та інших літературних джерел, що описують вже існуючі рішення та теоретичні концепції у сфері блокчейн технологій, їхню архітектуру, застосування та вплив на сферу охорони здоров'я.
2. Моделювання системи: застосування структурованих методів моделювання для проектування архітектури блокчейн-базованої інформаційної системи. Моделювання дозволить визначити ключові компоненти системи, їх взаємозв'язки та процеси обробки даних.
3. Використання програмних інструментів: підбір та застосування наявних програмних продуктів та технологій, які підтримують розробку інформаційних систем на базі блокчейну. Важливою частиною буде вибір і налаштування блокчейн фреймворку, який найкраще відповідатиме вимогам проекту.

Структура блокчейн-базованої інформаційної системи для охорони здоров'я. Система буде розроблена з використанням блокчейн технології для забезпечення незмінності та прозорості медичних записів, зокрема:

- Зберігання даних: використання блокчейну як основи для збереження важливих медичних даних, таких як діагнози, результати аналізів, історія хвороби пацієнта. Блокчейн забезпечує, що кожен запис є незмінним і верифікованим.
- Цифровий підпис: кожен блок міститиме цифровий підпис лікаря або

медичної установи, що гарантує автентичність запису. Цифрові підписи допомагають виявити спроби несанкціонованої зміни інформації.

- Контрольна сума: для кожного нового запису генерується контрольна сума, яка базується на стані попереднього блоку, тим самим забезпечуючи цілісність ланцюга блоків.
- Взаємозв'язок даних: інформація про звернення пацієнтів прив'язується не тільки до їхнього особистого медичного профілю, але й до попередніх записів в системі, забезпечуючи глибший контекст і точність діагностування.

Цей підхід не тільки підвищує довіру та безпеку медичних записів, але й значно ускладнює будь-які спроби фальсифікації або несанкціонованої зміни даних.

Дипломна робота структурована таким чином, щоб кожен розділ послідовно доповнював один одного, формуючи цілісне дослідження інформаційних систем у медицині з акцентом на використання блокчейн технологій. Результати дослідження сприяють підвищенню захисту даних та збільшенню відмовостійкості системи, тому можуть бути застосовані під час проектування сховищ даних.

Розділ 1: "Огляд існуючих систем та аналіз загальних тенденцій" зосереджується на вивченні існуючих медичних інформаційних систем. Описуються основні функціональні можливості цих систем, а також їх переваги та недоліки. Далі йде аналіз тенденцій використання блокчейн технологій у медичних системах, оцінюються переваги такого підходу для забезпечення безпеки медичних даних, а також виклики та обмеження, які виникають. Завершується розділ порівняльним аналізом традиційних і блокчейн-орієнтованих систем управління базами даних, в якому обговорюються критерії безпеки, швидкості обробки даних і масштабованості.

Розділ 2: "Постановка задачі та теоретична основа" описує проблематику, з якою стикається медичний заклад, та аналізує потреби цього закладу. Розглядається архітектура майбутньої інформаційної системи, включаючи вибір

блокчейн платформи та схему взаємодії компонентів системи. Також подається опис використовуваних технологій і інструментів розробки, включаючи конкретні блокчейн технології та мови програмування. Вимоги до системи розділені на функціональні та нефункціональні, включаючи заходи забезпечення безпеки та приватності даних.

Розділ 3: "Реалізація задачі" описує процес розробки системи: вибір та конфігурацію інструментів, створення архітектури бази даних, програмування функціоналу. Далі йдуть методи та інструменти тестування, оцінка продуктивності та безпеки системи. Описується демонстрація роботи системи через сценарії використання, інтерфейс користувача та управління даними. Завершується розділ оцінкою ефективності системи та можливостями її масштабування.

Висновки підсумовують основні результати дослідження, визначають внесок у розробку медичних інформаційних систем з використанням блокчейн технологій, і оцінюють перспективи подальшого розвитку в цій галузі.

Така структура допомагає читачу послідовно пройти шлях від огляду існуючих рішень до власне розробки і аналізу нової системи, забезпечуючи глибоке розуміння теми і її актуальності у сучасному медичному контексті.

РОЗДІЛ 1

ОГЛЯД ІСНУЮЧИХ СИСТЕМ ТА АНАЛІЗ ЗАГАЛЬНИХ ТЕНДЕНЦІЙ

1.1 Огляд існуючих інформаційних систем у медицині

1.1.1 Опис основних функціональних можливостей

Медична інформаційна система (MIS) являє собою інтегрований програмний комплекс, призначений для автоматизації основних операцій в медичних установах різного профілю. Такі системи забезпечують ефективне управління електронним документообігом, оптимізацію взаємодії з пацієнтами, моніторинг діяльності адміністративного персоналу та контроль за фінансовими та організаційними аспектами роботи [1]. Приклад оптимізації обміну інформації в електронній системі медичних записів зображено на рисунку 1.1.



Рис. 1.1 – Електронна система медичних записів [1]

На міжнародному рівні використовується термін HIS (Hospital Information System) для позначення систем, що включають управління всіма аспектами медичного обслуговування, включаючи юридичні питання. Ці системи можуть доповнюватися спеціалізованими модулями, такими як RIS (Radiology Information System) для радіології та PACS (Picture Archiving and Communication System) для зберігання медичних зображень. Також існують лабораторні

інформаційні системи та аптечні інформаційні системи, які можуть інтегруватися в рамках ширшої медичної інформаційної системи.

Медичні інформаційні системи (МІС) структуровано організовують різноманітні аспекти діяльності медичних установ, включаючи [2]:

- Реєстрацію пацієнтів та ведення електронних медичних карт;
- Обробку даних медичних досліджень;
- Автоматизацію робочих місць лікарів та медсестер;
- Керування розподілом і графіком використання ресурсів установи;
- Управління фінансами і облік;
- Адміністрування і забезпечення засобів зв'язку між співробітниками;
- Моніторинг медичних призначень та лікувальних стандартів.

Давайте розглянемо, які конкретні завдання можна вирішити за допомогою МІС та який вплив це матиме на організацію роботи.

Управління даними та оптимізація процесів. МІС дозволяє ефективно керувати великими масивами даних про пацієнтів та діяльність установи, забезпечуючи їх зберігання та доступність. Система сприяє уніфікації підходів до обробки медичної інформації, стандартизації документації та підвищенню якості медичного обслуговування, а саме: формування звітів, керування електронними картками, обмін оперативною інформацією між поліклініками та лікарнями, віддалене спостереження за пацієнтами, керування електронними картками (рис. 1.2).

Інтеграція даних та звітність. МІС сприяє створенню інтегрованих електронних структур для лікарень та їхніх філій, дозволяючи об'єднати різні медичні установи в єдину систему. Система надає гнучкі інструменти для формування та ведення звітності, що покращує управління ресурсами і контроль за діяльністю.

Доступність інформації. Всі дані в МІС легко доступні для аналізу та обробки, перетворюючи систему в обширний електронний архів. Завдяки налаштуванням доступу, різні користувачі можуть отримувати інформацію відповідно до своїх завдань і потреб, наприклад, через портали для пацієнтів чи

внутрішні медичні портали для спілкування лікарів.

Key Functionalities of Healthcare Information System

This Slide highlights key components of health information system for providing effective hospital services. It covers clinical system, material management and claims and billing record.



This slide is 100% editable. Adapt it to your need and capture your audience's attention.

Рис. 1.2 – Основні функціональні можливості інформаційної системи охорони здоров'я [3]

1.1.1.1 Огляд сучасних медичних інформаційних систем.

Medods – це платформа для управління роботою приватних медичних центрів та стоматологій, а також мережі клінік. Вона пропонується у локальній та хмарній версії (SaaS) і включає всі необхідні модулі для ефективного управління медичними установами [4]. Серед основних можливостей програми:

- Онлайн запис пацієнтів на прийом та управління їхніми електронними медичними картами;
- Автоматизація створення договорів та інших документів;
- Виставлення рахунків та відстеження платежів;
- Ведення обліку запасів;
- Планування маркетингових кампаній, включаючи email- та SMS-розсилки;

- Аналіз загальної статистики роботи установи.

Medods інтегрує в себе елементи CRM-системи з підтримкою управління розкладом і записом пацієнтів, а також інструменти для бізнес-аналітики.

MedElement – це медична інформаційна система, розроблена в Казахстані, що поєднує хмарні сервіси та розширену довідкову систему, призначену для лікарів, студентів медичних спеціальностей, а також усіх, хто піклується про здоров'я (рис. 1.3).



Рис. 1.3 – Головна сторінка сайту інформаційної системи MedElement [5]

MedElement застосовується для автоматизації роботи клінік, ВРТ-клінік, стоматологічних кабінетів, аптек, харчових відділів та приватних медичних практик.

Основні функціональні можливості MedElement включають:

- Довідкова система: MedElement включає обширні довідники захворювань, медичних термінів, лабораторних показників, лікарських засобів, а також огляди світової медичної періодики та інші інформаційні ресурси.
- Автоматизація медичної документації: Система підтримує електронне ведення медичних записів, формування звітів, облік медичних послуг і фінансів.
- Маркетингова інформація: Сбір та аналіз маркетингових даних для планування та проведення маркетингових кампаній.
- Хмарні сервіси: Переваги хмарної інфраструктури забезпечують зручність

і доступність інформації з будь-якого пристрою в будь-який час, що сприяє підвищенню ефективності роботи медичного персоналу[5].

MedElement є прикладом інтеграції сучасних технологій у сферу охорони здоров'я, забезпечуючи високий рівень інформаційної підтримки та автоматизації рутинних процесів медичних установ.

Doctor Eleks – це комплексне рішення, розроблене компанією Eleks у Львові, Україна, яке призначене для оптимізації роботи медичних клінік будь-якого розміру та профілю, включаючи приватні та державні установи [6].

Основні функціональні можливості Doctor Eleks включають:

- Електронна медична карта пацієнта: Забезпечує зберігання та доступ до медичних записів пацієнтів.
- Інструменти для редагування документів: Можливість використання шаблонів для створення та редагування медичних документів.
- Персоналізований робочий кабінет для лікарів: Включає інструменти для планування та управління їхньою діяльністю.
- Модуль реєстратури: Управління записами на прийом, планування роботи та звітність.
- Підсистема графіків роботи: Дозволяє формувати графіки з урахуванням вимог лікарів та пацієнтів.
- Гнучка система звітів: Технології для створення адаптивних звітів, аудит медичних документів.
- Підтримка модуля PACS та Web-клієнта: Для поліпшення доступності та взаємодії з системою.

Ці можливості роблять Doctor Eleks важливим інструментом для забезпечення ефективності та продуктивності роботи медичних клінік, забезпечуючи високий рівень управління медичними інформаційними ресурсами.

EMCiMED – це передова українська медична інформаційна система, призначена для медичних установ, приватних клінік та лабораторій (рис. 1.4). Система інтегрована з українською системою eHealth та побудована на модульному принципі, що дозволяє налаштовувати її конфігурацію залежно від

специфічних потреб кожного медичного закладу [7].

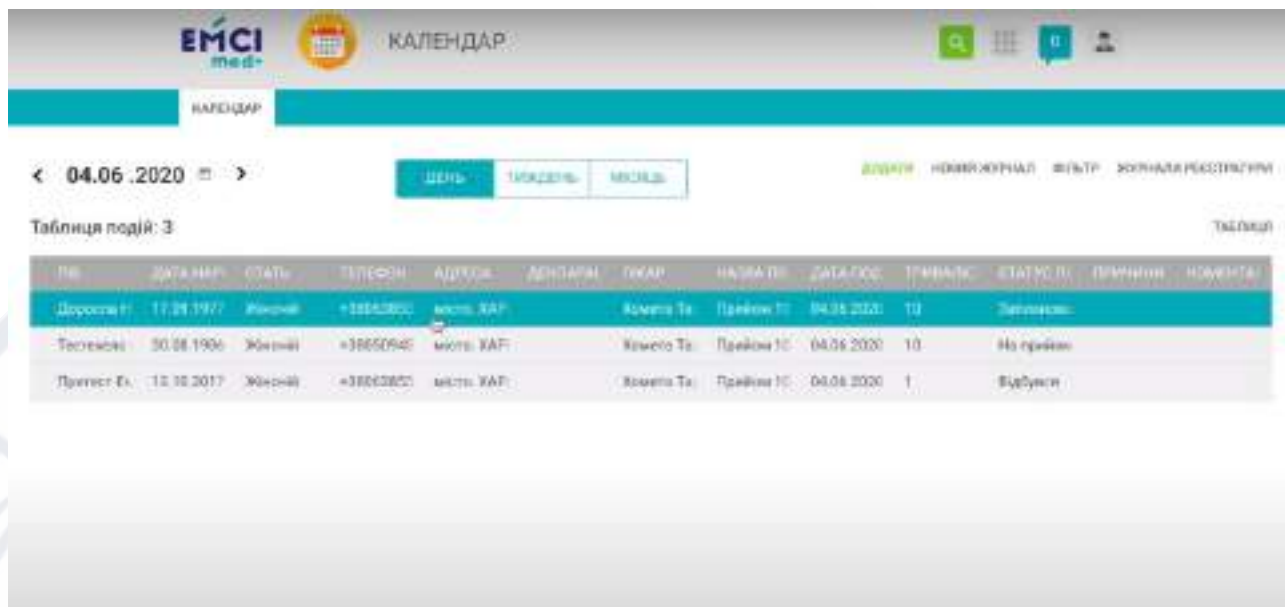


Рис. 1.4 – Медична інформаційна система EMCiMED [8]

Основні функціональні можливості EMCiMED включають:

- Модуль реєстратури: Управління записами пацієнтів та їхніми візитами.
- Управління персоналом: Інструменти для адміністрування та моніторингу роботи співробітників.
- Управління організацією: Засоби для керування всіма аспектами діяльності установи.
- Модуль поліклініки: Оптимізація процесів амбулаторного лікування.
- Стаціонар: Модуль для управління стаціонарними пацієнтами.

Додаткові модулі, які можна придбати:

- Облік медичних послуг: Модуль для управління наданням послуг та їхнього обліку.
- Управління запасами: Інструменти для контролю над запасами та ресурсами.
- Архів медичних зображень PACS: Система для зберігання та управління медичними зображеннями.

Залежно від потреб, систему можна налаштувати з використанням пакетів EMCiMED-Поліклініка та EMCiMED-Стаціонар, що включають специфічні модулі для оптимізації відповідних відділів медичних установ.

В Україні використання медичних інформаційних систем (МІС) є важливою складовою сучасної електронної системи охорони здоров'я eHealth. МІС дозволяють автоматизувати роботу медичних установ з Центральною базою даних (ЦБД) [9]. Згідно з Постановою Кабінету Міністрів України від 25 квітня 2018 року №411, взаємодія з ЦБД можлива тільки через МІС. Перелік МІС, які підключені до ЦБД eHealth, та опис їхніх функціональних модулів можна знайти на відповідному веб-сайті. Законодавство України дозволяє використовувати лише ті системи, які пройшли перевірку Міністерства охорони здоров'я та були підключені до системи eHealth.

1.1.2 Переваги та недоліки

1.1.2.1 Переваги використання медичних інформаційних систем.

Якщо медична інформаційна система (МІС) була правильно обрана та впроваджена, вона позитивно впливає на роботу організації. Проте, результати залежать від типу МІС, її функціональних можливостей та особливостей конкретного медичного закладу. Розглянемо основні переваги використання МІС для різних учасників процесу.

Користь для медичних установ:

- Зменшення паперової роботи: МІС усуває необхідність заповнення паперових форм. Всі записи єдині та централізовані, дозволяючи медичному персоналу ознайомлюватися з історією хвороб, результатами досліджень, та ходом лікування пацієнтів.
- Підвищення якості обслуговування та зниження людського фактору: Автоматизований документообіг допомагає зменшити кількість паперової роботи, утримувати актуальну інформацію про дослідження та надані послуги, що сприяє точнішій діагностиці та знижує ризик втрати важливих даних.
- Телемедицина: Лікарі мають можливість консультиватися в реальному часі з колегами та іншими фахівцями, обговорюючи постановку діагнозів та коригування лікування, а також вести дистанційний моніторинг стану пацієнтів.

- Координація роботи: Клінікам зручно використовувати онлайн-реєстратуру, вести єдині бази даних пацієнтів, розподіляти навантаження між філіями з урахуванням зайнятості та графіків спеціалістів, а також оцінювати попит на певні медичні послуги.

Користь для пацієнтів:

- Доступ до власних медичних даних: Завдяки МІС пацієнти мають можливість швидко отримувати результати лабораторних аналізів, слідкувати за ними разом з лікарем, записуватися на прийом та підтримувати зворотній зв'язок.
- Зниження ризиків підробки та втрати медичних даних: Оскільки пацієнти можуть самостійно моніторити свої дані, це зменшує можливість їхньої втрати чи фальсифікації.
- Система онлайн-реєстрації: Дозволяє уникнути черг у лікарнях, спрощуючи процес запису на прийом.

Використання медичних інформаційних систем (МІС) приносить значні переваги як для медичних установ, так і для пацієнтів. МІС значно покращують якість медичного обслуговування, оптимізують процеси в медичних установах і підвищують задоволеність пацієнтів, сприяючи більшій ефективності та безпеці медичних процедур.

1.1.2.2 Недоліки використання медичних інформаційних систем.

Хоча медичні інформаційні системи (МІС) пропонують багато переваг, вони також можуть мати деякі недоліки та виклики для медичних установ. Ось декілька з них:

1. Висока вартість впровадження та обслуговування: Встановлення МІС може бути дорогим, особливо для малих або початкових медичних установ. Вартість включає не тільки покупку програмного забезпечення, але й апаратну складову, обслуговування та оновлення системи.
2. Складність впровадження: Процес інтеграції МІС може бути складним та часом затратним, вимагаючи значних ресурсів і тривалого часу для впровадження, особливо в установах з великою кількістю співробітників

чи складною інфраструктурою.

3. Тренінг персоналу: Для ефективного використання МІС необхідно навчання медичного та адміністративного персоналу. Це може бути складно для деяких співробітників, особливо для тих, хто менш знайомий з цифровими технологіями.
4. Проблеми зі згодою на конфіденційність та безпеку даних: Управління конфіденційністю і безпекою пацієнтських даних є ключовим викликом. Помилки в системі безпеки або неавторизований доступ можуть призвести до витоку особистих даних.
5. Залежність від технологій: Сильна залежність від МІС може створити ризики, пов'язані з відмовою обладнання чи програмних помилок, що може призвести до призупинення роботи медичної установи.
6. Стандартизація та інтеграція: Взаємодія МІС з іншими системами (наприклад, між різними медичними установами) може бути ускладнена через відсутність стандартизації. Це може обмежити обмін даними та інтеграцію систем.
7. Спротив змінам: Частина медичного персоналу може сприймати введення МІС як загрозу звичному порядку речей, що може призвести до спротиву впровадженню нових процесів.

Ці недоліки можуть ускладнити процес впровадження та ефективного використання медичних інформаційних систем, вимагаючи ретельного планування, управління та постійної підтримки з боку медичних установ.

Медичні інформаційні системи (МІС) можуть також мати певні недоліки для пацієнтів. Ось декілька з них:

1. Конфіденційність та безпека даних: Одним з найбільших занепокоєнь є ризик витоку персональних медичних даних через хакерські атаки або неналежне управління даними. Порухення конфіденційності може мати серйозні наслідки для приватного життя пацієнтів.
2. Залежність від технологій: Надмірна залежність від систем може створити проблеми, коли є технічні збої. Зокрема, це може призвести до затримок у

доступі до медичної допомоги або помилок у лікуванні.

3. Втрата особистого контакту: Цифровізація процесів може зменшити особистісний вимір медичної допомоги, коли спілкування між лікарем та пацієнтом зводиться до обміну електронними повідомленнями, що може негативно вплинути на якість обслуговування.
4. Складність у використанні: Не всі пацієнти можуть бути технологічно обізнаними, тому інтерфейси деяких МІС можуть бути занадто складними для користувачів похилого віку або тих, хто не володіє комп'ютерною грамотністю.
5. Спротив змінам: Деякі пацієнти можуть сприймати введення МІС як загрозу традиційним методам надання медичних послуг, особливо якщо вони відчують занепокоєння щодо нових технологій.
6. Нерівний доступ до систем: Пацієнти, які живуть у регіонах з обмеженим доступом до інтернету або технологій, можуть мати складнощі з доступом до переваг МІС, що створює додатковий розрив у якості медичного обслуговування.
7. Недостатній захист прав пацієнтів: У разі помилок або технічних збоїв у системі, пацієнти можуть зіткнутися з труднощами в доказуванні своїх прав на конфіденційність або на якісне лікування.

Ці недоліки вимагають уважного врахування та зусиль зі сторони розробників МІС та медичних установ для забезпечення того, щоб системи були зручними, безпечними та ефективними для всіх користувачів.

1.2 Аналіз тенденцій використання блокчейн технологій у медичних інформаційних системах

1.2.1 Переваги блокчейну для медичних даних

Блокчейн у сфері охорони здоров'я використовується для обміну клінічними даними, виставлення рахунків, управління ланцюжками поставок ліків, а також для розробки ліків і проведення клінічних досліджень. Технології блокчейн здатні повністю змінити спосіб отримання, зберігання та обміну клінічною інформацією між партнерами, платниками та пацієнтами [10]. Крім того,

використання блокчейну забезпечує високу безпеку та збереження даних, що є важливим для захисту конфіденційності.

У сучасному світі потреба в якісних медичних послугах задовольняється завдяки впровадженню інноваційних технологій. Блокчейн відіграє вирішальну роль у трансформації сфери охорони здоров'я. Система охорони здоров'я дедалі більше орієнтується на пацієнтів і зосереджується на двох основних цілях: забезпечення доступних медичних послуг та відповідних ресурсів у будь-який час. Блокчейн допомагає організаціям забезпечити належний догляд за пацієнтами та ефективну роботу медичних установ.

Обмін медичною інформацією є одним з найтрудомісткіших і повторюваних процесів, що веде до високих витрат, але завдяки технології блокчейн ці процеси значно спрощуються і пришвидшуються. За допомогою блокчейн-технологій громадяни можуть брати участь у навчальних програмах у сфері охорони здоров'я. Крім того, дослідження та обмін даними про суспільне здоров'я сприяють покращенню лікування різних спільнот.

Найважливішими проблемами в управлінні охороною здоров'я завжди були захист даних, їх обмін та взаємодія між різними учасниками процесу. Саме ці проблеми успішно вирішує блокчейн. Технологія забезпечує безпеку даних, полегшує їх обмін, забезпечує інтеграцію, цілісність, а також миттєве оновлення та доступ до інформації [11]. Існує також занепокоєння щодо захисту даних, особливо в персоналізованій медицині. Пацієнти та медичний персонал потребують безпечних засобів запису та консультування даних без ризиків для їхньої безпеки, і саме тут блокчейн стає важливим інструментом для вирішення цих питань.

1.2.2 Проблеми та обмеження

Охорона здоров'я – це складний сектор, що безпосередньо взаємодіє з нами на всіх рівнях – фізичному, психічному та фінансовому. Тому впровадження інноваційних технологій потребує особливої уваги та дослідження. Незважаючи на ентузіазм щодо впровадження технології блокчейн, сектор охорони здоров'я не поспішає активно використовувати її. Однак, впровадження блокчейну може

мати вирішальне значення для оптимізації різних процесів та подолання проблем.

1. Відсутність швидкої інтеперабельності

Однією з головних проблем галузі охорони здоров'я є роз'єднаність і розпорошеність даних про пацієнтів між різними відділами, зацікавленими сторонами та системами [12]. Обмін медичними даними є основою ефективної системи охорони здоров'я, але системи часто вимагають від пацієнтів надавати медичні записи у вигляді паперових або електронних копій. Це неефективно через кілька причин:

- Пацієнти повинні отримати і доставити медичну документацію протягом 30 днів, що робить процес повільним.
- Записи можуть бути втрачені або викрадені під час транспортування, що є небезпечним.
- Історія пацієнта може бути неповною, якщо дані зберігаються в різних системах.
- Відсутність архітектури унеможливорює доступ до важливих даних, що впливає на точність лікування.

2. Неефективне та складне зберігання даних в ЕМЗ

Системи електронних медичних записів (ЕМЗ) є ефективним методом обміну даними між лікарнями та різними медичними установами. Однак, цей процес часто ускладнюється через розрізненість даних у різних ЕМЗ [13].

Це може спричинити:

- Професійне вигорання лікарів, які проводять багато часу за роботою з ЕМЗ поза робочим часом.
- Неправильні діагнози через недостатність або помилковість інформації в медичних записах.
- Складні, трудомісткі та ручні процеси, які перевантажують медичних працівників.

3. Обмежений доступ до даних про здоров'я населення

Медичні працівники та дослідники часто стикаються з фрагментарними

даними. Через відповідальність і фінансові наслідки, пов'язані з даними, постачальники не бажають ділитися інформацією про пацієнтів, навіть якщо вона анонімна. Дані необхідні на всіх рівнях:

- На місцевому рівні – для моніторингу здоров'я населення та втручань.
- На національному рівні – для розподілу ресурсів і планування.
- На глобальному рівні – для оцінки глобального тягаря хвороб і вимірювання розвитку охорони здоров'я.

4. Конфіденційність і безпека даних

Існує потреба в обміні даними, при цьому питання інформаційної безпеки та конфіденційності залишаються пріоритетними. Багато медичних установ все ще використовують застарілі системи для зберігання записів про пацієнтів. Це створює ризики:

- Порушення безпеки даних свідчать про недостатність системи для безпечного обміну конфіденційною інформацією.
- Системи охорони здоров'я сьогодні не є уніфікованими, що робить їх вразливими до кібератак.
- Згідно зі звітом I.V.M. «Вартість витоку даних у 2021 році», медична галузь має найвищу вартість витоку даних – в середньому \$9,23 млн.

5. Проблеми інтероперабельності

Сьогодні медичні дані містять великі обсяги інформації з різних джерел, таких як медичні знімки, звіти лікарів, лабораторні звіти та дані з носієвих пристроїв. Блокчейн може підтримувати культуру охорони здоров'я завдяки своїм можливостям [14]:

- Забезпечення безпечної передачі медичних записів.
- Управління ланцюжком поставок ліків.
- Захист даних і управління геномами.
- Підтримка інтероперабельності та оцифрованого відстеження медичних процесів.

Технологія блокчейн може значно покращити стан пацієнтів, зберігаючи при цьому кошти за конкурентною вартістю. Блокчейн дозволяє забезпечити

багаторівневу автентифікацію та прозорість процесу виписування рецептів. Децентралізована структура блокчейну дозволяє лікарям, пацієнтам та медичним працівникам швидко і безпечно обмінюватися інформацією, що сприяє покращенню якості медичних послуг.

1.3 Порівняльний аналіз систем управління базами даних (СУБД)

1.3.1 Традиційні СУБД проти блокчейн-орієнтованих СУБД

Технологія блокчейн викликає багато запитань щодо її відмінностей від традиційних баз даних. Для новачків обидва ці терміни можуть звучати схоже, але вони кардинально відрізняються. Деякі навіть вважають блокчейн «просто іншою базою даних», що є хибним уявленням. Щоб розібратися, розглянемо детальніше обидві технології.

Блокчейн найкраще визначити як технологію розподіленого реєстру, яка дозволяє декільком партнерам працювати разом у єдиній децентралізованій мережі. Вузли (ноди) в мережі можуть обмінюватися інформацією за допомогою алгоритму консенсусу, без потреби в централізованому органі. Всі транзакції в блокчейні проходять перевірку через алгоритм консенсусу, який гарантує, що лише валідні транзакції додаються до реєстру [15]. Це додає блокчейну цінність, прозорість, незмінність та безпеку.

На відміну від блокчейну, база даних є централізованим реєстром, яким керує адміністратор, як це видно з рис. 2.1. Бази даних мають можливість читання і запису даних, але лише користувачі з відповідними правами доступу можуть виконувати ці дії. Центральна система управління базою даних полегшує доступ до даних і їхнє зберігання, але також має недоліки, зокрема можливість пошкодження даних та зміну їх адміністратором.

Централізована база даних: у лікарні дані про пацієнтів зберігаються в централізованій базі даних, якою керує адміністратор. Адміністратор має повний контроль над даними, що може призвести до ризиків змін даних.

Блокчейн: у тій самій лікарні використовується блокчейн для зберігання даних про пацієнтів. Всі дані зберігаються в розподіленій мережі, що забезпечує безпеку і прозорість. Кожна транзакція перевіряється всіма вузлами, що

мінімізує ризик зміни даних.

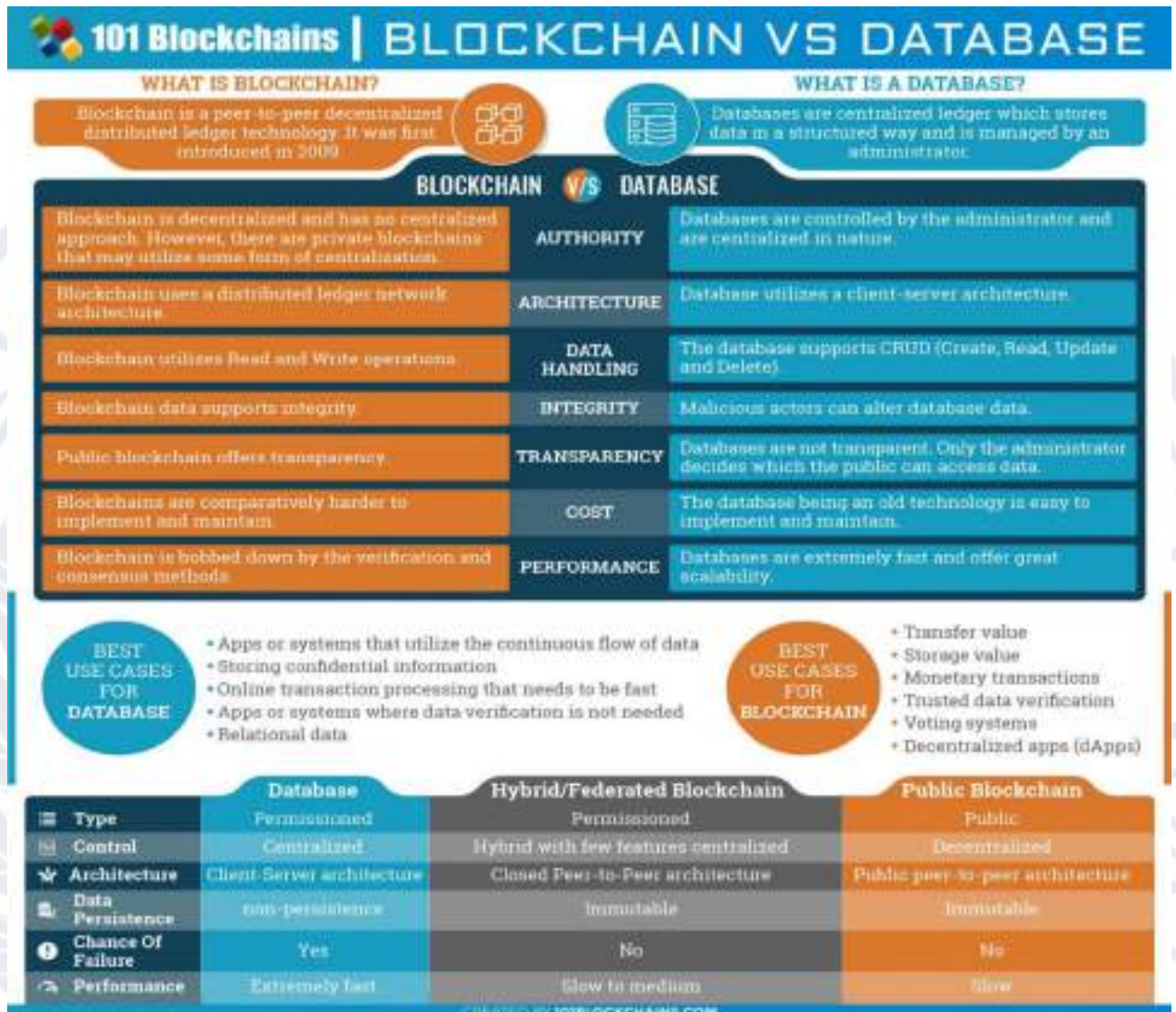


Рис. 2.1 – Порівняльний аналіз блокчейн та бази даних [16]

Порівняння традиційних СУБД і блокчейн-орієнтованих СУБД показує, що кожна з технологій має свої переваги та обмеження. Традиційні бази даних забезпечують легкість управління та швидкий доступ до даних, але мають ризики централізації [17]. Блокчейн, навпаки, пропонує децентралізований підхід з високою безпекою та прозорістю, але може мати обмеження у масштабованості та швидкості. Вибір між цими технологіями залежить від конкретних потреб і вимог сфери застосування.

1.3.2 Критерії порівняння: безпека, швидкість обробки даних, масштабованість та інше

Безпека традиційних СУБД:

- Безпека даних залежить від централізованого контролю та політик доступу, встановлених адміністратором [17].
- Централізована природа баз даних робить їх вразливими до внутрішніх загроз, таких як несанкціоновані зміни даних з боку співробітників.
- Для забезпечення безпеки та відновлення даних у разі збоїв потрібно регулярно створювати резервні копії, що не завжди виконується належним чином.

Блокчейн-орієнтовані СУБД:

- Всі дані зберігаються у розподіленій мережі, що забезпечує високий рівень безпеки завдяки криптографії.
- Дані, записані в блокчейн, не можуть бути змінені або видалені, що гарантує їхню цілісність.
- Завдяки децентралізованій структурі атаки на окремі вузли не впливають на всю систему.

Швидкість обробки даних традиційних СУБД:

- Центральний сервер може обробляти запити дуже швидко завдяки оптимізованим алгоритмам і структурам даних.
- Дані зберігаються централізовано, що дозволяє миттєво отримувати доступ до них.
- Сучасні СУБД можуть обробляти великий обсяг запитів в режимі реального часу, забезпечуючи високу продуктивність.

Блокчейн-орієнтовані СУБД:

- Процес валідації транзакцій через консенсус може бути повільним, особливо у великих мережах [18].
- Кожна транзакція повинна бути перевірена всіма вузлами, що може збільшити час обробки даних.
- Обробка даних у великих обсягах може викликати значні затримки через

необхідність досягнення консенсусу.

Масштабованість традиційних СУБД:

- Легко масштабуються шляхом додавання нових серверів або кластерів для обробки більших обсягів даних.
- Можуть використовувати різні методи оптимізації та балансування навантаження для підтримки високої продуктивності.
- Масштабованість залежить від апаратних ресурсів, таких як пам'ять і процесори.

Блокчейн-орієнтовані СУБД:

- Додавання нових вузлів до мережі може покращити розподіл навантаження, але не завжди вирішує проблеми з пропускнуою здатністю.
- Необхідність досягнення консенсусу може обмежувати масштабованість, особливо у великих мережах.
- Існують нові рішення, такі як шардінг та протоколи другого рівня, які можуть допомогти покращити масштабованість блокчейн-мереж [19].

Прозорість та відстежуваність традиційних СУБД:

- Центральний адміністратор має повний контроль над базою даних, що обмежує прозорість для кінцевих користувачів.
- Відстежування змін в даних може бути складним і вимагати додаткових механізмів аудиту.

Блокчейн-орієнтовані СУБД:

- Всі транзакції публічно доступні та можуть бути перевірені будь-яким учасником мережі.
- Кожна зміна записується в блокчейн, що забезпечує повну відстежуваність та аудит.

Управління даними традиційних СУБД:

- Адміністратор має повний контроль над даними, включаючи доступ, зміну та видалення.
- Легко вносити зміни в структуру даних та управління ними.

Блокчейн-орієнтовані СУБД:

- Учасники мають рівні права доступу до даних, що ускладнює централізоване управління.
- Зміни в даних можливі лише через додавання нових транзакцій, що ускладнює процес управління.

Кожна з цих технологій має свої переваги і недоліки, які визначаються конкретними потребами та вимогами до систем управління базами даних. Традиційні СУБД забезпечують швидкість та ефективність обробки даних, але можуть мати проблеми з безпекою та прозорістю. Блокчейн-орієнтовані СУБД пропонують високий рівень безпеки та прозорості, але можуть бути менш ефективними в обробці великих обсягів даних [20]. Вибір між цими технологіями повинен базуватися на специфічних вимогах та умовах використання.

1.4 Аналіз наукових робіт у галузі застосування блокчейн у медицині

Технологія блокчейн у сфері охорони здоров'я вивчається в багатьох наукових дослідженнях. Так, у роботі [21] представлений метод Healthcare Data Gateway (HDG), що базується на приватному блокчейні, коли пацієнти можуть отримувати доступи, централізовано керувати або ж контролювати свої записи. Зі статті [22] ми дізналися про публічний блокчейн, що використовує захищені методи шифрування. Даний метод заснований на збереженні даних в зашифрованих кодах та публічному збереженні їх в мережі блокчейн, але користувачі мали доступ до своїх записів та моніторингу. В статті [23] впроваджується використання Hyperledger, запропоновано зберігати у блокчейні тільки метадані і посилання на необхідну інформацію, а самі дані повинні бути в іншому сховищі. Дана розробка підвищує захист від DDOS атак, збільшує відмовостійкість. У роботі [24] розглянута структура, що основана на обміні та керуванні медичних відомостей через інтеграцію блокчейну і хмарного сховища. Ця архітектура застосовувалась для надання пацієнтам абсолютного доступу і контролю над власними записами без участі третьої сторони. Автори роботи [25] проводять ретельний аналіз впровадження технології блокчейн у хмарних

середовищах, що необхідно задля полегшення безпечної передачі даних електронних медичних записів (EHR) між учасниками процесу. Розподілений реєстр даних надається усім уповноваженим особам. Вся інформація, що зберігається в блокчейні, записується як хеш-значення, тому є захищеною від втручання. Інноваційні концепції розглянуто у роботі [26]. Стаття зосереджена на використанні платформи Hyperledger Fabric для забезпечення безпечного обміну медичними даними. Використання ланцюгової моделі контролю доступу Hyperledger може суттєво підвищити рівень безпеки та ефективності обміну медичними даними.

Висновок до розділу 1

У першому розділі було здійснено детальний огляд існуючих інформаційних систем (IC) у медичній галузі та проведено аналіз загальних тенденцій використання технології блокчейн у цих системах. Розглянуті матеріали дозволили зробити низку висновків, що можуть бути корисними для подальших досліджень та впроваджень.

Технологія блокчейн пропонує значні переваги для медичних інформаційних систем, зокрема:

- Безпека та конфіденційність: Децентралізована структура блокчейну забезпечує високий рівень захисту даних від несанкціонованого доступу та змін.
- Прозорість та відстежуваність: Кожна транзакція у блокчейні є прозорою та відстежуваною, що підвищує довіру до системи.
- Незмінність даних: Записи у блокчейні не можуть бути змінені або видалені, що забезпечує цілісність та достовірність інформації.

Однак, впровадження блокчейну у медичні інформаційні системи стикається з певними проблемами, такими як низька швидкість обробки транзакцій, обмежена масштабованість та складність інтеграції з існуючими системами.

Аналіз існуючих інформаційних систем у медичній галузі показав, що вони мають значний потенціал для покращення якості та ефективності медичних послуг. Використання технології блокчейн може значно підвищити безпеку,

прозорість та цілісність медичних даних. Водночас, існують певні виклики, які потребують додаткових досліджень та розробок для їх подолання. Традиційні СУБД та блокчейн-орієнтовані СУБД мають свої унікальні переваги та недоліки, і вибір між ними повинен базуватися на конкретних потребах та умовах використання.



РОЗДІЛ 2

ПОСТАНОВКА ЗАДАЧІ ТА ТЕОРЕТИЧНА ОСНОВА ДЛЯ РОЗРОБКИ МЕДИЧНОЇ СИСТЕМИ

2.1 Визначення проблеми та аналіз потреб медичного закладу

2.1.1 Огляд сучасних проблем управління медичними даними.

Сучасні системи управління медичними даними стикаються з низкою серйозних проблем, що впливають на ефективність роботи медичних закладів, безпеку пацієнтів та збереження конфіденційності (рис. 2.1). Централізовані бази даних, на яких базується більшість медичних систем, є вразливими до кібератак та втручання з боку сторонніх осіб. Це може призводити до викривлення або видалення важливої інформації, такої як діагнози чи результати аналізів, що має важливе значення для здоров'я пацієнтів.



Рисунок 2.1 – Вирішення проблем управління даними в охороні здоров'я (інфографіка) [27]

Крім того, існують труднощі з контролем доступу до таких даних, що часто не забезпечує достатньої прозорості та безпеки. Зловмисники або недобросовісні працівники можуть змінювати записи про пацієнтів, фальсифікуючи історії хвороб або додаючи неіснуючі діагнози. Це може мати особливо негативні наслідки в контексті військових комісій або інших ситуацій, де медична інформація може бути використана в політичних або юридичних цілях. Окрім цього, зберігання всієї бази даних в одному місці створює додаткові ризики через

централізований характер системи, де будь-яка помилка або збій в одному з елементів може призвести до втрати великого обсягу даних.

2.1.2 Аналіз поточних потреб медичних закладів

Сучасні медичні заклади стикаються з рядом важливих потреб, які вимагають вдосконалення існуючих інформаційних систем. Однією з ключових вимог є забезпечення безперервного доступу до медичної інформації, оскільки точність і актуальність даних про пацієнтів неймовірно важливі для їх лікування. Важливою потребою також є забезпечення достовірності та автентичності даних, щоб уникнути випадків фальсифікації або некоректних змін, які можуть вплинути на якість лікування [28]. Інтеграція різних інформаційних систем між медичними закладами стає ще однією нагальною вимогою, оскільки пацієнти часто отримують лікування у різних установах, і обмін даними між ними має бути швидким і безпечним. До того ж, забезпечення конфіденційності даних є критично важливим через необхідність захисту персональної інформації пацієнтів та відповідність міжнародним стандартам, таким як GDPR [29]. На рис. 2.2 відображено концепцію інтеграції медичних записів.



Рисунок 2.2 – Концепція оптимізації медичних записів на основі блокчейну[30]

2.1.3 Проблеми взаємодії між різними медичними установами

Взаємодія між різними медичними установами стикається з численними проблемами, які ускладнюють обмін інформацією та координацію лікувальних процесів. Однією з основних проблем є відсутність єдиного стандарту для зберігання та передачі медичних даних, що призводить до труднощів у сумісності різних інформаційних систем. Кожна медична установа може використовувати різні формати даних, бази даних або програмні рішення, що ускладнює або взагалі унеможлиблює обмін інформацією між ними. Це може призводити до затримок у доступі до важливих медичних даних або навіть до помилок у лікуванні, коли лікарі не мають повної інформації про пацієнта. Крім того, питання безпеки під час обміну даними також залишається невирішеним, оскільки передача конфіденційної інформації між установами може бути вразливою до несанкціонованого доступу. Інша проблема полягає у складності відстеження змін у даних та контролю за доступом до них у випадках, коли пацієнт звертається до різних закладів. Це ускладнює забезпечення повної прозорості та достовірності медичної інформації, що може мати негативний вплив на процес лікування та подальший моніторинг стану пацієнта.

2.1.4 Потреби в покращенні безпеки та приватності

Потреба в покращенні безпеки та приватності в медичних закладах є однією з ключових вимог сучасних інформаційних систем, адже пацієнти довіряють лікарям не тільки своє здоров'я, але й персональну інформацію, яка повинна бути належним чином захищена. Медичні дані містять велику кількість конфіденційної інформації про пацієнтів, включаючи діагнози, результати аналізів, історії лікування, особисті дані, такі як ідентифікаційні номери або адреси проживання, а також фінансові дані у випадках, коли система обробляє страхові виплати чи інші платежі. У зв'язку з цим, їх захист має бути на найвищому рівні для забезпечення довіри до системи з боку пацієнтів і медичних установ.

Однією з головних проблем є необхідність забезпечення конфіденційності персональних даних, щоб унеможливити їхній несанкціонований доступ з боку

третіх осіб або зловмисників. В умовах зростання кібератак і появи нових загроз, медичні інформаційні системи стають привабливою мішенню для хакерів, адже доступ до таких даних може бути використаний для вимагання викупу, шантажу чи інших злочинних дій. Особливо небезпечними є витoki інформації, коли дані пацієнтів стають загальнодоступними або передаються до рук недобросовісних компаній, які можуть використати їх для отримання прибутку. Щоб запобігти таким інцидентам, необхідно застосовувати сучасні методи шифрування та розмежування доступу до інформації, що дозволяє лише уповноваженим особам взаємодіяти з нею [31].

Також важливо гарантувати відстежуваність усіх змін, що вносяться в медичну інформацію, щоб мати можливість чітко бачити, хто, коли і які корективи вносив. Такий рівень прозорості допоможе уникнути фальсифікації або некоректних змін, які можуть негативно вплинути на лікувальний процес. Відстеження усіх змін дозволить зберегти повну історію оновлень, що є особливо важливим у разі виникнення медичних помилок чи конфліктних ситуацій, коли необхідно з'ясувати, на якому етапі були внесені ті чи інші дані. Це також підвищує відповідальність медичного персоналу, оскільки кожен має бути впевненим у коректності своїх дій, знаючи, що всі зміни можна відстежити.

Захист інформації також повинен відповідати міжнародним стандартам, таким як GDPR (General Data Protection Regulation), як зображено на рис. 2.3, що ставить додаткові вимоги до захисту приватності даних пацієнтів [32]. Згідно з цим регламентом, будь-яка інформаційна система, що обробляє персональні дані громадян, повинна забезпечувати їх надійне шифрування, мінімізувати обсяг зібраних даних та мати механізми видалення інформації на вимогу пацієнта. Важливо також забезпечити механізми контролю доступу, які дозволять розподіляти права доступу залежно від ролі користувача в системі. Лікарі, медсестри, адміністрація чи пацієнти повинні мати доступ тільки до тієї інформації, яка необхідна для виконання їхніх завдань, і це має бути чітко регламентовано.



Рисунок 2.3 – Загальний регламент про захист даних (GDPR) [33]

Ще одним важливим аспектом є забезпечення прозорості в управлінні даними. Пацієнти повинні мати можливість знати, як і хто використовує їхні дані, для яких цілей і хто має до них доступ. Система повинна надавати інструменти для інформування пацієнтів про їхні права на управління особистими даними, а також можливість надати або відкликати згоду на обробку певних даних [34]. Важливо, щоб пацієнт відчував контроль над своєю інформацією, що збільшить довіру до медичного закладу.

Таким чином, покращення безпеки та приватності в медичних закладах є критично важливим завданням, яке вимагає інтеграції передових технологій, таких як шифрування даних, контроль доступу та блокчейн, для захисту від загроз та забезпечення повної прозорості й підзвітності під час роботи з медичною інформацією.

2.1.5 Постановка задачі

Модельована інформаційна медична система має бути розрахована для використання у медичних закладах, і це визначає такі вимоги:

- ✓ Система має витримувати приблизно 500 одночасних активних запитів від лікарів, пацієнтів та адміністративного персоналу.
- ✓ Система повинна зберігати інформацію про пацієнтів, лікарів, медичні записи, ліки, платежі, обстеження.

- ✓ Система має бути реалізована у вигляді WebAPI для забезпечення інтеграції з веб-сайтами.
- ✓ Кожен запис у базі даних має бути забезпечений унікальною контрольною сумою (хешем), яка генерується під час внесення запису. унеможливорює її модифікацію без виявлення.
- ✓ У разі виявлення невідповідності контрольних сум система повина блокувати доступ до запису та генерувати сповіщення для адміністратора.
- ✓ Забезпечення низької затримки при додаванні нових записів.
- ✓ Відсутність єдиної точки відмови через розподілений характер блокчейну.

Ці вимоги дозволяють забезпечити не лише функціональність та зручність використання системи, але й надійний захист інформації

2.2 Архітектура інформаційної системи

2.2.1 Вибір платформи блокчейн

У даному проєкті для розробки інформаційної системи медичного закладу було обрано блокчейн-платформу Hyperledger Fabric. Ця платформа забезпечує високий рівень гнучкості, безпеки та масштабованості, що робить її ідеальним вибором для медичних інформаційних систем, де конфіденційність даних, безпека і можливість контролю за доступом до інформації мають першорядне значення.

Hyperledger Fabric дозволяє створювати приватні блокчейн-мережі, в яких доступ до даних можуть отримати лише певні учасники, що забезпечує необхідний рівень конфіденційності в межах медичних установ. Завдяки механізмам смарт-контрактів система може автоматизувати багато процесів, таких як перевірка прав доступу, внесення змін до медичних записів, а також спільна робота різних медичних закладів. Це сприяє підвищенню ефективності управління даними, скороченню часу обробки запитів та зменшенню ризику людських помилок.

Крім того, Hyperledger Fabric підтримує модульну архітектуру, що дозволяє гнучко адаптувати систему під конкретні вимоги медичних установ, додавати нові функції чи інтегрувати існуючі рішення [35]. Це особливо важливо для

великих медичних закладів або систем, що працюють у різних регіонах, оскільки платформа забезпечує стабільну роботу навіть при високому навантаженні і великій кількості користувачів. Інтеграція з IoT-пристроями для збору медичних показників у реальному часі також може бути реалізована через цю платформу, що робить її комплексним рішенням для цифровізації медичних процесів.

Таким чином, обрання Hyperledger Fabric як основи для розробки медичної інформаційної системи гарантує високий рівень безпеки, прозорості та надійності, що є критично важливими для збереження медичних даних та забезпечення їх коректної обробки. Основні характеристики та параметри Hyperledger Fabric:

1. Консорціумний блокчейн. Hyperledger Fabric є платформою для створення консорціумних блокчейнів (рис.2.4), де учасниками є зацікавлені сторони (медичні установи, страхові компанії, пацієнти). Це дозволяє чітко контролювати, хто має доступ до блокчейну, на відміну від публічних платформ, таких як Ethereum.

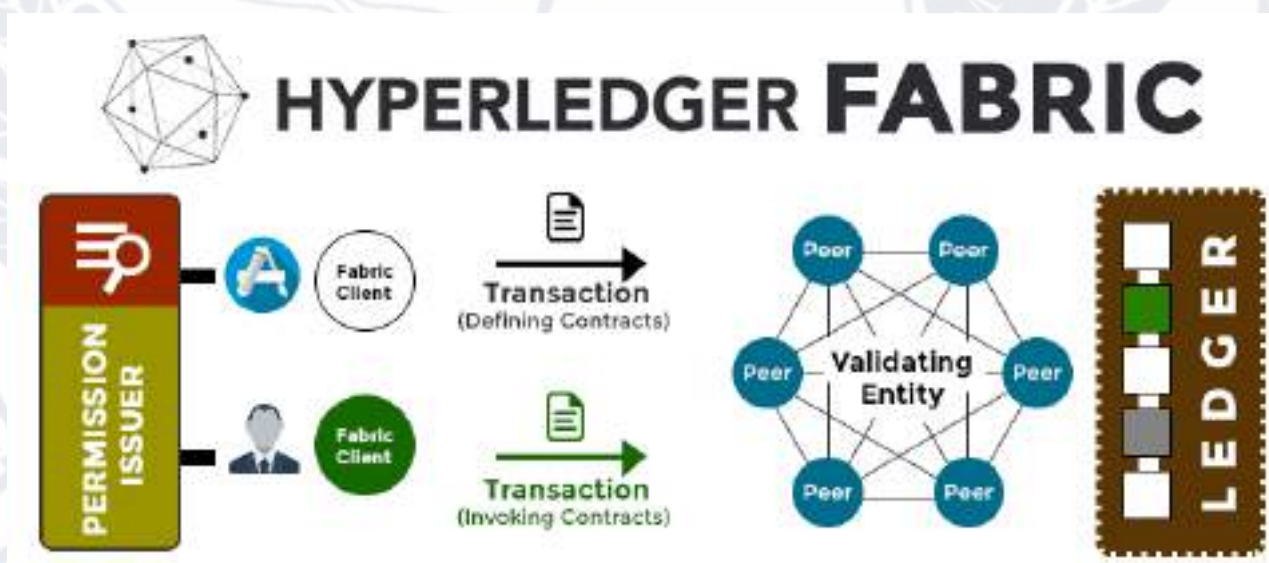


Рисунок 2.4 – Блокчейн-платформа Hyperledger Fabric [36]

2. Модульна архітектура. Fabric підтримує модульну архітектуру, що дозволяє конфігурувати систему відповідно до потреб конкретного медичного закладу. Основні модулі включають компоненти консенсусу, управління членством і смарт-контракти (Chaincode)[37]. Такий підхід дозволяє налаштовувати систему під конкретні вимоги медичних процесів.

3. Приватність і конфіденційність. Hyperledger Fabric підтримує канали – це механізм, що дозволяє створювати приватні підмережі всередині блокчейну, доступні лише для певних учасників [38]. Це ідеально підходить для медичних даних, оскільки забезпечує доступ до них лише уповноваженим користувачам. Наприклад, лікарі або страхові компанії можуть мати доступ до даних пацієнтів через захищені канали, а інші учасники – ні.

4. Механізм консенсусу. Fabric використовує механізм консенсусу Practical Byzantine Fault Tolerance (PBFT)[39], що забезпечує високий рівень надійності та безпеки навіть у випадку наявності зловмисників серед учасників мережі. Цей механізм дозволяє уникнути фальсифікацій і корупції даних, таких як спроби змінити діагноз або результати аналізів.

5. Смарт-контракти (Chaincode). У Hyperledger Fabric смарт-контракти називаються Chaincode, і вони використовуються для автоматизації бізнес-логіки. Наприклад, смарт-контракт може бути використаний для фіксації діагнозів, результатів аналізів і контролю за їх змінами. Це дозволяє забезпечити неможливість коригування вже записаних даних без залишення слідів в блокчейні.

6. Висока продуктивність та масштабованість. Fabric підтримує високу швидкість транзакцій та легко масштабується, що дозволяє обробляти великий обсяг даних у великих медичних установах або навіть на національному рівні. Продуктивність досягається за рахунок використання паралельної обробки транзакцій та різних рівнів доступу до даних.

7. Управління ідентифікацією (MSP). Fabric використовує механізм Membership Service Provider (MSP) для управління ідентифікацією користувачів і учасників мережі [40]. Це дозволяє чітко визначати, хто має право доступу до даних і які дії вони можуть виконувати в системі. Кожен учасник, включаючи медичні заклади, лікарів і пацієнтів, має свій цифровий сертифікат, який підтверджує його права в системі.

Переваги Hyperledger Fabric для медичних систем:

- Приватність та безпека: Платформа дозволяє створювати безпечні канали для передачі медичних даних, що відповідає вимогам конфіденційності.
- Неможливість зміни даних: Завдяки механізму смарт-контрактів і криптографічним функціям, дані про діагнози та медичні процедури не можуть бути змінені без відповідної фіксації.
- Масштабованість: Можливість інтеграції між кількома медичними закладами та легкої масштабованості під час зростання обсягів даних.

Таким чином, Hyperledger Fabric був обраний через його можливості забезпечення високого рівня безпеки, масштабованості та гнучкості, що дозволяє створювати надійну та захищену інформаційну систему для управління медичними даними на основі технології блокчейн.

2.2.2 Схема взаємодії компонентів системи

Схема взаємодії компонентів інформаційної системи медичного закладу на основі блокчейн-технології Hyperledger Fabric базується на кількох ключових елементах, які працюють разом для забезпечення безпеки, надійності та функціональності системи. Центральним компонентом є блокчейн-мережа, що складається з кількох вузлів (peer nodes), кожен з яких представляє медичні заклади, страхові компанії або інші організації, що беруть участь в обміні медичними даними. Кожен вузол має свою копію реєстру, в якому зберігаються всі транзакції, включаючи записи про діагнози, результати аналізів та історію лікування пацієнтів.

Основним інтерфейсом взаємодії між користувачами системи та блокчейном є смарт-контракти (Chaincode), які виконують бізнес-логіку і гарантують, що дані про пацієнтів додаються та змінюються лише за дотримання чітко визначених умов [41]. Наприклад, лікар може записати новий діагноз або результати аналізів через смарт-контракт, який автоматично перевірить коректність даних та збереже їх у блокчейн. Якщо хтось спробує змінити існуючий діагноз, система автоматично заблокує таку спробу або запише зміни в новий блок, зберігаючи історію всіх попередніх записів.

Для забезпечення конфіденційності даних між учасниками використовується механізм приватних каналів. Кожен канал є окремою мережею для передачі медичних даних між конкретними установами або лікарями, що мають доступ лише до певної інформації, відповідно до своєї ролі. Це дозволяє зберігати чутливі дані в безпеці, надаючи доступ лише тим, хто має відповідні повноваження.

Користувачі системи взаємодіють із нею через клієнтські додатки, що підключаються до блокчейн-мережі через API. Ці додатки можуть бути веб-інтерфейсами для лікарів, мобільними додатками для пацієнтів або інтеграційними модулями для зовнішніх медичних систем. Через API клієнти надсилають запити до смарт-контрактів, які взаємодіють з реєстром і повертають відповідну інформацію, наприклад, дані про стан здоров'я пацієнта.

Механізм ідентифікації користувачів і контроль доступу до даних здійснюється через систему сертифікації MSP (Membership Service Provider) (див. рис. 2.5). Кожен учасник мережі, будь то лікар, пацієнт або адміністратор, отримує унікальний цифровий сертифікат, який підтверджує його права та дозволяє виконувати певні дії в системі.



Рисунок 2.5 – Система сертифікації MSP [42]

Для забезпечення надійності транзакцій використовується механізм консенсусу, який гарантує, що всі учасники мережі зберігають однакові копії даних і що кожна транзакція підтверджується кількома вузлами до її запису в блокчейн. Це унеможливорює маніпуляції з даними та забезпечує надійність

зберігання медичних записів.

Таким чином, компоненти системи – блокчейн-мережа, смарт-контракти, канали для приватності, API для взаємодії клієнтів, система сертифікації та механізм консенсусу – взаємодіють для створення надійної, захищеної та децентралізованої медичної інформаційної системи.

2.3 Опис технологій та інструментів розробки

2.3.1 Блокчейн технології

Для реалізації інформаційної системи медичного закладу на основі блокчейн-технології було обрано платформу Hyperledger Fabric, яка надає всі необхідні інструменти для створення безпечної, надійної та масштабованої системи. Hyperledger Fabric є дозволеним блокчейном (permissioned blockchain), де кожен учасник має чітко визначені права та доступ до даних, що робить його ідеальним для використання в медичних системах, де важливо контролювати доступ до конфіденційної інформації пацієнтів.

Основні переваги Hyperledger Fabric:

1. Контроль доступу:
 - Кожен учасник мережі має чітко визначені права та доступ до даних, що забезпечує високий рівень безпеки та конфіденційності.
 - Можливість створення приватних каналів для передачі даних, що дозволяє окремим учасникам мережі взаємодіяти між собою, не відкриваючи доступ до інформації іншим учасникам. Це особливо важливо для збереження приватності медичних даних і забезпечення дотримання міжнародних стандартів, таких як GDPR.
2. Смарт-контракти (Chaincode):
 - Hyperledger Fabric підтримує використання смарт-контрактів, які дозволяють автоматизувати обробку медичних даних, забезпечуючи можливість запису діагнозів з гарантією їхньої незмінності [43].
 - Смарт-контракти можуть бути налаштовані для виконання різних завдань, таких як автоматичне оновлення медичних записів, управління доступом до даних та виконання інших адміністративних функцій.

3. Децентралізоване зберігання даних:

- Дані зберігаються у вузлах мережі, кожен запис у системі зберігається у вигляді транзакції, яку неможливо змінити без відповідного сліду, що забезпечує прозорість та надійність інформації[44].
- Децентралізована архітектура забезпечує високий рівень відмовостійкості та стійкості до атак, оскільки немає єдиної точки відмови.

4. Криптографічні методи:

- Кожен запис у ланцюзі блоків підтверджується криптографічними підписами, що виключає можливість його підробки або несанкціонованої зміни.
- Використання криптографічних методів забезпечує цілісність даних та гарантує, що інформація не може бути змінена без відповідного сліду.

5. Механізм консенсусу:

- Механізм консенсусу в Hyperledger Fabric забезпечує те, що всі учасники мережі погоджуються з кожною новою транзакцією перед тим, як вона буде записана в блокчейн, що забезпечує високий рівень довіри між учасниками[45].
- Консенсусний механізм дозволяє запобігати подвійним витратам та іншим потенційним проблемам, пов'язаним з цілісністю даних.

6. Масштабованість:

- Hyperledger Fabric дозволяє легко масштабувати систему, додаючи нові вузли та канали для обробки зростаючого обсягу даних та учасників.
- Масштабованість системи забезпечує її здатність ефективно працювати в умовах зростаючого навантаження та змінних вимог.

7. Інтеграція з іншими системами:

- Hyperledger Fabric легко інтегрується з іншими інформаційними системами та базами даних, що дозволяє створювати комплексні рішення для управління медичними даними.
- Можливість інтеграції з існуючими системами забезпечує безперебійну роботу та ефективне управління даними.

Загалом, технологія блокчейну, використана в даному проєкті, дозволяє створити систему, в якій дані медичних пацієнтів захищені від несанкціонованих змін, гарантуючи безпеку, конфіденційність та прозорість медичної інформації, що робить її надзвичайно корисною для сучасних медичних закладів. Використання Hyperledger Fabric забезпечує високий рівень довіри та надійності, що є важливим для медичних систем, де конфіденційність та цілісність даних мають вирішальне значення.

2.4 Вимоги до системи

2.4.1 Функціональні вимоги

Система повинна забезпечувати повноцінну реєстрацію користувачів, таких як лікарі, пацієнти та адміністрація, із застосуванням сучасних безпечних методів автентифікації, що дозволяють уникнути несанкціонованого доступу до медичних даних. Реєстрація повинна бути надійною, з підтримкою двофакторної автентифікації або біометричних даних для забезпечення високого рівня безпеки. Після реєстрації користувачі отримують доступ до своїх профілів і пов'язаних даних, а також можливість управління ролями, що визначає рівень їхнього доступу до інформації.

Однією з ключових функцій системи є можливість збереження та управління медичними даними пацієнтів. За допомогою технології блокчейн інформація про кожен візит до лікаря, результати аналізів та інші медичні записи зберігатимуться в незмінному вигляді, створюючи надійну історію хвороб пацієнтів. Блокчейн дозволяє зберегти цілісність даних і запобігає їх несанкціонованій модифікації, що забезпечує додатковий рівень безпеки та довіри з боку користувачів.

Система повинна також забезпечувати гнучкий механізм надання доступу до медичної інформації залежно від ролі користувача[46]. Лікарі матимуть повний доступ до даних пацієнтів, адміністрація – до управлінських і статистичних даних, а пацієнти – до своєї медичної інформації, з можливістю поділитися нею за потреби. Такий підхід гарантує конфіденційність медичних даних, а також їхню доступність тільки для авторизованих осіб.

Інтегровані цифрові сервіси повинні надавати можливість проведення онлайн-консультацій, які дозволять лікарям і пацієнтам взаємодіяти віддалено. Крім того, пацієнти зможуть записуватися на прийом через систему, зберігаючи свої візити в електронному календарі. Система також повинна забезпечувати можливість відстеження процесу лікування, зокрема динаміки стану пацієнта, надання рекомендацій і сповіщення про необхідність візитів або повторних аналізів (рис.2.8).

Для ефективного моніторингу здоров'я пацієнтів, система повинна включати спеціальний модуль, який аналізуватиме зібрані медичні показники та іншу інформацію, що дозволить лікарям оперативно реагувати на зміни у стані пацієнта. Цей модуль може бути інтегрований із різними пристроями для віддаленого збору даних, такими як смарт-годинники або медичні датчики, що допоможе виявляти ранні симптоми захворювань або зміни в показниках здоров'я в режимі реального часу.

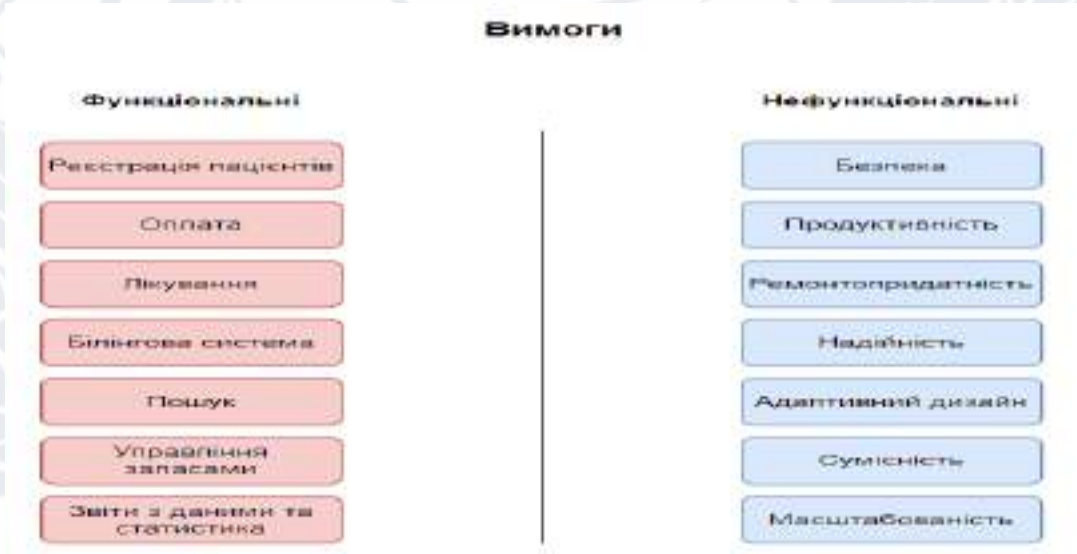


Рисунок 2.8 – Вимоги до системи

2.4.2 Нефункціональні вимоги

Нефункціональні вимоги до системи визначають ключові аспекти її надійності, безпеки та ефективності, які не лише забезпечують зручність користування, але й гарантують довіру до системи з боку користувачів. Одним із найважливіших параметрів є високий рівень безпеки, що досягається завдяки використанню блокчейн-технологій. Усі медичні дані пацієнтів повинні бути

зашифровані й зберігатися в незмінному вигляді, що унеможлиблює їх несанкціоноване редагування або крадіжку. Технологія блокчейн забезпечує децентралізовану структуру, яка значно зменшує ризики втручання зловмисників, а також підвищує стійкість до кібератак. Безпека даних є важливою, адже система працює з конфіденційною інформацією, тому всі рівні захисту повинні відповідати найсучаснішим стандартам, зокрема ISO/IEC 27001.

Масштабованість системи — ще один важливий нефункціональний аспект. Вона повинна бути розроблена таким чином, щоб з легкістю підтримувати зростання кількості користувачів та обсягу медичних даних. Це означає, що архітектура системи повинна бути побудована з урахуванням можливості її розширення без втрати продуктивності та зниження швидкості обробки запитів[47]. При збільшенні кількості пацієнтів і лікарів, система повинна адаптуватися до змін, забезпечуючи стабільну роботу без зависань або збоїв.

Важливою є також висока доступність системи. Оскільки вона повинна бути використана в медичному контексті, де кожна хвилина може мати значення для життя пацієнтів, система повинна функціонувати безперервно. Мінімальні простой та швидке відновлення після можливих збоїв є обов'язковими вимогами. Це передбачає використання надійних серверів, резервних копій даних, а також засобів для відновлення працездатності після аварійних ситуацій. Система повинна мати показники доступності на рівні 99.9%, що гарантуватиме її стабільну роботу.

Продуктивність системи повинна залишатися на високому рівні навіть при значному навантаженні. Це означає, що швидкість доступу до даних та виконання запитів повинна бути стабільною незалежно від кількості активних користувачів або обсягу інформації. Час очікування під час звернень до медичних записів або інших важливих функцій не повинен перевищувати кілька секунд. З метою підтримки високої продуктивності повинні бути застосовані технології оптимізації баз даних, розподілених обчислень і швидкісних серверів[48].

2.4.3 Інтеграційні вимоги

Інтеграційні вимоги системи відіграють важливу роль у забезпеченні її ефективної роботи в сучасній медичній екосистемі, де важливою є взаємодія з іншими технологіями та платформами. Система повинна мати здатність інтегруватися з існуючими медичними інформаційними системами (МИС), які вже використовуються в лікарнях і клініках. Це передбачає можливість обміну даними між різними електронними медичними записами (EMR), базами даних і спеціалізованими медичними платформами, що дозволить лікарям та іншим медичним працівникам легко отримувати доступ до актуальної інформації пацієнтів з різних джерел. Інтеграція повинна бути виконана з використанням стандартизованих протоколів обміну даними, таких як HL7 або FHIR, що забезпечить сумісність системи з різними медичними платформами [49].

Система також повинна підтримувати інтеграцію з різними базами даних, що використовуються для зберігання та обробки медичної інформації, включно з централізованими та розподіленими базами даних. Це важливо для забезпечення швидкого та надійного доступу до великого обсягу даних у реальному часі. Крім того, система повинна підтримувати підключення до Інтернету речей (IoT), зокрема медичних пристроїв і датчиків, які збирають показники здоров'я пацієнтів.

Крім того, система повинна мати можливість обміну даними з іншими блокчейн-системами, що дозволить налагодити співпрацю між різними медичними установами на децентралізованій основі. Така функція особливо важлива для забезпечення безперервного лікування пацієнтів, які можуть звертатися до різних лікарень або клінік. Завдяки цьому можна буде безпечно та швидко передавати медичні дані між закладами, уникаючи дублювання інформації та скорочуючи час на отримання необхідних даних. Обмін даними між різними блокчейн-системами повинен бути надійним і захищеним, з дотриманням конфіденційності та прав доступу до інформації.

2.4.4 Заходи забезпечення безпеки та приватності

Заходи забезпечення безпеки та приватності в інформаційній системі медичного закладу на основі блокчейн-технології спрямовані на захист медичних даних пацієнтів від несанкціонованого доступу, маніпуляцій та втрат. Один з ключових аспектів безпеки – це використання криптографічних методів для шифрування даних як під час їх зберігання, так і під час передачі між учасниками системи. Кожен запис у блокчейні захищається цифровими підписами та хешами, що забезпечує цілісність і незмінність даних. Усі транзакції фіксуються, і будь-які спроби несанкціонованого втручання негайно виявляються.

Для забезпечення конфіденційності інформації система використовує механізм приватних каналів у блокчейні, які дозволяють обмежити доступ до певних даних тільки для авторизованих користувачів [47]. Кожен учасник мережі, будь то лікар, медичний працівник чи пацієнт, отримує унікальний цифровий сертифікат для ідентифікації, що дозволяє чітко контролювати, хто має доступ до яких даних і які дії він може виконувати.

Важливим заходом є управління правами доступу через систему Role-Based Access Control (RBAC), що дозволяє чітко розмежувати повноваження користувачів на основі їхніх ролей в організації [50]. В якості ілюстрації рис. 2.9 Наприклад, лікар може мати доступ до всієї медичної інформації пацієнта, тоді як адміністративний персонал може мати доступ лише до обмежених даних, необхідних для виконання їхніх функцій.

Крім того, система повинна забезпечувати аудит всіх дій, пов'язаних із доступом до даних або їх зміною. Це дозволяє відстежувати кожен крок у взаємодії з медичними записами, що допомагає виявити будь-які спроби зловживань або порушень.

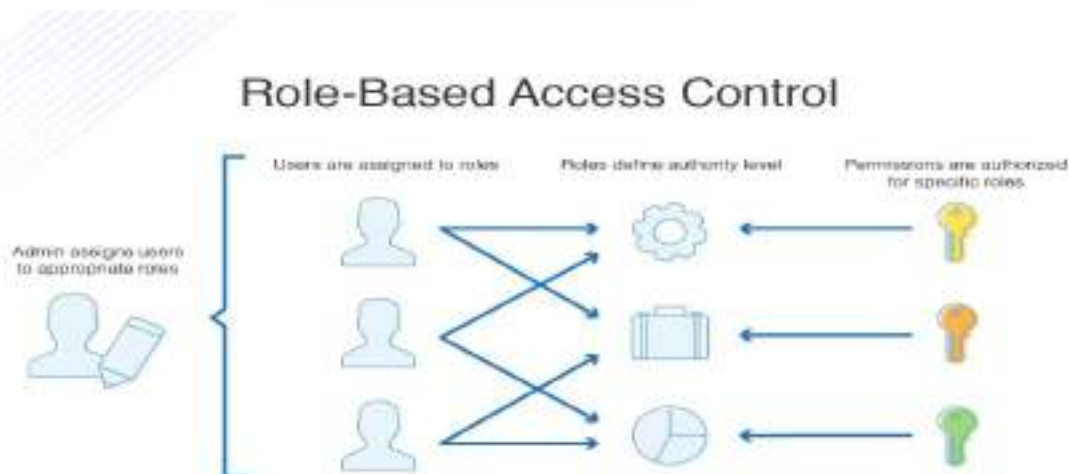


Рисунок 2.9 – Система Role-Based Access Control [51]

З метою дотримання міжнародних стандартів конфіденційності, таких як GDPR, система повинна забезпечувати можливість видалення або анонімізації персональних даних на вимогу пацієнта. Це включає в себе право пацієнтів контролювати свої дані та бути впевненими у їхній безпеці та конфіденційності.

Таким чином, заходи забезпечення безпеки та приватності в системі охоплюють комплекс криптографічних рішень, контроль доступу, моніторинг активності користувачів та відповідність міжнародним стандартам захисту персональних даних, що гарантує високий рівень захисту інформації та довіру з боку пацієнтів та медичних працівників.

Висновок до розділу 2

У процесі аналізу проблем медичного закладу та вибору відповідних технологій було виявлено низку викликів, з якими стикаються сучасні системи управління медичними даними. Основними проблемами є відсутність надійного механізму контролю за змінами медичної інформації, потреба в забезпеченні безпеки і конфіденційності даних, а також обмежена взаємодія між різними медичними установами. Виявлені проблеми суттєво впливають на ефективність медичних процесів, оскільки затримки у передачі або неправильне збереження даних можуть призводити до помилок у лікуванні пацієнтів.

Для вирішення цих проблем було запропоновано використання блокчейн-технології, яка здатна забезпечити захист даних від фальсифікацій, а також прозорість і контроль доступу до них. Блокчейн не тільки гарантує незмінність

збережених даних, але й забезпечує їхню доступність для всіх зацікавлених сторін із точністю до секунди. Крім того, блокчейн дозволяє забезпечити безпеку даних на рівні, який унеможлиблює їх несанкціоноване редагування чи доступ, оскільки кожен учасник має доступ лише до тих даних, що відповідають його рівню прав.

Застосування платформи Hyperledger Fabric надає необхідний функціонал для побудови децентралізованої системи, що гарантує збереження цілісності медичних записів, надає можливість відстежувати зміни та забезпечує захищену взаємодію між учасниками системи. Крім того, платформа дозволяє створювати смарт-контракти, що можуть автоматизувати різні медичні процеси, наприклад, перевірку відповідності даних або оновлення інформації про пацієнта в реальному часі. Вибір Python і Django як основних інструментів розробки сприяє швидкій реалізації системи з високою продуктивністю та надійністю, а також забезпечує легку інтеграцію з блокчейн-інфраструктурою. Ці інструменти дозволяють розробляти гнучкі та масштабовані рішення, що можуть адаптуватися до змін у вимогах системи чи кількості користувачів.

Таким чином, розроблена архітектура інформаційної системи на основі блокчейн-технологій та сучасних веб-інструментів дозволяє вирішити більшість проблем, пов'язаних із збереженням і обробкою медичних даних, забезпечуючи при цьому високий рівень захисту, прозорості та надійності для всіх учасників медичного процесу. Це дозволяє не тільки підвищити якість медичних послуг, але й спростити процес управління інформацією, мінімізуючи ризики, пов'язані з людським фактором і технічними помилками.

РОЗДІЛ 3

РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1. Розробка системи

3.1.1. Вибір та конфігурація інструментів

При створенні масштабованої, безпечної та ефективної ІС для медичного закладу потрібно дотримуватись наступних вимог:

Hyperledger Fabric потребує Fabric SDK (Python) для інтеграції з Django та сертифікатний центр (CA) для управління ідентифікацією користувачів. Django потребує встановленого Python та налаштованого середовища, а також інтеграції з базами даних через ORM. MySQL застосовується як основна реляційна база даних. PyCharm Professional C потрібен для створення та налагодження Django-додатків.

Вимоги до продуктивності: обробка запитів має підтримуватись високою частотою транзакцій (TPS) у блокчейні для великих медичних установ; час відповіді – система повинна реагувати на запити користувачів не більше ніж за 3-5 секунд, навіть при високому навантаженні; масштабованість полягає в можливості горизонтального масштабування (додавання вузлів) для збільшення обчислювальної потужності.

Для реалізації інформаційної системи медичного закладу на основі технології блокчейн було обрано інструменти та технології, що забезпечують гнучкість розробки, простоту налаштування та надійність. Вибір інструментів здійснено з огляду на доступність, сумісність між компонентами та можливість їх використання на платформі Windows 10 Pro.

1. Мова програмування Python 3.13.0

Python – це високорівнева мова програмування, яка підтримує широкий набір бібліотек для роботи з блокчейном, базами даних та веб-розробкою.

– Переваги:

- Великий вибір бібліотек (наприклад, web3.py для інтеграції з

Ethereum).

- Зручний синтаксис для швидкої розробки та тестування.
- Вбудована підтримка роботи з базами даних, зокрема MySQL.
- Конфігурація:

Для встановлення Python 3.13.0 слід:

- 1) Завантажити дистрибутив із офіційного сайту Python (<https://www.python.org>).
 - 2) Під час інсталяції відмітити опцію "Add Python to PATH" для коректної роботи через PowerShell.
2. База даних MySQL 8.0.40

MySQL – це потужна, серверна база даних, що підходить для проектів, які потребують масштабування на великі обсяги даних. Вона забезпечує надійність, безпеку та швидкий доступ до даних.

- Переваги:
 - Проста у використанні, має зручний інтерфейс.
 - Підтримка інтеграції з Django ORM (Object-Relational Mapping).
 - Масштабованість та надійність, підходить для обробки значних обсягів даних.
- Конфігурація:

У проекті база даних буде підключатися до віддаленого сервера з MySQL. Для адміністрування використовується графічний інтерфейс phpMyAdmin.

3. Фреймворк Django 5.1.1

Django – це популярний фреймворк для веб-розробки, який використовує Python і забезпечує швидку розробку із вбудованими механізмами безпеки (рис. 3.1). Він включає вбудований ORM для роботи з базами даних та підтримує інтеграцію з API для реалізації блокчейн-рішень.

- Переваги:
 - Висока безпека та вбудований захист від поширених атак (наприклад, CSRF).
 - Зручний інструментарій для створення адміністративної панелі.

- Підтримка REST API та інтеграція з блокчейном.
- Конфігурація:
 - 1) Встановлення Django через Python Package Manager (pip):
`pip install django==5.1.1`
 - 2) Створення нового проєкту:
`django-admin startproject medical_blockchain_system`



Рисунок 3.1 – Переваги Django Framework [52]

4. Операційна система Windows 10 Pro

Windows 10 Pro забезпечує сумісність з усіма обраними інструментами розробки та надає середовище для використання PowerShell для автоматизації та адміністрування.

5. Windows PowerShell

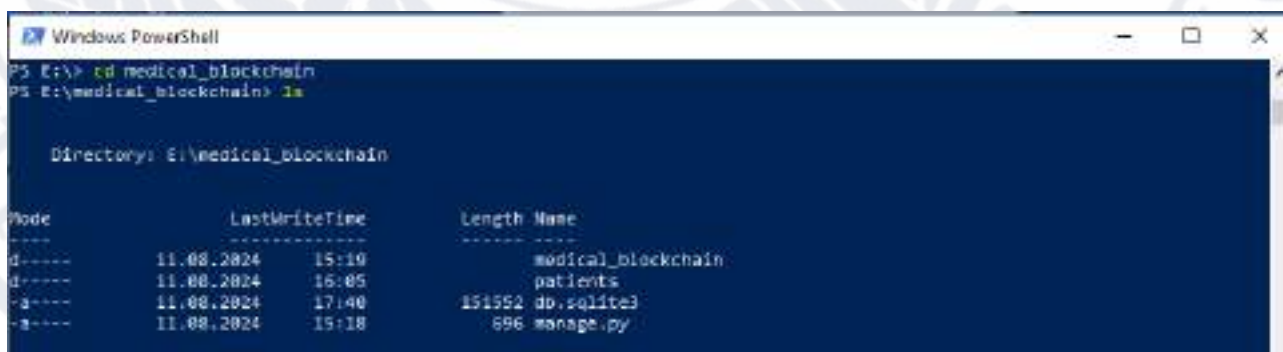


Рисунок 3.2 – Каталог продукту в середовищі Power Shell [53]

Windows PowerShell використовується для встановлення пакетів через pip, запуску Django-сервера та виконання тестових запитів до API(рис. 3.2).

- Конфігурація:

1) Для перевірки встановлених пакетів та версій:

```
python --version
```

```
pip list
```

2) Запуск локального сервера для тестування:

```
python manage.py runserver
```

Обрані інструменти та технології (Python 3.13.0, MySQL 8.0.40, Django 5.1.1 та інші) забезпечують повний цикл розробки інформаційної системи медичного закладу з підтримкою блокчейн-технологій. Використання легких баз даних та простих інструментів, таких як PyCharm, дає можливість швидко розгорнути та протестувати проєкт у середовищі Windows 10 Pro.

3.1.2. Створення архітектури бази даних

Представимо архітектуру бази даних для інформаційної системи медичного закладу. База даних, реалізована у форматі MySQL, містить як стандартні таблиці для аутентифікації користувачів у Django, так і спеціалізовані таблиці для зберігання даних пацієнтів і медичних записів. Нижче (рис. 3.3) описано структуру та призначення основних таблиць.

```
Database changed
mysql> SHOW TABLES;
+-----+
| Tables_in_medical_db |
+-----+
| auth_group             |
| auth_group_permissions |
| auth_permission        |
| auth_user              |
| auth_user_groups       |
| auth_user_user_permissions |
| django_admin_log       |
| django_content_type     |
| django_migrations      |
| django_session         |
| patients_medicalrecord  |
| patients_medicalrecordhashhistory |
| patients_patient       |
+-----+
```

Рисунок 3.3 – Перегляд основних таблиць бази даних медичної системи

1. Стандартні таблиці Django для управління користувачами та логами

auth_group

- Призначення: зберігає групи користувачів. Використовується для керування ролями та правами доступу.
- Основні поля:
 - id – первинний ключ
 - name – назва групи

auth_user

- Призначення: зберігає дані про користувачів системи.
- Основні поля:
 - id – первинний ключ
 - username, password, email – дані для аутентифікації
 - is_staff, is_active – статус користувача

auth_permission та auth_group_permissions

- Призначення: зберігають права доступу та зв'язок між групами і дозволами.

django_admin_log

- Призначення: логування дій адміністратора в системі.
- Основні поля:
 - id – первинний ключ
 - action_time – час виконаної дії
 - object_id, object_repr – ідентифікація змінених об'єктів

django_session

- Призначення: зберігання сесій користувачів для авторизації та підтримки стану.

2. Спеціалізовані таблиці для медичної інформації

patients_patient

- Призначення: зберігає основні дані про пацієнтів.
- Основні поля:
 - id – первинний ключ
 - first_name, last_name – ім'я та прізвище пацієнта

- Інші можливі поля: дата народження, контактна інформація

patients_medicalrecord

- Призначення: зберігає медичні записи, пов'язані з пацієнтами.
- Основні поля:
 - id – первинний ключ
 - diagnosis – діагноз пацієнта
 - Можливий зв'язок із таблицею patients_patient для відстеження записів за пацієнтом через зовнішній ключ.

3. Таблиці для системних налаштувань та міграцій
django_content_type та django_migrations

- Призначення: забезпечують роботу Django ORM з міграціями бази даних та відстеженням типів контенту в системі.

Зв'язки між таблицями

1. auth_user ↔ patients_medicalrecord

- кожен медичний запис може бути прив'язаний до користувача, який створив або редагував його (можливо, лікаря). Це може бути реалізовано через зовнішній ключ.

2. patients_patient ↔ patients_medicalrecord

- кожен запис в таблиці patients_medicalrecord має бути пов'язаний з конкретним пацієнтом через зовнішній ключ (patient_id).

Таблиці бази даних містять наступну інформацію:

Управління користувачами	ПІБ, електронна пошта, роль користувача (пацієнт, лікар, адміністратор), логін, пароль, дата останнього входу;
Пацієнти	ПІБ, стать, дата народження, адреса проживання, контактна інформація (телефон, email), дата реєстрації користувача, номер медичного страхування;

Лікарі	ПІБ, спеціалізація, контактна інформація (телефон, email), графік роботи, номер ліцензії, курси підвищення кваліфікації;
Медичні записи для лікарів	Медична картка(номер/ідентифікатор), діагноз та історія хвороби, план лікування, терапія, дата створення запису, лікар, який створив запис, відділення чи клініка, група крові та резус-фактор, алергії, хронічні захворювання, перелік призначених ліків (دوزи, курс лікування), дата наступного огляду, інформація про направлення до іншого фахівця, додаткові примітки лікаря
Направлення та обстеження	Лікар, який створив направлення, пацієнт, якому створено направлення, назва обстеження, попередній діагноз, дата створення направлення, термін дії направлення, ступінь важливості обстеження, назва обстеження, результати обстеження, дата проведення;
Госпіталізації	Пацієнт, відділення, дата, місцезнаходження у лікарні, контактні дані;
Медичні препарати	Назва, дозування, форма випуску, протипоказання, аналоги;
Відділення лікарні	Назва, місцезнаходження у лікарні, контактні дані, штат працівників;
Розклад лікарів	Лікар, кваліфікація, дата, часові слоти (вільні/зайняті)
Історія призначень	Пацієнт, призначення (опис процедур, консультацій), лікар, дата та час;
Ліки по програмі реімбурсації	Торгова назва ліків, назва діючої речовини, категорія реімбурсації, розмір компенсації, показання до застосування, строк дії програми;

Платежі та страхування	Пацієнт, сума, послуга, за яку сплачено, дата оплати, страхова компанія (якщо є);
Організаційна інформація	Назва закладу охорони здоров'я, адреса, контактна інформація, код за ЄДРПОУ, назва послуги, ціна послуги
Обладнання та ресурси лікарні	Назва, тип обладнання, стан (в робочому стані чи на ремонті), місцезнаходження

Архітектура бази даних побудована на основі стандартних компонентів Django та спеціалізованих таблиць для роботи з медичними даними. Такий підхід забезпечує:

- Надійне управління користувачами та їхніми правами доступу.
- Зручне зберігання інформації про пацієнтів та медичні записи.
- Можливість розширення функціоналу за допомогою модулів Django.

Завдяки використанню MySQL як бази даних система є простою у розгортанні та може бути легко протестована у локальному середовищі.

3.1.3 Програмування функціоналу

На цьому етапі здійснюється практична реалізація інформаційної системи медичного закладу з використанням Python та Django. Проект організовано у вигляді основного каталогу `medical_blockchain` та додатку `patients`. Основна мета – забезпечити управління пацієнтами та їхніми медичними записами в зручному та безпечному середовищі з базою даних MySQL.

1. Налаштування проекту Django

У конфігураційному файлі `settings.py` проект налаштовано для роботи з базою даних MySQL та основними модулями Django, такими як система авторизації, управління сесіями, шаблони та інші. Крім того, підключено додаток `patients` для роботи з медичними даними.

2. Структура бази даних та моделювання даних

База даних містить дві основні таблиці:

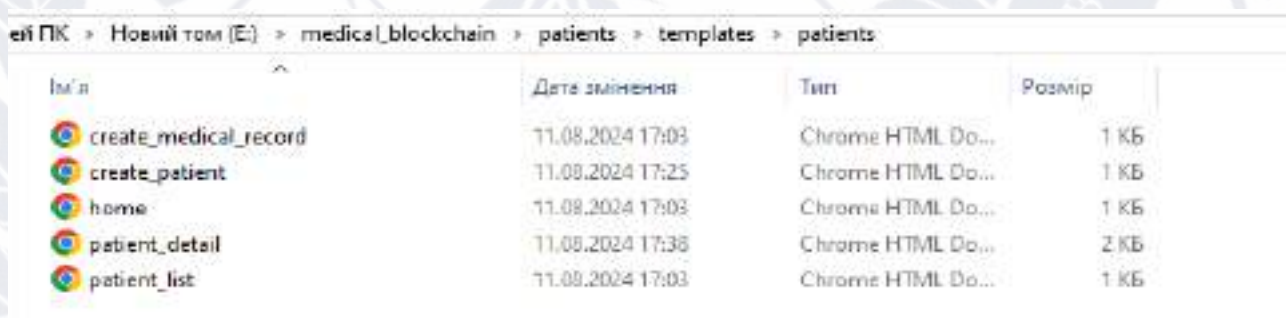
- Пацієнти (із полями для імені, прізвища, дати народження та контактної інформації та інше).
- Медичні записи (із прив'язкою до пацієнта, діагнозу та дати запису та інше).

Ця структура дозволяє зберігати детальну інформацію про кожного пацієнта та його медичну історію. Між записами та пацієнтами реалізовано зв'язок "один до багатьох".

3. Адміністративна панель

У систему інтегровано стандартну адмін-панель Django, що дозволяє зручно управляти даними пацієнтів та медичних записів без написання додаткового інтерфейсу. Через панель можна створювати, редагувати та видаляти записи.

4. Реалізація інтерфейсу користувача (рис. 3.4)



Ім'я	Дата змінення	Тип	Розмір
create_medical_record	11.08.2024 17:03	Chrome HTML Do...	1 KB
create_patient	11.08.2024 17:25	Chrome HTML Do...	1 KB
home	11.08.2024 17:03	Chrome HTML Do...	1 KB
patient_detail	11.08.2024 17:38	Chrome HTML Do...	2 KB
patient_list	11.08.2024 17:03	Chrome HTML Do...	1 KB

Рисунок 3.4 – Шаблони додатку

Для роботи користувачів створено декілька веб-сторінок:

- Головна сторінка з переліком усіх пацієнтів.
- Сторінка детальної інформації про пацієнта, де відображаються особисті дані та історія медичних записів.
- Форма для створення нового пацієнта або додавання медичного запису.

Шаблони HTML забезпечують відображення даних, а форма введення дозволяє користувачам швидко додавати нових пацієнтів та медичні записи.

5. Маршрутизація запитів

У проекті налаштовано маршрутизацію, щоб кожна сторінка була доступною за певною адресою. Головний маршрут веде на сторінку зі списком пацієнтів, а додаткові – на детальну інформацію про кожного пацієнта та форму для додавання нових даних.

6. Тестування функціоналу

Для перевірки правильності роботи системи написано модульні тести. Тести перевіряють, чи можна створювати нових пацієнтів, чи коректно працює прив'язка медичних записів до пацієнтів та чи відображаються дані у веб-інтерфейсі.

7. Утиліти та безпека даних

У проєкті реалізовано утиліту для хешування даних, що дозволяє забезпечити їх захист та перевіряти цілісність записів. Це важливо для використання блокчейн-технології, де кожен запис повинен бути унікально ідентифікований та захищений від змін.

8. Міграції бази даних

Для збереження структури даних використовуються міграції, що генеруються автоматично [54]. Це дозволяє оновлювати базу даних відповідно до змін у моделях без втрати вже існуючих даних.

Система дозволяє ефективно керувати даними пацієнтів і медичними записами, забезпечуючи простоту у використанні та захист інформації. Впровадження адмін-панелі Django робить управління даними зручним для медперсоналу. Блокчейн-компонент гарантує, що жоден запис не буде змінений або видалений безслідно, що підвищує безпеку та надійність збереження інформації.

3.2 Тестування системи

3.2.1 Методи та інструменти тестування

Тестування є важливим етапом розробки інформаційної системи, оскільки дозволяє перевірити функціональність, надійність та безпеку. Враховуючи специфіку системи, що базується на Django з використанням MySQL та Python, тестування охоплює як перевірку логіки роботи системи, так і інтеграцію компонентів.

1. Методи тестування (схематично зображені на рис. 3.5)

➤ Модульне тестування (Unit Testing)

– Перевірка окремих компонентів системи, таких як моделі,

представлення (views) та форми.

- Тестуються функції на рівні окремих модулів без залучення інших частин проекту.

➤ Інтеграційне тестування (Integration Testing)

- Використовується для перевірки взаємодії між компонентами, такими як форми, моделі та базові механізми Django.
- Наприклад, перевіряється, чи успішно створюються записи в базі даних після введення даних через форму.

➤ Функціональне тестування (Functional Testing)

- Оцінка відповідності функціональних можливостей вимогам. Тестується доступ до різних сторінок та коректність виконання CRUD-операцій (створення, читання, оновлення та видалення).

➤ Регресійне тестування (Regression Testing)

- Виконується після внесення змін у код, щоб переконатися, що нові зміни не порушили вже реалізовану функціональність.

➤ Тестування безпеки (Security Testing)

- Перевіряється, чи система правильно обробляє дані та чи немає вразливостей, таких як SQL-ін'єкції чи некоректне управління сесіями.

2. Інструменти тестування

- Вбудований модуль Django для тестування. Django надає вбудовані можливості для тестування через фреймворк unittest. Він дозволяє створювати та виконувати тести для моделей, форм та представлень.
- Python unittest. Використовується для модульного тестування, дозволяє створювати та запускати тести на рівні окремих функцій чи класів.
- Postman. Інструмент для тестування API-інтерфейсів, якщо система підтримує API. Дозволяє перевірити, чи коректно передаються та отримуються дані від сервера.
- Selenium. Використовується для автоматизованого тестування інтерфейсу користувача. За його допомогою можна перевіряти

коректність переходу між сторінками та обробку введених користувачем даних.

- Pytest. Альтернативний інструмент для тестування Python-коду, який дозволяє створювати простіші та більш гнучкі тести у порівнянні з unittest.



Рисунок 3.5 – Типи тестування програмного забезпечення [55]

3. Процес тестування

1. Підготовка тестових даних.

Введення тестових пацієнтів та медичних записів для перевірки роботи форм і відображення даних.

2. Запуск модульних тестів.

Виконання тестів для моделей та форм через команду `python manage.py test`.

3. Перевірка інтерфейсу.

За допомогою Selenium перевіряється, чи коректно працює веб-інтерфейс при взаємодії з користувачем.

4. Оцінка коректності запитів та відповідей.

За допомогою Postman перевіряються API-запити, якщо вони реалізовані.

5. Аналіз результатів.

Усі тести мають бути успішно виконані. У разі помилок виконується налагодження та повторне тестування.

Поєднання різних методів та інструментів тестування забезпечує високу якість розробленої системи та її відповідність вимогам. Це дозволяє мінімізувати ризик помилок, покращити безпеку та забезпечити зручний досвід для користувачів.

3.2.2 Оцінка продуктивності та безпеки

Оцінка продуктивності та безпеки є важливим етапом впровадження інформаційної системи медичного закладу на основі технології блокчейн. Продуктивність системи визначається швидкістю обробки запитів, ефективністю взаємодії з базою даних та здатністю обслуговувати одночасні підключення користувачів. Для перевірки цього використовуються стрес-тести з моделюванням реальних умов навантаження. За допомогою інструментів, таких як Apache JMeter або Locust, імітуються паралельні запити до API, щоб оцінити час відповіді, затримки та можливі вузькі місця [56]. У цьому процесі також перевіряється швидкість доступу до даних у MySQL, оскільки це впливає на загальну продуктивність системи, особливо під час обробки великих обсягів медичної інформації.

Що стосується безпеки, оскільки система зберігає конфіденційну медичну інформацію, особлива увага приділяється захисту даних. Проводиться аналіз наявності можливих вразливостей, таких як SQL-ін'єкції та міжсайтові сценарії (XSS). Тестування безпеки включає також перевірку управління сесіями, особливо коли використовується Django, щоб уникнути крадіжки сесій або їх підробки. Шифрування даних як на рівні зберігання в MySQL, так і під час передачі між клієнтом і сервером, є ключовим заходом для забезпечення безпеки. Крім того, впровадження блокчейн-компонента допомагає гарантувати цілісність даних, зменшуючи ризик несанкціонованої зміни медичних записів.

Додатково проводяться перевірки на відповідність стандартам безпеки, таким як GDPR, що регулюють обробку персональних даних. Використання системи аутентифікації та авторизації на основі Django дозволяє обмежити

доступ до чутливої інформації відповідно до ролей користувачів. Для оцінки стійкості до атак та потенційних загроз проводиться етичне хакерство та моделювання атак, таких як brute-force для перевірки паролів. Поєднання продуктивних і безпекових тестів гарантує, що система не лише швидко обробляє запити, але й надійно захищає дані пацієнтів, що є критично важливим для функціонування медичного закладу.

3.3 Демонстрація роботи системи

3.3.1 Сценарії використання

Демонстрація роботи системи проводиться на основі сценаріїв використання, що відображають типові ситуації взаємодії користувачів з інформаційною системою медичного закладу на основі блокчейн-технології. Ключовими учасниками є лікарі, пацієнти та адміністратори. Сценарії спрямовані на перевірку коректності функціональних можливостей системи, таких як реєстрація, ведення медичних записів та надання доступу до даних.

Перший сценарій: Реєстрація нового пацієнта. Адміністратор або лікар входить у систему, використовуючи свої облікові дані. Переходить до розділу «Пацієнти» та заповнює форму для додавання нового пацієнта, вказуючи ім'я, прізвище та інші необхідні дані. Після збереження інформації система створює новий запис у базі даних MySQL. Це підтверджується повідомленням про успішну реєстрацію та відображенням нового пацієнта в списку.

Другий сценарій: Створення медичного запису. Лікар, увійшовши в систему, вибирає пацієнта зі списку та додає новий медичний запис, вказуючи діагноз та рекомендації. Після підтвердження запис зберігається у базі даних, а блокчейн-технологія фіксує цей запис, що гарантує його цілісність і захищеність від змін у майбутньому. Усі записи доступні для перегляду тільки авторизованим користувачам відповідно до їхніх прав доступу.

Третій сценарій: Перегляд медичних даних пацієнта. Пацієнт отримує доступ до системи через власний акаунт, де може переглядати свої медичні записи та історію відвідувань. Доступ надається лише до тих даних, до яких він

має відповідні права. Це перевіряє коректність роботи аутентифікації та авторизації, реалізованих у Django.

Четвертий сценарій: Оновлення та видалення записів. Адміністратор тестує функціонал редагування даних пацієнта або видалення записів у випадку помилкового введення інформації. Після внесення змін система перевіряє, чи всі пов'язані записи коректно оновлено, а видалення підтверджується зникненням запису зі списку пацієнтів або медичних даних.

П'ятий сценарій: Тестування навантаження та безпеки. Моделюється одночасне підключення кількох користувачів, які виконують різні операції в системі (реєстрація, перегляд записів, створення нових даних). Це дозволяє переконатися, що система працює стабільно під навантаженням. Додатково перевіряється захист від несанкціонованого доступу та правильність керування сесіями.

Ці сценарії демонструють повний цикл роботи системи, її зручність та безпеку, а також готовність до використання в умовах реального медичного закладу.

3.3.2 Інтерфейс користувача та управління даними

Інтерфейс користувача системи медичного закладу на основі блокчейн-технології розроблено з урахуванням простоти, інтуїтивності та доступності для різних категорій користувачів: лікарів, пацієнтів та адміністраторів. Основний інтерфейс побудовано на фреймворку Django з використанням HTML, CSS та шаблонів, що забезпечує зручний веб-доступ через браузер на комп'ютері або мобільному пристрої (рис. 3.6). Усі форми та сторінки організовано таким чином, щоб користувачі могли швидко виконувати необхідні дії з мінімальною кількістю кроків.

На головній сторінці користувачі бачать панель навігації з основними розділами: «Головна», «Пацієнти», «Медичні записи», «Адміністрування» та «Профіль». Авторизація реалізована через стандартні Django-форми входу, що забезпечують контроль доступу та безпеку. Лікар або адміністратор може перейти до розділу пацієнтів та побачити список зареєстрованих пацієнтів із можливістю додати, редагувати чи видалити записи. Для додавання нових

пацієнтів або медичних записів система пропонує прості форми з обов'язковими полями для введення даних (рис. 3.7).



Рисунок 3.6 – Головна сторінка

Користувачий інтерфейс також підтримує фільтрацію та пошук пацієнтів за різними критеріями (наприклад, ім'я, дата народження, діагноз), що полегшує роботу лікарів та зменшує час на обробку інформації. Для перегляду детальної інформації про пацієнта користувач може натиснути на відповідний запис у таблиці, що відкриє окрему сторінку з усіма медичними даними та історією візитів. Важливі записи захищені від випадкових змін, і для редагування потрібне підтвердження.

Пацієнти через власний інтерфейс можуть переглядати лише свої медичні дані, що відображаються у зручному форматі з поділом за датами візитів та діагнозами. Це підвищує прозорість лікувального процесу та дозволяє пацієнту бути в курсі призначень та рекомендацій. Усі дії користувачів (створення, редагування, перегляд записів) записуються в лог-файли, що зберігаються в базі даних, що забезпечує аудит та підвищує безпеку.

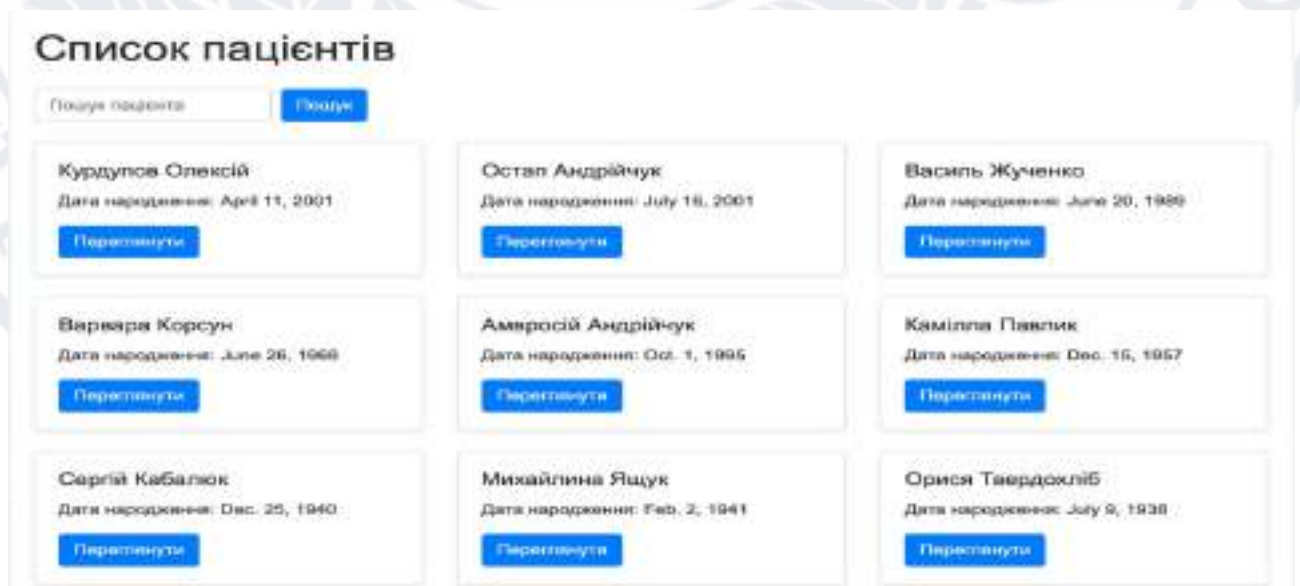


Рисунок 3.7 – Список пацієнтів

Управління даними здійснюється через MySQL, що дозволяє зберігати структуровані дані про пацієнтів і медичні записи. Блокчейн-технологія додає додатковий рівень безпеки: всі критичні записи (наприклад, діагнози та призначення) фіксуються у блокчейні, що гарантує їхню незмінність. Вбудовані механізми резервного копіювання бази даних та автоматичне логування сесій користувачів забезпечують стійкість системи до збоїв і несанкціонованих втручань. У підсумку, інтерфейс користувача розроблено так, щоб поєднувати простоту, функціональність та безпеку, що є критичними для ефективного функціонування медичного закладу.

3.4 Оцінка ефективності та можливості масштабування системи

Ефективність системи медичного закладу на основі блокчейн-технології оцінюється за кількома ключовими параметрами: швидкодія, стабільність під навантаженням, відповідність вимогам користувачів та надійність зберігання даних. Система демонструє високу ефективність у виконанні базових операцій, таких як реєстрація пацієнтів, створення та оновлення медичних записів, завдяки використанню фреймворку Django та бази даних MySQL. Django забезпечує швидку обробку запитів і надає зручні інструменти для оптимізації продуктивності, включаючи кешування та оптимізовані запити до бази даних.

Ефективність не знижується при збільшенні обсягу даних та кількості одночасних підключень, що є важливим фактором для розгляду можливостей масштабування. MySQL добре підходить для розподілених розгортань і великих навантажень. Масштабування системи також передбачає можливість інтеграції з хмарними платформами для зберігання великих обсягів даних та забезпечення доступу до них у режимі реального часу.

З точки зору безпеки та надійності, блокчейн додає значну цінність, оскільки забезпечує незмінність критичних даних і захист від несанкціонованих змін. Це дозволяє уникнути проблем, пов'язаних із підркокою медичних записів, і підвищує довіру до системи з боку користувачів. Водночас для підтримання ефективності необхідно врахувати можливі затримки при перевірці транзакцій у блокчейні, особливо при значному обсязі даних.

Можливість масштабування також залежить від архітектури самої системи. Django дозволяє легко додавати нові модулі та функціональні можливості, що забезпечує гнучкість у разі розширення вимог. Наприклад, при збільшенні кількості підключених користувачів або лікарень можна додати балансувальник навантаження та масштабувати серверні ресурси за допомогою контейнеризації (наприклад, Docker) або хмарних сервісів (AWS, Azure) [57] .

Отже, система є ефективною для експлуатації та має потенціал для масштабування при дотриманні відповідної архітектури та планування ресурсів.

Висновок до розділу 3

У цьому розділі було розглянуто реалізацію інформаційної системи медичного закладу на основі блокчейн-технології, зосереджуючи увагу на ключових аспектах її розробки, тестування, інтерфейсу користувача та оцінки ефективності.

Розробка системи включала вибір інструментів, таких як мова програмування Python, база даних , MySQL фреймворк Django та редактор коду PyCharm. Це забезпечило створення надійної архітектури з чіткою структурою каталогів, що спрощує управління проектом та його подальший розвиток. Основні функціональні можливості системи, зокрема реєстрація пацієнтів, створення медичних записів та управління даними, реалізовано з урахуванням зручності для користувачів.

Тестування системи підтвердило її працездатність та безпеку, а також виявило можливі зони для покращення. Методи тестування, зокрема модульне тестування та навантажувальне тестування, забезпечили високу якість програмного забезпечення та готовність до використання в реальних умовах.

Інтерфейс користувача системи розроблений з акцентом на простоту та інтуїтивність, що дозволяє лікарям, пацієнтам і адміністраторам ефективно взаємодіяти з функціоналом. Усі основні операції реалізовано через зручні форми та панелі навігації, що підвищує швидкість виконання завдань.

Оцінка ефективності системи показала, що вона здатна справлятися з основними операціями, проте можливість масштабування є важливим аспектом

для подальшого розвитку. Перехід на більш потужні бази даних та інтеграція з хмарними сервісами дозволить підтримувати стабільність та продуктивність у разі збільшення обсягу даних і кількості користувачів.

Отже, розроблена система демонструє високий потенціал для подальшого впровадження в медичні установи, завдяки своїй ефективності, безпеці та можливостям масштабування. Вона може стати надійним інструментом для управління медичними даними, підвищуючи якість обслуговування пацієнтів та сприяючи розвитку сучасних медичних технологій.

ВИСНОВКИ

У рамках дипломної роботи була досягнута основна мета — розробка моделі та прототипу інформаційної системи для медичного закладу, яка базується на використанні блокчейн технології. Проведене дослідження дозволило визначити сучасний стан управління медичними даними, виявити основні проблеми існуючих рішень та запропонувати інноваційний підхід для їх вирішення. Виконана робота дозволила підтвердити потенціал блокчейн технологій для підвищення ефективності управління медичними даними, забезпечення їхньої безпеки, доступності та оптимізації внутрішніх процесів медичного закладу.

В ході роботи було проведено детальний огляд сучасних інформаційних систем у сфері охорони здоров'я. Ідентифіковано переваги блокчейн технології, які включають незмінність даних, прозорість, децентралізоване зберігання та підтримку цифрових підписів.

Визначено вимоги до системи, включаючи функціональні (зберігання медичних записів, контроль доступу, забезпечення аудиту) та нефункціональні (висока продуктивність, безпека, масштабованість). Також спроектовано архітектуру системи, яка включає використання блокчейну для збереження даних, цифрові підписи для автентифікації записів, механізми перевірки даних і контроль доступу.

Розроблено програмний прототип системи, який реалізує ключові функціональні можливості, такі як збереження медичних записів, їх незмінність та інтеграцію із цифровими підписами. Використано блокчейн для забезпечення безпеки та прозорості даних. Кожен медичний запис пов'язаний із цифровим підписом лікаря, що гарантує його автентичність і цілісність.

Проведено комплексне тестування системи, яке підтвердило її функціональність, надійність та відповідність встановленим вимогам.

Виявлено та усунуто деякі недоліки, що дозволило підвищити загальну ефективність та стабільність системи. Тестування показало, що використання блокчейн технології дозволяє значно знизити ризик несанкціонованих змін даних. Використання модульного та навантажувального тестування забезпечило

високу якість програмного забезпечення та готовність до використання в реальних умовах. Інтерфейс користувача було розроблено з акцентом на простоту та інтуїтивність, що дозволяє лікарям, пацієнтам і адміністраторам ефективно взаємодіяти з функціоналом через зручні форми та панелі навігації.

В результаті оцінки впливу системи на медичний заклад було обґрунтовано, що розроблена система сприяє покращенню управління медичними даними завдяки незмінності, безпеці та доступності інформації. Запропоновано можливості масштабування та адаптації системи для використання в інших медичних установах.

Перспективи використання:

- ✓ Інноваційність: Використання блокчейн технології дозволило створити систему, яка забезпечує високий рівень захисту даних, прозорість і контроль за всіма операціями з медичними записам.
- ✓ Практична цінність: Запропонована система може бути впроваджена у медичних закладах для підвищення ефективності управління даними та оптимізації внутрішніх процесів.

Оцінка ефективності показала, що система здатна виконувати основні операції. В якості подальших досліджень необхідно дослідити питання масштабування системи, інтеграції з іншими інформаційними платформами, а також можливості використання додаткових технологій, таких як штучний інтелект, для аналізу даних.

Таким чином, розроблена інформаційна система демонструє високий потенціал для впровадження в медичні установи завдяки своїй ефективності, безпеці та можливостям масштабування. Система стане надійним інструментом для управління медичними даними, підвищуючи якість медичного обслуговування та сприяючи розвитку сучасних медичних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Priya Naha. What is Health Information System: Definition, Types & Examples. URL: <https://www.softwaresuggest.com/blog/types-of-health-information-system-examples/> (дата звернення: 14.04.2024)
2. Мина Ж. Електронна медицина: поняття, форми та стратегія розвитку / Ж. Мина, Т. Гакало // Львів : Видавництво Львівської політехніки, 2015. 134 с. (дата звернення: 14.04.2024)
3. What is the Purpose of Health Information Systems. URL: <https://blog.payrollschedule.net/> (дата звернення: 14.04.2024)
4. Мазик О.В. Модернізація інформаційно-комунікаційного забезпечення діяльності медичних установ / Інноваційна економіка – 5-6'2020. С. 97-102. URL: <http://inneco.org/index.php/innecoen/article/view/657/726> (дата звернення: 19.04.2024)
5. Офіційний сайт інформаційної системи MedElement. URL: <https://medelement.com/en> (дата звернення: 20.04.2024)
6. Березовська І., Триус Ю., Медична інформаційна система «ДОКТОР ЕЛЕКС»: основи роботи: навчальний посібник. Львів: Ліга прес. 2018, С. 186. (дата звернення: 20.04.2024)
7. Назірова Т., Костенко О. (2017): Огляд моделей розвитку EHEALTH та наявних медичних інформаційних систем. Проблеми створення єдиного медико-інформаційного простору. *НВ НЛТУ України*. т. 27 (№10) 2017 <https://doi.org/10.15421/40271027> (дата звернення: 26.04.2024)
8. Офіційний сайт медичної інформаційної системи EmsiMed. URL: <https://emci.ua/> (дата звернення: 26.04.2024)
9. Берщанський Є., Клим Г. (Жовтень 2023): Інформаційна система адміністрування медичного закладу. *IEEE, 13-та Міжнародна конференція з надійних систем, послуг і технологій*, ст. 1-4. DOI: [10.1109/DESSERT61349.2023.10416537](https://doi.org/10.1109/DESSERT61349.2023.10416537) (дата звернення: 30.04.2024)

10. Xue T., Fu Q., Wang C., and Wang X.-Y. (Sept. 2017) A medical data sharing model via blockchain, *Acta Automatica Sinica*. (2017) 43, no. 9, pp.1555–1562 DOI: [10.16383/j.aas.2017.c160661](https://doi.org/10.16383/j.aas.2017.c160661) (дата звернення: 30.04.2024)
11. Швороб І. Б. Новий підхід до збереження медичних даних. *Науковий вісник НЛТУ України*. 2016. Вип. 26.4. С. 382–390. URL: https://nv.nltu.edu.ua/Archive/2016/26_4/61.pdf (дата звернення: 04.05.2024)
12. Юхимець В.О., Терентюк В.Г., Науринський В.А, Куц В.В, Яровий В.В, Єрьоміна А.С., Мельник О.Л., Лісневич О.С. (2016): Автоматизована медична інформаційна система. Впровадження та оптимальні рішення. URL: <http://www.ifp.kiev.ua/ftp1/original/2016/yukhymets2016-8> (дата звернення: 04.05.2024)
13. Sinha A., Patel A., Jagdish M. (March 2022): Application of Blockchain in Healthcare. *ICAITPR*. DOI: [10.1109/ICAITPR51569.2022.9844186](https://doi.org/10.1109/ICAITPR51569.2022.9844186) (дата звернення: 10.05.2024)
14. P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom. (Jul. 2018) FHIRChain: Applying blockchain to securely and scalably share clinical data,” *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278. doi.org/10.1016/j.csbj.2018.07.004 (дата звернення: 10.05.2024)
15. Kuo T.-T., Kim H.-E., and Ohno-Machado L. (Sept. 2017): Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 2017, pp. 1211–1220 <https://doi.org/10.1093/jamia/ocx068> (дата звернення: 13.05.2024)
16. Ekblaw A. , Azaria A. , Halamka J., Lippman A. (Aug. 2016): A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data. *Proceedings of IEEE open & big data conference, 2016* (дата звернення: 13.05.2024)
17. Ісаєв Д. (Лютий 2018): Інтелектуальний аналіз даних в медицині. *Науковий потенціал* URL: <https://int-konf.org/en/2016/naukovij-potentsial-2016-16-18-03-2016/1230-isaev-d-v-intelektualnij-analiz-danikh-v-meditsini>, (дата звернення: 20.05.2024)

18. Dilawar N., Rizwan M., Ahmad F., Akram S. (2019): Blockchain: Securing Internet of Medical Things (IoMT). *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, 2019. pp. 82-88. URL: <http://dx.doi.org/10.14569/IJACSA.2019.0100110> (дата звернення: 20.05.2024)
19. Devi T., Bangaru Kamatchi S.; Deepa N. (Jan. 2023) Enhancing the Security for Healthcare Data using Blockchain Technology *ICCCI*, pp. 1-7. DOI: [10.1109/ICCCI56745.2023.10128545](https://doi.org/10.1109/ICCCI56745.2023.10128545) (дата звернення: 23.05.2024)
20. Matthew N.O. Sadiku, Kelechi Eze, Sarhan M. Musa. (May 2018) Block Chain Technology in Healthcare. *IJASRE*. vol. 4 no. 5 May (2018), pp. 5-8 DOI: [10.31695/IJASRE.2018.32723](https://doi.org/10.31695/IJASRE.2018.32723), (дата звернення: 28.05.2024)
21. Yue X., Wang H., Jin D., Li M., and Jiang W. (Aug. 2016): Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J Med Syst*, vol. 40, no. 10, p. 218, Aug. 2016, DOI: [10.1007/s10916-016-0574-6](https://doi.org/10.1007/s10916-016-0574-6) (дата звернення: 28.05.2024)
22. Mackey T., Kuo T., Gummadi B., Clauson K., Church G., Grishin D., Obbad K., Barkovich R. (March 2019): 'Fit-for-purpose?' Challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Medicine*, No. 68. doi.org/10.1186/s12916-019-1296-7 (дата звернення: 03.06.2024)
23. Petrenko A., Kyslyi R., PysmenI. (2018): Designing security of personal data in distributed health care platform, *Technology audit and production reserves*, vol. 4, no. 2(42) (2018) DOI: [10.15587/2312-8372.2018.141299](https://doi.org/10.15587/2312-8372.2018.141299) (дата звернення: 03.06.2024)
24. Chen Y., Ding S., Xu Z., Zheng H., and YangS. (Nov. 2018): Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J Med Syst*, vol. 43, no. 1, Nov. 2018, DOI: [10.1007/s10916-018-1121-4](https://doi.org/10.1007/s10916-018-1121-4) (дата звернення: 08.06.2024)
25. Sun J., Ren L., Wang S., Yao X. (Oct. 2020): A blockchain-based framework for electronic medical records sharing with fine-grained access control. *PubMed. eCollection* 2020. vol.15, no.10 (2020) DOI: [10.1371/journal.pone.0239946](https://doi.org/10.1371/journal.pone.0239946) (дата звернення: 08.06.2024)
26. Smitha Mohan M, Sujihelen L. (Sept. 2023): An efficient chain code for access control in hyper ledger fabric healthcare system. *e-Prime - Advances in Electrical*

Engineering, Electronics and Energy, vol. 5, September 2023, 100204
<https://doi.org/10.1016/j.prime.2023.100204> (дата звернення: 15.06.2024)

27. Ensuring Effective Healthcare Data Management: The Key Pillars, Benefits, and Challenges (31 Jan 2024) URL: <https://spsoft.com/tech-insights/effective-health-data-management/> (дата звернення: 15.06.2024)

28. Puneeth R., Parthasarathyb G. (May 2023): Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System. *IJE*, Vol. 36, No. 05, (May 2023), pp. 925-933. doi: [10.5829/ije.2023.36.05b.09](https://doi.org/10.5829/ije.2023.36.05b.09) (дата звернення: 23.06.2024)

29. Haddad, A., Habaebi M., Islam M., and Zabidi S. (Sept. 2021): Blockchain for Healthcare Medical Records Management System with Sharing Control. *2021 IEEE 7th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), Bandung, Indonesia, 2021: pp. 33–34. DOI: [10.1109/ICSIMA50015.2021.9526301](https://doi.org/10.1109/ICSIMA50015.2021.9526301)* (дата звернення: 12.07.2024)

30. Khekare G., Ghugare S., Khatri R., Majumder G. and Khekare U. (Apr. 2024): Blockchain Powered Integrated Health Profile and Record Management System for Seamless Consultation Leveraging Unique Identifiers. *Second International Conference on Emerging Trends in Information Technology and Engineering*, Vellore, India, 2024, pp. 1-9, DOI: [10.1109/ic-ETITE58242.2024.10493266](https://doi.org/10.1109/ic-ETITE58242.2024.10493266) (дата звернення: 21.07.2024)

31. Azaria A, Ekblaw A, Vieira T, Lippman A. (Aug. 2016): Medrec: Using blockchain for medical data access and permission management. *IEEE 2nd International Conference on Open and Big Data (OBD) Vienna, Austria, 2016 Aug; pp. 25–30. DOI: [10.1109/OBD.2016.11](https://doi.org/10.1109/OBD.2016.11)* (дата звертання: 10.08.24)

32. Iang S.; Cao J.; Wu H.; Yang Y.; Ma M.; He J. (Apr. 2018): Blochie: A blockchain-based platform for healthcare information exchange. *IEEE International Conference on Smart Computing (SMARTCOMP)*, pp.18–20 (2018). DOI: [10.1109/SMARTCOMP.2018.00073](https://doi.org/10.1109/SMARTCOMP.2018.00073) (дата звертання: 16.08.24)

33. Vyapi (Jan. 2023): General Data Protection Regulation (GDPR): Beginner's Guide

URL: <https://www.linkedin.com/pulse/general-data-protection-regulation-gdpr-beginners-guide-/> (дата звертання: 08.09.24)

34. Agbo C., Mahmoud Q., Eklund J. (Apr. 2019): Blockchain Technology in Healthcare: a Systematic Review. *Healthcare*, vol. 7(2), p. 56. doi.org/10.3390/healthcare7020056 (дата звертання: 11.09.24)

35. Uddin M., Memon M., Memon I., Ali I., Memon J., Abdelhaq M., Alsaqour R. (Febr. 2021): Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records/ *Comput. Mater. Continua*, vol.68 (2), DOI: [10.32604/cmc.2021.015354](https://doi.org/10.32604/cmc.2021.015354) (дата звертання: 11.09.24)

36. Tarasenko E. (Febr. 2023): Benefits of Blockchain Hyperledger Fabric. *Merehead* URL: <https://merehead.com/blog/benefits-of-blockchain-hyperledger-fabric/> (дата звертання: 14.09.24)

37. Antwi M., Adnane A., Ahmad F., Hussain R., M.H. ur Rehman, Kerrache C. (March 2021): The Case of Hyperledger Fabric as a Blockchain Solution for Healthcare Applications. *Blockchain Research and Applications*, vol. 2 (1), p. 100012. doi.org/10.1016/j.bcra.2021.100012 (дата звертання: 14.09.24)

38. Siyal A., Junejo A., Zawish M., Ahmed K., Khalil A., Soursou G. (Jan 2019): Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography* 3(1), p3. <https://doi.org/10.3390/cryptography3010003> (дата звертання: 19.09.24)

39. ZhengZ., Xie S., Dai H., Chen X., Wang H. (Sep. 2017): An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Big Data (BigData Congress)*, *IEEE International Congress on Big Data*, vol. 85 DOI: [10.1109/BigDataCongress.2017.85](https://doi.org/10.1109/BigDataCongress.2017.85) (дата звертання: 19.09.24)

40. Liu X., Wang Z., Jin C., Li F., Li G. (March 2016): A Blockchain-Based Medical Data Sharing and Protection Scheme. *IEEE Access* vol. 4, p. 99, <https://doi.org/10.1109/ACCESS.2019.2937685> (дата звертання: 22.09.24)

41. Sookhak M., Jabbarpour M., Safa N., Richard F. Y. (March 2021): Blockchain and Smart Contract for Access Control in Healthcare: A Survey, Issues and Challenges, and

Open Issues. *Journal of Network and Computer Applications*, vol. 178, pp. 102950. doi.org/10.1016/j.jnca.2020.102950 (дата звертання: 22.09.24)

42. Novriansyah N (May 2024): Demystifying Membership Service Provider (MSP) in Hyperledger Fabric, *Novai- Hyperledger Fabric*, URL:

<https://medium.com/novai-hyperledger-fabric-101/demystifying-membership-service-provider-msp-in-hyperledger-fabric-fc9630e4d16c> (дата звертання: 24.09.24)

43. Wang S., Yuan Y., Wang X., Li J., Qin R., Wang F-Y. (Jun. 2018): An Overview of Smart Contract: Architecture, Applications, and Future Trends. in *Proc. IEEE Intelligent Vehicles Symposium*, vol. 4, pp. 108–113, URL: <https://sci-hub.se/downloads/2020-09-02/45f9/wang2018.pdf> (дата звертання: 24.09.24)

44. Dagher G., Mohler J., Milojkovic M., Marella P. (May 2018): Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustainable Cities and Society*, vol.39, pp. 283–297, doi.org/10.1016/j.scs.2018.02.014 (дата звертання: 24.09.24)

45. Shahnaz A, Qamar U, Khalid A (Oct. 2019): Using Blockchain for Electronic Health Records. *IEEE Access*, vol. 7, pp. 5-8. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8863359> (дата звертання: 26.09.24)

46. Daraghmi, E.-Y., Daraghmi, Y.-A., Yuan, S.-M. (Nov. 2019): MedChain: a Design of Blockchain-Based System for Medical Records Access and Permissions Management. *IEEE Access*, vol. 7, pp. 164595 - 164613. DOI: [10.1109/ACCESS.2019.2952942](https://doi.org/10.1109/ACCESS.2019.2952942) (дата звертання: 26.09.24)

47. Zhang P., White J., Schmidt D., Lenz G., Rosenbloom S. (Jul. 2018), FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data, *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, DOI: [10.1016/j.csbj.2018.07.004](https://doi.org/10.1016/j.csbj.2018.07.004) (дата звертання: 30.10.24)

48. Angrish A, Craver B, Hasan M, Starly B (2018): A Case Study for Blockchain in Manufacturing: “FabRec”: A Prototype for Peer-to-Peer Network of Manufacturing Nodes. *Procedia Manufacturing*, 26: pp.1180–1192 DOI: [org/10.1016/j.promfg.2018.07.154](https://doi.org/10.1016/j.promfg.2018.07.154) (дата звертання: 30.10.24)

49. Kaur J., Rani R., Kalra N. (2021): Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records. *Concurrency and Computation: Practice and Experience*, 33(20), pp. 22-24, DOI: [org/10.1002/cpe.6369](https://doi.org/10.1002/cpe.6369) (дата звертання: 01.11.24)
50. Zlatolas N., Welzer.L., Lhotska T. (Apr. 2024): Data breaches in healthcare: security mechanisms for attack mitigation. *Cluster Comput* vol. 27, pp. 8639–8654, (2024) <https://doi.org/10.1007/s10586-024-04507-2> (дата звертання: 04.11.24)
51. Yang G, Li C, Marstein K. (2019): A blockchain-based architecture for securing electronic health record systems. *Concurrency Computat Pract Exper*, 33(14) DOI:[org/10.1002/cpe.5479](https://doi.org/10.1002/cpe.5479) (дата звертання: 04.11.24)
52. Chen et al., (2021): Data Access Control Based on Blockchain in Medical Cyber Physical Systems. *Secur. Commun. Networks*. DOI: [10.1155/2021/3395537](https://doi.org/10.1155/2021/3395537) (дата звертання: 07.11.24)
53. Riveros A., Iglesias J., (Aug, 2024): Exploring the Key Attributes of Blockchain for Medical Data Protection: A Systematic Review. *Innovation and Software*, 5(1) DOI: [10.1007/s10586-024-04507-2](https://doi.org/10.1007/s10586-024-04507-2) (дата звертання: 07.11.24)
54. Lee S., Kim J., Kwon Y., Kim T., and Cho S.: Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study, *J. Med. Internet Res.*, 2022, vol. 24, no. 3. DOI: [10.2196/29108](https://doi.org/10.2196/29108) (дата звертання: 08.11.24)
55. Eberhart A.: Release Management in the Low Code World (Oct 24, 2022) URL: <https://dashjoin.medium.com/release-management-in-the-low-code-world-ae1683eba431>. (дата звертання: 10.11.24)
56. Li, H., Zhu, L., Shen, M. (Jun. 2018): Blockchain-Based Data Preservation System for Medical Data. *J Med Syst* vol. 42, no.141 (2018). <https://doi.org/10.1007/s10916-018-0997-3> (дата звертання: 10.11.24)
57. Kosba A., Miller A., Shi E., Wen Z. and Papamanthou S. (May 2016): Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, 2016 *IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016, pp. 839-858, DOI: [10.1109/SP.2016.55](https://doi.org/10.1109/SP.2016.55) (дата звертання: 10.11.24)

ДОДАТОК А

```
from django.db.models.signals import post_save
from django.dispatch import receiver
from .models import MedicalRecord, MedicalRecordHashHistory
@receiver(post_save, sender=MedicalRecord)
def update_blockchain_chain(sender, instance, **kwargs):
    records = MedicalRecord.objects.filter(patient=instance.patient).order_by('visit_date',
'id')
    previous_hash = ""
    for record in records:
        new_hash = create_blockchain_record(
            record.patient.id,
            record.diagnosis,
            record.visit_date,
            record.analysis_results,
            record.complaint,
            record.treatment,
            previous_hash
        )
        if record.blockchain_hash != new_hash:
            if record.blockchain_hash:
                MedicalRecordHashHistory.objects.create(
                    medical_record=record,
                    blockchain_hash=record.blockchain_hash
                )
            record.blockchain_hash = new_hash
            record.save(update_fields=['blockchain_hash'])
            previous_hash = new_hash
```

ДОДАТОК Б

Технічна документація та опис архітектури

1. Загальна архітектура системи

Інформаційна система медичного закладу розроблена з використанням фреймворку Django і бази даних MySQL. Основна мета системи — забезпечити ефективне управління даними пацієнтів та їх медичними записами, із забезпеченням високого рівня безпеки та надійності завдяки застосуванню блокчейн-технології.

2. Використані технології та інструменти

- Мова програмування: Python
- Фреймворк: Django
- База даних: MySQL
- Сервер середовища розробки: вбудований сервер Django
- Редактор коду: PyCharm

3. Структура проєкту

Проект організовано у вигляді основного каталогу `medical_blockchain`, що містить додаток `patients`. Основні функціональні модулі розподілені між такими файлами:

- `settings.py` — конфігураційний файл, що налаштовує проєкт для роботи з базою даних, авторизацією, шаблонами тощо.
- `urls.py` — файл, що відповідає за маршрутизацію запитів.
- Каталог `templates` — містить HTML-шаблони для веб-інтерфейсу користувача.
- Каталог `patients` — додаток для управління пацієнтами та медичними записами.

4. Структура бази даних

База даних складається з таких основних таблиць:

- `auth_group` — таблиця для зберігання груп користувачів.
- `auth_group_permissions` — таблиця, що містить зв'язок між групами користувачів та їхніми дозволами.
- `auth_permission` — таблиця дозволів у системі.

- `auth_user` — таблиця користувачів системи.
- `patients_patient` — основна таблиця, де зберігаються дані про пацієнтів (ім'я, прізвище, дата народження, контактна інформація).
- `patients_medicalrecord` — таблиця медичних записів, що пов'язує кожен запис з пацієнтом, містить інформацію про діагноз і дату запису.

5. Опис таблиць пацієнтів і медичних записів

Таблиця `patients_patient`

- Поле `id` — унікальний ідентифікатор пацієнта.
- Поле `first_name` — ім'я пацієнта.
- Поле `last_name` — прізвище пацієнта.
- Поле `birth_date` — дата народження.
- Поле `contact_info` — контактна інформація.

Таблиця `patients_medicalrecord`

- Поле `id` — унікальний ідентифікатор запису.
- Поле `patient_id` — зовнішній ключ, що пов'язує запис із пацієнтом.
- Поле `diagnosis` — діагноз пацієнта.
- Поле `record_date` — дата медичного запису.

6. Взаємозв'язок між таблицями

- Між таблицями `patients_patient` і `patients_medicalrecord` реалізовано зв'язок "один до багатьох". Кожен пацієнт може мати кілька медичних записів, але кожен запис належить лише одному пацієнту.

7. Маршрутизація

У проєкті налаштовано такі маршрути:

- `/patients` — сторінка зі списком пацієнтів.
- `/patients/<id>` — детальна інформація про конкретного пацієнта.
- `/patients/add` — сторінка для створення нового пацієнта.
- `/patients/<id>/add_record` — сторінка для додавання медичного запису пацієнту.

8. Безпека

- Авторизація та аутентифікація — для доступу до адмін-панелі необхідні дані облікового запису.
- Хешування даних — використовуються утиліти для хешування медичних записів з метою забезпечення їхньої цілісності та захисту від змін, що є основою для блокчейн-технології.

9. Тестування

Система пройшла модульне та навантажувальне тестування:

- Модульне тестування — перевірка функціональності додавання пацієнтів, медичних записів та відображення даних.
- Навантажувальне тестування — тестування продуктивності при збільшенні кількості записів у базі даних.

Архітектура системи орієнтована на забезпечення зручного інтерфейсу користувача, ефективного управління медичними даними та високого рівня безпеки. Система є стабільною та готовою до використання, з можливістю масштабування у разі збільшення кількості даних та користувачів.

ДОДАТОК В

Приклад інтеграції з даними з інших інформаційних систем

Інтеграційна система	Опис інтеграції	Технології / Протоколи	Переваги інтеграції
Електронна медична картка (EMR)	Синхронізація даних про пацієнтів, включаючи історію хвороб, рецепти та результати аналізів	HL7, FHIR, REST API	Швидкий доступ до повної медичної історії пацієнта
Лабораторна інформаційна система (LIS)	Обмін результатами лабораторних досліджень, включаючи аналізи крові, сечі та інші біохімічні показники	SOAP, HL7, REST API	Оперативне оновлення даних лабораторних досліджень
Система обліку препаратів (PMS)	Інтеграція даних щодо медикаментів, їх доступності та видачі пацієнтам	FHIR, XML, API	Контроль за доступністю та обліком медпрепаратів
Теле-медична платформа	Передача даних пацієнтів для проведення дистанційних консультацій та моніторингу	WebRTC, REST API, HTTPS	Розширення доступу до медичних послуг
Система управління зображеннями (PACS)	Зберігання та доступ до рентгенівських, МРТ і КТ зображень	DICOM, HL7, API	Зручний доступ до медичних зображень

Платформа моніторингу життєвих показників	Передача даних з медичних пристроїв та сенсорів, що контролюють стан пацієнта в реальному часі	IoT, MQTT, HTTP	Моніторинг стану здоров'я пацієнта в реальному часі
Національна база даних пацієнтів	Обмін даними з національними медичними реєстрами для забезпечення єдиного доступу до інформації	HL7, FHIR, REST API, Blockchain	Забезпечення єдиної медичної інформації в масштабах країни

Ця таблиця описує типові варіанти інтеграції медичної блокчейн-системи з іншими системами, забезпечуючи зручний доступ до критично важливої інформації, необхідної для ефективного лікування та догляду за пацієнтами.

ДЕКЛАРАЦІЯ

про дотримання академічної доброчесності

Я, Курдупов Олексій Леонідович, Освітня програма «Комп'ютерні технології обробки даних», Моделювання інформаційної системи медичного закладу на основі технології блокчейн.,

Повністю вказується ПІБ та статус (освітня (освітньо-наукова) програма – для здобувачів вищої освіти, назва кваліфікаційної роботи)

що нижче підписалась/підписався, розуміючи та підтримуючи загальновизнані засади справедливості, доброчесності та законності,

ЗОБОВ'ЯЗУЮСЬ:

дотримуватися принципів та правил академічної доброчесності, що визначені законодавством України, локальними нормативними актами Донецького національного університету імені Василя Стуса, положеннями, правилами, умовами, визначеними іншими суб'єктами, та не допускати їх порушення.

ПІДТВЕРДЖУЮ:

що мені відомі положення статті 42 Закону України «Про освіту»;
що у даній роботі не представляла/представляв чийсь роботи повністю або частково як свої власні. Там, де я скористалася/скористався працею інших, я зробила/зробив відповідні посилання на джерела інформації;
що дана робота не передавалась іншим особам і подається вперше, не порушує авторських та суміжних прав закріплених статтями 21-25 Закону України «Про авторське право та суміжні права», а дані та інформація не отримувались в недозволений спосіб.

УСВІДОМЛЮЮ:

що ця робота може бути перевірена університетом на плагіат або інші порушення академічної доброчесності, в тому числі з використанням спеціалізованих сервісів;
що у разі порушення академічної доброчесності, до мене можуть бути застосовані процедури, передбачені законодавством України та Кодексом академічної доброчесності та корпоративної етики Донецького національного університету імені Василя Стуса, іншими локальними нормативними актами університету, та я можу бути притягнута/притягнутий до академічної відповідальності.

29.11.2024

(дата)

(підпис)