Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерних наук

Кафедра програмної інженерії

СПЕЦИФІКАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Програмна система для зберігання та захисту медичних даних на основі блокчейн-технології

Студент гр. ПЗПІ-21-8 Сюсько В.В.

# 2025 р.

# ЗМІСТ

[ВСТУП](#_heading=h.tk091npw4abb) 2

[1.1 Огляд продукту](#_heading=h.n0ls3dtxwbwa) 2

[1.2 Мета](#_heading=h.zfmurkbqozq) 2

[1.3 Межі](#_heading=h.2bzpkmbh5gdm) 3

[1.4 Посилання](#_heading=h.6qdtwc2adpgo) 3

[1.5 Означення та абревіатури](#_heading=h.qrf41gt282h8) 4

[2 ЗАГАЛЬНИЙ ОПИС](#_heading=h.b1kvlou36sx8) 6

[2.1 Перспективи продукту](#_heading=h.2qrl1m17kkzp) 6

[2.2 Функції продукту](#_heading=h.dj1ykwx4u3qc) 6

[2.3 Характеристики користувачів](#_heading=h.lk28lorw1oka) 7

[3 КОНКРЕТНІ ВИМОГИ](#_heading=h.ru3n3kn9961) 11

[3.1 Вимоги до зовнішніх інтерфейсів](#_heading=h.pdyvmde2h35e) 11

[3.2 Властивості програмного продукту](#_heading=h.ka7nqrtx184b) 13

[3.3 Атрибути програмного продукту](#_heading=h.6qb9vqg3q770) 16

[3.4 Вимоги бази даних](#_heading=h.kv1xltfn4xgm) 18

[3.5 Інші вимоги](#_heading=h.shvsizhouji9) 19

[4 ДОДАТКОВІ МАТЕРІАЛИ](#_heading=h.aikdysnvs4wb) 21

[4.1 UML діаграми прецедентів](#_heading=h.8bspjlkqw6qs) 21

# ВСТУП

## 1.1 Огляд продукту

Програмна система для зберігання та захисту медичних даних на основі блокчейн-технології є децентралізованим додатком (DApp), розробленим для вирішення проблеми верифікації фактичного надання медичних послуг в умовах української системи охорони здоров'я з принципом фінансування "гроші йдуть за пацієнтом".

Система забезпечує механізм обов'язкового підтвердження пацієнтами всіх медичних записів, створених медичними працівниками, що гарантує прозорість та достовірність медичних даних. Використання блокчейн-технології Ethereum забезпечує незмінність записів після їх фіксації в системі та повну відстежуваність всіх операцій.

Продукт складається з смарт-контракту, розгорнутого в блокчейні Ethereum, та веб-додатку з інтуїтивним користувацьким інтерфейсом, що забезпечує взаємодію різних категорій користувачів із системою через браузерний гаманець MetaMask.

## 1.2 Мета

Метою створення даної специфікації є визначення повного набору вимог до програмної системи для зберігання та захисту медичних даних на основі блокчейн-технології. Система має забезпечити надійне зберігання та захист медичних даних пацієнтів, впровадити механізм підтвердження медичних записів пацієнтами, запобігти створенню фіктивних медичних записів для отримання необґрунтованого фінансування з бюджету НСЗУ, підвищити прозорість медичних процесів та рівень довіри між пацієнтами та медичними працівниками, а також забезпечити повну відповідність сучасним вимогам щодо захисту персональних даних. Специфікація призначена для розробників, тестувальників, архітекторів системи та інших зацікавлених сторін, які беруть участь у процесі створення та впровадження системи.

## 1.3 Межі

Система включає функції реєстрації та авторизації користувачів через Ethereum гаманці, управління ролями користувачів (адміністратор, медичний працівник, пацієнт), створення медичних записів медичними працівниками, підтвердження або відхилення медичних записів пацієнтами, зберігання всіх медичних записів у блокчейні Ethereum, відображення історії медичних записів з відповідними змінами, пошук та фільтрацію медичних записів, підтримку української та англійської мов інтерфейсу, адміністрування системи та управління користувачами. Система не включає інтеграцію з існуючими медичними інформаційними системами на етапі початкового впровадження, автоматичне створення медичних записів з медичного обладнання, обробку платежів за медичні послуги, генерацію звітності для регулюючих органів, резервне копіювання даних поза блокчейном та підтримку інших мов окрім української та англійської.

## 1.4 Посилання

* Medicalchain - блокчейн-платформа для зберігання медичних записів з контролем доступу пацієнтами через смарт-контракти;
* Chronicled - децентралізована платформа для управління ланцюгами постачання медичних препаратів та забезпечення прозорості медичних даних;
* MedRec - система медичних записів на базі блокчейн-технології для безпечного обміну даними між медичними закладами;
* Solve.Care - блокчейн-платформа для координації взаємодії між пацієнтами, лікарями та медичними закладами;
* Guardtime - enterprise-рішення для забезпечення цілісності та автентичності медичних даних через криптографічні методи;
* HelsiMed - українська медична інформаційна система для управління електронними медичними картками;
* МІС ЕМСІМЕД - медична інформаційна система для автоматизації процесів у медичних закладах України;
* МедЕйр - платформа для управління медичними записами та взаємодії лікарів з пацієнтами в Україні.

## 1.5 Означення та абревіатури

Блокчейн – розподілена база даних, що складається з ланцюжка блоків, кожен з яких містить криптографічний хеш попереднього блока, часову мітку та дані транзакцій.

DApp (Decentralized Application) – децентралізований додаток, що працює на основі блокчейн-технології.

Ethereum – децентралізована платформа для створення та виконання смарт-контрактів.

Gas – одиниця виміру обчислювальних ресурсів, необхідних для виконання операцій в блокчейні Ethereum.

MetaMask – браузерний гаманець для взаємодії з блокчейном Ethereum.

НСЗУ – Національна служба здоров'я України.

Пацієнт – фізична особа, яка отримує медичні послуги та має право підтверджувати або відхиляти медичні записи.

Pending Record – медичний запис, що очікує підтвердження від пацієнта.

Смарт-контракт – програма, що виконується в блокчейні та автоматично виконує умови договору.

ЕСОЗ – електронна система охорони здоров'я.

UI/UX – користувацький інтерфейс/користувацький досвід.

Web3 – нове покоління інтернету, побудоване на блокчейн-технологіях.

АРІ – програмний інтерфейс застосування (Application Programming Interface).

JSON – формат обміну даними (JavaScript Object Notation).

Хеш – результат криптографічної хеш-функції, що використовується для забезпечення цілісності даних.

# 

# 

# 2 ЗАГАЛЬНИЙ ОПИС

## 2.1 Перспективи продукту

Програмна система для зберігання та захисту медичних даних є самостійним програмним продуктом, побудованим на основі трирівневої архітектури з використанням блокчейн-технології Ethereum. Система функціонує як децентралізований додаток (DApp), що забезпечує незалежність від централізованих серверів та гарантує незмінність збережених даних.

Архітектура системи складається з трьох основних рівнів: рівня доступу до даних, реалізованого через смарт-контракт MedicalRecords у блокчейні Ethereum; рівня бізнес-логіки, що містить JavaScript-модулі для взаємодії між клієнтським інтерфейсом та смарт-контрактом; презентаційного рівня, реалізованого за допомогою React.js з компонентним підходом до розробки користувацького інтерфейсу.

Система інтегрується з браузерним гаманцем MetaMask для автентифікації користувачів та підписання транзакцій. Взаємодія з блокчейном здійснюється через бібліотеку ethers.js, що забезпечує надійне з'єднання з мережею Ethereum. Управління станом додатку реалізовано через Redux з використанням селекторів для ефективного обчислення похідного стану.

Система підтримує роботу в різних блокчейн-мережах: локальній мережі Hardhat для розробки та тестування, тестових мережах Goerli та Mumbai для попереднього тестування, основній мережі Ethereum для продуктивного використання. Конфігурація системи дозволяє легко перемикатися між мережами без зміни основного коду.

## 2.2 Функції продукту

Система надає диференційований функціонал відповідно до ролей користувачів. Основні функції включають управління користувачами з підтримкою чотирьох типів ролей: адміністратор, лікар, пацієнт та незареєстрований користувач.

Функції для адміністраторів охоплюють повне управління системою, включаючи призначення ролі лікаря користувачам, перегляд та управління всіма користувачами системи, моніторинг активності системи через журнали подій, аналіз статистики використання системи, експорт даних для резервного копіювання, вирішення конфліктних ситуацій з підтвердженням записів.

Лікарі мають можливість створювати нові медичні записи для зареєстрованих пацієнтів, переглядати створені ними записи та їх статус підтвердження, редагувати медичні записи, що ще не підтверджені пацієнтами, видаляти медичні записи з відповідним маркуванням у системі, здійснювати пошук та фільтрацію записів за різними критеріями, переглядати всі медичні записи в системі для аналізу.

Пацієнти можуть реєструватися в системі як пацієнти через власний Ethereum гаманець, переглядати всі медичні записи, створені для них, підтверджувати фактичне надання медичних послуг через відповідний інтерфейс, відхиляти медичні записи з зазначенням причини відхилення, переглядати історію всіх змін у власних медичних записах, управляти особистими даними та налаштуваннями конфіденційності.

Система забезпечує створення pending записів, які потребують підтвердження пацієнта перед переведенням до основної бази медичних записів. Механізм підтвердження включає сповіщення пацієнтів про нові записи, інтерфейс для перегляду деталей записів, можливість затвердження або відхилення записів, автоматичне переведення затверджених записів до основної системи.

## 2.3 Характеристики користувачів

Система розрахована на три основні категорії користувачів з різними рівнями технічної підготовки та функціональними потребами.

Адміністратори системи є технічно підготовленими фахівцями у сфері інформаційних технологій, що мають досвід роботи з блокчейн-технологіями та розуміння принципів криптографії. Вони відповідальні за налаштування та підтримку системи, управління користувачами, моніторинг безпеки та вирішення технічних проблем. Адміністратори повинні мати базові знання мов програмування, розуміння архітектури децентралізованих додатків та досвід роботи з Ethereum.

Медичні працівники (лікарі) є основними користувачами системи з професійною медичною освітою та досвідом роботи у сфері охорони здоров'я. Вони мають базовий рівень комп'ютерної грамотності та готовність до освоєння нових технологій. Лікарі використовують систему для документування медичних послуг, ведення електронних медичних карток пацієнтів, взаємодії з колегами та забезпечення якості медичної допомоги. Від них очікується розуміння важливості конфіденційності медичних даних та дотримання етичних норм.

Пацієнти є кінцевими бенефіціарами системи з різним рівнем технічної підготовки – від початківців до досвідчених користувачів цифрових технологій. Вони зацікавлені у контролі над власними медичними даними, прозорості медичних процесів та захисті персональної інформації. Пацієнти потребують простого та інтуїтивного інтерфейсу, чіткої інформації про медичні записи та зрозумілих інструкцій для підтвердження або відхилення записів.

2.4 Загальні обмеження

Система функціонує в рамках технологічних обмежень блокчейн-платформи Ethereum, що впливає на швидкість обробки транзакцій та вартість операцій. Час підтвердження транзакцій залежить від завантаженості мережі та може становити від декількох секунд до декількох хвилин. Вартість виконання операцій (gas fees) змінюється відповідно до попиту на обчислювальні ресурси мережі.

Законодавчі обмеження включають необхідність дотримання вимог Закону України "Про захист персональних даних", Закону України "Про електронні документи та електронний документообіг", нормативних актів Міністерства охорони здоров'я України щодо ведення медичної документації. Система повинна забезпечувати відповідність міжнародним стандартам захисту медичних даних та принципам конфіденційності.

Технічні обмеження визначаються необхідністю наявності сучасного веб-браузера з підтримкою JavaScript та можливістю встановлення MetaMask, стабільного інтернет-з'єднання для взаємодії з блокчейн-мережею, достатньої кількості ETH на гаманці користувача для оплати транзакцій. Система вимагає базового розуміння принципів роботи з криптовалютними гаманцями від користувачів.

Операційні обмеження включають необхідність регулярного резервного копіювання конфігураційних файлів та приватних ключів, моніторинг стану блокчейн-мережі та своєчасне реагування на можливі збої, періодичне оновлення програмного забезпечення відповідно до змін у блокчейн-платформі.

2.5 Припущення й залежності

Система базується на припущенні стабільного функціонування блокчейн-мережі Ethereum та відсутності критичних вразливостей у протоколі. Передбачається, що користувачі мають базові навички роботи з комп'ютером та готовність до навчання використанню блокчейн-технологій.

Критичні залежності включають стабільність та безпеку мережі Ethereum, доступність та надійність браузерного гаманця MetaMask, постійну доступність інтернет-з'єднання для взаємодії з блокчейном, відсутність кардинальних змін у законодавстві щодо використання блокчейн-технологій у медицині.

Технологічні залежності охоплюють підтримку JavaScript та Web3 технологій у веб-браузерах, стабільність API інтерфейсів використовуваних бібліотек (React.js, ethers.js, Redux), сумісність з майбутніми версіями Ethereum та можливими оновленнями протоколу.

Організаційні припущення включають готовність медичних закладів до впровадження блокчейн-технологій, наявність технічної підтримки для навчання користувачів, достатнє фінансування для покриття витрат на транзакції у блокчейні, підтримку ініціативи з боку регулюючих органів охорони здоров'я.

# 

# 3 КОНКРЕТНІ ВИМОГИ

## 3.1 Вимоги до зовнішніх інтерфейсів

Система надає веб-інтерфейс, який працює в сучасних браузерах з підтримкою JavaScript ES6+ та Web3 технологій. Інтерфейс має адаптивний дизайн і забезпечує коректне відображення на пристроях з різними розмірами екранів – від настільних комп'ютерів до смартфонів.

Навігаційна панель є ключовим елементом інтерфейсу та містить назву системи "Medical Records DApp", поточний баланс користувача в криптовалюті ETH, скорочену адресу підключеного Ethereum гаманця у форматі 0x1234...5678, візуальне відображення поточної ролі користувача з кольоровими індикаторами (адміністратор – синій, лікар – зелений, пацієнт – помаранчевий), кнопку підключення MetaMask гаманця для неавторизованих користувачів та перемикач мови між українською та англійською з відповідними прапорцями.

Головне меню системи структуровано за функціональним призначенням і включає розділ "Форма" для створення нових медичних записів лікарями, розділ "Дані" для перегляду медичних записів залежно від ролі користувача, розділ "Записи на розгляді" для роботи з pending записами, які очікують підтвердження пацієнтами, розділ "Панель адміністратора" для управління користувачами та системою, розділ "Реєстрація пацієнта" для незареєстрованих користувачів, які хочуть стати пацієнтами системи.

Форма створення медичного запису є центральним інструментом для лікарів і містить поле для введення Ethereum адреси пацієнта з автоматичною валідацією формату та перевіркою статусу реєстрації, поле імені пацієнта з підтримкою кирилиці та латиниці, числове поле віку з обмеженням від 0 до 150 років, випадаючий список статі з варіантами "чоловіча", "жіноча" та "інше", текстове поле групи крові з валідацією стандартних груп крові, поле алергій для детального опису алергічних реакцій, поле діагнозу для медичного висновку, поле призначеного лікування з описом рекомендованої терапії. Форма також включає блок швидкого вибору з тестовими адресами пацієнтів для зручності розробки та тестування, динамічне відображення статусу валідації кожного поля з кольоровими індикаторами та інформативними підказками.

Таблиця медичних записів є адаптивною та відображає різний набір колонок залежно від ролі користувача. Для пацієнтів показуються ID запису, дата створення, ім'я, вік, стать, група крові, алергії, діагноз та лікування. Для лікарів додатково відображаються адреси пацієнта та лікаря, що створив запис, а також кнопки для видалення записів. Для адміністраторів доступна повна інформація з додатковими можливостями управління. Таблиця підтримує сортування за будь-якою колонкою, пошук за ключовими словами, фільтрацію за датою створення, діагнозом або іменем пацієнта.

Система не потребує спеціального апаратного забезпечення і працює на звичайних комп'ютерах, ноутбуках, планшетах та смартфонах з операційними системами Windows, macOS, Linux. Єдиною вимогою є наявність стабільного підключення до інтернету для взаємодії з блокчейн-мережею Ethereum.

Програмний інтерфейс системи базується на взаємодії з Ethereum через браузерний гаманець MetaMask, який забезпечує Web3 Provider API. Система використовує стандартні методи eth\_requestAccounts для запиту доступу до облікових записів користувача, eth\_getBalance для отримання поточного балансу, eth\_sendTransaction для відправки транзакцій у блокчейн, eth\_call для виклику read-only функцій смарт-контракту без витрачання газу.

Взаємодія зі смарт-контрактом MedicalRecords здійснюється через широкий набір методів, включаючи createPendingRecord для створення записів, що потребують підтвердження пацієнтом, approveRecord та rejectRecord для підтвердження або відхилення записів пацієнтами з можливістю додавання коментарів, getMyRecords для отримання списку особистих записів пацієнта, getAllRecords для отримання всіх записів у системі лікарями та адміністраторами, getMyPendingRecords та getDoctorPendingRecords для роботи з неопублікованими записами, getUserRole та isUserRegistered для перевірки ролей та статусу реєстрації користувачів, registerAsPatient для самостійної реєстрації пацієнтів, assignDoctor та removeDoctor для управління лікарями адміністраторами.

Технологічний стек включає бібліотеку ethers.js версії 5.x для надійної взаємодії з Ethereum, React.js версії 18.x для побудови сучасного компонентного користувацького інтерфейсу, Redux для централізованого управління станом додатку з передбачуваним потоком даних, react-router-dom для клієнтської маршрутизації між сторінками без перезавантаження, react-i18next для інтернаціоналізації та підтримки мультимовності, moment.js для роботи з датами та часом, react-blockies для візуалізації Ethereum адрес у вигляді унікальних іконок.

Комунікація з блокчейн-мережею відбувається через захищений HTTPS протокол з використанням JSON-RPC методів. Система підтримує роботу з різними Ethereum мережами через конфігуровані RPC endpoints: локальна мережа Hardhat за адресою http://127.0.0.1:8545 для розробки та тестування, тестова мережа Goerli для попереднього тестування в реальних умовах, основна мережа Ethereum для продуктивного використання. Всі транзакції підписуються локально в браузерному гаманці MetaMask з використанням приватного ключа користувача, при цьому система ніколи не має доступу до приватних ключів, що забезпечує максимальний рівень безпеки.

## 3.2 Властивості програмного продукту

Система управління користувачами забезпечує безпарольну автентифікацію через криптографічні підписи Ethereum гаманців, що є сучасним та безпечним підходом до ідентифікації. Реєстрація нових пацієнтів відбувається самостійно через виклик функції registerAsPatient смарт-контракту, що вимагає тільки підтвердження транзакції в MetaMask. Призначення ролі лікаря здійснюється виключно адміністратором через функцію assignDoctor з обов'язковою валідацією прав доступу на рівні смарт-контракту. Видалення ролі лікаря також можливе тільки адміністратором через removeDoctor для забезпечення контролю якості медичних послуг.

Функціонал створення медичних записів включає багатоетапну валідацію введених даних перед відправкою транзакції до блокчейну, автоматичну перевірку статусу цільового пацієнта на предмет того, чи зареєстрований він у системі, створення pending запису через createPendingRecord з усіма необхідними медичними даними, автоматичне емітування події RecordPending для сповіщення заінтересованих сторін, відображення реального статусу транзакції з індикаторами завантаження та результатом виконання. Система також перевіряє, чи має користувач права лікаря перед дозволом на створення записів.

Механізм підтвердження записів пацієнтами є ключовою особливістю системи і забезпечує відображення персоналізованого списку pending записів для конкретного пацієнта з повною медичною інформацією, детальний перегляд кожного запису з можливістю ознайомлення з усіма полями перед прийняттям рішення, можливість підтвердження через approveRecord або відхилення через rejectRecord з обов'язковим зазначенням причини відхилення, автоматичне переведення підтверджених записів до основної системи медичних записів з присвоєнням унікального ID, повне збереження історії всіх дій з записами через події блокчейну для аудиту та відстеження.

Система перегляду медичних записів надає диференційований рівень доступу з урахуванням ролі користувача: пацієнти мають доступ виключно до власних медичних записів через getMyRecords, лікарі можуть переглядати всі записи в системі через getAllRecords для професійної діяльності, адміністратори мають повний доступ до всіх даних та можливості управління системою. Відображення даних включає автоматичне форматування дат у зрозумілому для користувача вигляді з підтримкою локалізації, скорочення довгих Ethereum адрес до читабельного формату з можливістю перегляду повної адреси, кольорове кодування статусів записів для швидкого розуміння стану, сортування та фільтрацію записів за різними критеріями.

Вимоги до продуктивності включають час відгуку системи на операції читання даних з блокчейну не більше 2 секунд за нормальних умов мережі, час виконання транзакцій запису до 30 секунд з урахуванням специфіки блокчейну Ethereum та часу підтвердження блоків. Система повинна підтримувати одночасну роботу щонайменше 50 користувачів без значного погіршення продуктивності, що достатньо для більшості медичних закладів середнього розміру.

Інтерфейс користувача повинен залишатися відзивним під час виконання блокчейн-операцій з обов'язковим відображенням індикаторів завантаження, статусу транзакцій та прогресу виконання операцій. Система ефективно кешує отримані дані для зменшення кількості запитів до блокчейну та покращення користувацького досвіду, особливо при повторному перегляді тих самих записів.

Структура зберігання даних у смарт-контракті включає основну структуру Record з полями recordId для унікальної ідентифікації запису, timestamp для збереження часу створення, patient та doctor для адрес відповідних користувачів, name, age, gender для особистих даних пацієнта, bloodType, allergies для медично важливої інформації, diagnosis та treatment для професійних медичних висновків.

Структура PendingRecord для записів, що очікують підтвердження, розширює основну структуру додатковим полем status типу enum RecordStatus з можливими значеннями PENDING для очікування, APPROVED для підтверджених та REJECTED для відхилених записів. Система забезпечує цілісність зв'язків між pending записами та їх підтвердженими версіями через ретельно спроектовані маппінги.

Маппінги для ефективного доступу до даних включають recordToPatient для швидкого знаходження записів конкретного пацієнта, userRoles для зберігання та перевірки ролей користувачів, isRegistered для відстеження статусу реєстрації в системі, pendingRecords для управління неопублікованими записами, isDeleted для позначення логічно видалених записів без фізичного видалення з блокчейну.

Система подій емітує UserRegistered при успішній реєстрації нових користувачів з зазначенням ролі, DoctorAssigned при призначенні нових лікарів адміністратором, RecordPending при створенні записів, що потребують підтвердження, RecordApproved при успішному підтвердженні записів пацієнтами, RecordRejected при відхиленні записів з причиною, MedicalRecords\_\_AddRecord при додаванні записів до основної системи, MedicalRecords\_\_DeleteRecord при логічному видаленні записів.

Проектні обмеження включають обов'язкове використання мови Solidity версії 0.8.x для написання смарт-контракту з дотриманням сучасних практик безпечного програмування та уникненням відомих вразливостей типу reentrancy, overflow та доступу до неініціалізованих змінних. Код повинен проходити аудит безпеки перед розгортанням у основній мережі Ethereum.

Клієнтська частина використовує React.js з функціональними компонентами та сучасними хуками для управління станом, Redux для централізованого управління даними додатку, сучасні стандарти ES6+ JavaScript з підтримкою async/await для асинхронних операцій. Архітектура забезпечує модульність коду та легкість додавання нових функцій без порушення існуючої функціональності.

## 3.3 Атрибути програмного продукту

Надійність системи забезпечується використанням перевірених та стабільних блокчейн-технологій з багаторічною історією успішної експлуатації, всебічним тестуванням смарт-контрактів у контрольованих тестових мережах перед розгортанням у продукції, комплексною обробкою помилок та винятків на всіх рівнях архітектури системи, автоматичним створенням резервних копій конфігураційних файлів та детальними інструкціями для відновлення системи у разі збоїв.

Система повинна забезпечувати коефіцієнт готовності не менше 99.5% з урахуванням залежності від доступності блокчейн-мережі Ethereum, яка сама має високі показники надійності. Час відновлення після локальних збоїв клієнтської частини не повинен перевищувати 10 хвилин, тоді як відновлення після проблем з блокчейном залежить від глобального стану мережі Ethereum.

Обробка помилок включає інтелектуальне перехоплення та користувацьке відображення помилок транзакцій з поясненням можливих причин та способів вирішення, валідацію всіх введених даних на клієнтській стороні перед відправкою для запобігання невдалим транзакціям, автоматичні механізми повторних спроб для тимчасових збоїв мережі, збереження стану форм при короткочасних перериваннях з'єднання для зручності користувачів.

Доступність системи передбачає цілодобову роботу без планових перерв, окрім критичних оновлень безпеки, які не повинні перевищувати 2 години на квартал та проводитися в години мінімального навантаження з обов'язковим попереднім сповіщенням користувачів через всі доступні канали комунікації.

Стратегія резервування включає регулярне збереження ABI смарт-контракту та адрес розгортання в різних мережах, створення резервних копій конфігураційних файлів системи, підтримання актуальної документації для розгортання та відновлення, розробку детальних інструкцій для відновлення доступу користувачів у разі втрати даних.

Безпека системи базується на криптографічних принципах блокчейну та включає автентифікацію користувачів виключно через цифрові підписи Ethereum гаманців без передачі або зберігання будь-яких паролів чи інших чутливих автентифікаційних даних. Авторизація грунтується на ролях, збережених безпосередньо у смарт-контракті, з обов'язковою перевіркою прав доступу перед виконанням будь-яких операцій модифікації даних.

Захист персональних даних включає використання виключно HTTPS з'єднань для всіх комунікацій, ретельну валідацію всіх введених користувачем даних для запобігання SQL-ін'єкціям та іншим атакам, захист від XSS атак через правильне екранування всіх динамічних даних, застосування Content Security Policy заголовків для додаткового рівня захисту, регулярне оновлення всіх залежностей для усунення відомих вразливостей.

Аудит безпеки проводиться перед кожним значним оновленням системи з залученням зовнішніх експертів, документуванням всіх знайдених вразливостей та обов'язковим усуненням критичних проблем перед релізом.

Зручність використання забезпечується інтуїтивним дизайном інтерфейсу, що не вимагає спеціальної підготовки для базового використання, наданням детальних та зрозумілих інструкцій для всіх категорій користувачів, відображенням інформативних повідомлень про помилки з практичними порадами щодо їх усунення, повною підтримкою української та англійської мов з можливістю легкого додавання інших мов, адаптивним дизайном для комфортної роботи на різних типах пристроїв від настільних комп'ютерів до смартфонів.

Супроводжуваність коду забезпечується дотриманням стандартів чистого коду з детальними коментарями, використанням зрозумілих назв змінних та функцій, модульною архітектурою для легкості модифікації окремих компонентів, комплексною документацією API для розробників.

Система версіювання включає semantic versioning для всіх компонентів системи, git flow для організованого управління процесом розробки, автоматизовані тести для перевірки функціональності після кожної зміни, CI/CD pipeline для автоматичного тестування та розгортання нових версій.

## 3.4 Вимоги бази даних

Структура зберігання даних реалізована у блокчейні Ethereum через спеціально розроблений смарт-контракт MedicalRecords, який забезпечує децентралізоване та незмінне зберігання всіх медичних записів. Основна структура Record оптимізована для мінімізації витрат газу при збереженні повноти необхідної медичної інформації.

Індексація даних здійснюється через систему маппінгів, що забезпечують швидкий доступ до записів за унікальним ідентифікатором, адресою пацієнта для отримання персональних записів, адресою лікаря для перегляду створених ним записів. Система підтримує ефективний пошук без необхідності перебору всього масиву записів, що критично важливо для продуктивності.

Цілісність даних гарантується властивостями блокчейн-технології та додатково забезпечується валідацією на рівні смарт-контракту. Атомарність операцій забезпечує повний відкат змін у разі будь-яких помилок під час виконання транзакції. Валідація включає перевірку коректності Ethereum адрес, неможливість створення записів з порожніми обов'язковими полями, відповідність форматів введених даних очікуваним типам.

Незмінність підтверджених записів є фундаментальною властивістю системи, що гарантується криптографічними методами блокчейну. Після підтвердження пацієнтом запис не може бути змінений без залишення відповідних слідів у блокчейні. Видалення записів здійснюється тільки логічно через маркування спеціальним прапорцем, при цьому дані фізично залишаються у блокчейні для аудиту.

Повна історія всіх операцій зберігається через систему подій блокчейну, що дозволяє відстежити будь-які зміни в записах, час їх створення, підтвердження або відхилення, особи, що виконували дії. Ця інформація незмінна та може використовуватися для юридичного аудиту.

Резервне копіювання у традиційному розумінні не потрібне, оскільки блокчейн Ethereum сам є розподіленою системою зберігання з тисячами копій на різних вузлах по всьому світу. Однак система забезпечує експорт конфігураційних даних, включаючи ABI смарт-контракту, адреси розгортання у різних мережах, налаштування мереж. Процедури відновлення детально документовані з покроковими інструкціями для швидкого відновлення доступу до системи у разі локальних проблем.

## 3.5 Інші вимоги

Інтернаціоналізація системи реалізована через бібліотеку react-i18next, що забезпечує підтримку української та англійської мов з архітектурою, яка дозволяє легко додавати нові мови без зміни основного коду. Всі текстові рядки винесені в окремі JSON файли з логічною структурою, що полегшує переклад та підтримку.

Локалізація включає не тільки переклад текстів, але й адаптацію форматів дат, чисел, валют відповідно до культурних особливостей регіону. Інтерфейс перемикання мов реалізований через зручний випадаючий список з прапорцями країн та доступний на всіх сторінках системи. Вибрана мова зберігається в локальному сховищі браузера для збереження налаштувань між сесіями.

Правові вимоги включають повну відповідність законодавству України щодо захисту персональних даних та ведення медичної документації. Система забезпечує дотримання принципів мінімізації даних, збираючи тільки необхідну для медичних цілей інформацію, прозорості обробки через чіткі повідомлення користувачам про використання їх даних, забезпечення права на доступ, виправлення та видалення персональних даних.

# 4 ДОДАТКОВІ МАТЕРІАЛИ

## 4.1 UML діаграми прецедентів

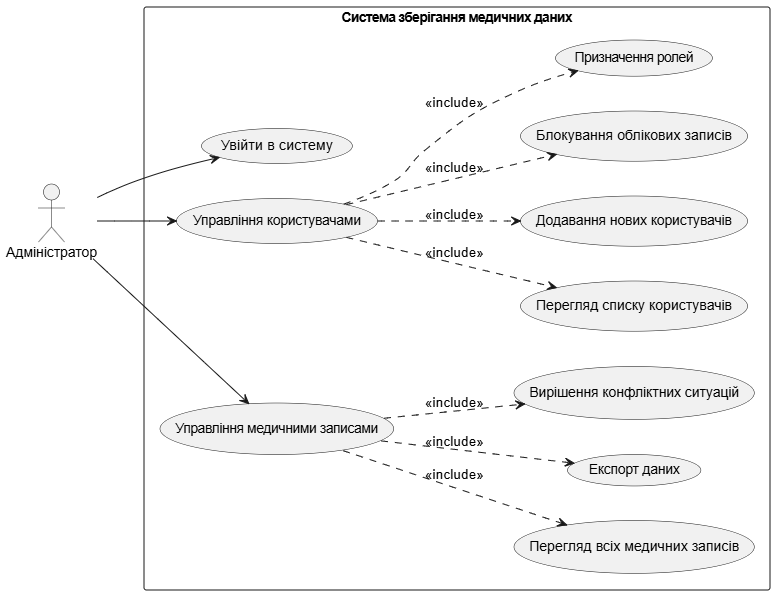


Рисунок 3.1 – Use Case діаграма для Адміністратора (рисунок виконаний самостійно)

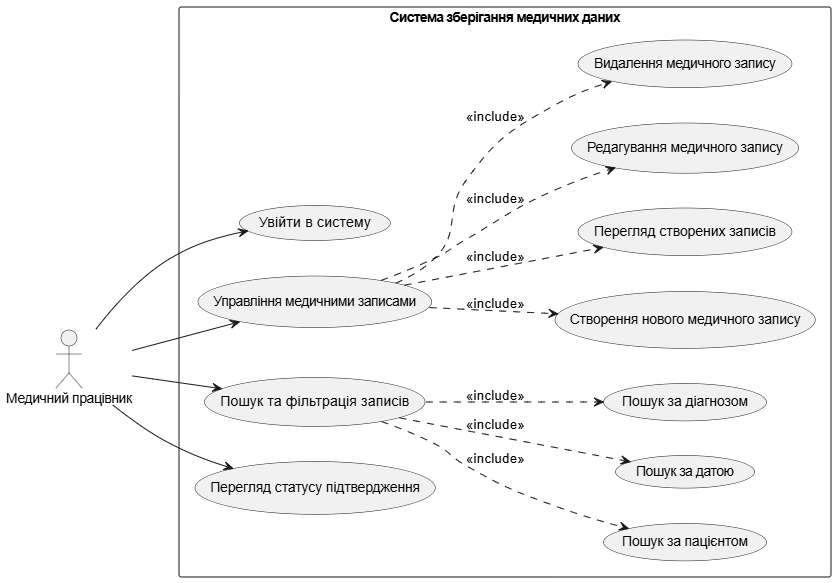


Рисунок 3.2 – Use Case діаграма для Медичного працівника (рисунок виконаний самостійно)

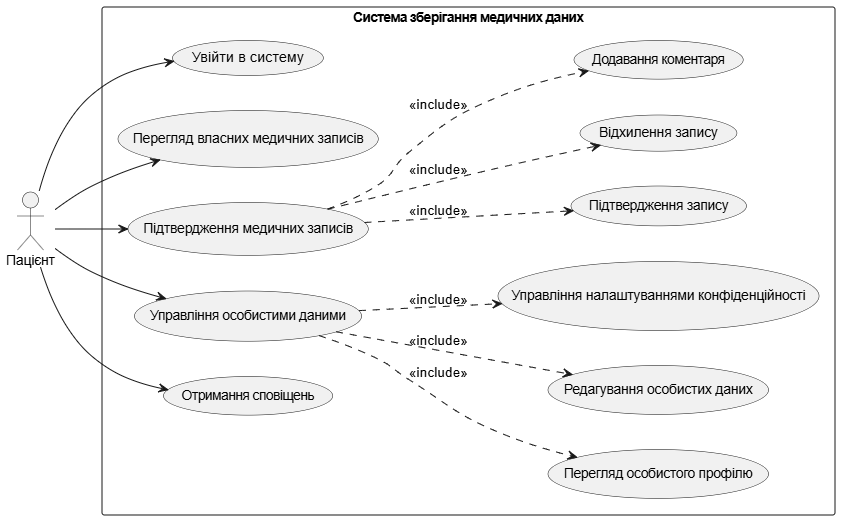


Рисунок 3.3 – Use Case діаграма для Пацієнта (рисунок виконаний самостійно)

4.2 Архітектурні схеми

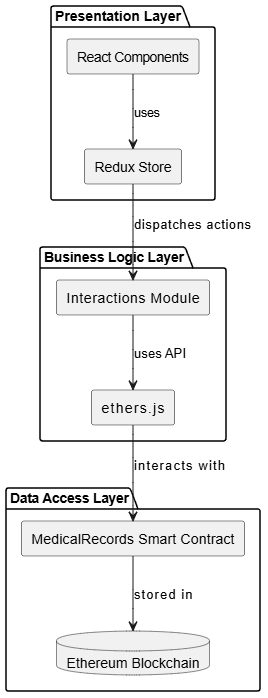


Рисунок 3.4 – Схема архітектури програмного забезпечення (рисунок виконаний самостійно)

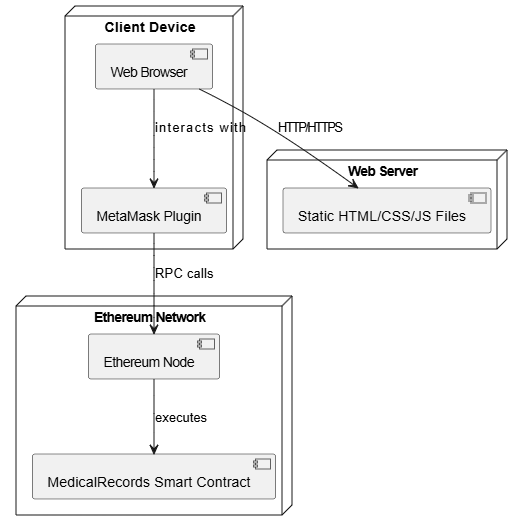


Рисунок 3.5 – Діаграма розгортання системи (рисунок виконаний самостійно)

4.3 Структури даних

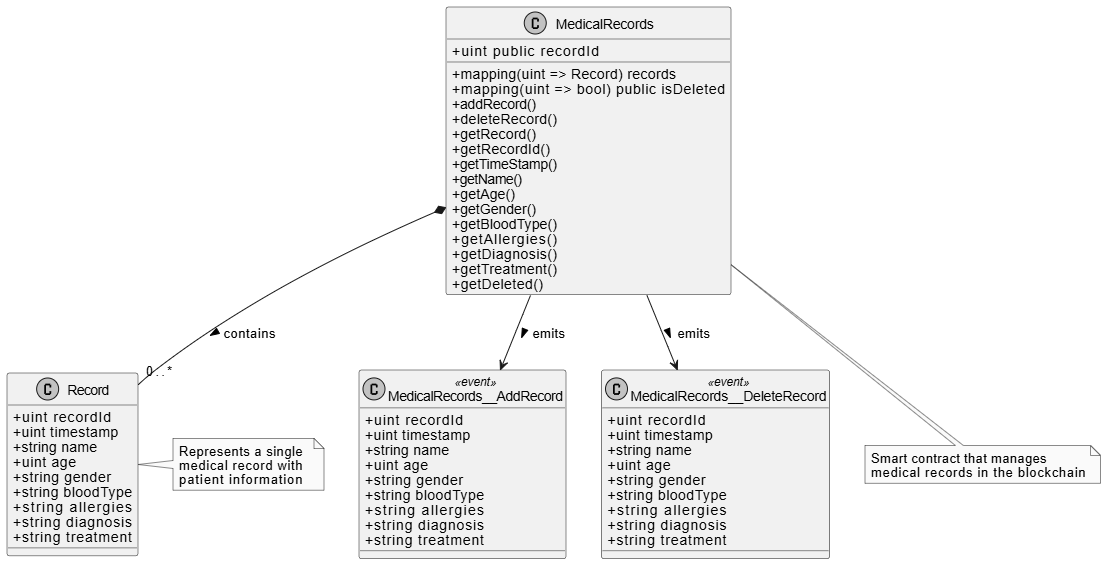


Рисунок 3.6 – ER-діаграма структури даних смарт-контракту (рисунок виконаний самостійно)