**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА ТА АРХІТЕКТУРИ**

Факультет автоматизації і інформаційних технологій
Кафедра кібербезпеки та комп'ютерної інженерії

# *Система управління доступом в медичних інформаційних технологіях*

***Виконала*** студентка 2-ого курсу, група БІКСм-24:
Балобольченкова Марія Ігорівна
***Керівник:***
к.т.н., доцент Ізмайлова О.В.

2025 рік

## *Вступ*

| | |
|---|---|
| **Об’єкт дослідження** | Медичні інформаційні системи (МІС) як комплексні програмні засоби, що забезпечують збір, зберігання, обробку та захист медичних даних. |
| **Предмет дослідження** | Моделі та методи управління доступом в медичній інформаційній системі, включно з процесами автентифікації, авторизації та реалізації політик доступу. |
| **Мета дипломної роботи** | Дослідження моделей та методів управління доступом для медичної інформаційної системи з урахуванням сучасних вимог до інформаційної безпеки. |

## Задача

*Ключові задачі, що розв’язуються в роботі:*

- проаналізувати предметну область та нормативно-правові вимоги щодо захисту медичних даних;
- розглянути та порівняти моделі контролю доступу та запропонувати підхід до контролю доступу;
- змоделювати процеси управління доступом (UML, IDEF);
- розробити алгоритм роботи системи контролю доступу;
- реалізувати компонент «Електронна медична карта» на базі Django з акцентом на контроль доступу.

## Актуальність

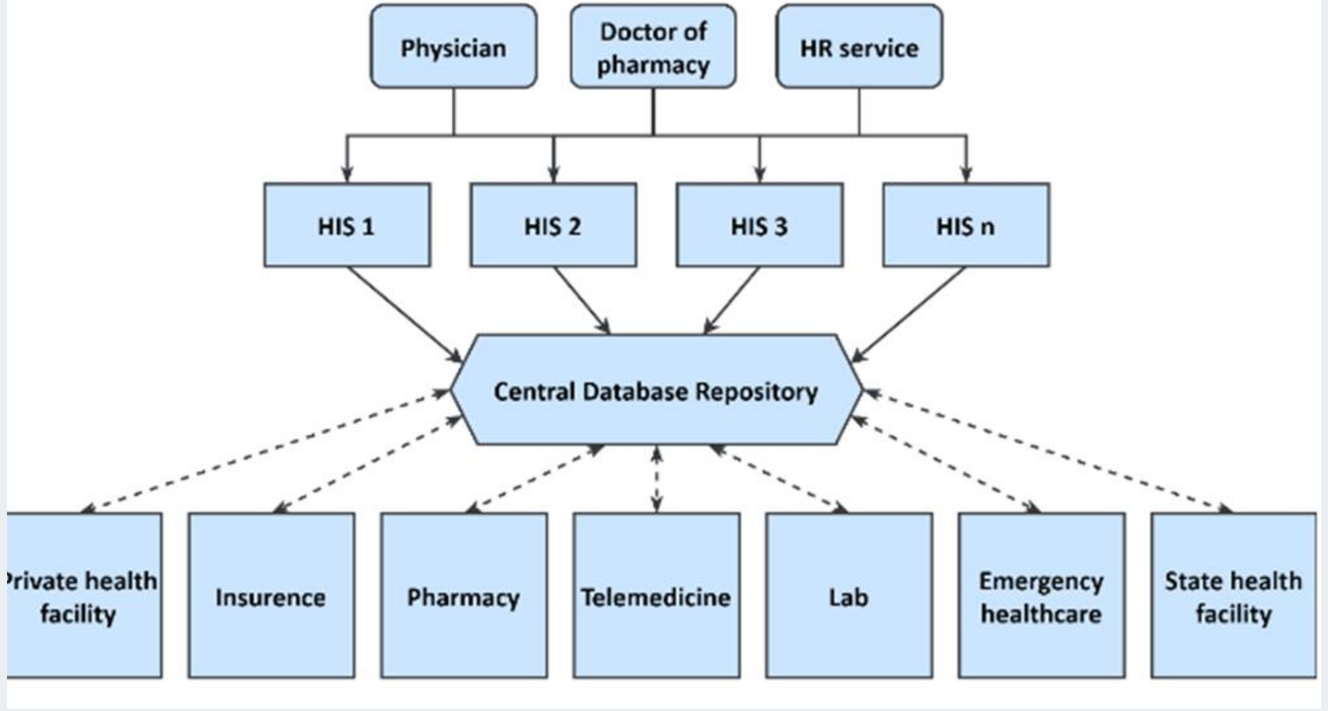
МІС опрацьовують великі обсяги конфіденційної інформації, що робить їх вразливими до кіберзагроз. ***Неналежне управління доступом*** до цих систем може призвести до витоку персональних даних, несанкціонованої зміни медичних записів, збоїв у роботі медичних установ і значних репутаційних та фінансових втрат. ***Тому дане дослідження*** може бути корисним для вдосконалення механізмів управління доступом та забезпечення надійного функціонування сучасних медичних систем.

# *Аналіз предметної області*

Заклади охорони здоров’я використовують комплексні рішення: телемедичні платформи, мобільні додатки, лабораторні системи, сховища медичних зображень.

Такі комплексні підходи зокрема в Україні(ЕСОЗ/eHealth), включають в себе:

- медичні інформаційні системи та їх підсистеми;
- центральну базу даних;
- програмне/апаратне забезпечення;
- мережеве з’єднання...



# ***Медичні інформаційні системи. Класифікація***

***Медична інформаційна система*** – це програмне забезпечення(ПЗ), за допомогою якого є можливим збір, зберігання, обробка та передача медичних даних.

*Класифікація медичних інформаційних систем (МІС):*

За типом користувачів:
- медичний персонал, адміністратори, пацієнти, державні структури.

За рівнем охоплення:
- локальні, регіональні, національні.

За способом розгортання:
- локальні, хмарні, гібридні.

За архітектурою:
- монолітні, SOA, мікросервісні, багатошарові, подієві, CQRS.

# *Аналіз існуючих рішень та нормативно-правової бази*

*Головні недоліки існуючих МІС*

- Обмежені механізми автентифікації
- Централізоване зберігання даних
- Низька прозорість доступу до персональних медичних даних
- Проблеми з надмірним навантаженням на систему та не зручного інтефейсу
- Ризики, пов’язані з приватним статусом сервісів
- Відсутність механізмів, які вимагає міжнародна практика (HIPAA, GDPR).

*В українських МІС доступ до даних формується під впливом:*

- закону України «Про захист персональних даних» та стандартів ЕСОЗ;
- закону України «Про інформацію»;
- постанови КМУ «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем».

# *Ключові загрози для управління доступом у МІС*

**Несанкціонований доступ**

Слабкі паролі, повторне використання токенів, відсутність багатофакторної автентифікації.

**Отримання зайвих прав**

Неправильні ролі або надмірні привілеї користувачів.

**Викрадення сесій**

Використання активної сесії легального користувача.

*Способи реалізації загроз*

- Brute-force – підбір паролів
- Фішинг / соціальна інженерія
- Спуфінг – видавання себе за легального користувача
- MITM – перехоплення трафіку
- SQL-ін’єкції та XSS – атаки на веб-застосунки
- Крадіжка пристроїв або носіїв інформації

# *RBAC. SWOT-аналіз.*

***Контроль доступу на основі ролей (Role-Based Access Control, RBAC)*** – це модель авторизації, яка оптимізує керування правами користувачів шляхом об’єднання дозволів у ролі.

**ПЕРЕВАГИ** (S)

- Проста у розумінні та управлінні
- Масштабується для організацій із чіткою структурою
- Зменшує адміністративне навантаження
- Чітке розмежування доступу

**НЕДОЛІКИ** (W)

- Обмежена гнучкість у динамічних середовищах
- Складно керувати великою кількістю ролей
- Може потребувати додаткових політик для складних сценаріїв доступу

**ПОТЕНЦІЙНЕ ВИКОРИСТАННЯ** (O)

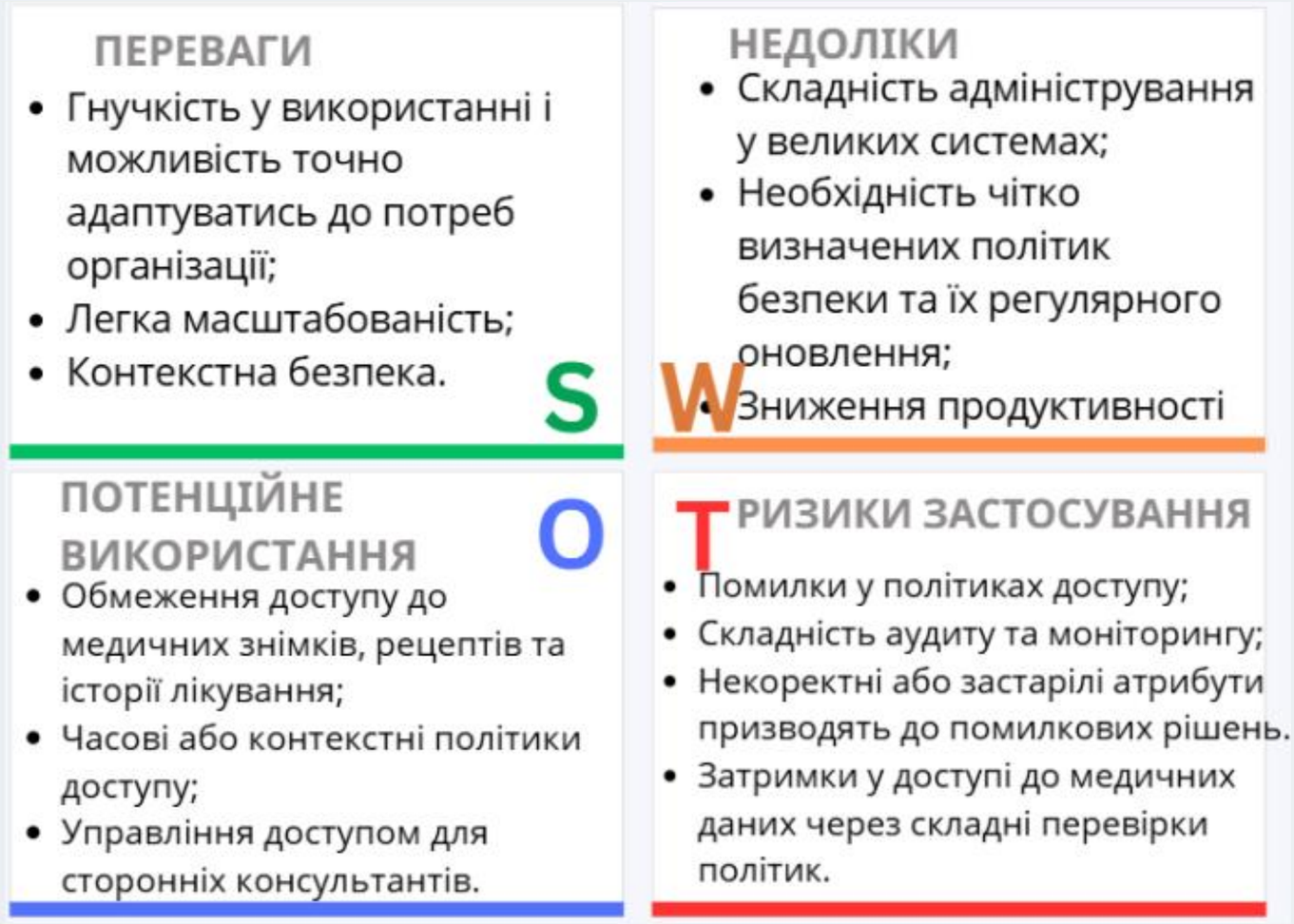
- Використання в лікарнях та клініках із чіткою ієрархією персоналу
- Керування доступом до медичних записів, результатів аналізів, модулів системи
- Автоматизація зміни прав доступу

**РИЗИКИ ЗАСТОСУВАННЯ** (T)

- Неузгодженість та надмірна складності управління великою к-стю ролей
- Неможливість швидко реагувати на нестандартні сценарії доступу
- Перевантаження адміністративного персоналу

# *ABAC. SWOT-аналіз.*

***Контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC)*** – це модель безпеки, якій притаманно використовування атрибутів для прийняття рішень щодо доступу.



# *PBAC. SWOT-аналіз.*

***Контроль доступу на основі політик (Policy-Based Access Control, PBAC)*** – це модель керування доступом, у якій рішення приймаються на основі визначених політик безпеки.

**S — ПЕРЕВАГИ**

- Детальний контроль доступу;
- Відповідність принципу “нульової довіри”;
- Зниження ризику внутрішніх загроз;
- Аудит дій

**W — НЕДОЛІКИ**

- Складність розробки та необхідність тестувати політики безпеки;
- Культурна та організаційна зміна;
- Потенційний вплив на продуктивність.

**O — ПОТЕНЦІЙНЕ ВИКОРИСТАННЯ**

- Реалізація динамічних політик;
- Адаптація до режимів надзвичайних ситуацій.

**T — РИЗИКИ ЗАСТОСУВАННЯ**

- Помилки у політиках доступу;
- Високі вимоги до підтримки;
- Технічні ризики;
- Організаційний опір.

# *MAC. SWOT-аналіз.*

***Обов'язковий контроль доступу (Mandatory Access Control, MAC)*** – це модель, яка обмежує можливості звичайних користувачів самостійно надавати або забороняти доступ до об’єктів файлової системи.

**ПЕРЕВАГИ** — **S**

- Високобезпечний спосіб контролю доступу;
- Захист від внутрішніх загроз;
- Чітка ієрархічна структура.

**НЕДОЛІКИ** — **W**

- Складність адміністрування;
- Дороге впровадження;
- Низька гнучкість.

**ПОТЕНЦІЙНЕ ВИКОРИСТАННЯ** — **O**

- Військові медичні установи;
- Розмежування доступу до модулей системи;
- Використання в інтегрованих системах охорони здоров’я, де дані пацієнтів обробляються різними підсистемами.

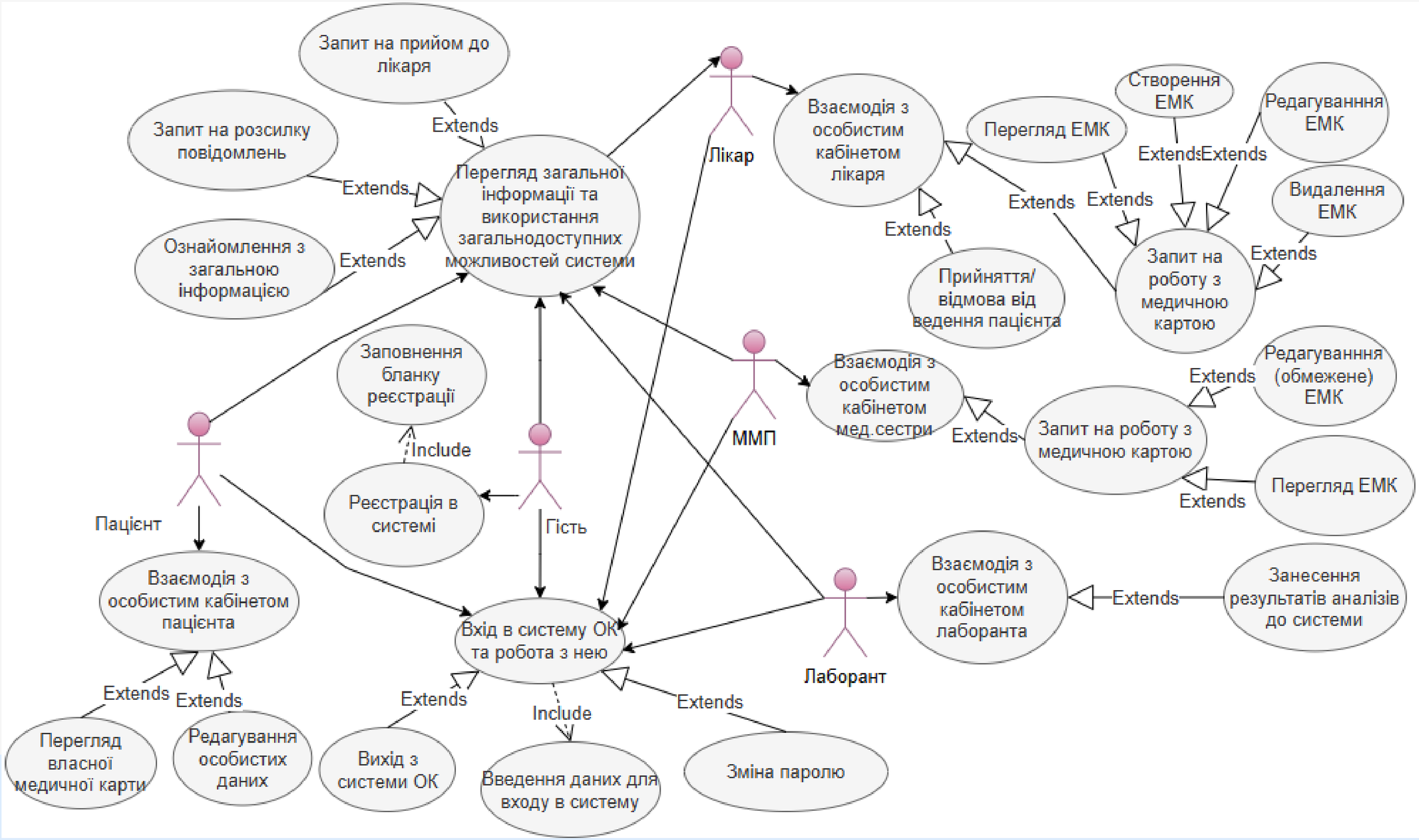
**ТРИЗИКИ ЗАСТОСУВАННЯ** — **T**

- Людський фактор в адмініструванні;
- Зниження продуктивності;
- Високі витрати на впровадження і підтримку.

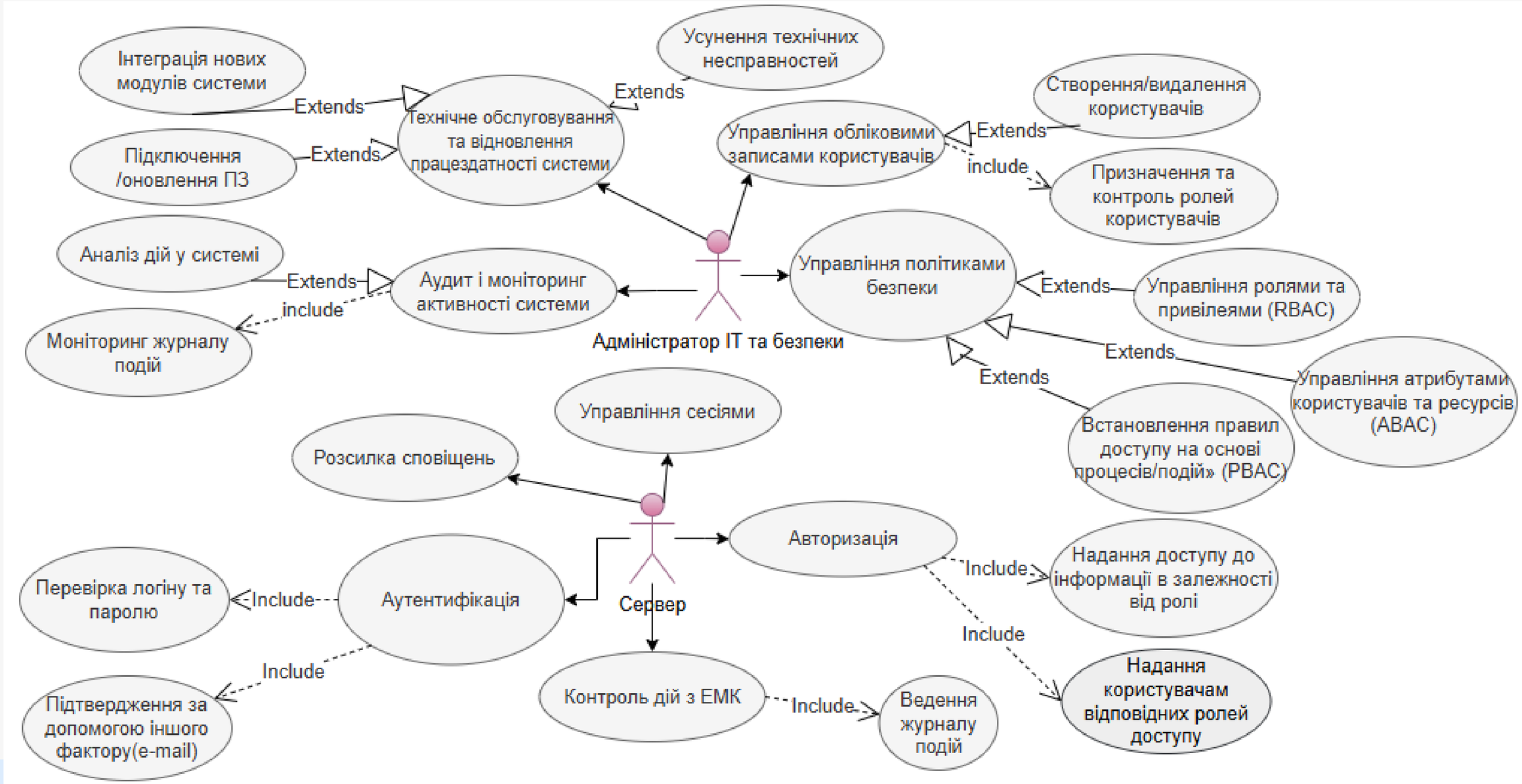
# Порівняння

| Модель | Основний принцип | Гнучкість | Управління | Підтримка | Сфера застосування |
|---|---|---|---|---|---|
| RBAC | Доступ за ролями користувачів | Низька - середня | Ролі розподіляються централізовано (проста) | Низькі-середні | Організації зі стабільними, добре визначеними ролями |
| ABAC | Доступ на основі атрибутів користувача, ресурсів та контексту | Висока | Потребує визначення атрибутів і правил (середня) | Високі вимоги | Складні системи з динамічними умовами доступу |
| PBAC | Доступ на основі політик, що описують правила доступу (“якщо…то”) | Дуже висока | Потребує створення та підтримки політик безпеки (висока) | Дуже високі вимоги | Де потрібна адаптація доступу під різні сценарії (наприклад, надзвичайні ситуації) |
| MAC | Поділ системи на рівні секретності, рівні доступу для користувачів контроль адміністратора | Низька | Адміністратор централізовано встановлює правила (висока) | Середні-високі вимоги | Високозахищені системи (військові, державні, критичні інфраструктури) |

# UML: діаграма прецедентів для користувачів



# UML: діаграма прецедентів адмістрування системи



# Політики доступу

Політики доступу для модулю «Медична карта» реалізовано через поєднання RBAC+ABAC+PBAC, що дозволяє враховувати не лише роль користувача, а й низку додаткових параметрів.

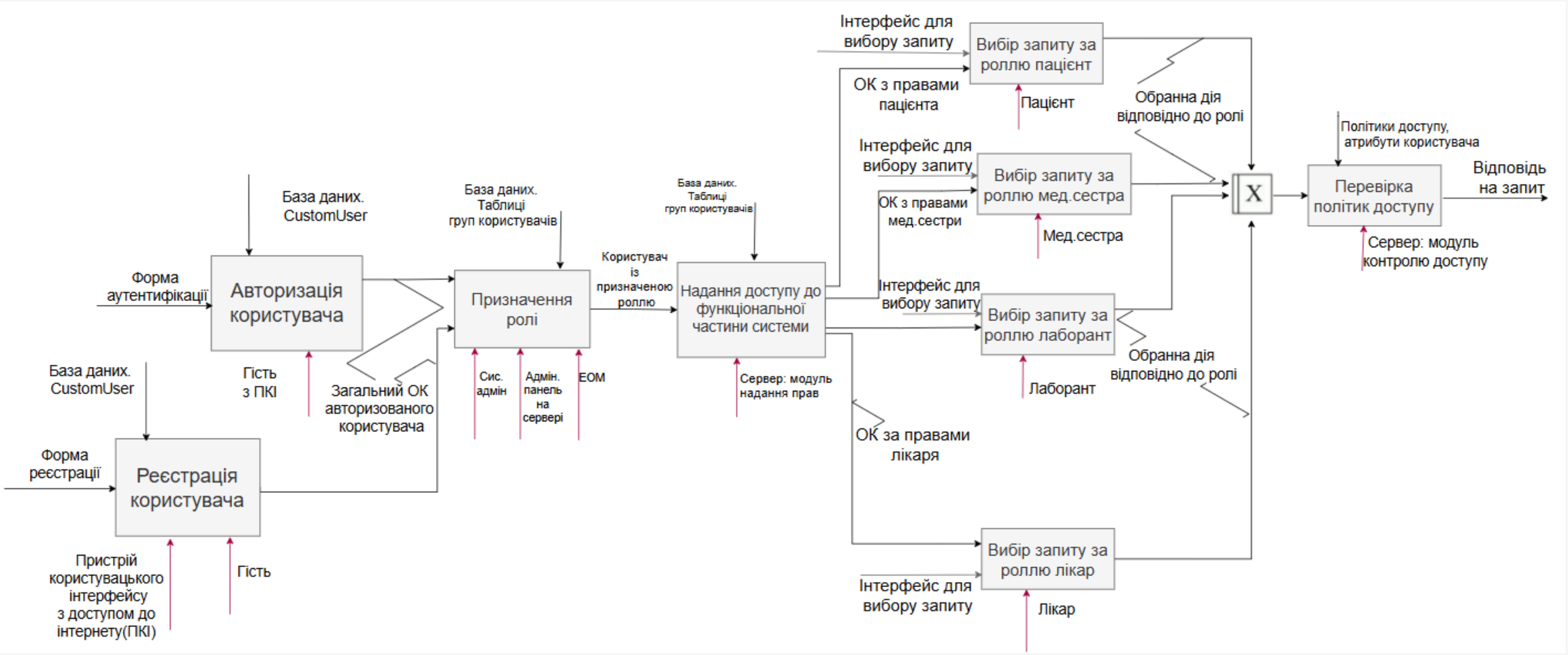
Доступ лікаря визначається його спеціалізацією, рівень залученості лікаря у ведення пацієнта, робочою зміною або режимом екстреного доступу. Такий підхід забезпечує гнучке, безпечне та ситуаційно адаптивне управління доступом до електронної медичної карти.

Таблиця 3.1 – Політики доступу для лікарів

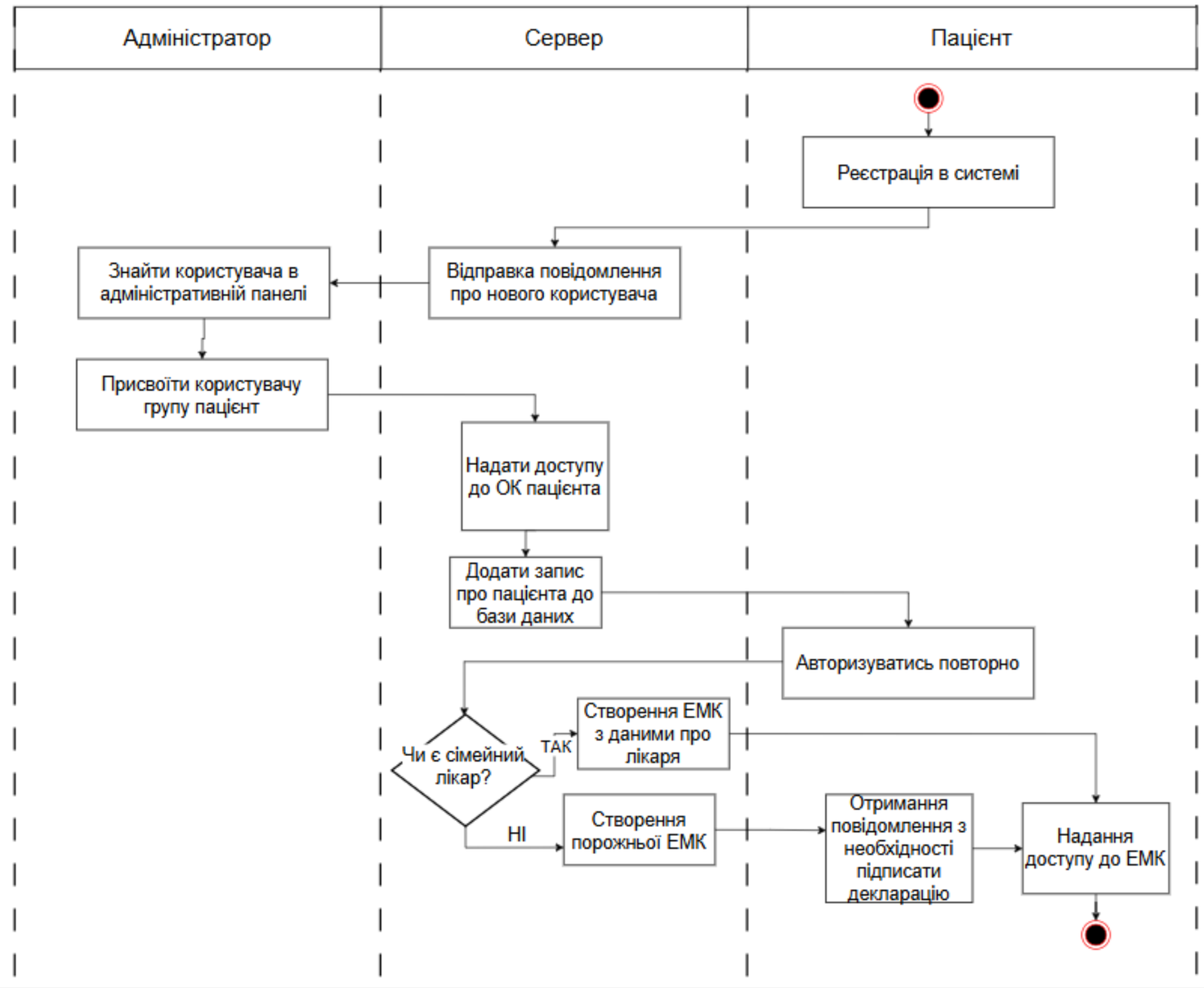
| Умова / Ситуація | Модель доступу | Логіка (правило політики) |
|---|---|---|
| **Лікар має спеціалізацію “терапевт”** | ABAC | Атрибут `specialization="therapist"` дозволяє ініціювати процес підписання декларацій із пацієнтами. |
| **Терапевт підписує декларацію з пацієнтом** | PBAC (на основі ABAC) | Після підписання лікар отримує атрибут `is_family_doctor=True`. |
| **Сімейний лікар** | RBAC + ABAC | Якщо `user.role="doctor"` і `user.is_family_doctor=True`, він має повні права на зміну та перегляд записів. |
| **Лікар іншої спеціалізації (не сімейний)** | PBAC | Може переглядати карти лише своїх пацієнтів або тих, хто надав дозвіл. Редагування можливе тільки після дозволу від сімейного лікаря або пацієнта. |

# IDEF: модель чорної скриньки

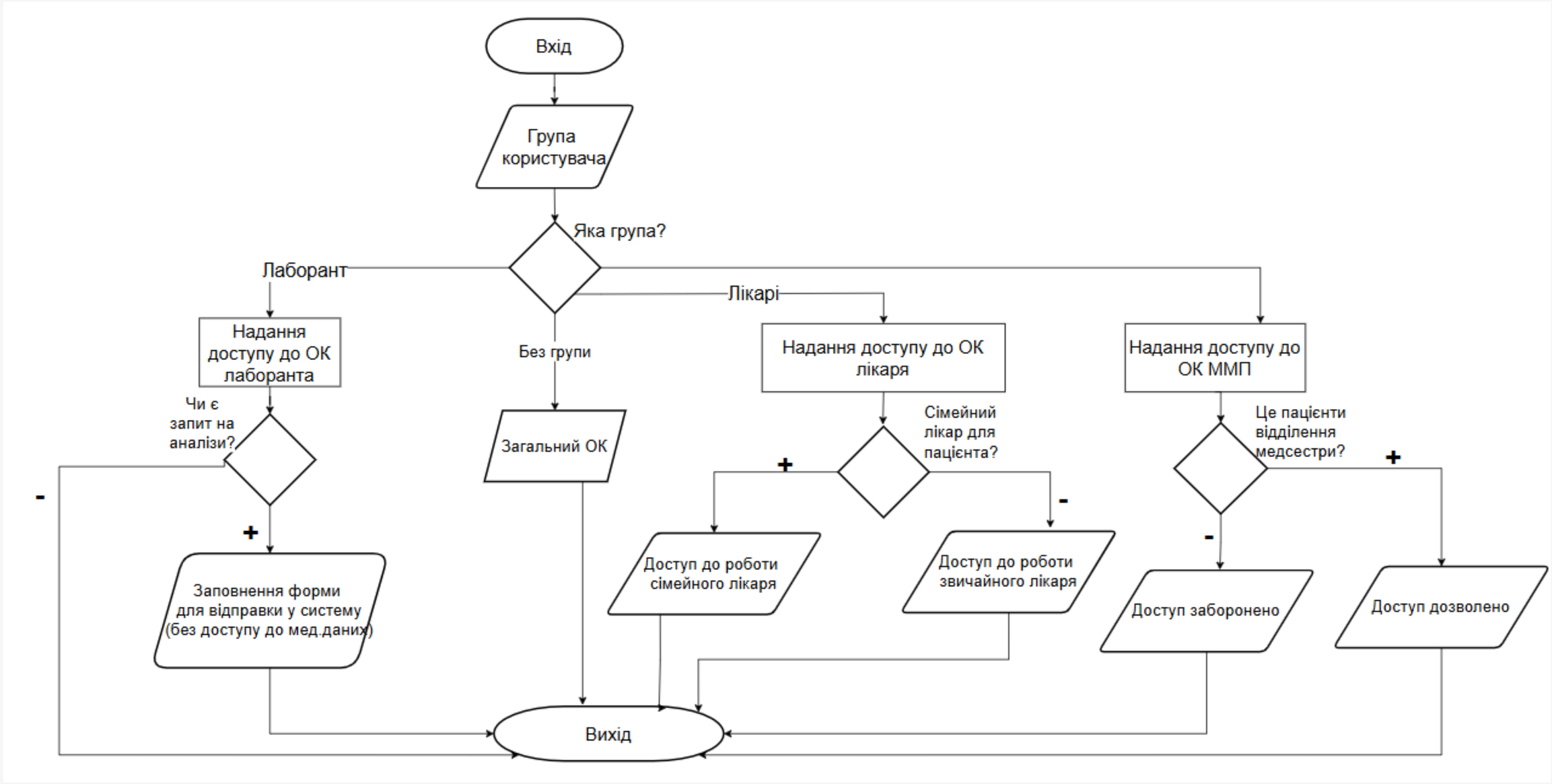
# IDEF: декомпозиція моделі чорної скриньки (послідовність процесів керування доступом в МІС)



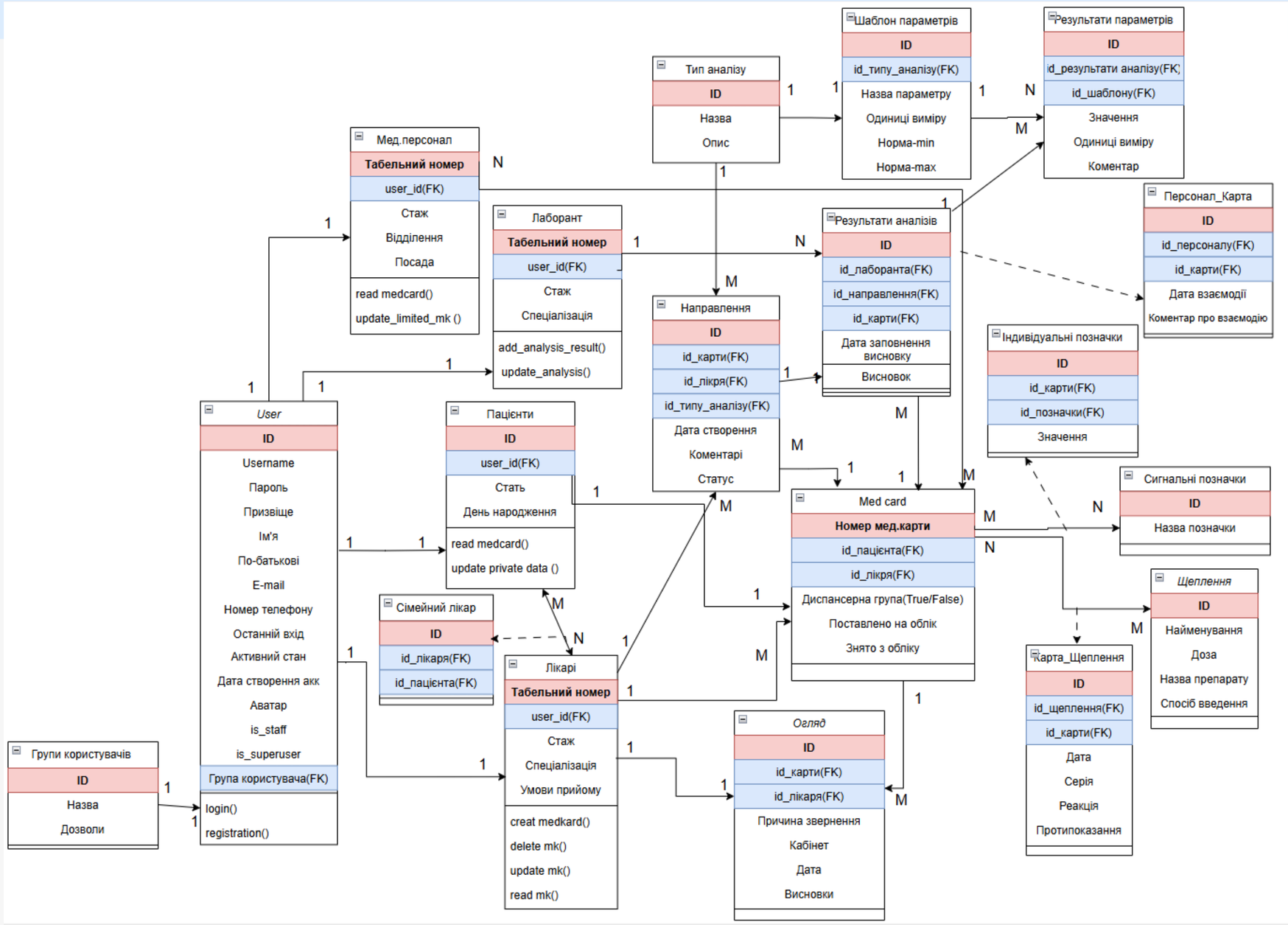
# Діаграма діяльності надання доступу до ЕМК пацієнту



# Алгоритм надання доступу до системи мед.персоналу



# UML: діаграма класів



# *Засоби реалізації та структура проєкту*

*Засоби реалізації*

***Серверна частина:*** Python 3.12, Django 5.2

***База даних:*** PostgreSQL

***Інтерфейс:*** HTML, CSS, Bootstrap, Django Templates

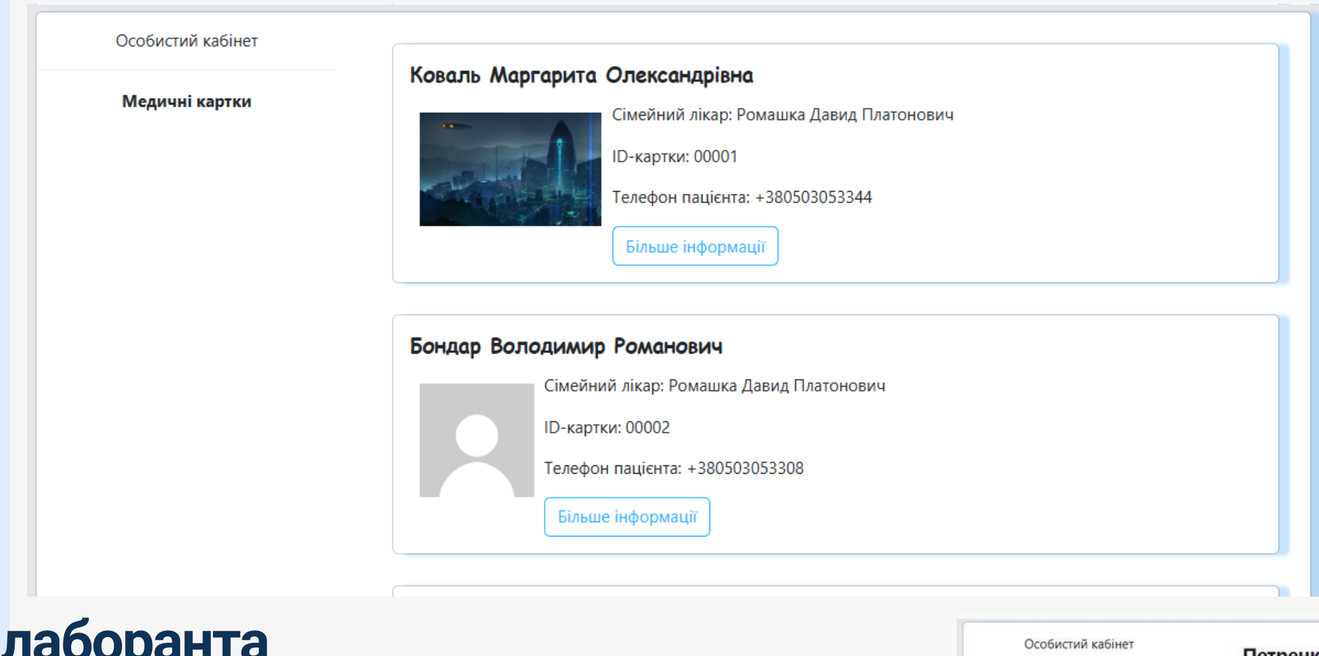
***Інструменти:*** VS Code, Git, GitHub

*Структурно проєкт поділений на 4 додатки, відповідно до вимог фреймворку:*

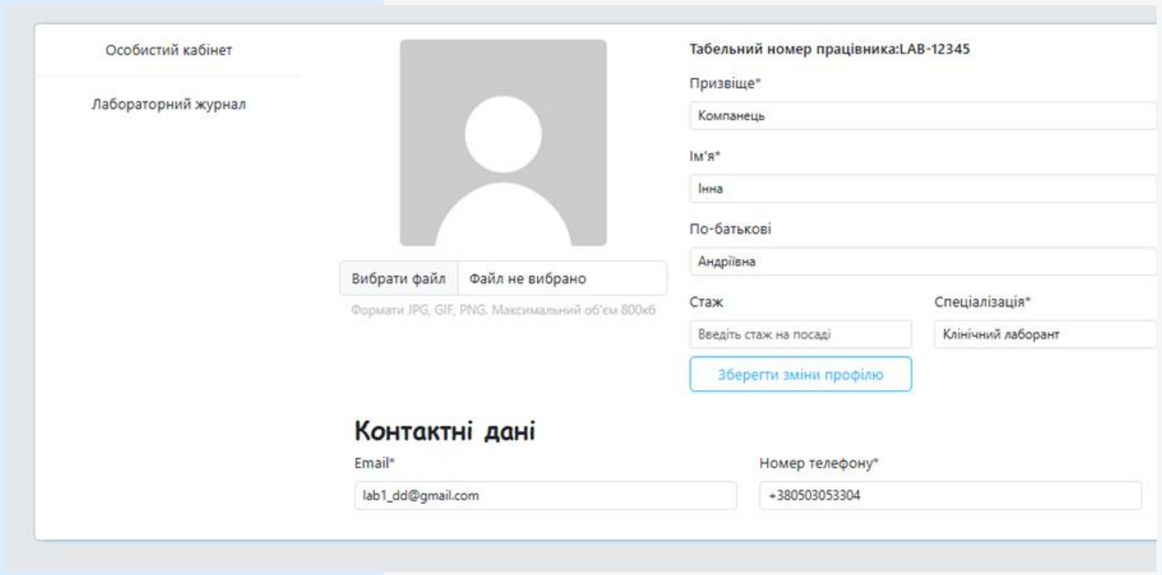
- public_app – оброблює загальнодоступні сторінки сайту.
- users_app – відповідає за роботу з користувачем.
- cards_app – реалізує управління ЕМК пацієнтів.
- laboratory_app – відповідає за облік, збереження та оброблення результатів лабораторних аналізів.

# *Особистий кабінет*

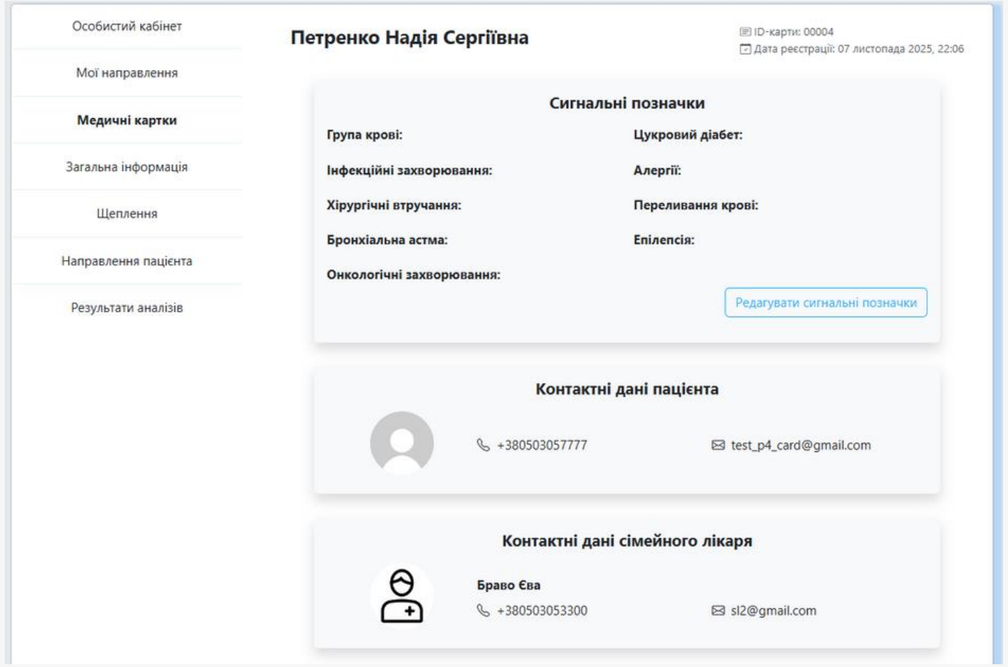
## ОК мед.персоналу: мед.карти



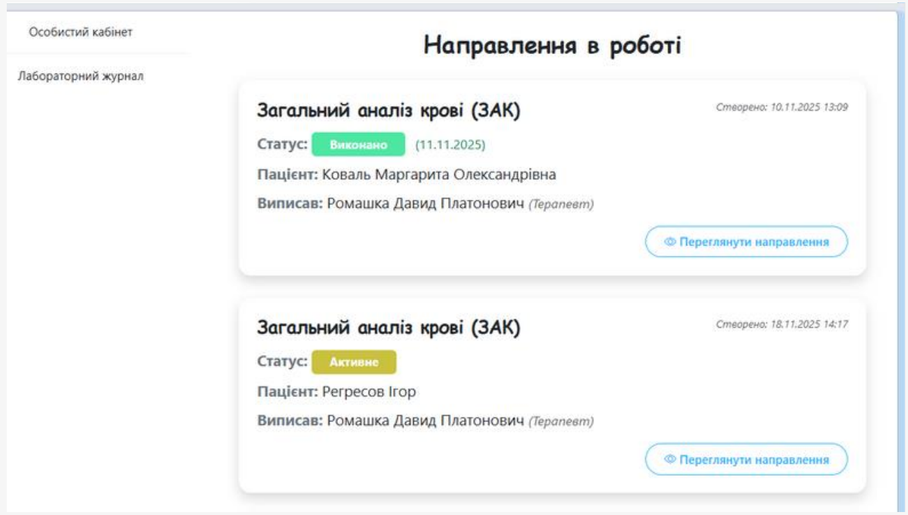

## ОК лаборанта

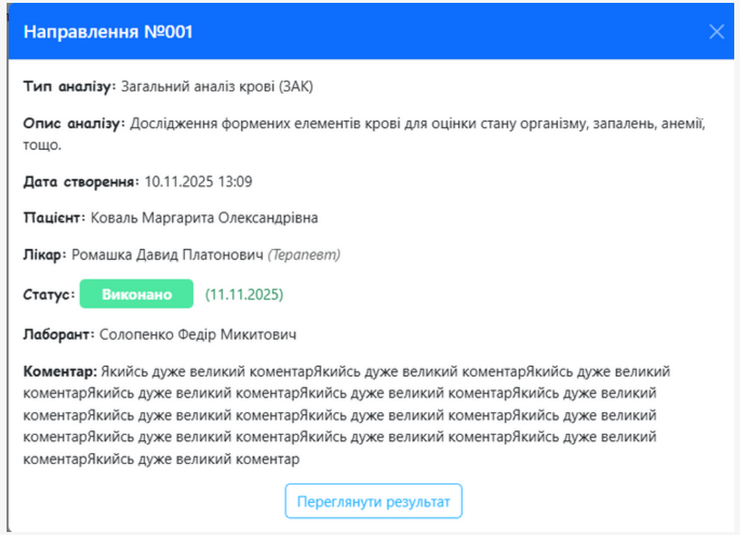


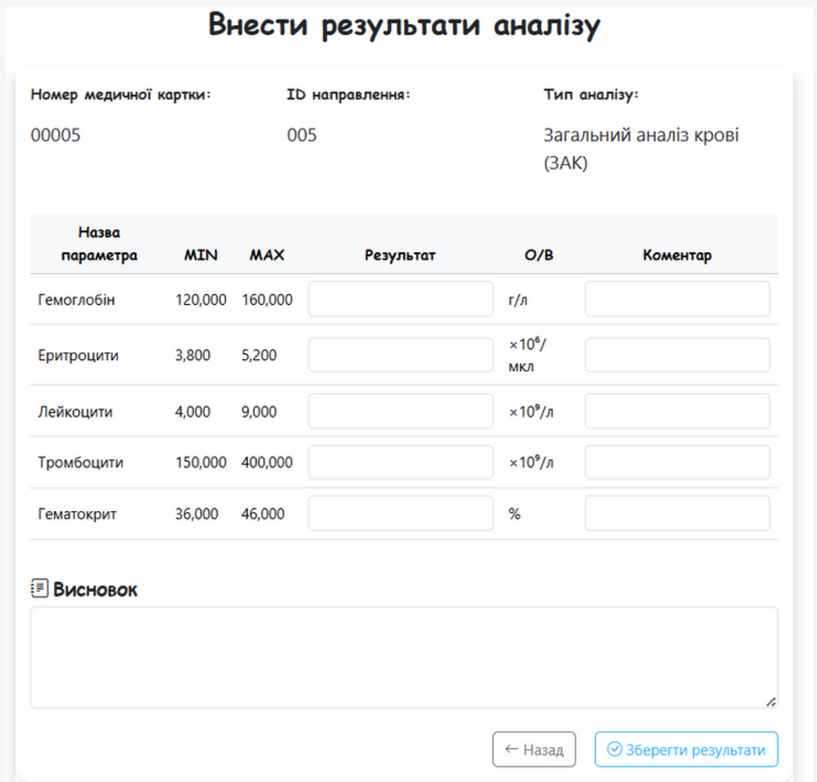

## Карта вибраного пацієнта лікарем



# Лабораторія



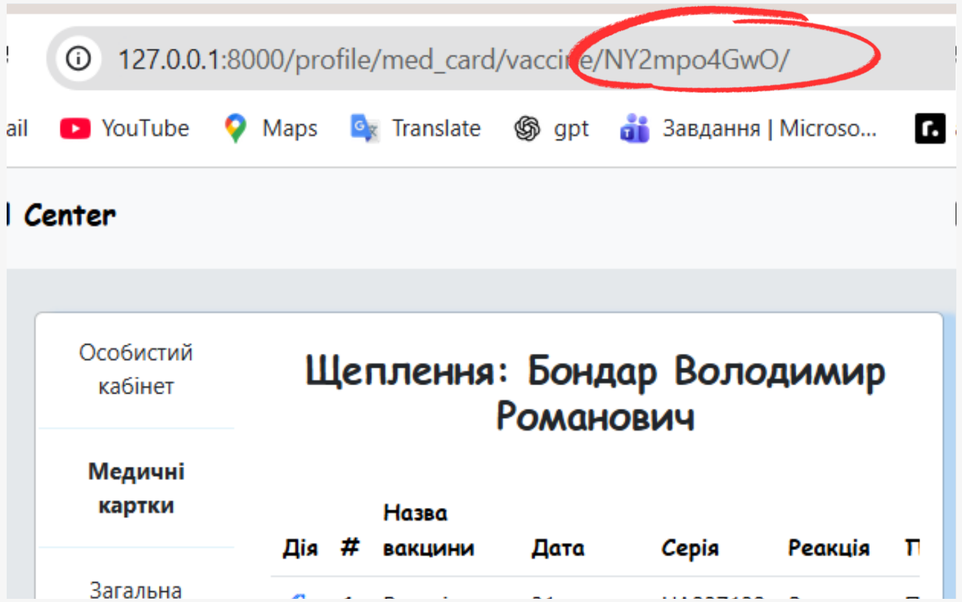




# Засоби захисту

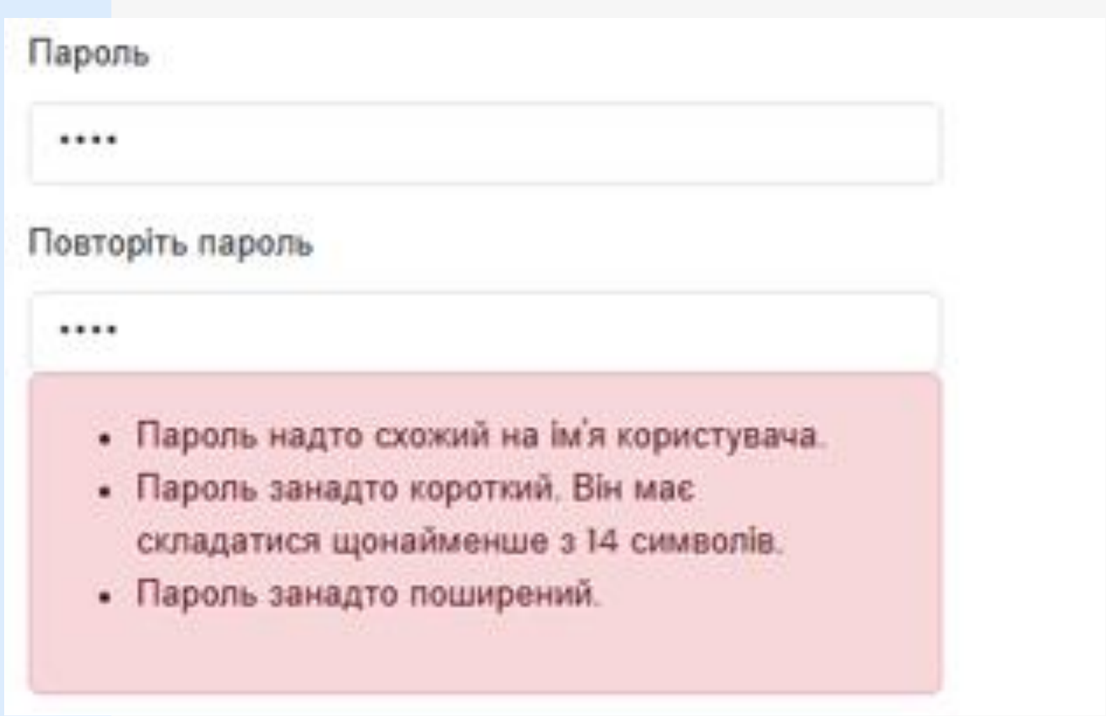
## Хешування паролів

| | id [PK] bigint | password character varying (128) |
|---|---|---|
| 1 | 1 | pbkdf2_sha256$1000000$ZuKnkFud... |
| 2 | 2 | pbkdf2_sha256$1000000$FBAHuK7... |
| 3 | 3 | pbkdf2_sha256$1000000$BfmNQng... |
| 4 | 4 | pbkdf2_sha256$1000000$bXsEDRF6... |
| 5 | 5 | pbkdf2_sha256$1000000$g1gv41nq... |

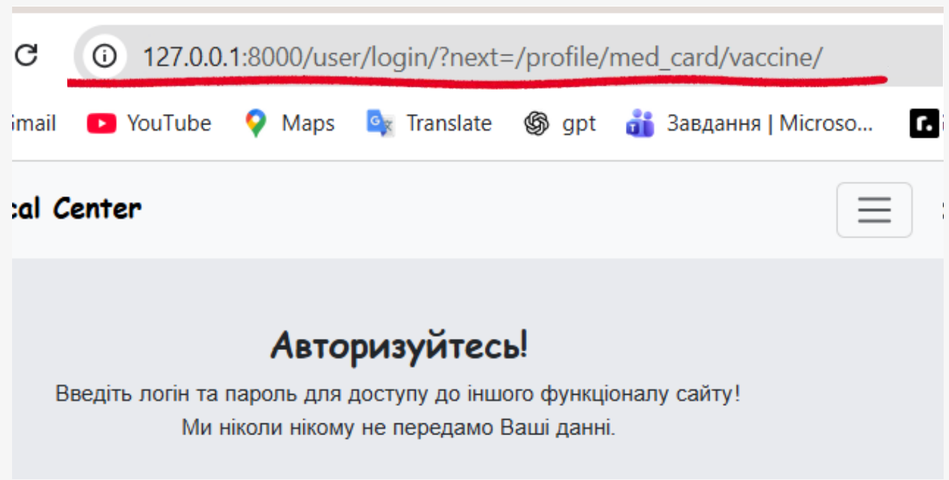
## Обфускація даних в url-адресах




## Стандартизовані паролі




## Перенаправлення на вхід



# *Висновки*

У роботі проведено дослідження питань інформаційної безпеки в МІС, класифіковано системи, визначено їхні ризики та проаналізовано сучасні моделі управління доступом.

Порівняння моделей RBAC, ABAC, PBAC і MAC та виконаний SWOT-аналіз показали, що жодна модель окремо не покриває повний спектр вимог до захисту МІС, тому запропоновано комбіновану модель RBAC+ABAC+PBAC.

У практичній частині удосконалено модуль електронної медичної картки на основі фреймворку Django 5.2: розширено систему ролей, додано нові функції та посилено механізми автентифікації, авторизації й захисту від веб-загроз.

Отримані теоретичні та практичні результати підтверджують можливість створення сучасної, безпечної та масштабованої МІС, придатної для подальшого розвитку та інтеграції з компонентами електронної системи охорони здоров’я.

# *Висновки. Публікації*

В рамках міжнародної науково-практичних конференцій молодих вчених «БУД-МАЙСТЕР-КЛАС-2024» та «БУД-МАЙСТЕР-КЛАС-2025» мною було представлено дві наукові тези:

- «Безпека web-додатків: SQL-ін’єкції – один з найпопулярніших методів кібератак» (2024), де висвітлено актуальні загрози та необхідність застосування безпечних підходів до розробки;
- «Застосування фреймворку Django для побудови безпечної інформаційної системи управління доступом на прикладі медичної сфери» (2025), де обґрунтовано ефективність використання Django та сучасних моделей контролю доступу у МІС.

# Дякую за увагу!