Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Юрій КРАВЧЕНКО
«_____»_____20__ року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»

на тему:

ВИКОРИСТАННЯ РІШЕНЬ ІНТЕРНЕТУ РЕЧЕЙ В СУЧАСНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Виконав: студент групи МІТ -41

Михайло ДРИГА _____
(ім'я ПРІЗВИЩЕ) (підпис)

Керівник: асистент кафедри мережевих та інтернет технологій

к.т.н., асистент Костянтин ГЕРАСИМЕНКО _____
(посада, ім'я ПРІЗВИЩЕ) (підпис)

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій
_____ Юрій КРАВЧЕНКО
«_____»_____20__ року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти **Дризі Михайлу Сергійовичу**
(прізвище ім'я по-батькові)

1. Тема роботи: Використання рішень Інтернету речей в сучасних інфокомунікаційних мережах затверджена на засіданні кафедри МІТ « 7 » грудня 2022р. протокол № 5
2. Термін здачі закінченої роботи «26» травня 2023 р.
3. Вихідні дані до проекту (роботи)
   Спроектувати мережеву інфраструктуру з підтримкою Інтернету речей для охорони здоров'я адаптовану до унікальних вимог цього домену.
   Проаналізувати кожен відділ закладу охорони здоров'я.
4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, обсяг – 35-40 стор.)
   Особливості сучасних інфокомунікаційних мереж.
   Перспективні рішення для інфокомунікаційних мереж: Інтернет речей, віртуалізація тощо.
   Огляд рішень Інтернету речей для інфокомунікаційних мереж.
   Проектування мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров'я адаптовану до унікальних вимог цього домену.
5. Перелік графічного матеріалу 14 слайдів

Дата видачі завдання
Керівник роботи к.т.н., асистент Герасименко Костянтин Васильович

Завдання прийняв до виконання Дрига Михайло Сергійович

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий	23.02.2023	
2	Розділ 1	10.03.2023	
3	Розділ 2	24.03.2023	
4	Розділ 3	01.04.2023	
5	Розділ 4	01.05.2023	
6	Доповідь та слайди	23.05.2023	
7	Пояснювальна записка	25.05.2023	

Здобувач вищої освіти Дрига Михайло Сергійович

Керівник Герасименко Костянтин Васильович

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Використання рішень Інтернету речей в сучасних інфокомунікаційних мережах» складається зі вступу, основної частини, що містить 4 розділи, висновків і списку літератури та джерел.

Загальний обсяг роботи – 72 сторінки. Робота містить 23 рисунки. Список використаних джерел включає 7 джерел.

Об’єкт дослідження – рішення Інтернету речей в сучасних інфокомунікаційних мережах.

Мета роботи – розкриття особливостей сучасних інфокомунікаційних мереж, аналіз перспективних рішень для інфокомунікаційних мереж, та огляд рішень Інтернету речей для інфокомунікаційних мереж.

Предмет дослідження – проектування мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров'я адаптовану до унікальних вимог цього домену.

Метод дослідження – порівняльний аналіз рішень для інфокомунікаційних мереж.

Для досягнення цієї мети було проведено комплексний аналіз галузі охорони здоров’я для визначення конкретних вимог, викликів і цілей. На основі цього аналізу було розроблено мережеву інфраструктуру з урахуванням таких факторів, як передача даних у реальному часі, безпека даних, сумісність, масштабованість і продуктивність.

Було проведено технологічну оцінку для оцінки існуючої мережевої інфраструктури та технологій, які використовуються в закладах охорони здоров’я. Також було оцінено сумісність, масштабованість і взаємодію існуючих систем із пристроями та додатками, що підтримують IoT.

Розроблено мережеву архітектуру, що визначає розміщення шлюзів, датчиків і сховища. У топології мережевої інфраструктури були розглянуті різні підрозділи охорони здоров’я, включаючи операційні, відділення інтенсивної терапії, лабораторії, відділення невідкладної допомоги, амбулаторні клініки, телемедицину, адміністрування та виставлення рахунків, а також дослідження та освіту.

Комунікаційні протоколи, такі як MQTT, CoAP і HL7, були оцінені та порівняні на основі їхніх характеристик, щоб забезпечити ефективну та надійну передачу даних у додатках IoT для охорони здоров’я.

Було розроблено стратегії керування даними, спрямовані на масштабованість, безпеку та конфіденційність. Передові методи аналітики, включно з машинним навчанням і штучним інтелектом, були досліджені, щоб отримати цінну інформацію з даних IoT охорони здоров’я.

Впроваджуючи запропоновані стратегії та рекомендації, організаціями охорони здоров’я може бути створена безпечна, ефективна та масштабована екосистема Інтернету речей, яка покращує обслуговування пацієнтів, підвищує ефективність роботи та забезпечує конфіденційність і безпеку даних.

Ключові слова: інфраструктура, проектування, IoT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT — Internet of Things (Інтернет речей)
SDN — software-defined networking (програмно-конфігурована мережа)
VNF — virtual network functions (віртуальні мережеві функції)

ВСТУП

Стрімкий розвиток інформаційно-комунікаційних технологій докорінно змінив способи зв'язку, спілкування та обміну інформацією. Сучасне суспільство значною мірою покладається на безперебійне функціонування інформаційно-комунікаційних мереж для забезпечення різних критично важливих послуг і додатків. У міру того, як ці мережі стають все більш складними і взаємопов'язаними, виникають нові виклики, що вимагають інноваційних рішень для забезпечення їхньої ефективності, безпеки і масштабованості. Одним з таких рішень, що має великі перспективи, є Інтернет речей (IoT).

Шляхом критичного аналізу та порівняння з відомими рішеннями проблеми обґрунтовано актуальність та доцільність даної дипломної роботи. В умовах розвитку сучасних інфокомунікаційних мереж дослідження рішень IoT має вирішальне значення для розвитку відповідної галузі науки та промисловості.

Для того, щоб спиратися на існуючий обсяг знань, необхідно коротко проаналізувати напрацювання зарубіжних та вітчизняних вчених з досліджуваної проблеми. Незважаючи на значний прогрес у розумінні та впровадженні рішень IoT, все ще існують аспекти, які ще не отримали належного висвітлення в науковій літературі. Дана дипломна робота зробить внесок у цю сферу, досліджуючи інтеграцію Інтернету речей в сучасні інфокомунікаційні мережі, зокрема, зосереджуючись на викликах та можливостях, які виникають в результаті цієї інтеграції.

Практичне значення отриманих результатів дослідження може бути корисним для різних зацікавлених сторін у сфері інформаційно-комунікаційних мереж. Наступні положення цієї роботи мають потенційне практичне значення:

Організації охорони здоров'я, які значною мірою покладаються на інфокомунікаційні мережі, можуть отримати вигоду від запропонованих рішень IoT. Результати дослідження можуть сприяти розробці інноваційних додатків і

послуг, оптимізації використання ресурсів, вдосконаленню процесів прийняття рішень і підвищенню загальної операційної ефективності охорони здоров'я.

Таким чином, дана дипломна робота має на меті спроектувати мережеву інфраструктуру для охорони здоров’я з підтримкою Інтернету речей. Шляхом вирішення невирішених раніше частин загальної проблеми та на основі існуючих наукових знань, дане дослідження спрямоване на підвищення ефективності роботи мережі, забезпечення інтелектуального управління мережею, а також забезпечення мережевої безпеки та конфіденційності. Практичне значення отриманих результатів має потенційну користь для охорони здоров’я, що в кінцевому підсумку сприятиме розвитку галузі інформаційно-комунікаційних мереж.

1 ОСОБЛИВОСТІ СУЧАСНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Еволюція інформаційно-комунікаційних мереж

Інформаційні та комунікаційні мережі значно розвинулися протягом багатьох років (Рис. 1.1), змінивши спосіб підключення, спілкування та обміну інформацією. Повинно бути розглянуто еволюцію цих мереж, починаючи від традиційних дротових мереж до появи сучасних цифрових мереж. Важливими є ключові віхи, технологічні досягнення та зміни парадигми, які вплинули на їхній розвиток. Розуміння цієї еволюції має вирішальне значення для розробки мережевої інфраструктури з підтримкою Інтернету речей, адаптованої до унікальних вимог конкретної сфери, наприклад охорони здоров'я.

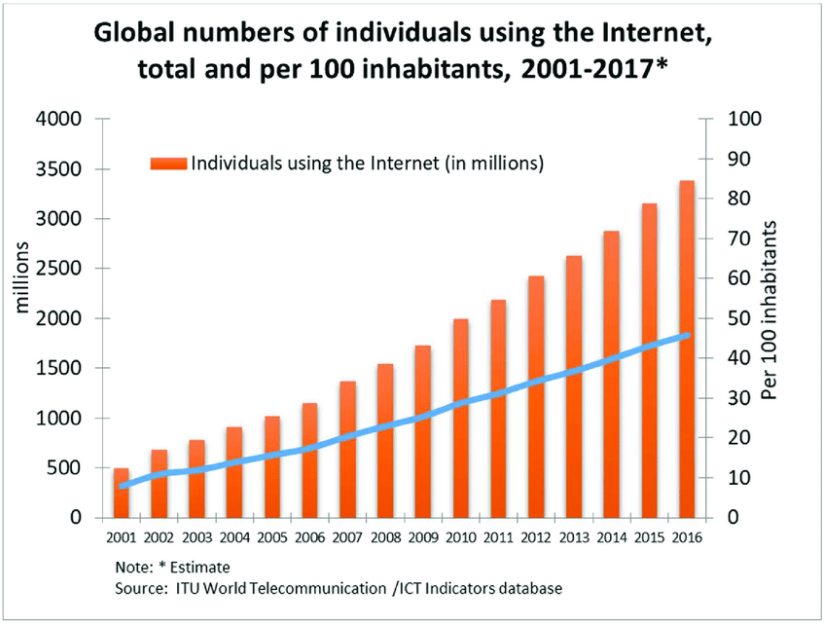

Рисунок 1.1 – Розвиток інформаційно-комунікаційних технологій у світі

Еволюція інформаційних і комунікаційних мереж почалася зі створення традиційних дротових мереж. Ці мережі покладалися на фізичну інфраструктуру, таку як мідні кабелі та волоконно-оптичні кабелі, для передачі сигналів даних. Спочатку ці мережі були обмежені щодо пропускної здатності та пропускної здатності, пропонуючи переважно послуги голосового зв'язку. Проте з розвитком

технологій впровадження цифрової сигналізації та методів мультиплексування дозволило передавати дані через ці мережі.

Попит на швидшу та надійнішу передачу даних призвів до розвитку широкосмугових та високошвидкісних мереж. Широкосмугові технології, такі як цифрова абонентська лінія (DSL), кабельні мережі та волоконна оптика, забезпечили користувачам більшу пропускну здатність і покращене підключення. Цей прогрес підтримав доставку мультимедійного вмісту, потокове відео та служби зв’язку в реальному часі.

Сучасні інформаційні та комунікаційні мережі демонструють кілька ключових характеристик і функцій, які визначають їх роботу та можливості:

- Глобальне підключення: сучасні мережі пропонують глобальне підключення, забезпечуючи безперебійне спілкування та обмін даними через географічні кордони;
- Масштабованість: ці мережі можуть масштабуватися для збільшення кількості користувачів, пристроїв і послуг;
- Сумісність: вони підтримують взаємодію між різними пристроями, платформами та протоколами, забезпечуючи безперебійний зв’язок та інтеграцію;
- Надійність і резервування: сучасні мережі включають механізми резервування та відмовостійкості для забезпечення високої надійності та доступності;
- Безпека даних: заходи безпеки, такі як шифрування, автентифікація та контроль доступу, інтегровані для захисту даних, що передаються через мережу;
- Якість обслуговування (QoS): механізми QoS забезпечують оптимальну продуктивність, затримку, пропускну здатність і надійність для різних типів програм і послуг.

1.2 Конвергенція технологій

Конвергенція різних технологій, включаючи телекомунікації, обчислення та мережі передачі даних, зіграла ключову роль у формуванні сучасних інформаційних і комунікаційних мереж. Конвергенція телекомунікаційних, обчислювальних мереж і мереж передачі даних означає інтеграцію цих технологій в єдину мережеву інфраструктуру. Традиційно ці домени працювали незалежно, з окремою інфраструктурою та спеціальним обладнанням. Однак прогрес у технології полегшив їх інтеграцію, що призвело до більш ефективних і універсальних мережевих архітектур.

Конвергенція технологій забезпечує гнучкість у плані розгортання та управління мережею. З'явилися технології програмно-визначеної мережі (SDN) і віртуалізації мережевих функцій (NFV), які дозволяють динамічну конфігурацію мережі, централізоване керування та швидке розгортання нових послуг. Ця гнучкість сприяє масштабуванню мережі, адаптації до мінливих вимог і надання послуг на основі конкретних вимог.

Конвергенція технологій приносить декілька переваг інформаційним та комунікаційним мережам:

- Розширене підключення: конвергенція забезпечує безперебійне підключення та спілкування в різних доменах, що веде до покращеної співпраці, обміну даними та взаємодії з користувачем;
- Економія: консолідація функцій та інфраструктури зменшує експлуатаційні витрати, оскільки більше не потрібні окремі мережі. Крім того, використання віртуалізації та спільних ресурсів максимізує використання ресурсів, додатково оптимізуючи витрати;

- Покращене надання послуг: Конвергенція дозволяє надавати конвергентні служби, які інтегрують голос, відео та дані, покращуючи загальний досвід користувача та створюючи нові інноваційні програми.

Незважаючи на свої переваги, конвергенція технологій також створює проблеми:

- Складність: інтеграція різних технологій створює складності з точки зору проектування мережі, управління та сумісності. Забезпечення бездоганної інтеграції та сумісності між різними компонентами може бути складним завданням;
- Безпека та конфіденційність: конвергенція технологій збільшує поверхню атаки та вводить нові ризики для безпеки. Захист даних, забезпечення конфіденційності та безпека мережевої інфраструктури стають критичними міркуваннями;
- Набір навичок і досвід: для конвергенції потрібні кваліфіковані фахівці з досвідом у багатьох сферах, включаючи телекомунікації, обчислення та мережі передачі даних. Подолання розриву в навичках і розвиток міждисциплінарних знань може бути складним завданням.

1.3 Масштабованість і гнучкість

Масштабованість і гнучкість мають першочергове значення в сучасних мережах через експоненціальне зростання трафіку даних і динамічний характер вимог користувачів. Мережі мають бути здатними об’єднувати все більшу кількість підключених пристроїв, обробляти великі обсяги даних і адаптуватися до технологічних тенденцій, що розвиваються. Масштабованість гарантує, що мережі можуть рости та розширюватися відповідно до цих вимог, а гнучкість дозволяє ефективно розподіляти ресурси та здатність адаптуватися до мінливих вимог.

Сучасні інформаційні та комунікаційні мережі стикаються з постійним зростанням потреб користувачів і трафіку даних. З поширенням підключених пристроїв, Інтернету речей (IoT) і нових технологій мережі повинні бути масштабованими, щоб обробляти постійно зростаючий обсяг даних. Масштабованість передбачає розробку мережевих архітектур і протоколів, які можуть врахувати зростання кількості користувачів, пристроїв і послуг без шкоди для продуктивності, надійності або якості обслуговування.

Масштабованість і гнучкість є властивими характеристиками сучасних мережевих архітектур (Рис. 1.2). Вони досягаються за допомогою різних механізмів, включаючи модульний дизайн, розподілені системи та хмарні обчислення. Модульна конструкція дозволяє за потреби розширювати мережеві компоненти, забезпечуючи плавне масштабування. Розподілені системи розподіляють обчислювальну потужність і ресурси між кількома вузлами, підвищуючи масштабованість і відмовостійкість. Хмарні обчислення забезпечують масштабовану та гнучку інфраструктуру для мережевих служб, уможливлюючи розподіл ресурсів за вимогою та динамічне масштабування. Також технології програмно-визначеної мережі (SDN) і віртуалізації мережевих функцій (NFV) сприяють масштабованості та гнучкості. SDN відокремлює рівень керування від рівня даних, що забезпечує централізоване управління та контроль, спрощує конфігурацію мережі та забезпечує масштабованість. NFV віртуалізує мережеві функції, дозволяючи динамічно розподіляти та об’єднувати служби, підвищуючи гнучкість і оптимізуючи ресурси.

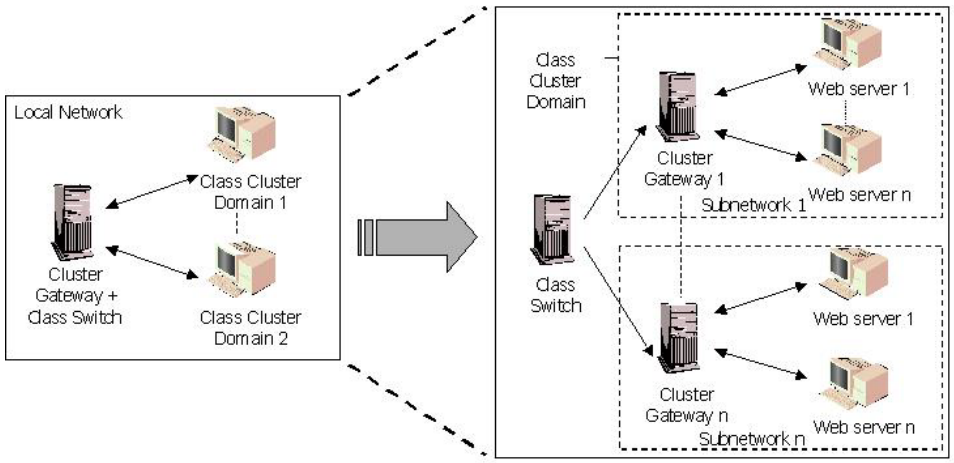

Рисунок 1.2 – Приклад масштабованості і гнучкості

Мережеві протоколи відіграють важливу роль у досягненні масштабованості та гнучкості. Такі протоколи, як IPv6, MPLS і BGP, були розроблені з урахуванням масштабованості, що забезпечує ефективну адресацію, маршрутизацію та керування трафіком. Ці протоколи забезпечують плавне розширення мереж, підтримку більших адресних просторів і оптимізацію ефективності маршрутизації. Такі протоколи, як якість обслуговування (QoS) і інженерний трафік, забезпечують гнучкість розподілу мережевих ресурсів. Механізми QoS визначають пріоритет трафіку, гарантуючи, що критично важливі програми отримують необхідні вимоги до пропускної здатності та затримки. Розробка трафіку забезпечує динамічну маршрутизацію трафіку та балансування навантаження, адаптацію до мінливих умов мережі та оптимізацію використання ресурсів.

Масштабованість і гнучкість є вирішальними міркуваннями при проектуванні мережевої інфраструктури з підтримкою Інтернету речей, адаптованої до конкретної сфери, як-от охорона здоров’я. Середовище охорони здоров’я потребує мереж, які можуть працювати зі зростаючою кількістю пристроїв Інтернету речей, розміщувати медичні додатки з інтенсивним об’ємом даних і адаптуватися до мінливих вимог охорони здоров’я. Масштабованість гарантує, що мережа може розвиватися відповідно до цих вимог, а гнучкість

дозволяє ефективно розподіляти ресурси, пріоритезувати критичний медичний трафік та інтегрувати з існуючими системами охорони здоров’я.

1.4 Надійність і доступність

Надійність та доступність є основними вимогами до сучасних мереж. Надійність означає здатність мережі постійно надавати послуги та дані без збоїв. З іншого боку, доступність означає здатність мережі залишатися доступною та працювати для користувачів, коли їм це потрібно. Обидва атрибути мають вирішальне значення для забезпечення безперебійної роботи систем зв’язку, підтримки критично важливих додатків і підтримки задоволеності користувачів.

Надійність і доступність мають першочергове значення ддя мережевої інфраструктури охорони здоров'я з підтримкою Інтернету речей. Послуги охорони здоров’я значною мірою залежать від підключення до мережі для виконання різноманітних завдань, зокрема моніторингу в реальному часі, передачі даних, телемедицини та віддаленої діагностики. Будь-які збої або простої в мережі можуть мати серйозні наслідки, потенційно вплинувши на обслуговування та безпеку пацієнтів. Тому розробка мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров’я вимагає сильного акценту на надійності та доступності.

Стійкість є ще одним важливим аспектом надійності мережі. Стійкість передбачає здатність мережі швидко відновлюватися після збоїв і відновлювати нормальну роботу. Цього можна досягти за допомогою таких технологій, як мережі самовідновлення, механізми автоматичного відновлення після збоїв, а також швидке виявлення та усунення несправностей. Системи керування мережею, які відстежують стан і продуктивність мережі, можуть відігравати важливу роль у проактивному виявленні та вирішенні потенційних проблем, мінімізуючи час простою та максимізуючи надійність.

Доступність мережі має вирішальне значення, особливо в таких сферах, як охорона здоров’я, де необхідний безперервний доступ до критично важливих послуг. Доступність гарантує, що медичні працівники можуть покладатися на мережу для своєчасного доступу до даних пацієнтів, співпраці з колегами та дистанційних консультацій. Це забезпечує безперебійну роботу медичних пристроїв, телемедичних рішень та інших життєво важливих програм охорони здоров’я.

Щоб досягти високої доступності мережі, можна розгорнути резервні мережеві компоненти, такі як маршрутизатори, комутатори та системи живлення, щоб усунути окремі точки відмови. Крім того, методи балансування навантаження та механізми організації трафіку можуть розподіляти мережевий трафік між кількома шляхами, запобігаючи перевантаженням і забезпечуючи безперервне надання послуг. Надійні стратегії резервного копіювання та аварійного відновлення також необхідні для мінімізації часу простою в разі катастрофічних подій або непередбачених збоїв.

Також доступність мережі має вирішальне значення для підтримки моніторингу в режимі реального часу, віддаленого догляду за пацієнтами та інтеграції пристроїв IoT в охорону здоров’я. Мережа має бути розроблена так, щоб обробляти зростаючий обсяг даних, створених цими пристроями, забезпечувати надійне з’єднання та визначати пріоритетність критично важливих медичних послуг. Зосереджуючись на надійності та доступності, мережева інфраструктура на основі Інтернету речей може забезпечити міцну основу для надання ефективних і безперебійних медичних послуг.

1.5 Якість обслуговування

Якість обслуговування означає здатність мережі забезпечувати передбачувану та надійну роботу, гарантуючи, що різні типи мережевого трафіку отримують необхідний рівень обслуговування. Це передбачає встановлення пріоритетів і керування мережевими ресурсами для досягнення конкретних цілей рівня обслуговування та гарантування певного рівня продуктивності для критичних програм або потоків даних. QoS має вирішальне значення в сучасних мережах, де співіснують різні програми з різними вимогами, включаючи зв'язок у реальному часі, потокове передавання мультимедіа, передачу даних і пристрої IoT.

У контексті теми дипломної роботи QoS відіграє життєво важливу роль у додатках охорони здоров'я (Рис. 1.3). Це гарантує, що критично важливі медичні дані, такі як моніторинг пацієнтів у режимі реального часу, телемедичні консультації та медична візуалізація, мають пріоритет, щоб відповідати суворим вимогам догляду за пацієнтами та безпеки.

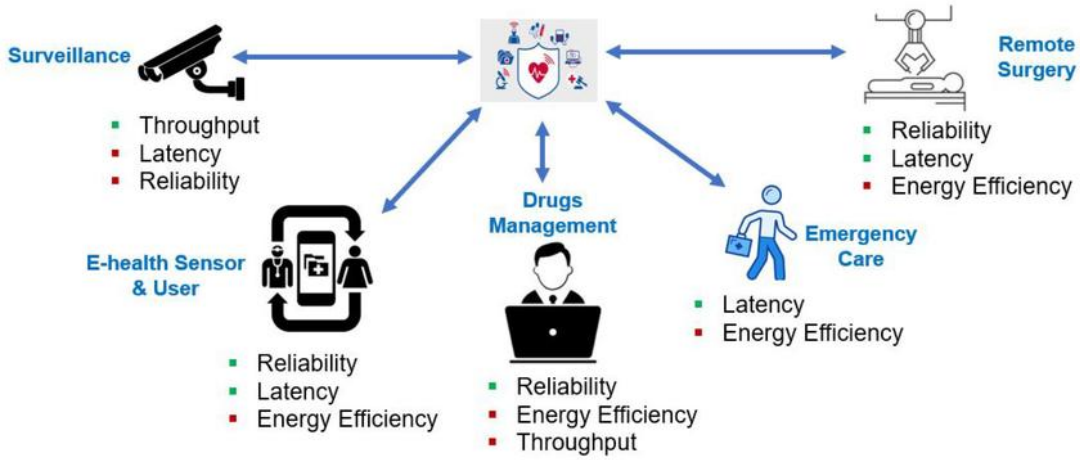

Рисунок 1.3 – Вимоги до якості обслуговування в мережі IoT в охороні здоров'я

Кілька факторів впливають на QoS інформаційних і комунікаційних мереж. Ці фактори включають:

- Продуктивність мережі: загальна продуктивність мережі, включаючи її пропускну здатність, безпосередньо впливає на QoS. Мережа з високопродуктивними можливостями може забезпечити кращий QoS, ефективно обробляючи більші навантаження трафіку та забезпечуючи швидшу передачу даних;
- Затримка: затримка означає затримку під час передачі даних через мережу. Висока затримка може негативно вплинути на програми в реальному часі та інтерактивне спілкування, що призведе до затримок, тремтіння та зниження якості обслуговування. Низька затримка є важливою для програм охорони здоров'я, які вимагають даних у реальному часі, наприклад віддаленого моніторингу та телемедичних консультацій.

Для забезпечення оптимального QoS у мережевих середовищах використовуються різні методи та механізми. До них належать:

- Пріоритезація трафіку: Пріоритезація трафіку на основі його важливості та вимог забезпечує відповідний розподіл мережевих ресурсів. Механізми диференційованих послуг (DiffServ) і якості обслуговування (QoS), як-от класифікація трафіку, маркування та алгоритми постановки в чергу, дозволяють мережевим адміністраторам визначати пріоритетність критичного трафіку охорони здоров'я, гарантуючи, що він отримує необхідну пропускну здатність і низьку затримку;
- Управління смугою пропускання: ефективні методи керування смугою пропускання, такі як формування та контроль трафіку, допомагають регулювати мережевий трафік і запобігати перевантаженням;
- Угоди про якість обслуговування: угоди про рівень обслуговування (SLA) між постачальниками послуг і користувачами окреслюють узгоджені параметри QoS, включаючи затримку, втрату пакетів і пропускну здатність.

2 ПЕРСПЕКТИВНІ РІШЕННЯ ДЛЯ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

2.1 Віртуалізація в інформаційно-комунікаційних мережах

Технології віртуалізації стали фундаментальною опорою сучасних інформаційних і комунікаційних мереж, уможливлюючи абстракцію апаратних ресурсів і створення віртуалізованих мережевих функцій і послуг. Ці технології, зокрема мережева віртуалізація, віртуалізація серверів і програмно-визначена мережа (SDN), пропонують безпрецедентні можливості для проектування та керування мережевими інфраструктурами, адаптованими до конкретних вимог галузі охорони здоров’я.

Віртуалізація мережі, як ключова технологія віртуалізації, дозволяє створювати кілька віртуальних мереж у спільній фізичній мережевій інфраструктурі. Відокремлюючи логічні мережі від базової фізичної інфраструктури, віртуалізація мережі покращує використання ресурсів і покращує ізоляцію та безпеку. З іншого боку, віртуалізація сервера дозволяє розділити фізичний сервер на кілька віртуальних машин, кожна з яких працює під керуванням власної операційної системи та програм. Цей метод оптимізує обчислювальні ресурси шляхом консолідації кількох віртуальних серверів на одному фізичному хості.

Переваги віртуальних мережевих функцій численні. По-перше, вони забезпечують підвищену гнучкість і масштабованість, дозволяючи мережевим операторам динамічно розподіляти та перерозподіляти ресурси на основі попиту. Ця масштабованість особливо актуальна в охороні здоров’я, де мережева інфраструктура повинна адаптуватися до коливань трафіку даних і вимог різних пристроїв IoT. По-друге, віртуалізація підвищує гнучкість, уможливлюючи швидку реконфігурацію та адаптацію мережевих служб. Ця гнучкість має важливе значення в галузі охорони здоров’я, де мережева інфраструктура повинна

підтримувати різноманітні додатки та відповідати мінливим потребам. Нарешті, віртуалізація оптимізує використання ресурсів шляхом ефективного розподілу обчислювальних ресурсів, сховища та мережевих ресурсів. Ця ефективність перетворюється на економію коштів.

Підсумовуючи, технології віртуалізації, включаючи віртуалізацію мережі, віртуалізацію серверів і SDN, пропонують безпрецедентні можливості для проектування мережевих інфраструктур із підтримкою Інтернету речей для охорони здоров'я. Абстракція апаратних ресурсів і створення віртуалізованих мережевих функцій і послуг пропонують численні переваги, включаючи покращену масштабованість, гнучкість і використання ресурсів. Досліджуючи методи віртуалізації для керування мережею а також вивчаючи практичні приклади з реального світу, є можливість отримати цінну інформацію та практичні знання, необхідні для розробки мережевої інфраструктури, яка відповідає унікальним вимогам IoT для охорони здоров'я.

2.2 Програмно-визначена мережа (SDN)

SDN являє собою зміну парадигми в архітектурі мережі, відокремлюючи площину управління від площини даних і централізуючи мережеве керування. Традиційні мережі покладалися на механізми розподіленого керування, де мережеві пристрої приймали незалежні рішення щодо пересилання. На відміну від цього, SDN представляє централізовану площину керування, що дозволяє адміністраторам програмно контролювати та керувати поведінкою мережі за допомогою програмного контролера.

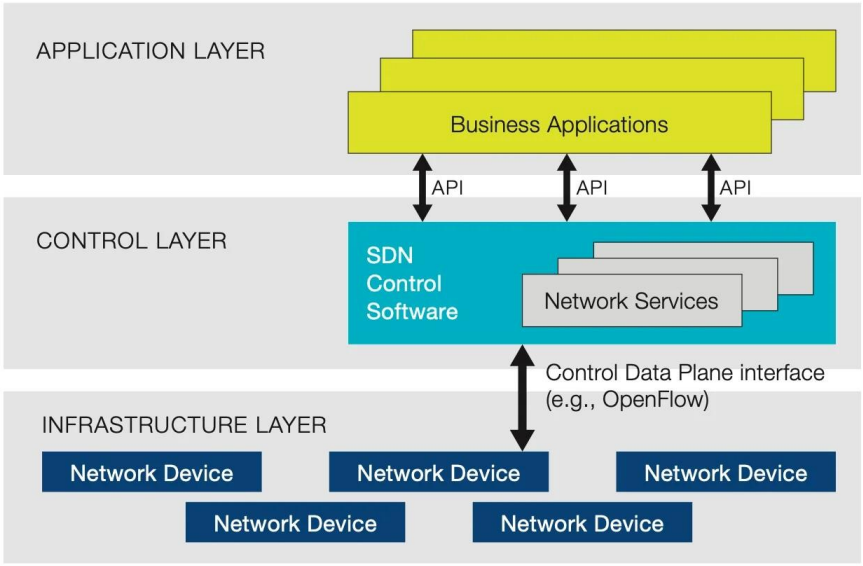

Рисунок 2.1 – Компоненти SDN

Архітектура SDN складається з трьох ключових компонентів: площини даних, площини керування та контролера SDN (Рис. 2.1). Площина даних містить мережеві пристрої, такі як комутатори та маршрутизатори, відповідальні за пересилання пакетів даних. Площина керування, централізована в SDN, містить мережевий інтелект і керує логікою керування для пересилання пакетів. Контролер SDN діє як центральний оркестр, взаємодіючи з площиною керування та керуючи мережевими пристроями за допомогою різних протоколів.

SDN пропонує низку переваг, які мають велике значення для розробки мережевої інфраструктури, що підтримує Інтернет речей у сфері охорони здоров'я. По-перше, спрощене керування мережею досягається за допомогою централізованої площини керування. Це спрощення оптимізує конфігурацію мережі, моніторинг і усунення несправностей, зменшуючи адміністративні витрати та операційні складності.

По-друге, SDN забезпечує можливість програмування, дозволяючи мережевим адміністраторам визначати та застосовувати мережеві політики за

допомогою програмно-визначених правил. Ця можливість програмування забезпечує динамічну реконфігурацію мережі, швидке розгортання нових сервісів і ефективний розподіл ресурсів, що є ключовими аспектами в сценаріях Інтернету речей у сфері охорони здоров'я, де гнучкість і оперативність є життєво важливими.

Крім того, SDN забезпечує покращену видимість мережі та контроль, забезпечуючи детальну інженерію трафіку, контроль якості обслуговування (QoS) і реалізацію політики безпеки. Завдяки централізованій площині керування адміністратори мережі мають цілісне уявлення про мережу, сприяючи проактивному моніторингу, оптимізації трафіку та пом'якшенню загроз.

Мережеві операційні системи (NOS) є важливим компонентом середовищ SDN, діючи як програмний рівень між контролером SDN і мережевими пристроями. NOS забезпечує необхідну абстракцію та інтерфейси для зв'язку з мережевими пристроями, забезпечуючи функції контролю та управління.

У мережах охорони здоров'я SDN забезпечує основу для розробки інфраструктури з підтримкою Інтернету речей. Це забезпечує безпроблемну інтеграцію та керування різноманітними пристроями та датчиками IoT, полегшуючи збір, аналіз і моніторинг даних у реальному часі. SDN також забезпечує точне керування доступом, безпечну передачу даних і динамічне застосування політики, забезпечуючи конфіденційність і безпеку конфіденційної медичної інформації.

Підсумовуючи, програмно-визначена мережа (SDN) відіграє вирішальну роль у сучасних інформаційних і комунікаційних мережах, пропонуючи значні переваги для проектування мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров'я. Розділення площини керування та площини даних, централізоване керування, можливість програмування та динамічна

реконфігурація є ключовими особливостями SDN. Досліджуючи контролери SDN, мережеві операційні системи та протокол OpenFlow, а також досліджуючи випадки використання в реальному світі, ми можемо використовувати потенціал SDN для розробки мережевої інфраструктури, яка відповідає конкретним потребам IoT у сфері охорони здоров'я.

2.3 Віртуалізація мережевих функцій (NFV)

NFV — це архітектурна структура, яка спрямована на віртуалізацію мережевих функцій, які традиційно реалізуються на виділених апаратних пристроях. Він відокремлює мережеві функції від пропрієтарного обладнання та дає змогу розгортати їх як програмні екземпляри, що працюють на стандартизованих апаратних серверах або хмарних середовищах. Цей перехід від апаратних пристроїв до програмних віртуальних мережевих функцій (VNF) забезпечує значну гнучкість, масштабованість і економію коштів.

Архітектура NFV передбачає віртуалізацію мережевих функцій і їх розгортання як VNF на стандартизованому обладнанні або хмарних платформах. Мережеві функції, такі як брандмауери, маршрутизатори, балансувальники навантаження та системи виявлення вторгнень, абстрагуються від спеціального апаратного забезпечення та інкапсульовані в програмні VNF. Ці VNF можна динамічно створювати, масштабувати та об'єднувати разом для створення гнучких мережевих служб, адаптованих до конкретних вимог.

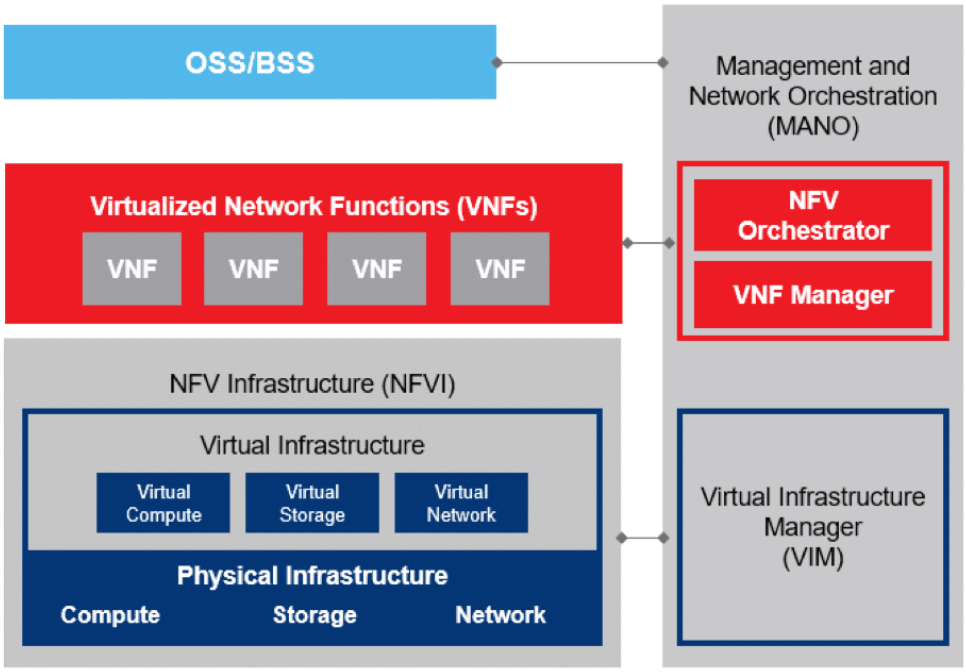

Рисунок 2.2 – Визначення елементів архітектури NFV - взаємозв'язки

NFV приносить численні переваги інформаційним і комунікаційним мережам, узгоджуючи їх із цілями розвитку мережевої інфраструктури IoT, орієнтованої на охорону здоров'я. По-перше, NFV забезпечує підвищену гнучкість, дозволяючи мережевим операторам ефективніше розгортати, масштабувати та керувати мережевими функціями. Завдяки VNF організації можуть динамічно розподіляти ресурси, адаптуватися до мінливих моделей трафіку та швидко запроваджувати нові послуги, підвищуючи гнучкість і швидкість реагування в сценаріях Інтернету речей у сфері охорони здоров'я.

По-друге, NFV веде до значної економії коштів, усуваючи потребу в спеціальних апаратних пристроях. Використовуючи стандартизоване апаратне забезпечення або хмарні ресурси, організації можуть досягти кращого використання ресурсів і скоротити капітальні витрати. Крім того, NFV спрощує процеси обслуговування та оновлення, ще більше знижуючи експлуатаційні витрати.

Крім того, NFV дозволяє надавати та керувати мережевими послугами за допомогою програмно-визначених механізмів. Ця автоматизація покращує швидкість обслуговування, скорочує час підготовки та підвищує ефективність роботи. Це також сприяє масштабованості та еластичності мережі, дозволяючи динамічно розподіляти мережеві ресурси на основі попиту, забезпечуючи оптимальну продуктивність у середовищі IoT для охорони здоров'я.

ONAP — це платформа з відкритим вихідним кодом для наскрізної автоматизації та оркестровки мережі, що підтримує розгортання NFV. Він пропонує модульну та розширювану структуру для проектування послуг, оркестровки та забезпечення. ONAP дозволяє керувати та координувати складні мережеві служби, що включають кілька VNF, забезпечуючи ефективну та надійну роботу.

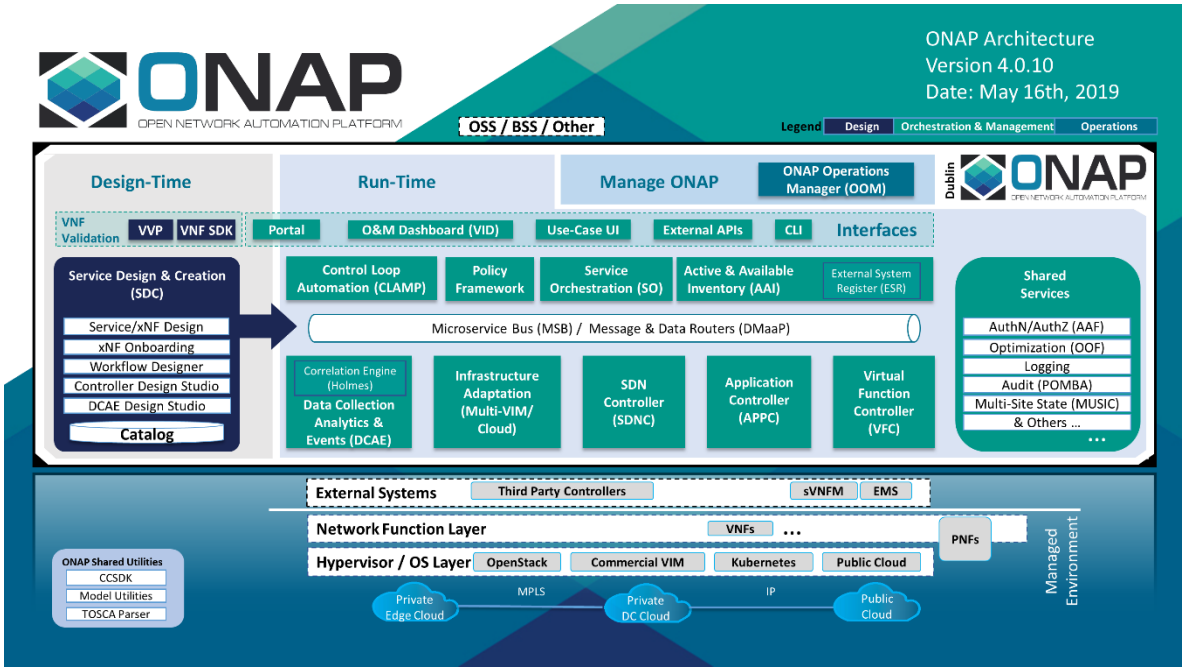

Рисунок 2.3 – Архітектура ONAP

Приклади включають постачальників телекомунікацій, які використовують NFV для покращення надання послуг, покращення масштабованості та забезпечення швидкого розгортання послуг. Постачальники хмарних обчислень також прийняли NFV, щоб пропонувати мережеві послуги, які можна надавати на

вимогу та адаптувати до вимог клієнта. Крім того, NFV відіграє вирішальну роль у сценаріях периферійних обчислень, де пристрої з обмеженими ресурсами можуть перевантажувати мережеві функції у віртуалізоване середовище для підвищення продуктивності та ефективності.

У контексті медичного Інтернету речей тематичні дослідження демонструють, як NFV забезпечує динамічне розгортання та керування мережевими функціями для підтримки критично важливих медичних послуг. Ці розгортання зосереджені на забезпеченні високої доступності, масштабованості та ефективного використання ресурсів у середовищі охорони здоров’я.

Підсумовуючи, віртуалізація мережевих функцій (NFV) трансформувала інформаційні та комунікаційні мережі шляхом віртуалізації мережевих функцій і розгортання їх як програмних екземплярів. NFV пропонує такі переваги, як підвищена гнучкість, економія коштів і швидке розгортання послуг. Організація розгортання NFV за допомогою таких інфраструктур, як ETSI MANO та ONAP, забезпечує ефективне керування та координацію VNF. Реальні приклади з телекомунікацій, хмарних обчислень і периферійних обчислень демонструють практичне застосування NFV у різноманітних мережевих середовищах, у тому числі його потенціал для розробки мережевої інфраструктури, що підтримує Інтернет речей у сфері охорони здоров’я.

2.4 Інші перспективні рішення

Граничні обчислення — це парадигма розподіленого обчислення, яка наближає обчислення та зберігання даних до краю мережі, ближче до пристроїв і джерел даних, які генерують дані. Обробляючи дані та запускаючи програми ближче до джерела, периферійні обчислення зменшують затримку, покращують час відгуку та підвищують загальну продуктивність мережі. Він забезпечує аналіз даних у режимі реального часу, прийняття рішень і локальне зберігання, що

робить його дуже придатним для чутливих до часу додатків і сценаріїв, де дані потрібно обробляти на межі, наприклад, IoT для охорони здоров’я.

Граничні обчислення мають потенціал трансформувати охорону здоров’я, забезпечуючи швидшу та ефективнішу обробку даних, уможливлюючи моніторинг і аналіз у реальному часі, а також сприяючи швидкому реагуванню на важливі медичні процедури. Він також усуває проблеми щодо конфіденційності та безпеки даних, зберігаючи конфіденційні медичні дані локалізованим і зменшуючи потребу в передачі даних на централізовані хмарні сервери.

Розрізання мережі — це нова технологія, яка дозволяє створювати кілька віртуальних мереж у спільній фізичній мережевій інфраструктурі. Це дозволяє мережевим операторам розподіляти мережеві ресурси, включаючи пропускну здатність, затримку та якість обслуговування, щоб відповідати конкретним вимогам різних програм або груп користувачів. Кожен сегмент мережі працює як незалежний екземпляр мережі, налаштований відповідно до потреб конкретних програм, послуг або галузей.

Розрізання мережі пропонує значний потенціал для розробки мережевої інфраструктури IoT, орієнтованої на охорону здоров’я. Це дозволяє створювати спеціальні сегменти мережі, адаптовані до програм охорони здоров’я, забезпечуючи необхідну якість обслуговування, низьку затримку та високу надійність. Наприклад, сегмент мережі, призначений для віддаленого моніторингу пацієнтів, може визначати пріоритет пропускної здатності для передачі даних у реальному часі, тоді як інший сегмент для медичних зображень може визначати пріоритети з низькою затримкою та високою пропускною здатністю.

У сфері охорони здоров’я мережі 5G можуть підтримувати телемедичні послуги в режимі реального часу, дистанційний моніторинг пацієнтів і давати відеоконсультації з високою роздільною здатністю. Висока пропускна здатність і

низька затримка мереж 5G полегшують передачу великих наборів медичних даних, таких як медичні зображення або дані пацієнтів у реальному часі, що дозволяє медичним працівникам швидко приймати обґрунтовані рішення. Крім того, мережі 5G можуть підтримувати широке підключення, дозволяючи бездоганно інтегрувати велику кількість пристроїв і датчиків IoT у мережі охорони здоров'я.

Реальні приклади та тематичні дослідження демонструють практичну реалізацію та вплив цих рішень у різних мережевих сценаріях. Ці приклади включають успішне розгортання периферійних обчислень у середовищі охорони здоров'я, демонструючи їх ефективність у покращенні догляду за пацієнтами, оптимізації використання ресурсів і уможливленні аналізу даних у реальному часі на краю мережі. Крім того, тематичні дослідження висвітлюють застосування нарізки мережі в мережах охорони здоров'я, демонструючи, як можна створювати налаштовані зрізи мережі для підтримки конкретних служб охорони здоров'я, таких як віддалений моніторинг або телемедицина.

Крім того, тематичні дослідження демонструють трансформаційний потенціал технологій 5G в охороні здоров'я. Вони ілюструють, як мережі 5G забезпечують високошвидкісне з'єднання з низькою затримкою для цілого ряду програм охорони здоров'я, від переносних пристроїв до віддалених.

3 ОГЛЯД РІШЕНЬ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

3.1 IoT в охороні здоров’я

Швидкий розвиток технологій IoT відкрив нові можливості для революції в наданні медичної допомоги. Застосування IoT в охороні здоров’я має потенціал для значного покращення результатів лікування пацієнтів, підвищення ефективності роботи та зміни способу надання медичних послуг. Цей підрозділ слугує вступом до трансформаційної ролі IoT у секторі охорони здоров’я.

Концепція IoT в охороні здоров’я обертається навколо взаємопов’язаності медичних пристроїв, датчиків і систем, що забезпечує безперебійний обмін даними та інформацією. Завдяки інтеграції технологій IoT у медичне середовище постачальники медичних послуг можуть збирати дані в режимі реального часу з різних джерел, віддалено контролювати пацієнтів і приймати рішення на основі даних для більш персоналізованого та ефективного лікування.

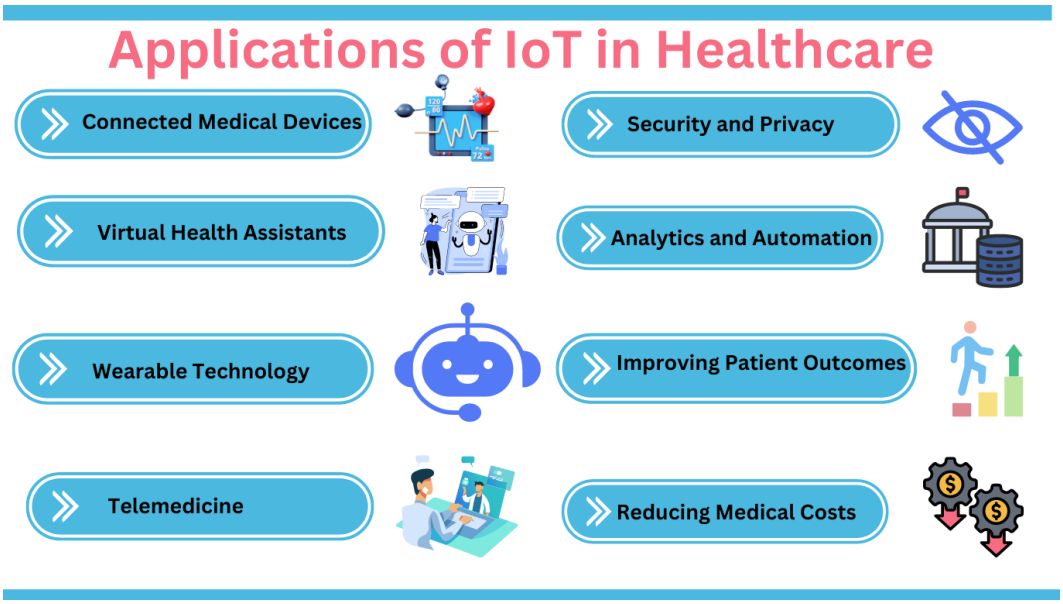

Рисунок 3.1 – Додатки IoT в охороні здоров’я

Однією з ключових переваг IoT в охороні здоров’я є можливість передачі даних у реальному часі. Підключені медичні пристрої та датчики можуть збирати життєво важливі показники, інформацію про здоров’я пацієнта та дані про навколишнє середовище в режимі реального часу, дозволяючи медичним працівникам віддалено контролювати пацієнтів, виявляти аномалії та оперативно втручатися, коли це необхідно. Ця можливість моніторингу в реальному часі має потенціал для значного покращення результатів лікування пацієнтів, особливо для осіб із хронічними захворюваннями або тих, хто потребує постійного моніторингу.

Крім того, IoT в охороні здоров’я може сприяти підвищенню операційної ефективності. Автоматизуючи різні процеси та використовуючи пристрої з підтримкою Інтернету речей, організації охорони здоров’я можуть оптимізувати робочі процеси, скоротити ручні завдання та оптимізувати розподіл ресурсів. Наприклад, системи управління запасами, що використовують датчики Інтернету речей, можуть відстежувати медичне приладдя, забезпечуючи своєчасне поповнення запасів і мінімізуючи відходи. Програми дистанційного моніторингу та телемедицини також можуть зменшити потребу в частих відвідуваннях лікарень, звільняючи ресурси охорони здоров’я та покращуючи доступність медичної допомоги.

Підсумовуючи, запровадження IoT в охороні здоров’я підкреслює його трансформаційний потенціал у покращенні надання медичної допомоги, покращенні результатів лікування пацієнтів та підвищенні операційної ефективності. Концепція взаємопов’язаних медичних пристроїв і систем є основою рішень IoT в охороні здоров’я. Розробка надійної та захищеної мережевої інфраструктури має вирішальне значення для підтримки унікальних вимог медичних додатків Інтернету речей, включаючи передачу даних у реальному часі, безпеку даних та взаємодію.

3.2 Архітектура Інтернету речей для охорони здоров’я

Рішення Інтернету речей для охорони здоров’я покладаються на чітко визначену архітектуру, яка забезпечує бездоганну інтеграцію та взаємодію різних компонентів і систем. У цьому підрозділі наведено огляд архітектури рішень IoT для охорони здоров’я та досліджено різні рівні, залучені до створення таких архітектур.

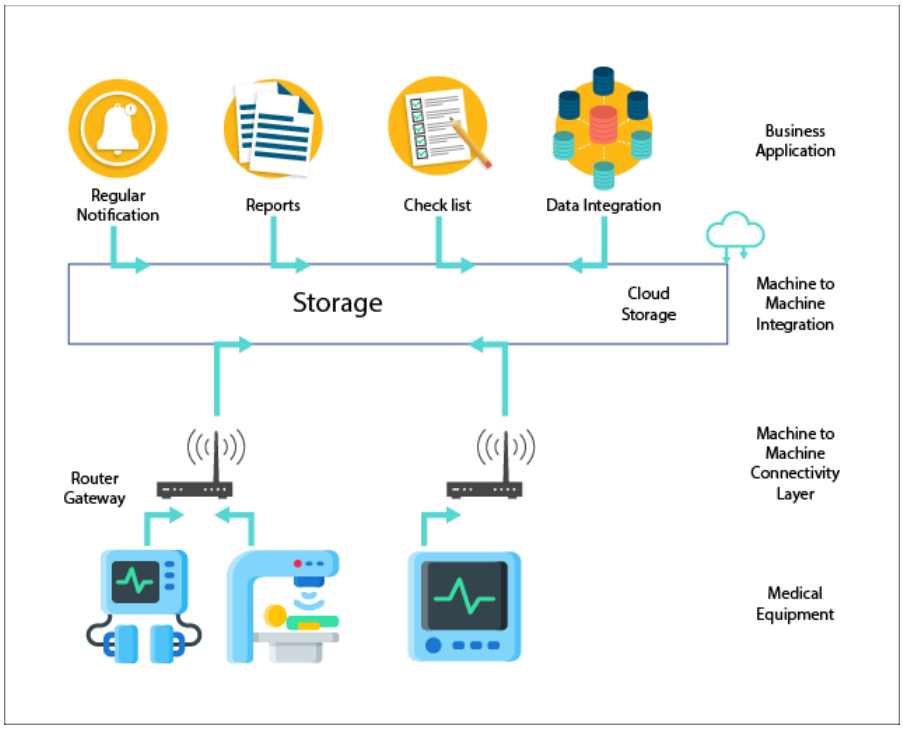

Рисунок 3.2 – Приклад архітектури

Сенсорний рівень: сенсорний рівень формує основу архітектури IoT для охорони здоров’я. Він включає в себе датчики, медичні пристрої, носії та інші засоби збору даних, які збирають інформацію в реальному часі про стан здоров’я пацієнтів, умови навколишнього середовища та інші відповідні параметри. Ці датчики відіграють вирішальну роль у зборі точних і своєчасних даних, які є основою для подальшої обробки та аналізу.

Мережевий рівень: мережевий рівень забезпечує інфраструктуру підключення, яка забезпечує безперебійну передачу даних між сенсорним рівнем та іншими компонентами архітектури IoT. Він охоплює технології дротового та бездротового зв'язку, такі як Wi-Fi, Bluetooth, стільникові мережі або спеціалізовані протоколи зв'язку для охорони здоров'я. Надійна та безпечна передача даних має важливе значення для забезпечення цілісності та конфіденційності конфіденційної медичної інформації.

Рівень проміжного програмного забезпечення: рівень проміжного програмного забезпечення діє як міст між нижніми рівнями та прикладним рівнем архітектури IoT. Це полегшує обробку даних, інтеграцію та керування. Цей рівень включає такі компоненти, як шлюзи даних, хмарні служби та периферійні обчислювальні платформи. Дані, зібрані на сенсорному рівні, обробляються, узагальнюються та перетворюються на значущу інформацію, яку можуть використовувати програми та служби охорони здоров'я.

Рівень додатків. Рівень додатків — це найвищий рівень архітектури IoT, на якому розробляються та розгортаються спеціальні додатки та послуги для охорони здоров'я. Ці програми використовують оброблені дані для забезпечення моніторингу в реальному часі, діагностичної підтримки, прогнозної аналітики, дистанційного керування пацієнтами та інших медичних послуг. Вони дозволяють медичним працівникам приймати обґрунтовані рішення, покращувати догляд за пацієнтами та оптимізувати надання медичної допомоги.

Розробка масштабованої, безпечної та сумісної архітектури IoT для охорони здоров'я породжує кілька проблем і міркувань. Масштабованість має вирішальне значення для забезпечення зростаючої кількості підключених пристроїв і збільшення обсягу даних, що генеруються в медичних середовищах. Заходи безпеки, такі як шифрування даних, контроль доступу та автентифікація, необхідні для захисту конфіденційної інформації пацієнта від несанкціонованого

доступу або порушення даних. Взаємодія забезпечує бездоганну інтеграцію та зв'язок між різними пристроями, системами та програмами, забезпечуючи ефективний обмін даними та співпрацю між постачальниками медичних послуг і зацікавленими сторонами.

3.3 Комунікаційні протоколи IoT для охорони здоров'я

Ефективні протоколи зв'язку необхідні для безпечного та ефективного обміну даними в мережах IoT. У контексті програм охорони здоров'я, де надійна передача даних у режимі реального часу є критичною, вибір відповідних протоколів зв'язку стає ще більш важливим. У цьому підрозділі розглядаються комунікаційні протоколи, які спеціально підходять для додатків Інтернету речей у сфері охорони здоров'я, включаючи:

- MQTT (телеметричний транспорт із чергою повідомлень): MQTT — це легкий протокол на основі публікації та підписки, який широко використовується в програмах IoT, зокрема в охороні здоров'я. Він розроблений для ефективного спілкування в середовищах з обмеженими ресурсами. Модель публікації-підписки MQTT дозволяє пристроям публікувати дані центральному брокеру, який потім доставляє дані зацікавленим передплатникам. Він забезпечує асинхронний зв'язок у режимі реального часу, що робить його придатним для додатків, які вимагають своєчасного оновлення, наприклад віддаленого моніторингу пацієнтів і систем оповіщення;
- CoAP (Constrained Application Protocol): CoAP — це спеціалізований протокол, розроблений для обмежених пристроїв IoT, особливо тих, що працюють у середовищах із низьким енергоспоживанням і низькою пропускною здатністю. Він побудований на основі архітектури RESTful і використовує для зв'язку протокол UDP. CoAP забезпечує ефективне виявлення ресурсів, простий обмін повідомленнями та підтримку

багатоадресного зв'язку. Його енергоефективність і простота роблять його добре придатним для додатків Інтернету речей у сфері охорони здоров'я, таких як портативні пристрої та системи інтер'єрного проживання;

- HL7 (Сьомий рівень охорони здоров'я): HL7 — широко використовуваний стандарт для обміну даними в галузі охорони здоров'я та взаємодії. Він визначає набір протоколів, форматів і стандартів для електронного обміну клінічними та адміністративними даними. HL7 полегшує інтеграцію різних систем охорони здоров'я, таких як електронні медичні записи (EHR), медичні пристрої та додатки для охорони здоров'я. Його надійність, гнучкість і широке застосування в галузі охорони здоров'я роблять його критично важливим протоколом для сумісності та безперебійного обміну даними.

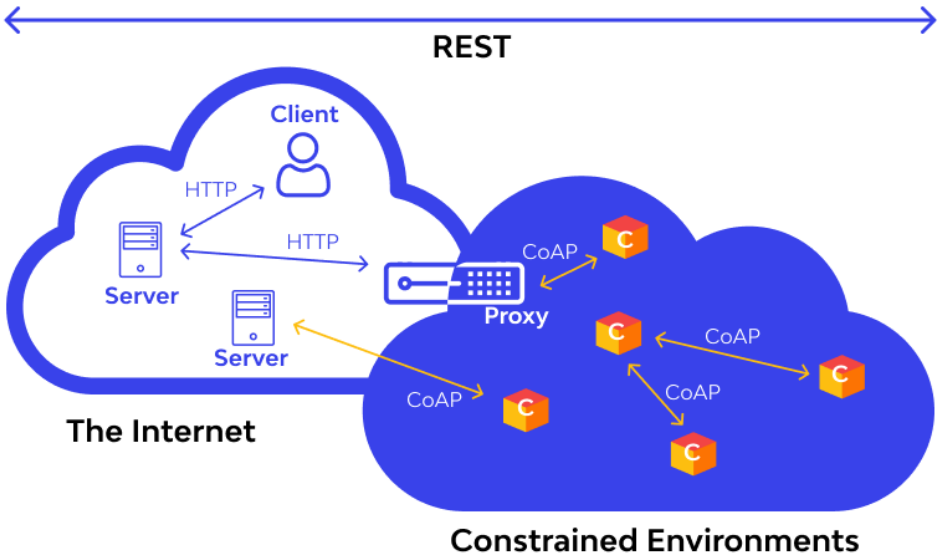

Рисунок 3.3 – Приклад CoAP

Вибираючи протоколи зв'язку для додатків Інтернету речей у сфері охорони здоров'я, слід враховувати кілька факторів:

- Розмір даних: потрібно враховувати розмір даних, що передаються, і можливості залучених пристроїв. Такі протоколи, як MQTT і CoAP,

розроблені для ефективної передачі даних невеликого розміру, тоді як HL7 підтримує обмін великими та складнішими даними охорони здоров'я;

- Надійність: оцінка необхідності надійної передачі даних. MQTT і CoAP забезпечують механізми для надійної доставки повідомлень, гарантуючи, що дані не будуть втрачені або пошкоджені під час передачі;
- Енергоефективність: споживання енергії є вирішальним аспектом, особливо для пристроїв IoT з живленням від батареї. Такі протоколи, як CoAP, з їхньою легкою конструкцією та низькими накладними витратами є більш енергоефективними порівняно з іншими протоколами;
- Інтероперабельність: потрібно враховувати вимоги до інтероперабельності екосистеми Інтернету речей у сфері охорони здоров'я. HL7, будучи широко поширеним стандартом, забезпечує сумісність і повну інтеграцію з існуючими системами та технологіями охорони здоров'я.

Таким чином, вибір відповідних протоколів зв'язку має важливе значення для додатків Інтернету речей у сфері охорони здоров'я. MQTT, CoAP і HL7 є відомими протоколами в галузі охорони здоров'я, кожен з яких пропонує унікальні функції та переваги. При виборі протоколу слід враховувати такі фактори, як розмір даних, надійність, енергоефективність і взаємодію, щоб підтримувати головну мету розробки мережевої інфраструктури, що підтримує Інтернет речей для охорони здоров'я, адаптованої до унікальних вимог цього домену.

3.4 Управління даними та аналітика в IoT охорони здоров'я

Ефективні протоколи зв'язку необхідні для безпечного та ефективного обміну даними в мережах IoT. У контексті програм охорони здоров'я, де надійна передача даних у режимі реального часу є критичною, вибір відповідних протоколів зв'язку стає ще більш важливим. У цьому підрозділі розглядаються комунікаційні протоколи, які спеціально підходять для додатків Інтернету речей у сфері охорони здоров'я, включаючи MQTT, CoAP і HL7.

Управління даними та аналітика відіграють важливу роль у використанні повного потенціалу рішень Інтернету речей у сфері охорони здоров'я. З розповсюдженням підключених пристроїв і датчиків генеруються величезні обсяги даних, що створює як проблеми, так і можливості. Впровадження рішень для управління даними та аналітикою:

- Методи зберігання даних. Обробка величезної кількості даних, створених медичними пристроями IoT, потребує ефективних методів зберігання даних. Традиційним базам даних може бути важко масштабувати та обробляти швидкість і різноманітність даних IoT;
- Безпека та конфіденційність даних. Дані охорони здоров'я є дуже конфіденційними та підпадають під суворі правила безпеки та конфіденційності. Захист інформації про пацієнта, забезпечення цілісності даних і запобігання несанкціонованому доступу є критично важливими факторами в IoT охорони здоров'я.;
- Розширена аналітика: для отримання значущої інформації з даних Інтернету речей охорони здоров'я потрібні передові методи аналітики. Алгоритми машинного навчання (ML) і штучного інтелекту (AI) можна використовувати для аналізу зібраних даних, виявлення закономірностей і створення прогнозів або рекомендацій.

Завдяки ефективному управлінню та аналізу медичних даних IoT постачальники медичних послуг можуть отримати цінну інформацію для покращення догляду за пацієнтами, раннього виявлення захворювань та оптимізованого розподілу ресурсів. Для досягнення основної мети — розробки мережевої інфраструктури, що підтримує Інтернет речей для охорони здоров'я, адаптованої до унікальних вимог цього домену, важливо вирішити проблеми та скористатися можливостями, які надає управління даними та аналітика в IoT в галузі охорони здоров'я.

3.5 Стандарти та правила Інтернету речей у сфері охорони здоров’я

Стандарти та правила є важливими компонентами успішного розгортання та експлуатації рішень Інтернету речей у галузі охорони здоров’я. Вони містять вказівки та вимоги, які забезпечують взаємодію, безпеку даних і етичне використання технологій IoT. У цьому підрозділі наведено огляд ключових стандартів і нормативних актів, що стосуються галузі Інтернету речей у сфері охорони здоров’я, підкреслюючи їх значення та наголошуючи на важливості дотримання цих стандартів і нормативних актів. Стандарти та правила Інтернету речей у сфері охорони здоров’я наступні:

- Закон про перенесення та підзвітність медичного страхування (HIPAA). Він встановлює стандарти захисту та конфіденційності індивідуальної інформації про здоров’я, відомої як захищена інформація про здоров’я (PHI). Відповідність нормам HIPAA має вирішальне значення при розробці та впровадженні рішень Інтернету речей у сфері охорони здоров’я, оскільки це забезпечує конфіденційність даних пацієнтів, контролює доступ до PHI та вимагає заходів безпеки для захисту від несанкціонованого розголошення;
- Загальний регламент захисту даних (GDPR): GDPR — це всеосяжний нормативний акт, прийнятий у Європейському Союзі (ЄС), який регулює збір, обробку та зберігання персональних даних, у тому числі даних про здоров’я. Організації охорони здоров’я, які працюють в ЄС або обробляють дані громадян ЄС, повинні дотримуватися GDPR;
- Continua Health Alliance: Continua Health Alliance – це організація, яка сприяє взаємодії та сумісності технологій охорони здоров’я. Він надає рекомендації та програми сертифікації для забезпечення бездоганної інтеграції та сумісності пристроїв, програм і систем Інтернету речей. Дотримання стандартів Continua Health Alliance забезпечує ефективну

взаємодію рішень IoT для охорони здоров'я, сприяючи обміну даними та заохочуючи взаємодію пристроїв і послуг для охорони здоров'я;

- Міжнародна організація стандартизації (ISO): ISO розробила низку стандартів, застосовних до галузі охорони здоров'я та розгортання IoT. ISO 27799 фокусується на управлінні інформаційною безпекою в організаціях охорони здоров'я, тоді як ISO 80001 стосується управління IT-мережами, що містять медичні пристрої. Ці стандарти містять вказівки щодо управління ризиками, забезпечення якості та контролю безпеки, специфічні для середовищ Інтернету речей у сфері охорони здоров'я. Дотримання стандартів ISO підвищує безпеку даних, безпеку пацієнтів і дотримання нормативних вимог.

Рисунок 3.4 – Вимоги щодо відповідності HIPAA

Дотримання відповідних стандартів і правил має вирішальне значення при розробці мережевої інфраструктури, що підтримує Інтернет речей для охорони здоров'я. Дотримання цих стандартів забезпечує захист конфіденційності пацієнтів, безпеку даних і взаємодію систем IoT. Це також зміцнює довіру між пацієнтами, постачальниками медичних послуг і регуляторними органами, сприяючи широкому впровадженню рішень IoT в охороні здоров'я. Розглядаючи та узгоджуючи ці стандарти та правила, може бути досягнуто мети щодо розробки

мережевої інфраструктури з підтримкою Інтернету речей, адаптованої до унікальних вимог галузі охорони здоров’я.

4 РОЗРОБКА ТА ДОСЛІДЖЕННЯ РІШЕННЯ, ПРОЕКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ З ПІДТРИМКОЮ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ОХОРОНИ ЗДОРОВ'Я АДАПТОВАНУ ДО УНІКАЛЬНИХ ВИМОГ ЦЬОГО ДОМЕНУ

4.1 Визначення вимог та цілей

Перше що потрібно розглянути це зацікавлені сторони та їхні потреби які включають в себе постачальників медичних послуг, пацієнтів та адміністраторів.

Постачальники медичних послуг потребують повної інтеграції даних: мережева інфраструктура повинна забезпечувати інтеграцію даних із багатьох джерел, таких як медичні пристрої, електронні записи про стан здоров’я (EHR) і системи моніторингу, щоб забезпечити комплексне уявлення про стан здоров’я пацієнта. Також постачальникам медичних послуг потрібні можливості моніторингу в режимі реального часу для відстеження життєво важливих показників пацієнтів, дотримання ліків і загального стану здоров’я. Система повинна генерувати попередження та сповіщення для медичних працівників у разі критичних подій або аномалій. Захист даних пацієнтів має вирішальне значення, тому мережева інфраструктура має включати надійні заходи безпеки, щоб забезпечити конфіденційність, цілісність і доступність даних.

Пацієнти в свою чергу потребують постійного моніторингу та індивідуального догляду, що дозволить їм залишатися вдома, отримуючи необхідні медичні послуги. Інфраструктура мережі повинна забезпечувати віддалений моніторинг життєво важливих показників, нагадування про прийом ліків та інтерактивне спілкування з постачальниками медичних послуг.Також пацієнти хвилюються щодо конфіденційності та безпеки своїх медичних даних. Інфраструктура має надавати пріоритет конфіденційності даних, управлінню згодою та дозволяти пацієнтам контролювати інформацію про своє здоров’я.

Адміністратори ж потребують мережеву інфраструктуру яка має бути масштабованою та сумісною, здатною підтримувати велику кількість підключених пристроїв та інтегруватися з існуючими системами охорони

здоров’я, такими як EHR та лікарняні інформаційні системи. У свою чергу рішення має бути економічно ефективним з точки зору розгортання, обслуговування та операційних накладних витрат. Воно повинне забезпечувати баланс між продуктивністю та доступністю.

В свою чергу Цілі мережевої інфраструктури містять в собі:

1. Покращення моніторингу пацієнтів:

– Увімкнення постійного моніторингу життєво важливих показників пацієнтів, дозволяючи постачальникам медичних послуг виявляти критичні події та реагувати на них у режимі реального часу;
– Сприяння віддаленому моніторингу пацієнтів, скорочуючи повторну госпіталізацію та надаючи персоналізований догляд поза медичними закладами.

2. Підвищення операційної ефективності:

– Оптимізація процесів збору, агрегації та аналізу даних, зменшивши ручні зусилля та можливі помилки;
– Покращення координації медичної допомоги між медичними працівниками за допомогою спільного доступу до інформації про пацієнтів і централізованих каналів зв’язку.

3. Увімкнення віддалених медичних послуг:

– Сприяння послугам телемедицини, дозволяючи пацієнтам отримувати медичні консультації, дистанційну діагностику та подальше спостереження без фізичних візитів;
– Покращення доступності медичних послуг, особливо для пацієнтів у віддалених районах або з обмеженою мобільністю.

4. Забезпечення безпеки та конфіденційності:

- Застосування надійних заходів безпеки, щоб захистити дані пацієнтів від несанкціонованого доступу або злому;
- Дотримання правил конфіденційності, дозволяючи пацієнтам контролювати свої дані та надаючи доступ лише авторизованим медичним працівникам.

4.2 Технологічна оцінка

Розглядаючи існуючу мережеву інфраструктуру та технології, потрібно виділити локальні мережі (LAN) і глобальні мережі (WAN), електронні медичні записи (EHR) і системи обміну медичною інформацією (HIE) а також медичні прилади та датчики.

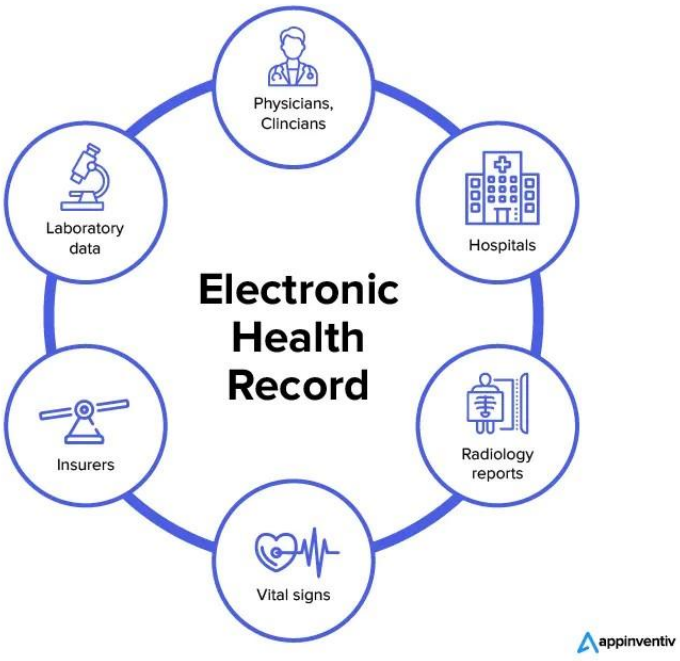

Рисунок 4.1 – Будова EHR

Більшість закладів охорони здоров’я створили локальні та глобальні мережі для підтримки внутрішнього зв’язку та підключення до зовнішніх мереж. Локальні мережі забезпечують локальне підключення в межах закладу, а глобальні мережі забезпечують зв’язок між різними місцями та зовнішніми системами. Існуюча інфраструктура LAN і WAN може служити основою для

впровадження IoT в охороні здоров’я, але може вимагати вдосконалення для обробки збільшеного трафіку даних від пристроїв IoT. EHR зазвичай використовуються для зберігання та керування медичними записами пацієнтів в електронному вигляді, сприяючи ефективному обміну інформацією між постачальниками медичних послуг. Також системи HIE дозволяють обмінюватися інформацією про здоров’я між різними організаціями охорони здоров’я, забезпечуючи безперервність медичної допомоги. Беручи ло уваги IoT, повинна бути інтеграція пристроїв і додатків IoT з існуючими системами EHR і HIE так як має вирішальне значення для безперебійної інтеграції даних і забезпечення цілісного уявлення про здоров’я пацієнтів. Медичні заклади використовують різні медичні пристрої та датчики для моніторингу життєво важливих показників пацієнтів, таких як частота серцевих скорочень, артеріальний тиск і температура.

Рисунок 4.2 – Будова HIE

Розглядаючи нові технології та рішення IoT потрібно виділити протоколи підключення IoT, Edge Computing і Fog Computing, а також рішення безпеки та конфіденційності. Пристрої IoT потребують надійних і ефективних варіантів підключення. Загальні протоколи, такі як Wi-Fi, Bluetooth і Zigbee, можна

використовувати залежно від конкретних випадків використання. Технології глобальної мережі з низьким енергоспоживанням (LPWAN), такі як LoRaWAN або NB-IoT, можуть бути придатними для віддаленого моніторингу пацієнтів у районах з обмеженим покриттям мережі. Та при виборі протоколу підключення слід враховувати такі фактори, як швидкість передачі даних, радіус дії, енергоспоживання та вимоги до безпеки.

Для обробки й аналізу даних, згенерованих Інтернетом речей, ближче до джерела даних може бути використано периферійні обчислення та туманні обчислення, які зменшують затримку та вимоги до пропускної здатності мережі.

Також важливим є сумісність, масштабованість і взаємодія:

Сумісність:

- Існуючі системи охорони здоров’я, такі як EHR та HIE, слід оцінити на їх сумісність із технологіями IoT;
- Необхідно розробити інтерфейси та API, щоб забезпечити безперебійну інтеграцію та обмін даними між пристроями IoT та існуючими системами.

Масштабованість:

- Мережева інфраструктура повинна бути розроблена таким чином, щоб враховувати зростаючу кількість пристроїв IoT і зростаючий обсяг генерованих даних;
- Розгляд масштабованості має включати ємність мережі, можливості зберігання та обчислювальні ресурси.

Взаємодія:

- Взаємодія між різними пристроями IoT, програмами та існуючими системами охорони здоров’я має важливе значення для безперебійного потоку даних і співпраці;

- Стандарти та протоколи, такі як HL7 FHIR (Fast Healthcare Interoperability Resources), слід розглянути для забезпечення сумісності та сумісності.

4.3 Проектування архітектури мережі

Топологія мережі:

- Топологія мережі розроблена для підтримки розподіленої та взаємопов’язаної системи, яка полегшує обмін даними та зв’язок між пристроями IoT, шлюзами та серверними системами;
- Запроваджено комбінацію локальних мереж (LAN) і глобальних мереж (WAN), для забезпечення як локального підключення в межах медичних установ, так і підключення в різних місцях;
- Хмарні рішення використовуються для централізованого зберігання та аналізу даних, створених IoT, забезпечуючи масштабованість і легкий доступ.

Рисунок 4.3 – Топологія лікарні

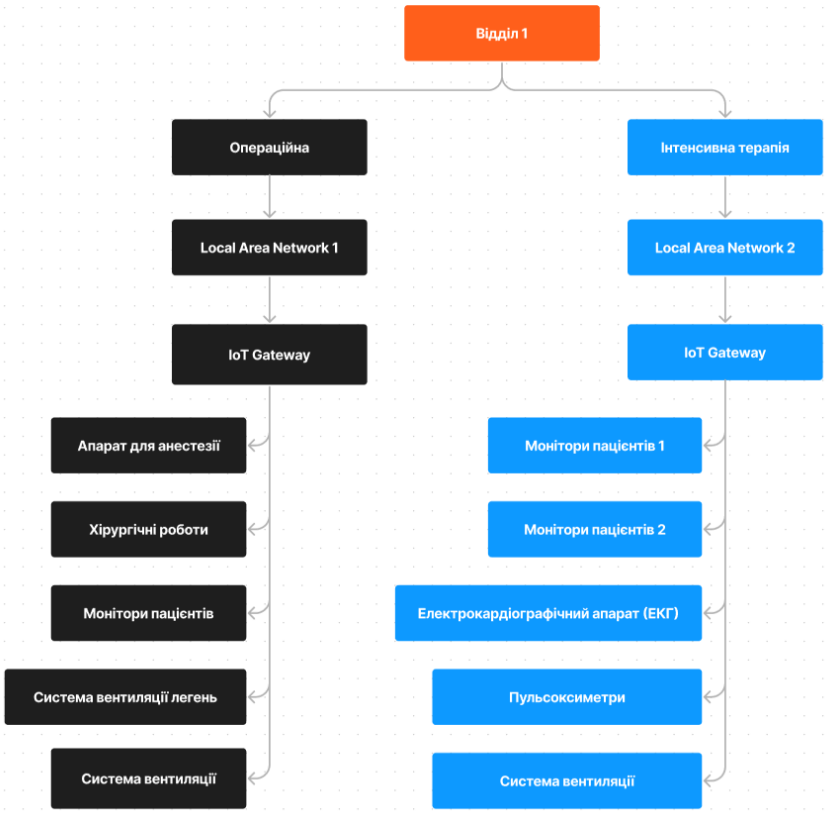

Рисунок 4.4 – Топологія першого відділу

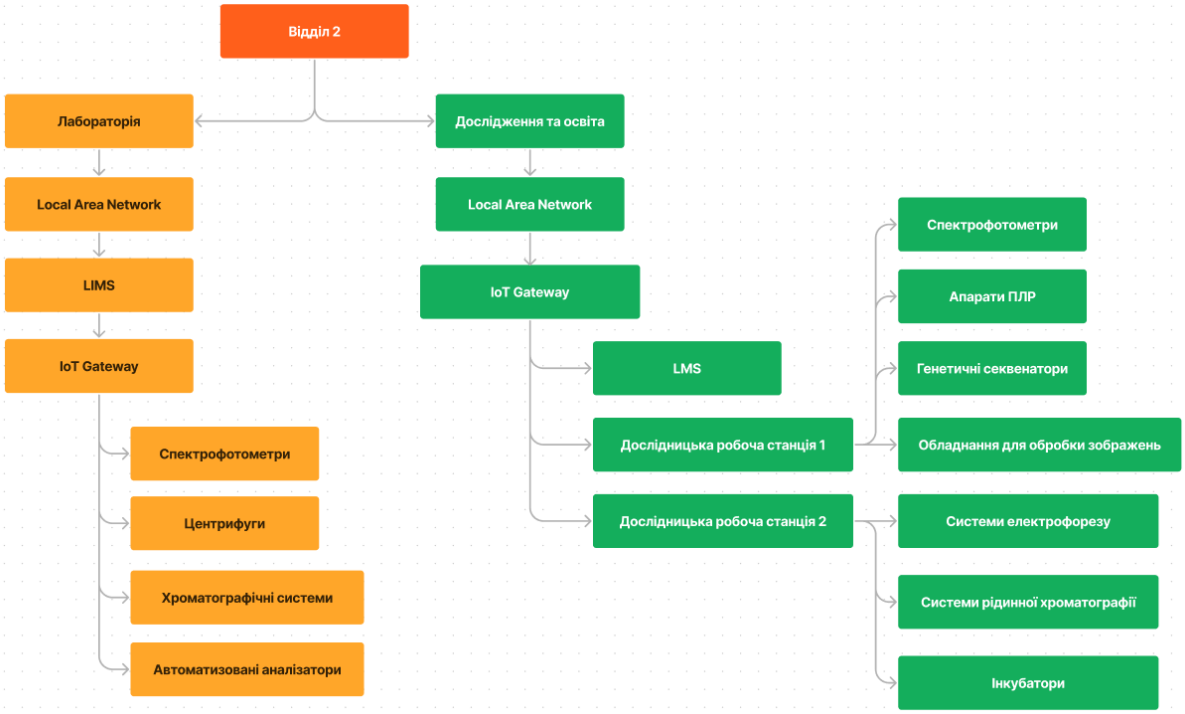

Рисунок 4.5 – Топологія другого відділу

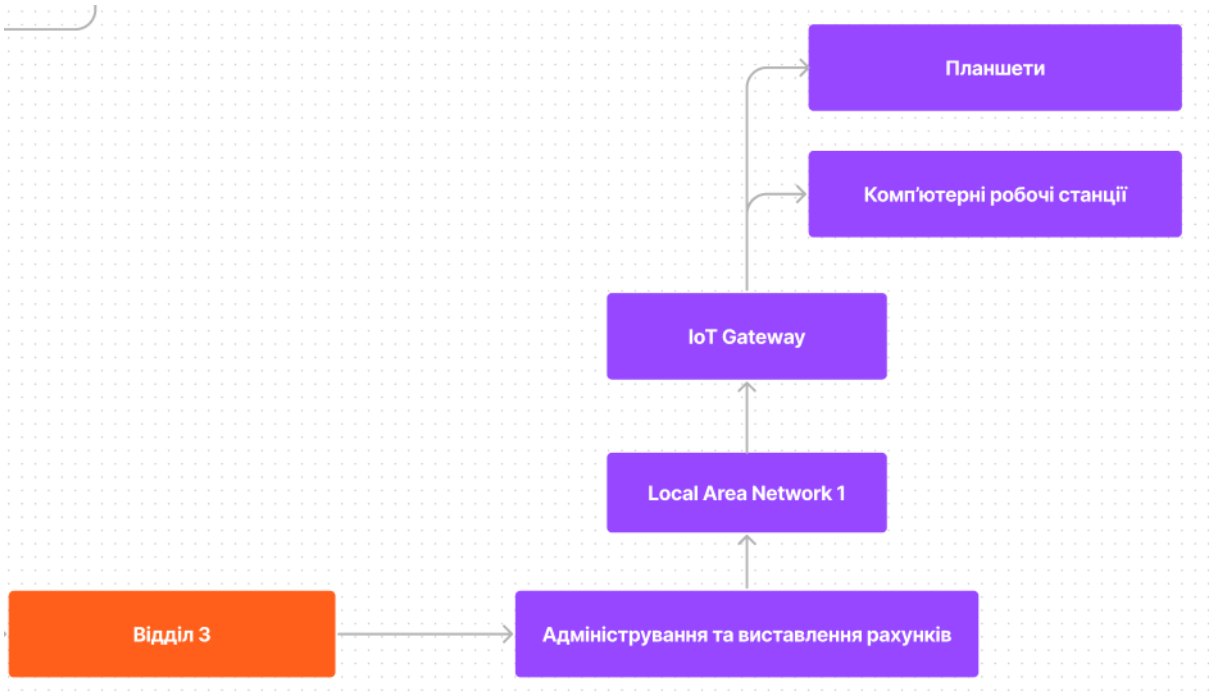

Рисунок 4.6 – Топологія третього відділу

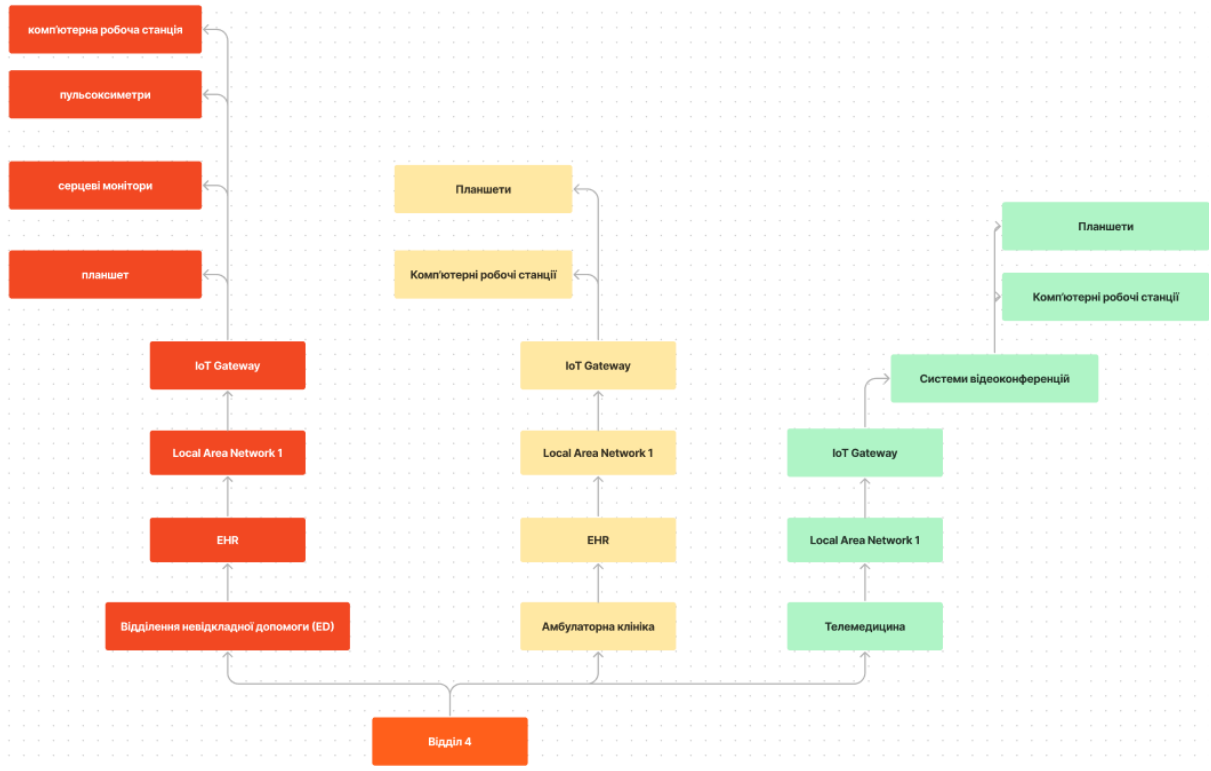

Рисунок 4.7 – Топологія четвертого відділу

Розташування шлюзів і датчиків:

- Шлюзи діють як посередники між пристроями IoT та мережевою інфраструктурою, полегшуючи збір, агрегацію та передачу даних;
- Шлюзи стратегічно розташовані, щоб забезпечити оптимальне покриття та підключення, враховуючи такі фактори, як щільність пристроїв IoT, радіус дії мережі та потужність сигналу;
- Датчики розгорнуто на основі конкретних випадків використання та вимог до моніторингу, таких як життєві показники пацієнта, умови навколишнього середовища або стан обладнання;
- Розміщення датчиків враховує такі фактори, як радіус дії датчика, вимоги до живлення та потреба в передачі даних у реальному часі або періодичній.

Зберігання та обробка даних:

- Дані, створені в Інтернеті речей, повинні надійно зберігатися та оброблятися, щоб забезпечити можливість моніторингу в реальному часі, аналізу даних і прийняття рішень;
- Розподілені системи зберігання можна використовувати для обробки великого обсягу даних, створених пристроями IoT, і забезпечити відмовостійкість і резервування;
- Рішення Edge Computing або Fog Computing (Рис.4.1) можна використовувати для обробки та аналізу даних ближче до джерела даних, зменшуючи затримку та вимоги до пропускної здатності мережі;
- Хмарні платформи зберігання та обробки можна використовувати для централізованого зберігання, аналізу та довгострокового архівування даних.

	Вимоги до затримки	Вимоги до пропускної здатності
Traditional Cloud Computing	Високі	Високі
Edge Computing	Низькі	Помірні
Fog Computing	Низькі	Помірні

Рисунок 4.8 – Порівняння вимог до затримки та пропускної здатності для традиційних хмарних обчислень, периферійних обчислень і туманних обчислень в установах охорони здоров’я

Масштабованість, надійність і продуктивність:

- Архітектура мережі повинна бути розроблена таким чином, щоб відповідати вимогам щодо масштабованості IoT в охороні здоров’я;
- Розміри масштабованості повинні включати пропускну здатність мережі, можливості зберігання та обчислювальні ресурси для обробки зростаючої кількості пристроїв IoT і трафіку даних;
- Для забезпечення високої доступності та надійності мережевої інфраструктури мають бути реалізовані механізми резервування та відмовостійкості;
- Слід запровадити механізми якості обслуговування (QoS), щоб визначити пріоритетність передачі даних у реальному часі, гарантуючи своєчасну доставку та низьку затримку для критично важливих програм охорони здоров’я.

Безпека та конфіденційність:

- Надійні заходи безпеки повинні бути інтегровані в мережеву архітектуру для забезпечення безпеки та конфіденційності даних;
- Слід запровадити механізми шифрування, автентифікації та контролю доступу для захисту конфіденційних даних пацієнтів;
- Необхідно впровадити сегментацію та ізоляцію мережі, щоб запобігти несанкціонованому доступу та запобігти потенційним порушенням безпеки;
- Необхідно забезпечити дотримання відповідних норм і стандартів щодо захисту даних, наприклад HIPAA (Закон про перенесення та підзвітність медичного страхування) щодо конфіденційності даних пацієнтів.

4.4 Протоколи зв'язку

Для розробки мережевої інфраструктури, яка підтримує IoT для охорони здоров'я, дуже важливо ретельно вибрати відповідні протоколи зв'язку, які відповідають конкретним потребам додатків IoT для охорони здоров'я. Ось оцінка та вибір протоколів зв'язку, які зазвичай використовуються в IoT охорони здоров'я:

MQTT (телеметричний транспорт черги повідомлень):

- MQTT — це легкий протокол обміну повідомленнями на основі публікації та підписки, який широко використовується в програмах IoT;
- Він розроблений для обмежених пристроїв і ненадійних мереж з низькою пропускною здатністю;
- MQTT забезпечує ефективну передачу даних, мінімальні накладні витрати та підтримує надійну доставку повідомлень;
- Використовується для додатків, що вимагають обміну даними в реальному часі, таких як віддалений моніторинг пацієнтів і системи телеметрії.

CoAP (протокол обмеженого застосування):

- CoAP — це спеціалізований протокол веб-передачі, розроблений для пристроїв і мереж з обмеженими ресурсами;
- Він забезпечує ефективний зв’язок між пристроями IoT і підтримує взаємодію запитів/відповідей;
- CoAP є легким, з невеликими накладними витратами та низьким енергоспоживанням;
- Він добре підходить для додатків Інтернету речей у сфері охорони здоров’я, де пристрої з обмеженими ресурсами, наприклад переносні пристрої та датчики навколишнього середовища, потребують зв’язку з серверними системами.

HL7 (Сьомий рівень здоров'я):

- HL7 — це набір стандартів для обміну, інтеграції, спільного використання та пошуку електронної медичної інформації;
- Визначає формати обміну повідомленнями та протоколи для обміну клінічними та адміністративними даними в даній системі охорони здоров’я;
- Використовується в медичному IoT для забезпечення взаємодії та стандартизації обміну даними між різними медичними пристроями та системами;
- Забезпечує бездоганну інтеграцію пристроїв Інтернету речей, електронних медичних записів (EHR) та інших інформаційних систем охорони здоров’я.

DICOM (цифрове зображення та комунікація в медицині):

- DICOM — широко поширений стандарт для обміну, зберігання та передачі даних медичних зображень;
- Забезпечує комплексну структуру для взаємодії між медичними пристроями для візуалізації, системами архівування зображень і зв’язку (PACS) та іншими системами охорони здоров’я;
- Необхідний у додатках IoT для охорони здоров’я, які включають медичні пристрої візуалізації, такі як рентгенівські апарати, ультразвукові пристрої та сканери МРТ.

Bluetooth (BLE) і Zigbee:

- Bluetooth Low Energy (BLE) і Zigbee — це протоколи бездротового зв’язку, які зазвичай використовуються в програмах IoT;

– BLE підходить для зв’язку між пристроями на короткій відстані, що робить його ідеальним для переносних пристроїв для здоров’я та сенсорних мереж у закладах охорони здоров’я;
– Zigbee — це протокол з низьким енергоспоживанням і низькою швидкістю передачі даних, придатний для автоматизації будівель, віддаленого моніторингу пацієнтів і додатків для домашнього медичного обслуговування.

Протокол	Розмір даних	Надійність	Енергоефективність	Сумісність
MQTT	Від малого до великого	Високий рівень	Висока енергоефективність	Достатня сумісність
CoAP	Від малого до середнього	Високий рівень	Висока енергоефективність	Достатня сумісність
HL7	Від малого до великого	Високий рівень	Змінна енергоефективність	Чудова сумісність
Bluetooth	Від малого до середнього	Помірний рівень	Висока енергоефективність	Обмежена сумісність
Zigbee	Від малого до середнього	Високий рівень	Висока енергоефективність	Обмежена сумісність

Рисунок 4.9 – Порівняння характеристик протоколів MQTT, CoAP, HL7, Bluetooth і Zigbee

У таблиці (Рисунок 4.7) розглядаються такі характеристики як:

– Розмір даних: вказує діапазон розміру даних, який протокол може ефективно обробляти, враховуючи накладні витрати та вимоги до пропускної здатності. Він класифікується як малий, середній або великий;
– Надійність: вказує на надійність доставки повідомлень і механізмів обробки помилок, які забезпечує протокол. Його класифікують як надійний або помірний;
– Енергоефективність: вказує на рівень енергоефективності, запропонований протоколом, що має вирішальне значення для пристроїв IoT з живленням від батареї. Його класифікують як енергозберігаючий або змінний;

- Взаємодія: вказує на рівень взаємодії та сумісності з іншими медичними пристроями, системами та платформами. Він класифікується як хороший, відмінний або обмежений.

4.5 Керування даними адреси та аналіз

Щоб створити мережеву інфраструктуру, яка підтримує IoT для охорони здоров'я, а також ефективно керувати та аналізувати адресні дані, створені медичними пристроями IoT, було розглянуто стратегії зберігання даних, масштабованості, безпеки, конфіденційності та передових методів аналітики.

В цьому проектуванні було обрано такі методи зберігання даних як:

- Хмарне сховище Amazon S3 буде використовуватись як масштабоване та безпечне рішення для хмарного сховища, наприклад для зберігання та керування медичними даними IoT. Також буде використовуватись резервування даних і механізми резервного копіювання хмарних провайдерів для надійності;
- Розподілена файлова система Hadoop (HDFS), для обробки великомасштабного зберігання даних, паралельної обробки та відмовостійкості;
- Граничне сховище: розгорнуті периферійні пристрої зберігання, такі як NAS (мережеве сховище) або межові шлюзи з можливостями локального зберігання, задля зберігання та обробки даних IoT у реальному часі на межі мережі.

Використання горизонтально масштабованої архітектури, яка може обробляти зростаючий обсяг і різноманітність медичних даних IoT. Також використання таких технологій, як контейнеризація та мікросервіси, щоб забезпечити легку масштабованість із збільшенням кількості пристроїв IoT і джерел даних.

За безпеку та конфіденційність відповідають надійні заходів безпеки такі як: наскрізне шифрування, безпечні протоколи зв'язку (HTTPS) і багатофакторна автентифікація, щоб захистити дані IoT охорони здоров'я від несанкціонованого доступу та злому.
Також потрібно дотримуватись правил конфіденційності, таких як HIPAA, анонімізуючи або деідентифікуючи дані пацієнтів, коли це необхідно. Встановлення детального контролю доступу та журналів аудиту обов'язково потрібне для забезпечення відповідності та відстеження.

Також під час проектування були вибрані розширені методи аналітики, такі як:

- Використання фреймворків машинного навчання, таких як TensorFlow та PyTorch, для розробки прогнозних моделей для аналізу даних IoT охорони здоров'я. Навчання моделі виявляти закономірності, аномалії та прогнозувати стан здоров'я;
- Використання таких методів штучного інтелекту, як обробка природної мови (NLP) (Рис. 4.10) і комп'ютерне бачення, щоб отримати інформацію з неструктурованих даних охорони здоров'я, таких як медичні зображення, клінічні нотатки та наукові статті;
- Впровадження аналітики в реальному часі за допомогою фреймворку потокової обробки Apache Kafka, щоб забезпечити моніторинг у реальному часі, сповіщення та прийняття рішень на основі потоків даних IoT.

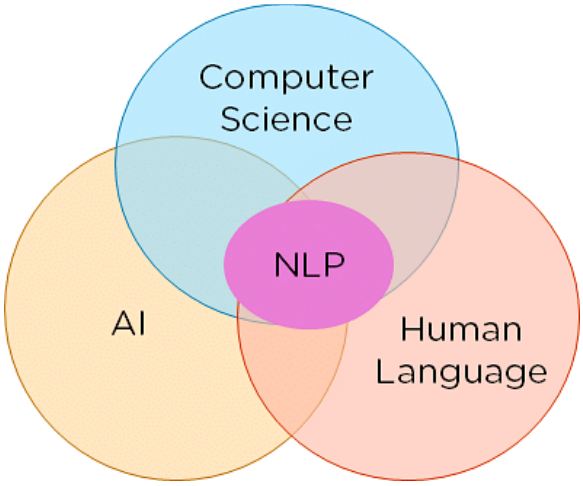

Рисунок 4.10 – Складові NLP

Управління даними та відповідність вимогам відіграють вирішальну роль у забезпеченні безпеки, конфіденційності та цілісності даних у середовищі IoT охорони здоров’я. У контексті проектування мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров’я управління даними та відповідність охоплюють різні практики, політики та процеси, які організації повинні впроваджувати для ефективного керування та захисту даних.

Під час проектування було вибрано наступні впровадження для управління даними та відповідності:

- Створення комплексної структури керування даними, включаючи політику щодо даних, право власності на дані та методи керування життєвим циклом даних, щоб забезпечити якість, цілісність даних і відповідність нормативним вимогам;
- Впровадження інструментів та методів керування даними для моніторингу та забезпечення контролю доступу до даних, походження даних і дотримання правил конфіденційності;
- В майбутньому, впровадження регулярних аудитів та оцінок, щоб забезпечити дотримання політики керування даними та підтримувати стандарти керування даними.

4.5 Забезпечення безпеки та конфіденційності

Під час проектування було створено детальний план впровадження для забезпечення безпеки та конфіденційності в мережевій інфраструктурі з підтримкою Інтернету речей для охорони здоров’я.

Було обрано застосування наскрізного шифрування для даних під час передавання та зберігання а також використання галузевих стандартних алгоритмів шифрування, таких як AES (Advanced Encryption Standard) та RSA (Rivest-Shamir-

Adleman), щоб захистити конфіденційні медичні дані від несанкціонованого доступу або перехоплення. Необхідним є і застосовування шифрування до комунікацій пристроїв IoT, даних, що зберігаються в базах даних, і даних, що передаються між різними компонентами мережевої інфраструктури.

Управління доступом є фундаментальним аспектом забезпечення безпеки та цілісності даних у мережевих інфраструктурах із підтримкою Інтернету речей для охорони здоров'я. Це передбачає впровадження механізмів і політик, які контролюють і обмежують доступ до конфіденційних даних і ресурсів на основі попередньо визначених правил і дозволів. Для цього було вибрано встановлення надійного механізму контролю доступу, щоб обмежити неавторизований доступ до пристроїв і даних IoT для охорони здоров'я та використання керування доступом на основі ролей (RBAC) (Рис. 4.11), щоб визначити детальні дозволи доступу на основі ролей і обов'язків користувачів. Для гарантування доступу до мережі та її ресурсів лише авторизованим особам було впроваджено застосування надійних механізмів автентифікації, таких як ім'я користувача/пароль, багатофакторна автентифікація та біометрична автентифікація.

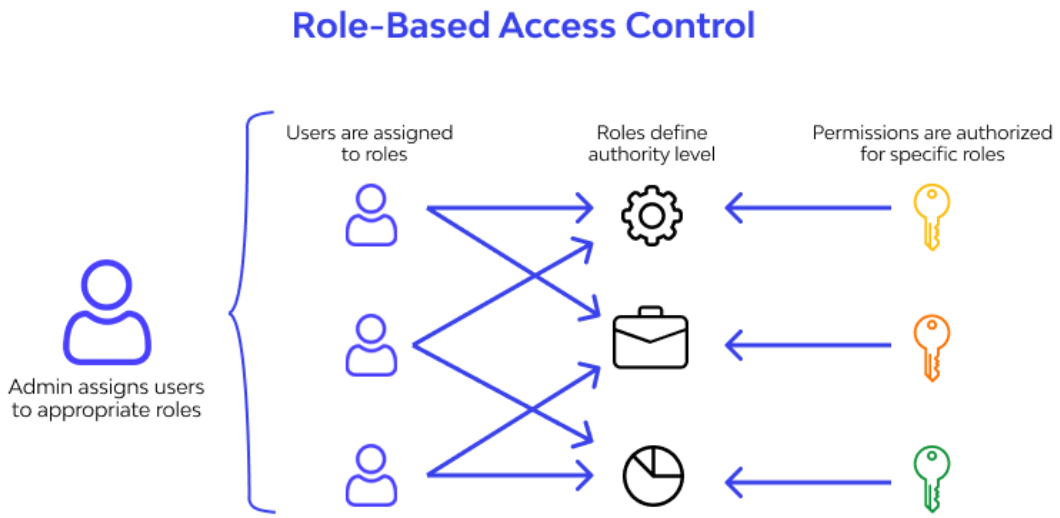

Рисунок 4.11 – Приклад RBAC

Безпека пристроїв є критично важливим аспектом забезпечення цілісності, доступності та конфіденційності мережевих інфраструктур із підтримкою Інтернету речей у сфері охорони здоров'я. Це передбачає впровадження заходів для захисту пристроїв IoT від несанкціонованого доступу, втручання та експлуатації, ключовими з яких є застосування безпечних механізмів завантаження та автентифікації пристроїв, щоб лише надійні й авторизовані пристрої IoT могли підключатися до мережі та використання безпечних механізмів оновлення мікропрограми та програмного забезпечення, щоб виправляти вразливості та гарантувати, що на пристроях працюють найновіші оновлення безпеки.

Для запобігання доступу неавторизованих пристроїв до мережі використовуються сертифікати пристроїв та унікальних ідентифікаторів для автентифікації та авторизації пристроїв IoT.

Сегментація мережі є важливою стратегією в розробці безпечної мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров'я. Він включає в себе поділ мережі на окремі сегменти або підмережі, кожна з яких має власний набір засобів контролю безпеки та політик доступу. Для цього було запроваджено сегментацію мережі, щоб ізолювати різні частини мережі та створити межі безпеки.

Також потрібне розділення пристроїв IoT, даних пацієнтів і адміністративнх систем на окремі сегменти мережі, щоб обмежити вплив потенційного порушення безпеки.

Для забезпечення сегментації мережі та контролювання потоку трафіку між сегментами використовуються брандмауери, віртуальні приватні мережі (VPN) або віртуальних локальних мереж (VLAN).

Моніторинг безпеки та реагування на інциденти є важливими компонентами надійної системи безпеки для мережевих інфраструктур із підтримкою Інтернету речей у сфері охорони здоров'я. Вони включають безперервний моніторинг мережевої діяльності, виявлення інцидентів безпеки та своєчасне реагування на

пом’якшення потенційних загроз. Впровадження системи моніторингу безпеки, потрібне для постійного відстеження мережевого трафіку, поведінки пристроїв IoT і шаблони доступу до даних на предмет будь-яких аномалій або порушень безпеки.

Для виявлення та блокування шкідливих дій у реальному часі потрібне налаштування системи виявлення та запобігання вторгненням (IDS/IPS). Також не менш важливим є розроблення плану реагування на інциденти, у якому описано процедури швидкого та ефективного реагування на інциденти безпеки.

Конфіденційність даних і відповідність вимогам є критично важливими факторами при проектуванні та експлуатації мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров’я. Захист даних пацієнтів і забезпечення відповідності відповідним нормам є важливими для збереження довіри та виконання вимог законодавства. Одним з головних запроваджень є забезпечення дотримання відповідних нормативних актів, таких як HIPAA (Закон про перенесення та підзвітність медичного страхування) і GDPR (Загальний регламент захисту даних) (Рис. 4.12).

Для захисту конфіденційності пацієнтів впроваджується анонімність або деідентифікація даних пацієнта, коли це необхідно.

Також важливим є встановлення політики збереження та видалення даних, щоб відповідати нормативним вимогам і забезпечити безпечне та своєчасне видалення даних, які більше не потрібні.

Рисунок 4.12 – Складові GDPR

Поінформованість про безпеку та навчання відіграють вирішальну роль у забезпеченні безпечного та відповідального використання мережевих інфраструктур із підтримкою Інтернету речей у сфері охорони здоров'я. Забезпечуючи належну освіту та підготовку персоналу, організації охорони здоров'я можуть розвивати культуру безпеки та покращувати загальну безпеку. Проводення регулярних програм підвищення обізнаності щодо безпеки та навчальні програми для медичного персоналу та іншого персоналу, є обов'язковим щоб навчити їх найкращим практикам безпеки та конфіденційності даних.

Також безпека залежить і від підвищення обізнаності про важливість безпечного використання пристрою, надійних паролів і дотримання правил і процедур безпеки.

Оцінка безпеки третьою стороною є цінною практикою для оцінки ефективності заходів безпеки, реалізованих у мережевій інфраструктурі з підтримкою Інтернету речей для охорони здоров'я. Це передбачає залучення незалежної та досвідченої охоронної фірми для проведення комплексної оцінки стану безпеки мережі. Для виявлення вразливих місць та забезпечення ефективності засобів контролю безпеки потрібне виконання регулярних оцінок

безпеки та тестування на проникнення мережевої інфраструктури. Також потрібне залучення сторонніх експертів із безпеки або аудиторів для проведення незалежної оцінки та перевірки заходів безпеки, реалізованих у мережевій інфраструктурі.

Характеристика	AES (Advanced Encryption Standard)	RSA (Rivest-Shamir-Adleman)
Довжина ключа	Підтримує ключі довжиною 128, 192 і 256 біт	Підтримує ключі довжиною від 1024 до 4096 біт
Швидкість шифрування	Швидкі та ефективні операції шифрування та дешифрування	Операції шифрування можуть бути повільнішими порівняно з AES
Швидкість дешифрування	Швидкі та ефективні операції дешифрування	Операції дешифрування можуть бути повільнішими порівняно з AES
Вплив на продуктивність	Низький вплив на продуктивність системи	Операції шифрування та дешифрування можуть вплинути на продуктивність, особливо з великими розмірами ключів
Відповідні випадки використання	Симетричне шифрування для великих обсягів даних	Асиметричне шифрування для безпечного обміну ключами та цифрових підписів
Генерація ключів	Відносно швидкий процес генерації ключів	Генерація ключів може бути дорогою з точки зору обчислень
Апаратне прискорення	Підтримує апаратне прискорення для покращення продуктивності	Підтримує апаратне прискорення для покращення продуктивності
Розподіл ключів	Потрібні безпечні механізми розподілу ключів	Потрібні безпечні механізми розподілу ключів
Генерація/ перевірка підпису	Не застосовується	Підходить для створення та перевірки цифрового підпису
Вимоги до ресурсів	Вимагає менше обчислювальних ресурсів	Вимагає більше обчислювальних ресурсів

Рисунок 4.13 – Порівняння характеристик алгоритмів шифрування, таких як AES (Advanced Encryption Standard) та RSA (Rivest-Shamir-Adleman)

ВИСНОВОК

Підсумовуючи, проектування мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров’я представляє унікальні виклики та вимоги, які були ретельно розглянуті, щоб забезпечити надання безпечних, надійних та ефективних послуг охорони здоров’я. У цій дипломній роботі досліджено різні аспекти проектування такої мережевої інфраструктури, беручи до уваги специфічні потреби галузі охорони здоров’я.

Під час цього дослідження ми визначили та проаналізували вимоги, виклики та цілі IoT в охороні здоров’я, враховуючи точки зору зацікавлених сторін, таких як постачальники медичних послуг, пацієнти та адміністратори. Ми оцінили існуючу мережеву інфраструктуру та технології, дослідивши нові рішення IoT, які можуть відповідати визначеним вимогам.

Архітектура мережі була розроблена з урахуванням таких факторів, як передача даних у реальному часі, безпека даних, сумісність і масштабованість. Топологія різних підрозділів охорони здоров’я, включаючи операційні, відділення інтенсивної терапії, лабораторії, відділення невідкладної допомоги, амбулаторні клініки, телемедицину, адміністрування та виставлення рахунків, а також дослідження та освіту, була викладена для забезпечення повного розуміння мережевої інфраструктури.

Комунікаційні протоколи, такі як MQTT, CoAP і HL7, були оцінені та порівняні на основі їхніх характеристик, щоб забезпечити ефективну та надійну передачу даних у додатках IoT для охорони здоров’я. Стратегії управління даними, включаючи методи зберігання даних і передові методи аналітики, були

досліджені для обробки величезних обсягів даних, створених медичними пристроями IoT.

Особливу увагу було приділено плануванню безпеки та конфіденційності, спрямованому на захист конфіденційних медичних даних і забезпечення дотримання відповідних стандартів і правил, таких як HIPAA та GDPR. Для захисту пристроїв Інтернету речей і передачі даних запропоновано шифрування, контроль доступу, механізми автентифікації та методи керування даними.

Крім того, було враховано безпеку пристроїв, сегментацію мережі, обізнаність про безпеку та навчання для підвищення загальної безпеки мережевої інфраструктури з підтримкою IoT. Підкреслюється важливість сторонніх оцінок безпеки для оцінки ефективності заходів безпеки та виявлення вразливостей.

Підсумовуючи, проектування мережевої інфраструктури з підтримкою Інтернету речей для охорони здоров’я вимагає цілісного підходу, який враховує конкретні потреби та виклики цієї сфери. Використовуючи рекомендації та стратегії, запропоновані в цій дипломній роботі, організації охорони здоров’я можуть закласти міцну основу для безпечної, ефективної та масштабованої екосистеми Інтернету речей, яка підтримує надання високоякісних медичних послуг, приділяючи пріоритет конфіденційності пацієнтів і безпеці даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стаття ICT (information and communications technology, or technologies) URL: https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies. (електронний ресурс)

2. ACM Digital Library. URL: https://dl.acm.org/. (електронний ресурс)

3. European Medicines Agency (EMA) website. URL: https://www.ema.europa.eu/. (електронний ресурс)

4. «Інтернет речей в охороні здоров'я: від теорії до практики» Арвінда Саті. (книга, один автор)

5. IoT for Healthcare LinkedIn group URL: https://www.linkedin.com/groups/13817552/. (електронний ресурс)

6. Healthcare Information and Management Systems Society (HIMSS). URL: https://www.himss.org/. (електронний ресурс)

7. An Overview of Network Communication Technologies for IoT URL: https://www.researchgate.net/publication/345813266_An_Overview_of_Network_Communication_Technologies_for_IoT. (електронний ресурс)

ДОДАТОК А

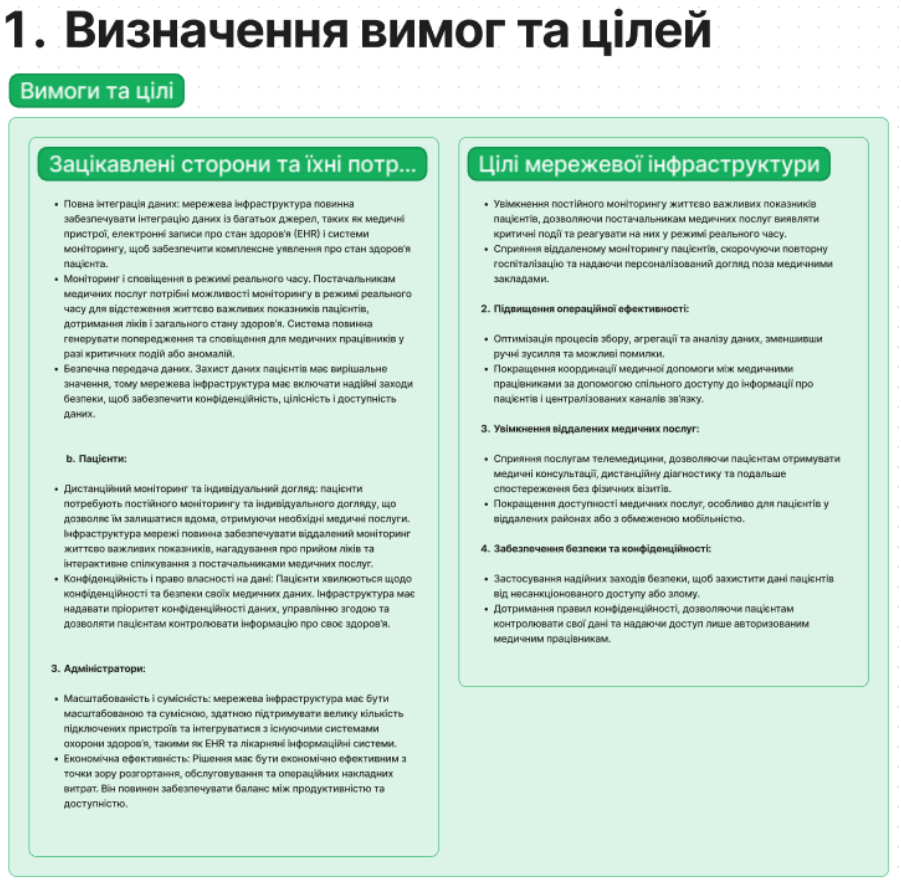

Рисунок А.1 – Визначення вимог та цілей

2. Технологічна оцінка

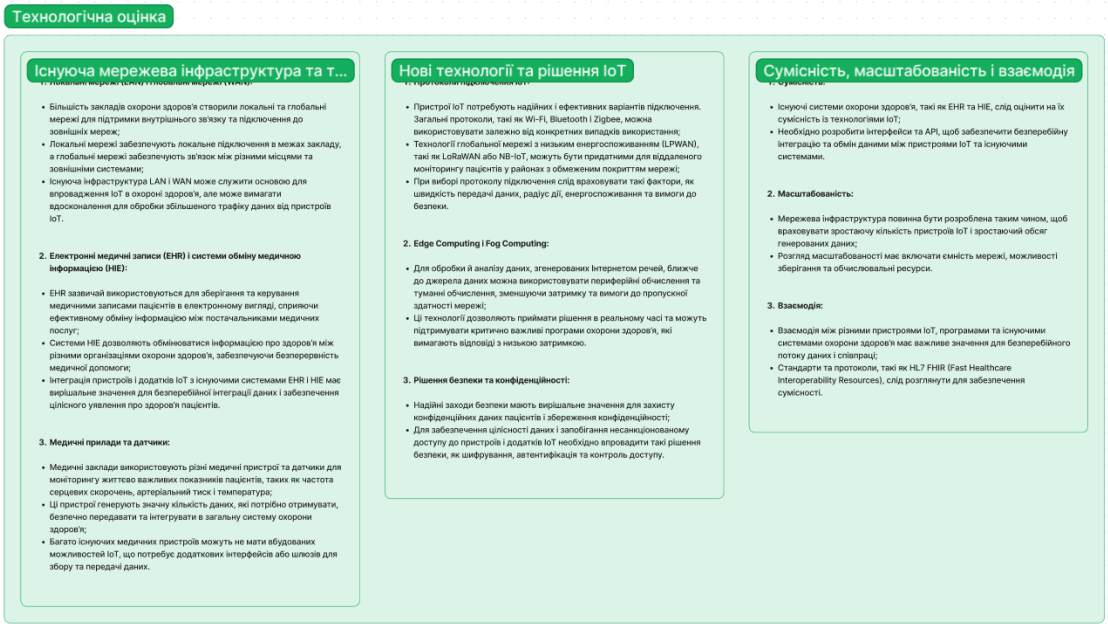

Рисунок А.2 – Технологічна оцінка

3. Проектування архітектури мережі

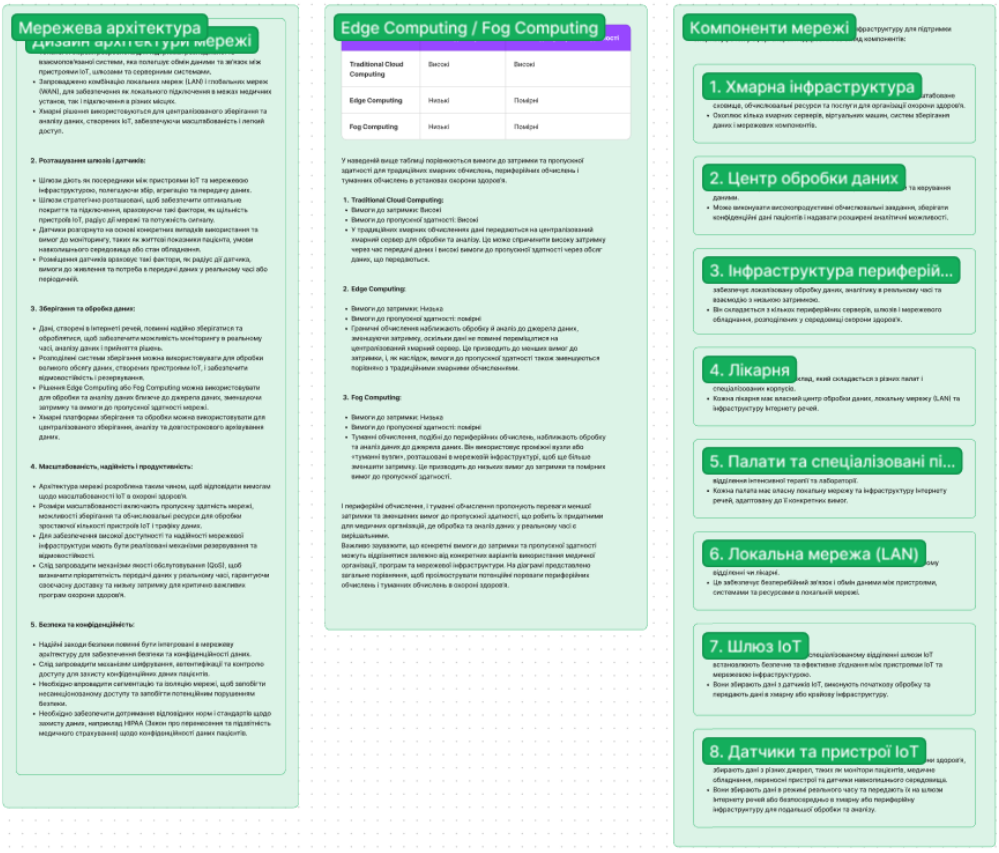

Рисунок А.3 – Проектування архітектури мережі

4. Протоколи зв’язку

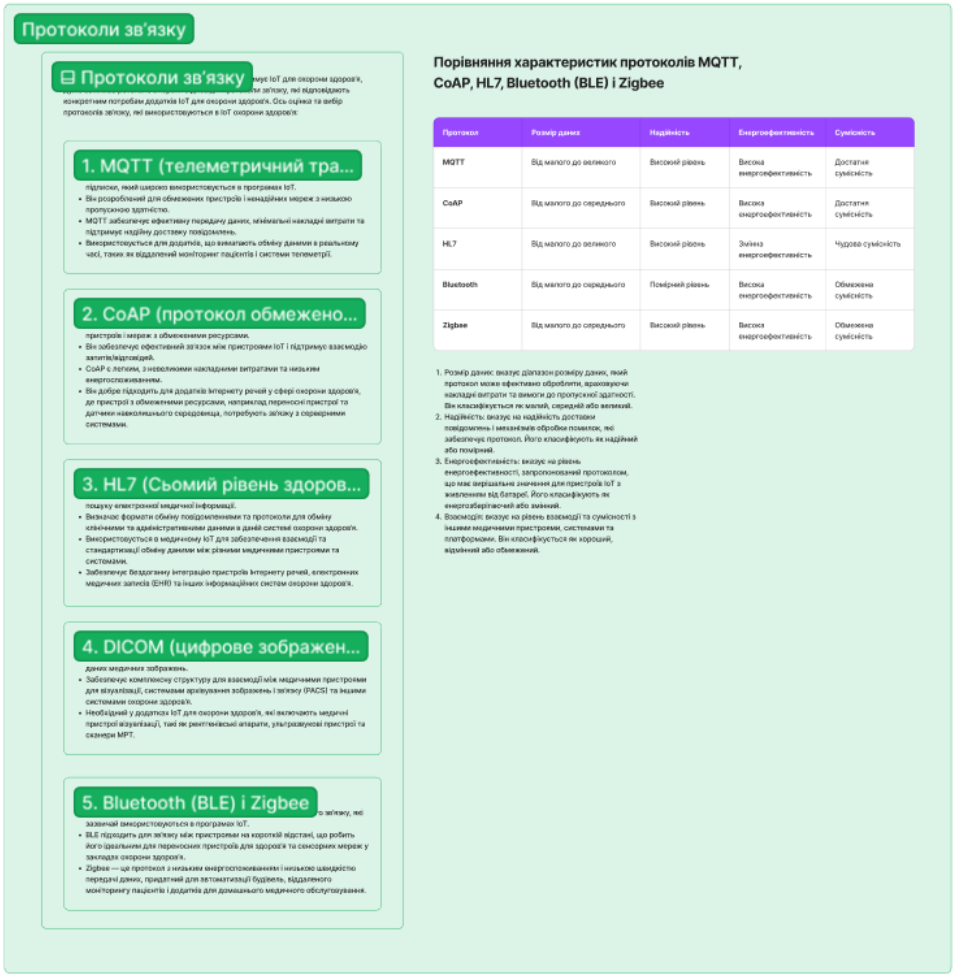

Рисунок А.4 – Протоколи зв’язку

Рисунок А.5 – Керування даними адреси та аналіз

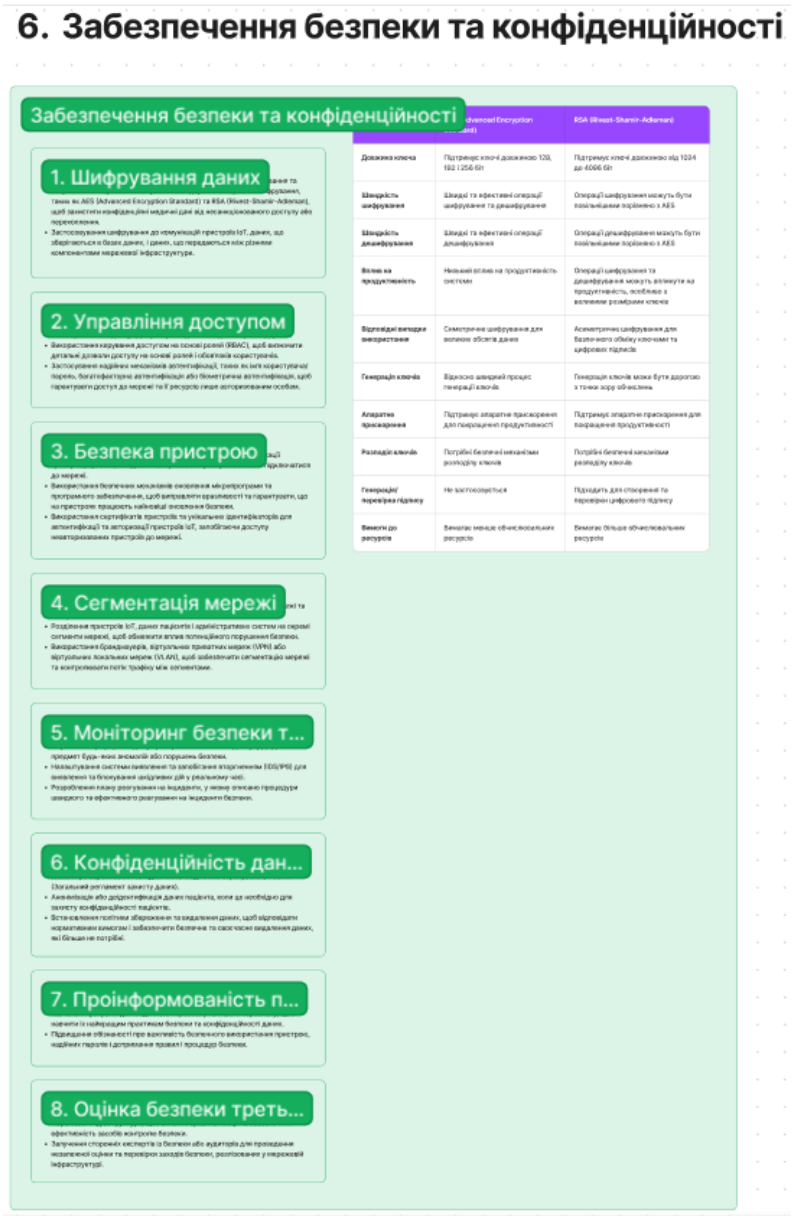

Рисунок А.6 – Забезпечення безпеки та конфіденційності

Рисунок А.7 – Топологія мережі з описом відділів лікарн