# ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
КАФЕДРА ЕОМ

# Дослідження, проєктування та розробка програмних компонентів для системи зберігання та передачі конфіденційної інформації

Автор:
Ст.гр. СПм-23-3
Рагулін О.Є.

Кваліфікаційна робота
Другий (магістерський) рівень

Керівник:
Доцент кафедри ЕОМ
Шматко О.В.

Харків
2025

1

## АКТУАЛЬНІСТЬ ТЕМИ

**Захист медичних даних** – критичне завдання. Конфіденційна інформація про пацієнтів потребує надійного захисту від несанкціонованого доступу.

**Цифровізація медицини.** Швидке впровадження електронних медичних систем потребує ефективних програмних рішень для безпечної передачі та зберігання даних.

**Нормативні вимоги.** Необхідність дотримання міжнародних стандартів безпеки та приватності (GDPR, HIPAA тощо).

**Зростання кіберзагроз.** Кількість атак на медичні інформаційні системи щороку зростає, що вимагає впровадження сучасних криптографічних і захисних технологій.

**Потреба у гнучких програмних компонентах.** Актуально розробляти модульні рішення, які легко інтегруються в існуючі IT-системи медичних закладів.

2

# ОБ'ЄКТА ТА ПРЕДМЕТ

**Об'єктом дослідження** є системи передачі медичної інформації, які забезпечують ефективний обмін даними між медичними закладами, фахівцями та пацієнтами з урахуванням необхідності гарантування конфіденційності, цілісності та доступності цих даних.

**Предметом дослідження** є методи та інструментальні засоби проєктування та розробки програмних компонентів, необхідних для побудови захищених систем обміну медичною інформацією.

3

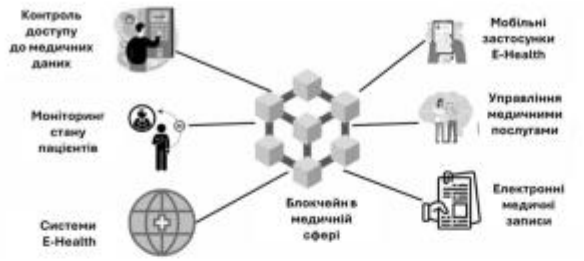
# МЕТА ТА ЗАДАЧІ РОБОТИ

**Метою даної роботи** є підвищення рівня конфіденційності, цілісності та доступності медичної інформації шляхом проєктування та реалізації програмних компонентів, які забезпечують надійний і безпечний обмін цією інформацією між усіма учасниками медичного процесу.

Для досягнення поставленої мети необхідно виконати такі основні задачі:

1. Проаналізувати існуючі архітектури систем електронної охорони здоров'я, що використовують блокчейн-технології.
2. Визначити функціональні та нефункціональні вимоги до цільової системи.
3. Розробити архітектуру програмних компонентів, що включає смарт-контракти, механізми авторизації, шифрування, логування та аудиту доступу.
4. Реалізувати прототип системи та забезпечити взаємодію між її компонентами.
5. Провести тестування з точки зору безпеки, продуктивності та відповідності функціональним вимогам.

4




## СФЕРИ ЗАСТОСУВАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ

5

## ПОРІВНЯННЯ БЛОКЧЕЙН-РІШЕНЬ ДЛЯ ЕЛЕКТРОННИХ МЕДИЧНИХ ЗАПИСІВ (EHR)

| Система / Платформа | Блокчейн-платформа | Основні функції | Особливості реалізації | Джерело |
|---|---|---|---|---|
| HealthChain | Hyperledger Fabric (IBM) | Конфіденційність, масштабованість, безпека | Приватна permissioned-мережа; використання смарт-контрактів (chaincode) для контролю доступу | [6], [7] |
| Ancile | Ethereum | Контроль доступу, безпека, конфіденційність, інтероперабельність | Смарт-контракти керують правами доступу до EHR; публічний блокчейн | [8] |
| MedRec | Ethereum | Розподілений контроль над доступом до EHR | Орієнтація на інтеграцію з медичними закладами; зберігає метадані, а не самі дані | [9] |
| DPS (Li et al.) | Ethereum | Зберігання та підтвердження цілісності медичних даних | Проста схема збереження та перевірки медичних записів | [10], [11] |
| MedBlock | Не вказано (ймовірно Ethereum) | Зберігання та обмін медичними записами | Забезпечує зручну взаємодію між пацієнтами та медичними закладами | [12] |

6

# ФУНКЦІОНАЛЬНІ ВИМОГИ

| Актор | Сценарій використання | Функціональні вимоги |
|---|---|---|
| Пацієнт | Надання згоди на обробку медичних даних | F4 – Надання згоди |
| | Відкликання згоди на обробку даних | F2 – Контроль доступу через смарт-контракти |
| | Перегляд історії доступу до своїх записів | F3 – Журналізація дій користувачів |
| Медичний працівник | Запит доступу до медичних записів пацієнта | F2 – Контроль доступу через смарт-контракти |
| | Внесення нових медичних записів | F6 – Перевірка цілісності даних |
| | Пошук та перегляд історії медичних записів | F7 – Пошук, перегляд і фільтрація |
| Адміністратор системи | Створення та конфігурація смарт-контрактів | F2, F4 – Контроль доступу, згода |
| | Управління вузлами та мережею блокчейну | F1 – Реєстрація та автентифікація |
| | Забезпечення технічного обслуговування | F1 – Інфраструктурне адміністрування |

7

# НЕФУНКЦІОНАЛЬНІ ВИМОГИ

| № | Нефункціональна вимога | Критерій вимірювання | Цільове значення |
|---|---|---|---|
| 1 | Захищене зберігання даних | Тип архітектури зберігання | Гібридна: IPFS + хеші у блокчейні |
| 2 | Автоматизоване управління згодою пацієнта | Час обробки запиту на зміну згоди | Не більше 2 секунд |
| 3 | Простежуваність і доказ походження даних | Повнота журналу змін | 100% збереження історії змін у блокчейні |
| 4 | Міжсистемна сумісність | Підтримка відкритих медичних стандартів | HL7 FHIR (v4.0 і вище), REST API |
| 5 | Надійність і відмовостійкість | Доступність системи (Uptime) | Не менше 99.9% на місяць |
| 6 | Масштабованість і продуктивність | Кількість оброблених транзакцій на секунду (TPS) | Мінімум 100 TPS при піковому навантаженні |
| 7 | Перевірка цілісності даних | Час хеш-верифікації запису | Не більше 500 мс |

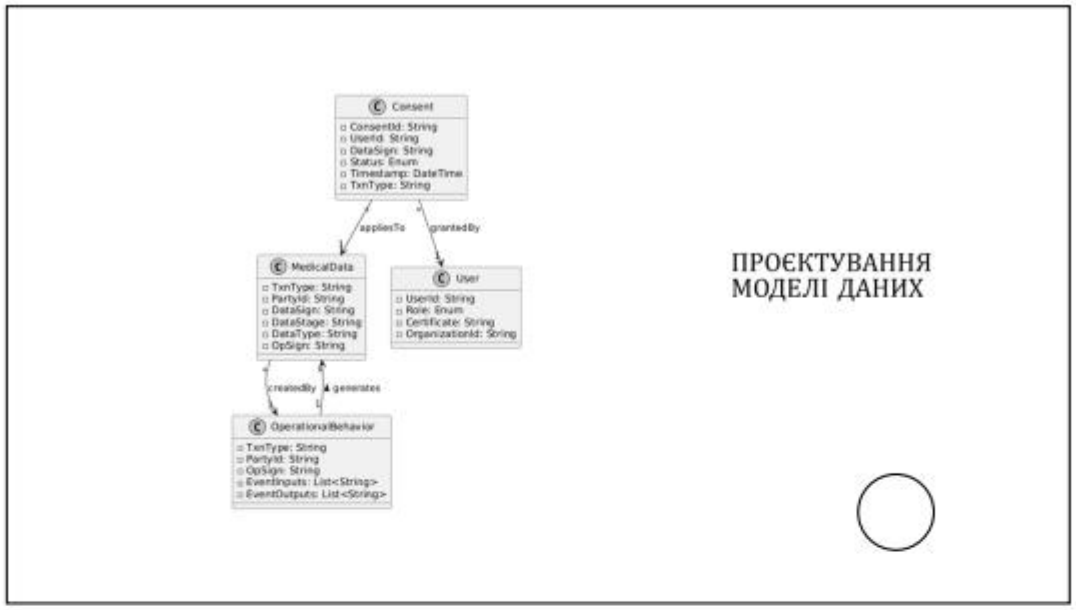
8

# АРХІТЕКТУРА СИСТЕМИ

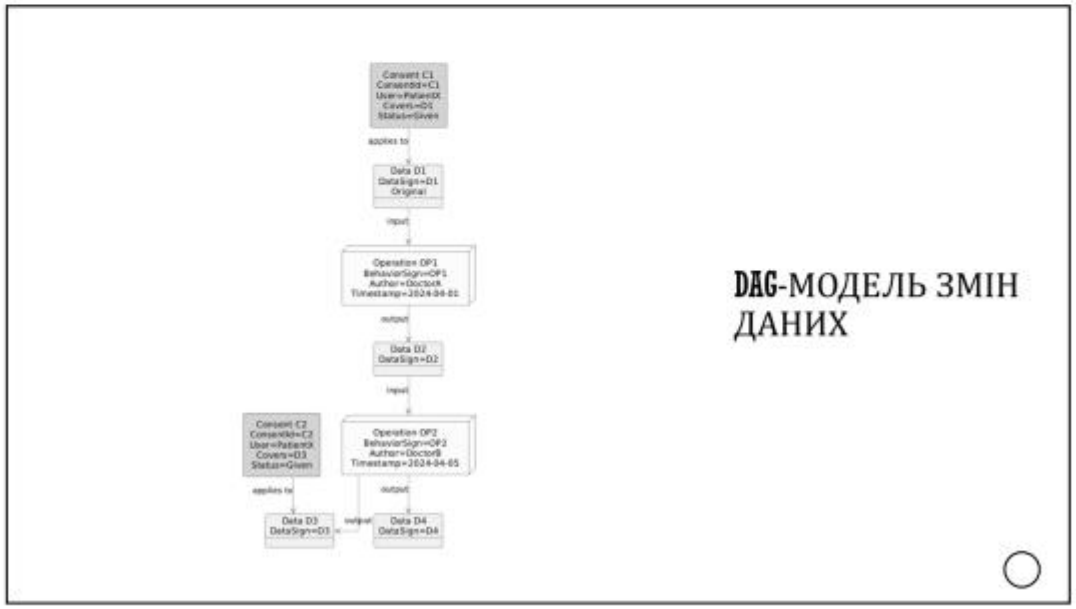
9

# ДІАГРАМА ВАРІАНТІВ ВИКОРИСТАННЯ

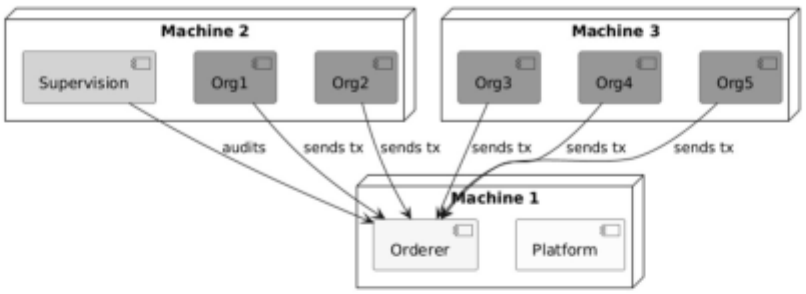
10


Consent
ConsentId: String
UserId: String
DataSign: String
Status: Enum
Timestamp: DateTime
TxnType: String
appliesTo
grantedBy
MedicalData
TxnType: String
PartyId: String
DataSign: String
DataStage: String
DataType: String
OpSign: String
User
UserId: String
Role: Enum
Certificate: String
OrganizationId: String
createdBy
generates
OperationalBehavior
TxnType: String
PartyId: String
OpSign: String
EventInputs: List<String>
EventOutputs: List<String>
ПРОЄКТУВАННЯ
МОДЕЛІ ДАНИХ

11


Consent C1
ConsentId=C1
User=PatientX
Covers=D1
Status=Given
applies to
Data D1
DataSign=D1
Original
input
Operation OP1
BehaviorSign=OP1
Author=DoctorA
Timestamp=2024-04-01
output
Data D2
DataSign=D2
input
Consent C2
ConsentId=C2
User=PatientX
Covers=D3
Status=Given
Operation OP2
BehaviorSign=OP2
Author=DoctorB
Timestamp=2024-04-05
applies to
output
Data D3
DataSign=D3
output
Data D4
DataSign=D4
DAG-МОДЕЛЬ ЗМІН
ДАНИХ

12




# ЕКСПЕРИМЕНТАЛЬНА ПЛАТФОРМА

13

| Тип даних | Кількість записів | Формат | Примітки |
|---|---|---|---|
| **Пацієнти** | 5 000 | JSON | Основні відомості та медична історія |
| **Призначення лікарів** | 12 000 | JSON/XML | Рецепти, плани лікування, консультації |
| **Діагностичні результати** | 7 500 | JSON/DICOM | Дані аналізів, зображення, висновки |
| **Запити доступу** | 15 000 | JSON | Запити від різних організацій системи |

# ЕКСПЕРИМЕНТАЛЬНІ ДАННІ

14

Результати завантаження медичних даних

| Кількість організацій | Send Rate (TPS) | Throughput (TPS) | Max Latency (c) | Avg Latency (c) |
|---|---|---|---|---|
| 3 | 1361.7 | 1349.3 | 2.05 | 0.11 |
| 7 | 794.7 | 782.8 | 2.28 | 0.37 |

Результати завантаження поведінкових даних

| Кількість організацій | Send Rate (TPS) | Throughput (TPS) | Max Latency (c) | Avg Latency (c) |
|---|---|---|---|---|
| 3 | 1256.3 | 1247.1 | 2.03 | 0.10 |
| 7 | 789.9 | 778.6 | 2.04 | 0.37 |

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ ІЗ ЗАВАНТАЖЕННЯ ТА ЗАПИТІВ ДАНИХ

15

# ДОСЛІДЖЕННЯ ПРОСТЕЖУВАНОСТІ ДАНИХ (DATA PROVENANCE)

| Метод | Тип трасування | TPS |
|---|---|---|
| Naive-forward | Пряме | 0.54 |
| Naive-backward | Зворотне | 388.6 |
| DAG-forward | Пряме | 10 214 |
| DAG-backward | Зворотне | 10 086 |

16

# ЗАЛЕЖНІСТЬ TPS ВІД ДОВЖИНИ ШЛЯХУ ДЛЯ РІЗНИХ МЕТОДІВ

| Довжина шляху | Naive-backward (TPS) | DAG-forward (TPS) | DAG-backward (TPS) |
|---|---|---|---|
| **1** | 388.6 | 10 214 | 10 086 |
| **2** | 252.9 | 7 943 | 7 826 |
| **3** | 168.1 | 6 210 | 6 123 |
| **4** | 102.4 | 4 581 | 4 508 |
| **5** | 56.3 | 3 211 | 3 183 |
| **6** | 39.5 | 2 105 | 2 080 |
| **≥7** | 35.6 | 528 | 519 |

17

# ПОРІВНЯННЯ З ІСНУЮЧИМИ СИСТЕМАМИ

| Критерій | Пропонована система | MedRec | FHIRChain | MeDShare | Ancile |
|---|---|---|---|---|---|
| Блокчейн-платформа | **Hyperledger Fabric** | Ethereum | Ethereum | Fabric | Ethereum |
| Тип блокчейну | **Приватний (permissioned)** | Публічний | Публічний | Приватний | Публічний |
| Зберігання медичних даних | **Гібридне (IPFS + hash)** | Метадані | Метадані + FHIR | IPFS | Off-chain |
| Контроль доступу через смарт-контракти | **Так** | Частково | Так | Так | Так |
| Надання/відкликання згоди | **Так** | Частково | Ні | Так | Так |
| Підтримка HL7 FHIR | **Повна** | Ні | Часткова | Часткова | Так |
| Аудит та журнал дій | **Так** | Частково | Частково | Так | Так |
| Простежуваність походження даних | **Так** | Ні | Ні | Частково | Так |
| Масштабованість (TPS) | **Висока (≥100 TPS)** | Низька | Середня | Висока | Середня |
| Інтероперабельність з HIS/EHR | **Так** | Ні | Так | Частково | Так |

18

# ПУБЛІКАЦІЇ ЗА ТЕМОЮ РОБОТИ

19

# ВИСНОВКИ:

🔍 **1. Дослідження проблеми.** Проведено комплексний аналіз сучасних рішень у сфері захисту медичних даних. Виявлено обмеження існуючих систем (MedRec, FHIRChain тощо) щодо функціональності, масштабованості та відповідності стандартам безпеки.

🛠 2. **Розробка власного рішення.** Запропоновано архітектуру медичної інформаційної системи нового покоління з такими ключовими особливостями:

- гібридне зберігання (блокчейн + IPFS);
- смарт-контракти для керування доступом;
- повна простежуваність походження даних;
- використання Hyperledger Fabric для масштабованості.

🧩 **3. Інноваційність підходу.** Система забезпечує контрольовану децентралізацію, прозорість дій користувачів, аудит, гнучке управління згодою на обробку даних пацієнтів.

📊 **4. Порівняльний аналіз.** Рішення показало вищі результати за критеріями безпеки, продуктивності та нормативної відповідності порівняно з існуючими аналогами.

📑 **5. Практична цінність.** Система має потенціал впровадження в закладах охорони здоров'я як частина національної цифрової трансформації медичної галузі.

20

ДОДАТОК Б

НАУКОВА ПУБЛІКАЦІЯ

ISSN 2073-7394

Національний університет
"Полтавська політехніка імені Юрія Кондратюка"

National University
"Yuri Kondratyuk Poltava Polytechnic"

# Системи управління, навігації та зв'язку

# Control, navigation and communication systems

**Випуск 2 (80)** **Issue 2 (80)**

**Щоквартальне видання**

**Засноване у 2007 році**

У журналі відображені результати наукових досліджень з розробки та удосконалення систем управління, навігації та зв'язку у різних пробпемних галузях.

**Засновник і видавець:**
Національний університет
"Полтавська політехніка імені Юрія Кондратюка"

**Телефон:**
+38 (050) 302-20-71

**E-mail редколегії:**
kuchuk_nina@ukr.net

**Інформаційний сайт:**
http://journals.nupp.edu.ua/sunz

**Quarterly**

**Founded in 2007**

Journal represent the research results on the development and improvement of control, navigation and communication systems in various areas

**Founder and publisher:**
National University
"Yuri Kondratyuk Poltava Polytechnic"

**Phone:**
+38 (050) 302-20-71

**E-mail of the editorial board:**
kuchuk_nina@ukr.net

**Information site:**
http://journals.nupp.edu.ua/sunz

*За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор*

*Журнал індексується міжнародними наукометричними базами: Index Copernicus (ICV = 82.05), General Impact Factor, Google Scholar, Academic Resource Index, Scientific Indexed Service*

*Затверджений до друку Вченою Радою Національного університету "Полтавська політехніка імені Юрія Кондратюка" (протокол від 12 березня 2025 року № 5).*

*Ідентифікатор медіа R30-04135 згідно з рішенням Національної ради України з питань телебачення і радіомовлення від 25.04.2024 № 1416*

*Включений до "Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора наук, кандидата наук та ступеня доктора філософії" до категорії Б – наказами МОН України від 17.03.2020 № 409 та від 09.02.2021 № 157*

**Полтава • 2025**

© Національний університет "Полтавська політехніка імені Юрія Кондратюка"

*Помелуйко Д. А., Єрьоміна Н. С., Петров С. В., Іщенко Н. В., Волощук О. Б.* Методи масштабування kubernetes кластеру в хмарному середовищі ..... 176
*Пономаренко О. Є., Горбачов В. О.* Метод пошуку вузьких місць в складних мережах для підвищення ефективності обчислювальних ресурсів ..... 181
*Samborskyi Ie., Peleshok Ye.* Synthesis of logical-dynamic information and event management systems for computer security structures ..... 186
*Терених Д., Харченко В. С.* Автоматизація створення класифікаторів: алгоритми і програмне забезпечення для формування множини стратегій розгортання та забезпечення надійності рою БПЛА ..... 197
*Шандиба А. С., Сітніков В. І., Ніколаєв О. С., Кібірєв Д. О.* Нанесення цифрових водяних знаків з використанням геометрії карт ..... 208
*Шматко О. В., Разулін О. Є., Кравченко П. О., Буслов П. В.* Дослідження архітектурних рішень для побудови безпечної системи зберігання та передачі конфіденційних даних ..... 215

**ЦИВІЛЬНА БЕЗПЕКА ..... 4**

*Бірук Я. І., Шаманський С. Й., Климчук А. В.* Дослідження ефективності електромагнітних екранів резонансного типу ..... 224
*Глива В. А., Кашлєв М. С.* Екранування шуму будівельного обладнання ..... 228
*Левченко Л. О., Аушева Н. М., Ткаченко Т. М.* Моделювання зміни температури на поверхнях теплоізоляційних покриттів ..... 232
*Токарський О. І., Зозуля Л. А., Галонько Я. О., Москаленко О. О.* Засоби нормалізації фізичних факторів середовища приміщень спеціального призначення ..... 236

**ЗВ'ЯЗОК, ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА ..... 5**

*Bikchentayev M., Boriak B.* Integration of SDR into UAV systems ..... 241
*Kostiantyn P., Komar O.* Assessment of the impact of sparsity and Geman-McClure regularization on signal reconstruction accuracy ..... 245
*Руденко В. В.* Огляд протоколу LoRa та перспективи використання ..... 251
*Sadovnykov B., Lysechko V.* A method for searching and recognising objects in a video stream by calculating interframe deltas ..... 256
*Syvolovskyi I., Zhuchenko O.* A method of hierarchical clustering of nodes in distributed telecommunication systems using graph algorithms ..... 263

**АЛФАВІТНИЙ ПОКАЖЧИК** ..... 272

---

***Організації авторів***

Федеральний інститут Парани, Парана, Бразилія
Вище професійне училище № 7, Кременчук, Україна
Державний торговельно-економічний університет, Київ, Україна
Державний університет «Київський авіаційний інститут», Київ, Україна
Київський національний університет будівництва і архітектури, Київ, Україна
Київський фаховий коледж зв'язку, Київ, Україна
Кременчуцький національний університет імені Михайла Остроградського, Кременчук, Україна
Національна академія Служби безпеки України, Київ, Україна
Національна академія статистики, обліку та аудиту, Київ, Україна
Національний аерокосмічний університет «ХАІ», Харків, Україна
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна
Національний технічний університет України «КПІ імені Ігоря Сікорського», Київ, Україна
Національний університет оборони України, Київ, Україна
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Харківський національний автомобільно-дорожній університет, Харків, Україна
Харківський національний університет радіоелектроніки,

***Authors affiliation***

Instituto Federal do Parana, Parana, Brazil
Higher Vocational School No. 7, Kremenchuk
State University of Trade and Economics, Kyiv, Ukraine
State University "Kyiv Aviation Institute," Kyiv, Ukraine
Kyiv National University of Construction and Architecture, Kyiv, Ukraine
Kyiv Vocational College of Communication, Kyiv
Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk, Ukraine
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
National Academy of Statistics, Accounting and Audit, Kyiv, Ukraine
National Aerospace University "KHAI", Kharkiv, Ukraine
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
National Technical University "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
National Defence University of Ukraine, Kyiv
National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
Kharkiv National Automobile and Highway University, Kharkiv, Ukraine
Kharkiv National University of Radio Electronics,