Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Цифровізація медичних закладів з використанням інформаційної технології Інтернету речей

Виконав: студент VI курсу, групи СТм-61
спеціальності 126 Інформаційні системи та технології
(шифр і назва спеціальності)

_____ Дзюба Д.Ю.
(підпис) (прізвище та ініціали)

Керівник _____ Дмитроца Л.П.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Мацюк О.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Петрик М.Р.
(підпис) (прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«____» _____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 126 Інформаційні системи та технології
(шифр і назва спеціальності)

Студенту Дзюбі Денису Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Цифровізація медичних закладів з використанням інформаційної технології Інтернету речей

Керівник роботи Дмитроца Леся Павлівна, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_28_» _жовтня_ 2021 року № _4/7-911_

2. Термін подання студентом завершеної роботи 21 грудня 2021 р.

3. Вихідні дані до роботи наукові літературні джерела щодо теми кваліфікаційної роботи

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналіз предметної області. 2 Архітектура та схеми існуючих цифрових лікарень. 3. Енергоефективна автентифікація на основі PUF пристроїв в Інтернеті медичних речей (IoMT). 4 Охорона праці та безпека в надзвичайних ситуаціях. Висновки. Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сторінка. 2 Мета та об'єкт дослідження. 3 Завдання дослідження. 4 Актуальність дослідження. 5 Концепція цифрової лікарні. 6 Цифрова трансформація системи охорони здоров'я в Україні. 7 Інтернет речей та розумна система охорони здоров'я. 8. Розумна електронна медична допомога. 9 Архітектура для IoMT. 10 Нові технології в IoMT. 9 Різноманітні давачі. 10 Автентифікація пристрою на основі PUF. 11 Автентифікація на Основі PUF для E-HealthCare.12 Висновки. 13 Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Дмитроца Л.П., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. в.		

7. Дата видачі завдання 27 вересня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	27.09.2021-29.09.2021	*Виконано*
2.	Аналіз літературних джерел	30.09.2021-03.10.2021	*Виконано*
3.	Обгрунтування актуальності дослідження	04.10.2021-10.10.2021	*Виконано*
4.	Аналіз предмету дослідження та предметної області	11.10.2021-17.10.2021	*Виконано*
5.	Оформлення розділу «Аналіз предметної області»	18.10.2021-24.10.2021	*Виконано*
6.	Оформлення розділу «Архітектура та схеми існуючих	25.10.2021-31.10.2021	*Виконано*
	цифрових лікарень»		
7.	Оформлення розділу «Енергоефективна	01.11.2021-07.11.2021	*Виконано*
	Автентифікація на основі PUF пристроїв в Інтернеті		
	Медичних речей (IoMT)»		
8.	Виконання завдання до підрозділу «Охорона праці»	08.11.2021-11.11.2021	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	12.11.201-14.11.2021	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	15.11.201-24.11.2021	*Виконано*
11.	Нормоконтроль	25.11.2021-28.11.2021	*Виконано*
12.	Перевірка на плагіат	01.12.2021	*Виконано*
13.	Попередній захист кваліфікаційної роботи	07.12.2021	*Виконано*
14.	Захист кваліфікаційної роботи	22.12.2021	

Студент _____ Дзюба Д.Ю.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Дмитроца Л.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Цифровізація медичних закладів з використанням інформаційної технології Інтернету речей// Кваліфікаційна робота освітнього рівня «Магістр» // Дзюба Денис Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СТм-61 // Тернопіль, 2021 // с. – 64 , рис. – 17, додат. – 2 , бібліогр. – 61 .

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, IOT, PUF, ЕЛЕКТРОННА ОХОРОНА ЗДОРОВ'Я, ЦИФРОВІЗАЦІЯ, ЦИФРОВА ЛІКАРНЯ, РОЗУМНА ЛІКАРНЯ, IOMT.

Проведено аналіз наукових статей та публікацій по темі кваліфікаційної роботи.

Розглянуто архітектуру цифрових лікарень, схеми існуючих в ній технологій, а саме IoMT.

Досліджено Інтернет речей та розумну систему охорони здоров'я, запропоновано використання технології IoMT разом із пристроями з фізичною неклонованою функцією (PUF), штучним інтелектом, SDN.

Представлено протокол автентифікації IoMT на основі PUF, що здатний автентифікувати пристрої, не вимагаючи високої обчислювальної потужності від кінцевих пристроїв.

Обґрунтовано доцільність впровадження інформаційної технології Інтернет речей на основі PUF в системі електронного здоров'я для підвищення якості надання медичних послуг та запропоновано розділити процес автентифікації на три етапи, які в результаті покращують захист інформації та зменшують ризики випадкового або навмисного втручання.

ANNOTATION

Digitalization of health-care institutions with Internet-of-Things information technology// Qualification thesis Master Degree // Dziuba Denys Yuriiovych // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science, group STm-61 // Ternopil, 2021 // Pages – 64, Fig. – 17, Annexes – 2 , References – 61.

Keywords: INTERNET OF THINGS, IOT, PUF, ELECTRONIC HEALTHCARE, DIGITALIZATION, DIGITAL HOSPITAL, SMART HOSPITAL, IOMT.

The analysis of scientific articles and publications on the topic of qualification work is carried out.

The architecture of digital hospitals, schemes of the existing technologies in it, namely IoMT are considered.

The Internet of Things and a smart healthcare system have been studied, the use of IoMT technology together with devices with physical non-cloned function (PUF), artificial intelligence, SDN has been proposed.

PUF-based IoMT authentication protocol is presented, which is able to authenticate devices without requiring high computing power from end devices.

The expediency of PUF-based Internet of Things information technology in the e-health system to improve the quality of medical services is substantiated and it is proposed to divide the authentication process into three stages, which improve information protection and reduce the risk of accidental or intentional interference.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CRM (англ. Customer Relational Management) – призначений для оптимізації бізнес-процесів, для взаємодії з потенційними та існуючими клієнтами.

DHCP (англ. Dynamic Host Configuration Protocol) – це стандартний протокол програмного рівня, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі.

EHR (англ. Electronic Health Record) – електронний медичний запис.

IoT (англ. Internet of Things, IoT) – концепція мережі, що складається з взаємопов’язаних фізичних пристроїв, що мають вбудовані датчики, а також програмного забезпечення, що дозволяє передавати та обмінюватися даними між фізичним світом та комп’ютерними системами за допомогою стандартних протоколів зв’язку.

ML (англ. Machine Learning) – машинне навчання.

NLP (англ. Natural Language Processing) – обробка природної мови

SDN (англ. Software-defined Networking) – мережа передачі даних, в якій рівень управління мережею відокремлений від пристроїв передачі даних і реалізований в програмному забезпеченні, є формою віртуалізації обчислювальних ресурсів.

PUF – (англ. Physical Unclonable Functions).

TCP – (англ. Transmission Control Protocol) – разом з протоколом IP є основним протоколом Інтернету, який дав назву моделі TCP/IP.

WAN (англ. Wide Area Network) – комп'ютерна мережа, що охоплює великі території.

ІКТ – інформаційно-комунікаційні технології.

IoMT (англ. Internet of Medical Things) – Інтернет медичних речей.

ІТ – інформаційні технології.

МІС – медичні інформаційні системи.

ЦБД – центральна база даних.

ЗМІСТ

ВСТУП

Актуальність теми роботи. Пандемія коронавірусу продемонструвала нагальну необхідність прискорення цифровізації охорони здоров'я. Зрештою, пацієнти по всьому світу, які опинилися в ситуації ізоляції, були серйозно обмежені в своїх можливостях отримувати ряд медичних послуг. Так, за даними Всесвітньої організації охорони здоров'я (ВООЗ), 68% країн зіткнулися з перебоями в наданні медичних послуг, які, зокрема, включали моніторинг діабету, гіпертонії, скринінг на рак і багато іншого. Ця ситуація створювала серйозну загрозу зростанню смертності не тільки від COVID-19, але і від загострення важких хронічних захворювань, і змушувала медичні установи нарощувати потенціал і організовувати дистанційні онлайн-консультації як для пацієнтів, так і для лікарів. Тобто телемедицина почала активно розвиватися.

Мета дослідження – обґрунтування доцільності впровадження інформаційної технології Інтернет речей в системі електронного здоров’я для підвищення якості надання медичних послуг. Розглянути та дослідити нові інформаційні технології – PUF, Blockchain, штучний інтелект та інші для різних аспектів Інтернет медичних речей (IoMT), таких як безпека, конфіденційність, діагностика та лікування. Вдосконалення існуючих IoT рішень для медичних закладів.

Для досягнення вказаної мети була необхідність виконання таких **завдань**:

- Провести аналіз науково-технічних джерел щодо актуальності дослідження, розглянуто основні питання;
- Визначити концепцію цифрової лікарні;
- Зробити дослідження електронної охорони здоров’я в Україні та закордоном;
- Здійснити огляд IoT для розумної системи охорони здоров’я та нових технологій в IoMT;

- Запропонувати новий метод енергоефективної автентифікації на основі IoT разом з технологією PUF.
- Імплементувати експерементальну установку прототипу з використанням IoT.

Об'єктом дослідження є технології Інтернет-речей разом із PUF та їх впровадження в структуру цифрової лікарні.

Предмет дослідження – сукупність теоретично-практичних досліджень і проблем розвитку цифрових медичних послуг, інформаційні технології PUF, штучний інтелект, Інтернет медичних речей (IoMT) .

Науковою новизною роботи є вдосконалення існуючих цифрових рішень для закладів охорони здоров'я. Дослідження інформаційної технології PUF для різних аспектів IoMT, що покращить безпеку, конфіденційність, діагностику та лікування в медичних закладах.

Практичне значення: Розроблено енергоефективну автентифікацію на основі PUF пристроїв в IoMT. Таке впровадження покращує захист інформації та зменшує ризик випадкового або навмисного втручання, а також запобігає створенню помилок або нещасних випадків під час передачі даних кінцевими девайсами.

Апробація результатів магістерської роботи: окремі результати роботи представленні на двох наукових конференціях:

1. IX науково-технічна конференція «Інформаційні моделі, системи та технології». На тему: «Пристрої з фізичною неклонованою функцією (PUF)».

2. XIX міжнародна науково-практична конференція «Математичне та програмне забезпечення інтелектуальних систем (МПЗІС)». На тему: «Цифрова лікарня на основі Інтернету речей».

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Дворічна пандемія вплинула на системи охорони здоров'я в усьому світі більше, ніж в інших областях. Навантаження на неї залишається високою і змушує адаптуватися до нових умов. Медицину часто вважають консервативною галуззю, але високий попит на послуги в поєднанні з необхідністю забезпечити персонал змушує багато лікарень і клінік змінювати підходи і впроваджувати нові розробки і технології – телемедичні послуги, рішення в області штучного інтелекту, які можуть значно знизити ризики. Пов'язано це і зі складною епідеміологічною ситуацією, і з навантаженням на лікарів. Наприклад, у США, за даними McKinsey, у квітні 2020 року 46% пацієнтів користувалися телемедициною, хоча у 2019 році їх частка не перевищувала 11 % [1].

Наприклад, за даними Всесвітньої організації охорони здоров'я (ВООЗ), 68% країн зіткнулися зі збоями в галузі охорони здоров'я, які включали моніторинг діабету, гіпертонії, скринінг на рак і багато іншого. Ця ситуація створювала серйозну загрозу зростанню смертності не тільки від COVID-19, але і від загострення важких хронічних захворювань, і змушувала медичні установи нарощувати потенціал і організовувати дистанційні онлайн-консультації як для пацієнтів, так і для лікарів. Тобто телемедицина почала активно розвиватися.

В Україні, завдяки медичній реформі, основні процеси в клініках також почали оцифровуватися. Спочатку МІС (Медичні інформаційні системи) були встановлені в установах первинної медичної допомоги, а в минулому році була підключена система вторинної медичної допомоги. Завдяки цьому українці змогли зареєструватися у лікарів онлайн, а також підписати декларацію з сімейним лікарем, отримувати електронні рецепти і багато іншого.

Тому цифровізація медичних послуг сьогодні є найбільш популярним напрямком роботи для IT-фахівців. IT-компанії конкурують один з одним і прагнуть створювати найбільш зручні медичні інформаційні системи,

встановлювати їх в якомога більшій кількості клінік, будувати цифрові мережі, що з'єднують медичні установи різного рівня тощо [2].

1.1 Концепція цифрової лікарні

Цифрова лікарня – це концепція, що сприяє підвищенню продуктивності персоналу, полегшенню роботи лікарні, підвищенню якості процесів і забезпеченню безпеки пацієнтів за рахунок інтеграції найсучасніших технологій. Таких як: медичні пристрої, інтелектуальні інформаційні системи, системи керування об'єктами і автоматизовані системи, сервіси на основі визначення місцезнаходження, сенсори та цифрові комунікаційні засоби в процесах охорони здоров'я. Звичайні лікарні трансформуються у цифрові та пропонують послуги за допомогою цієї концепції. Швидкість та ефективність бізнес-процесів зростають, витрати на папір та документи скорочуються до нуля, помилки, згенеровані людиною, зводяться до мінімуму. Процеси діагностики та лікування проводять не тільки в лікарняних стінах, а й дистанційно. За допомогою цифрових лікарень дані про стан здоров’я негайно та ретроспективно отримуються уповноваженим органом, іншими закладами охорони здоров’я та пацієнтами, і їх можна передавати за допомогою сенсорів, камер та систем раннього попередження, не вимагаючи від людей подальшого спостереження. Можна приймати швидкі та правильні рішення системи підтримки прийняття рішень, а правильні ліки вводяться потрібному пацієнту, у правильних дозах та в потрібний час за допомогою закритої системи доставки лікарських засобів. Завдяки широкому доступу до цифрових лікарень можна буде скористатись усіма цими перевагами та запропонувати пацієнтам найефективніші послуги з охорони здоров’я у найкоротші терміни. Персонал лікарні не матиме зайвого навантаження і рідше буде помилятися.

Лікарні, що проходять трансформацію відповідно до потреб сучасності прагнуть інтегрувати сучасні технології (телемедицина, мобільна охорона здоров'я, цифрові лікарні і т.д.) в процеси обслуговування і переносять свої

послуги у віддалені регіони з концепцією «цифровий лікарні» без обмежень за часом і простору на відміну від традиційних структур, що надають послуги, що залежать від фізичного місця розташування.

Концепція цифрової лікарні – це практика, що виходить на передній план і інвестується розвиненими країнами в останні роки. Сполучені Штати зробили крок вперед, створивши першу в світі лікарню без ліжок в Міссурі під назвою віртуальний центр допомоги милосердя, який пропонує дистанційну діагностику і методи лікування [3]. А, наприклад, Туреччина уважно стежить за розвитком подій у світі і відповідно вносить зміни в сферу охорони здоров'я, тому в 2013 році були розпочаті роботи зі створення «цифрової лікарні», а в 2016 році була заснована одна з чотирьох цифрових лікарень вищого рівня в Європі (Державна лікарня Tiре). Результати цифрових лікарень показують, що лікарні, які практикують цю систему, отримують ефективність 35% [4].

Нові науково-технічні інновації зробили можливим збір, архівування, обробку та візуалізацію великої кількості різних даних та явищ скрізь у лікарнях, які займаються біомедициною, медичною інженерією, клінічною діагностикою, санітарною економікою, адміністрацією лікарні та культурою [5] .

Спільний обмін медичними інформаційними ресурсами та адаптація до місцевих обставин дозволяє здійснювати обробку інформації та комунікаційні функції на повній платформі, яка пропонує повноту представлення керівництва лікарні та майбутнього медичного середовища [6].

За даними Міністерства охорони здоров'я, цифрову лікарню можна визначити як лікарню, де в адміністративних, фінансових і медичних процесах використовується максимальний рівень інформаційних технологій, всі види засобів зв'язку і медичних пристроїв інтегровані один з одним та з іншими інформаційними системами, а медичний персонал і пацієнти можуть обмінюватися даними всередині або за межами лікарні за допомогою телемедицини і мобільних медичних практик [7]. Цифрова лікарня є важливою метою будівництва лікарні, що має важливе значення для сприяння розвитку

медицини та підвищення якості охорони здоров'я [8].

Використання інформаційно-комунікаційних систем для профілактики, діагностики, лікування та моніторингу захворювань та надання медичних консультацій у медичних закладах описується терміном «Електронна охорона здоров'я» [9]. У цьому контексті «Цифрова лікарня, мобільна медицина, телемедицина та роботизована медицина» визначаються як підкомпоненти електронної охорони здоров'я.

Цифрова лікарня надає лікарняні послуги окремим особам за межами лікарняних стін (в будинках, на станціях швидкої допомоги і т.д.) шляхом інтеграції інформаційних і комунікаційних технологій в клінічні та адміністративні робочі процеси, щоб пропонувати високоякісні медичні послуги, а також з'єднувати медичний персонал і підрозділи, що працюють у віддалених місцях один від одного.

Незважаючи на значний прогрес, досягнутий деякими країнами, багато країн все ще потребують інституційної підтримки для розробки та консолідації національних стратегій електронного здоров’я та/або цифрового здоров’я та реалізації їх планів дій, що зазвичай вимагає більших ресурсів та можливостей [10]. У наступних підпунктах розглянемо систему охорони здоров’я України, а також лікарні Туреччини, як один з прикладів найкращої практики.

1.2 Цифрова трансформація системи охорони здоров’я в Україні

Під час пандемії коронавірусу система охорони Здоров'я України була краще підготовлена, оскільки протягом чотирьох років у цій галузі поступово розвивалася цифровізація. Інформаційні системи охорони здоров'я та закупівель ліків, електронна система охорони здоров'я стали основою для впровадження цифрових інструментів під час пандемії. Багато галузей, які повинні були розвиватися протягом наступних кількох років, отримали найвищий пріоритет і збільшили фінансування під час пандемії, включаючи збір інформації, електронні інструменти, бази даних та їх інтеграцію [11].

1.2.1 Електронна система охорони здоров'я в Україні

Електронна система охорони здоров'я це свого роду двокомпонентна система, в котрій користувач може взаємодіяти з центральною базою даних через МІС (медичну інформаційну систему).

Система eHealth включає в себе:

- Центральну базу даних (ЦБД) – інформаційно-телекомунікаційна система, яка включає певні реєстри, передбачені законом, програмні модулі, інформаційну систему національної служби здоров’я України, в частині, яка затребувана для виконання державних фінансових гарантій. Також надає можливість створювати, робити перегляд, розмінюватися інформацією та документами між реєстрами, державними цифровими ресурсами, диджиталізованими медичними інформаційними системами.
- МІС (електронну медичну інформаційну систему) – інформаційно-телекомунікаційна система, що робить процес автоматизації в роботі господарюючих суб'єктів у сфері охорони здоров'я, утворювати, переглядати, обмінюватися інформацією в електронному вигляді, включаючи центральну базу даних (при підключенні) [12].

Архітектуру системи зображено на рисунку 1.1

Рисунок 1.1 – Архітектура системи охорони здоров’я

Цілями цієї системи є:

- забезпечення прозорості фінансування охорони здоров’я;
- надання можливості працювати без паперу, поступовий перехід на електронний облік (електронний рецепт, електронна картка, електронне направлення);
- формування бізнес-середовища для створення нових електронних сервісів;
- створення простору для інновацій в медицині (машинне навчання, великі дані, блокчейн тощо)
- сприяння розвитку медичного IT-ринку.

Ключові ролі системи:

- eZdorovya керує центральною базою даних eHealth та контролює розвиток електронної системи охорони здоров'я в Україні.
- МОЗ України формулює політику в галузі охорони здоров'я та відповідає за проведення реформ.
- НСЗУ проводить дослідження та зужиткує дані для прогнозування потреб населення в медичних послугах, створення програми медичних гарантій, проведення платежів установам за медичні послуги.
- Бізнес (MIC) – системи, що дозволяють автоматизувати роботу медичних установ з ЦБД.

До найпопулярніших медичних систем, що зараз існують в Україні відносяться: Helsi, Health24, Doctor Eleks, Medics, аптечна мережа 911 [12].

1.2.2 Електронні лікарняні

З 1 жовтня 2021 року всі установи охорони здоров'я України підійшли по-новому до оформлення електронних лікарень. З цього часу пацієнти не носитимуть паперові лікарняні документи на роботу. Якщо пацієнт захворіє, то зможе повідомити своєму роботодавцю номер електронного лікарняного.

Електронні лікарні будуть розділені на дві частини. Медичний висновок

– це документ після огляду лікаря, що містить загальний діагноз. Лікар вносить його до реєстру і завіряє електронним підписом. Пацієнт отримає SMS-повідомлення про це. Звідти, через кілька секунд, лікарняний потрапляє до Реєстру Пенсійного фонду. І там формується електронна довідка про непрацездатність – це саме той документ, за яким нараховуються виплати. Пацієнт також отримає повідомлення про це по телефону, вже від ПФУ. Роботодавець зможе побачити лікарняний на порталі Пенсійного фонду України.

Інформація, що міститься в медичному висновку, підписується лікарем особисто електронним підписом. Це дає розуміння, що медичний працівник несе повну відповідальність за дані, які він туди вводить. Спроба їх підробити (наприклад, видати лікарняний людині, яка не хворіла) – може призвести до позбавлення ліцензії як і лікаря, так і медичного закладу. За будуть стежити співробітники Фонду соціального страхування.

Електронні лікарняні листи формуються автоматично, що зручно для громадян України. Більше немає необхідності збирати довідки та стояти в черзі. Це прискорить процес отримання виплат. Крім того, кожен бажаючий зможе перевірити інформацію про себе в особистому кабінеті на веб-порталі Пенсійного фонду України. Це зробить процес більш відкритим і знизить корупційні ризики [13].

1.2.3 Найсучасніша система моніторингу у лікарні швидкої допомоги

У Львівській міській лікарні швидкої медичної допомоги створено нове відділення інтенсивної терапії на 31 ліжко. Це реанімаційне відділення, яке буде надає невідкладну допомогу людям з різними нейротравмами. Також тут встановлена надсучасна , універсальна система моніторингу та найсучасніший в Україні пристрій для визначення стану згортання крові.

Реанімація повністю обладнана всім потрібним: є нові ліжка, нові пульти, апарати штучної вентиляції легень, бронхоскоп, монітори. Також

встановлений один апарат для діалізу, тому що тут є палата екстракорпоральної детоксикації. Тобто це окреме відділення інтенсивної терапії з палатою, де отримують допомогу люди з тяжкою нирковою недостатністю.

У лікарні встановлена найсучасніша у світовій медицині спеціальна система моніторингу – так званий модуль транспортного моніторингу, який може контролювати всі критичні функції організму пацієнта в будь-якій точці лікарні і навіть за її межами. Лікар може переглядати отримані дані в режимі онлайн через центральну станцію моніторингу в офісі [14].

1.2.4 Пріоритетні напрями МОЗ до 2023 року

Міністерство охорони здоров'я оголосило, що до 2023 року за допомогою проєктів цифрової трансформації вони планують створити електронний кабінет для пацієнтів, забезпечити якість ліків і боротися з соціально небезпечними захворюваннями.

Серед найбільш пріоритетних напрямків до 2023 року Міністерство охорони здоров'я виділяє:

- розвиток медичних послуг та управління медичною інформацією (електронна система охорони здоров’я – eHealth);
- забезпечення якості та безпеки лікарських засобів, медичних виробів (е-ліки);
- популяризація здорового способу життя, захист населення від інфекційних захворювань і боротьба з соціально небезпечними захворюваннями (е-громадське здоров’я).

Кожен з напрямів містить свої власні підпроєкти, зокрема:

- eHealth: електронний кабінет пацієнта, електронна лікарня, диджиталізованитй план лікування, електронні медичні обстеження, модуль конфіденційних даних, електронні медичні звіти (про тимчасову непрацездатність або повну непрацездатність людини, для отримання права на водіння транспортним засобом, або навіть про смерть);
- е-ліки: електронна система керування резервом лікарських засобів

та медичних виробів «eStock», удосконалення Державного реєстру лікарських засобів, створення Державного реєстру медичних виробів, електронний рецепт на інсулін, наркотичні засоби та на всі ліки, що відпускаються за рецептом;

- е-громадське здоров’я: електронна об’єднана інформаційна система епіднагляду за інфекційними захворюваннями, медична інформаційна система «Моніторинг соціально значущих захворювань», інформаційний фонд в галузі громадської охорони здоров'я.

1.3 Приклад найкращої практики на основі лікарень Туреччини

Концепція цифрової лікарні останнім часом є однією з передових практик в секторі охорони здоров'я. Тому багато лікарень в Європі пройшли процеси трансформації та ініціювали заходи з акредитації для отримання сертифікату «цифрової лікарні». Наприклад, у 2016 році лікарні в Туреччині були перевірені HIMSS (акредитаційне агентство), і 18 лікарень отримали «Стадія 6», а одна лікарня отримала цифровий сертифікат лікарні вищого рівня «Стадія 7». HIMSS – це некомерційна організація, заснована в 1961 році, що об'єднує 52 000 медичних установ, 600 фірм і 250 асоціацій/фондів по всьому світу зі структурами в США, Європі та Азії (EMRAM). Модель впровадження EMR (EMRAM) являє собою восьмиступінчасту модель, яка дозволяє відстежувати ваш прогрес у порівнянні з іншими організаціями охорони здоров'я по всій Європі і по всьому світу [15]. Метою його створення є забезпечення оптимального використання інформаційних технологій при наданні та розвитку медичних послуг. Рівні цифровізації лікарень оцінюються EMRAM на міжнародному рівні. У цьому процесі перевіряється рівень використання інформаційних систем в діяльності організацій охорони здоров'я. HIMSS використовує загальноприйняту акредитацію та стандартну модель EMRAM для оцінки цифрових процесів та визначення стадій роботи лікарень-кандидатів. У цій моделі лікарні оцінюються від 1 до 7, а ті, хто завершує процес цифровізації до 6-го і 7-го стадій, отримують сертифікати. Завдяки

системі EMRAM HIMSS полегшує адаптацію лікарень до постійно зростаючих інформаційних технологій охорони здоров'я відповідно до міжнародних стандартів.

Щоб лікарня стала цифровою лікарнею, вона повинна бути оцінена і нагороджена сертифікатом акредитуючого агентства HIMSS. Коли критерії в виконані, лікарні звертаються до агентства HIMSS. Експерти, призначені HIMSS, перевіряють відповідну лікарню на місці і оцінюють її відповідно до опублікованих критеріїв і видають відповідний сертифікат [16].

1.3.1 Стадії та критерії цифрової лікарні HIMSS EMRAM

Стадії та критерії цифрової лікарні HIMSS EMRAM:

- Стадія 0. У ній описуються лікарні, де навіть основні підрозділи клінічної підтримки (аптека, лабораторія та радіологія) і процеси не включені в цифрове середовище.
- Стадія 1. У ній описується, що цифрові системи встановлюються в основних підрозділах клінічної підтримки (аптека, лабораторія і радіологія).
- Стадія 2. Інформаційні системи зберігання клінічних даних (CDR) надсилають всю медичну інформацію та результати пацієнтів до системи, доступної для перегляду лікарями. Ця система відправляє дані в електронну історію хвороби пацієнта або архів клінічних даних, отримує зворотний зв'язок і пересилає їх в підсистеми. Система може отримувати і відправляти документи з медичними зображеннями і забезпечувати обмін інформацією між лікарнями.
- Стадія 3. Клінічні документи, що стосуються медсестринства (життєві показники, протоколи, сестринські записки, eMAR) та/або записи електронного обліку та введення замовлення, а також системи відстеження замовлення повинні бути інтегровані з електронними записами пацієнтів та сховищем клінічних даних принаймні в одному процесі обслуговування. Перший етап підтримки прийняття клінічних рішень може бути відпрацьований для перевірки помилок при введенні замовлення. Дані про

взаємодію між лікарськими засобами, ліками/продуктами харчування, лікарськими засобами/лабораторіями зазвичай є в аптеці. Медичні знімки в архіві зображень повинні бути доступні з системи через інтранет для лікарів поза відділенням радіології.

● Стадія 4. На цій стадії доступний другий етап систем підтримки прийняття клінічних рішень для обґрунтованих медичних протоколів. У цій системі будь-який ліцензований лікар може написати замовлення та додати медсестру для свого доступу до даних у системі комп'ютеризованого запису лікаря (CPOE). Якщо система комп'ютеризованого введення медичного замовлення використовується в зоні надання стаціонарної допомоги та попередні етапи завершені, то цей етап також вважається завершеним.

● Стадія 5. Медичні зображення в повноцінному архіві радіологічних зображень і системі зв'язку (PACS) відкриті для доступу всіх лікарів і відправляються в інші місця через інтранет. На цьому етапі, якщо графічні документи кардіологічного відділення (ЕКГ і т.д.) вводяться в систему PACS, лікарні нараховуються додаткові бали.

● Стадія 6. Повноцінна система документування лікарів діє на практиці принаймні в одній стаціонарній клініці. Система клінічної підтримки третього етапу забезпечує керівництво всіма клінічними процесами. Система управління ліками із замкнутим циклом і система кодованих ліків повністю впроваджені на практиці. Для забезпечення максимальної безпеки пацієнтів на практиці застосовуються інші технології автоматизованої ідентифікації та автоматизовані системи доставки, такі як електронна запис про прийом ліків і комп'ютеризована запис про замовлення лікаря/електронний рецепт і штрих-кодування або RFID (радіочастотна ідентифікація), інтегровані з фармацевтикою. Таким чином, відповідно до принципу «5 прав (правильний пацієнт, правильні ліки, правильна доза, правильний маршрут і правильний час)», розроблений з метою запобігання помилковому вживанню наркотиків, ідентифікаційні дані пацієнта та штрих-код ліків перевіряються біля ліжка пацієнта.

● Стадія 7. Лікарня на даному етапі ніколи не використовує паперові документи при наданні послуг. Всі дані, документи та медичні зображення обробляються в електронному вигляді. Дані, що зберігаються в цифровому середовищі, аналізуються і використовуються для підвищення якості медичної допомоги, забезпечення безпеки пацієнтів і надання ефективних послуг. Відповідні дані стандартизовані в електронному вигляді та готові до використання та обміну інформацією уповноваженими особами та установами (керівництвом, іншими лікарнями тощо). Лікарня забезпечує безперервність даних всіх процесів обслуговування і публікує такі дані. На цьому етапі медичні матеріали, такі як продукти крові, також стають доступними через систему введення ліків із замкнутим циклом [17].

1.3.2 Державна лікарня Tipe

Під час нагородження державної лікарні Tipe з сертифікатом «Цифрова лікарня, стадія 7» було визначено такі заходи:

● Прийом пацієнтів, госпіталізація та інші клінічні процеси, консультації та направлення переміщуються на безпаперову цифрову платформу.

● Цлікарні впроваджуються такі практики, як електронний рецепт та електронний підпис.

● Замовлення на МРТ, рентген, ЕКГ, кров та інші аналізи укладаються без документів у комп’ютерному середовищі. Результати цих замовлень надходять у цифрове середовище. Ці результати можуть бути доступні будь-де як медичним працівникам, так і пацієнтам за допомогою телефонів та планшетів.

● Усі сформовані дані (записи, результати, рахунки-фактури тощо) архівуються в цифровому середовищі, і забезпечується безпека інформації.

● Накази лікарів про лікування негайно та за допомогою віддаленого доступу повністю обробляються в онлайн-середовищі.

● За допомогою комп'ютерних терміналів, розміщених в палатах

пацієнтів, медсестри вводять інформацію про лікування в систему без використання будь-якого паперу або документа.

- Завдяки системі введення ліків із замкнутим циклом потрібний лікарський засіб вводиться потрібному пацієнту в потрібних дозах, правильним шляхом та в потрібний час.
- Всі адміністративні документи і кореспонденція в лікарні (за винятком документів про закупівлі, як того вимагає законодавство) відслідковуються в електронній системі, і в документах використовується електронний підпис.
- Такі програми, як системи бюджетування та оповіщення про запаси, використовуються для постійного перегляду ресурсів.
- Компоненти інфраструктури, такі як пожежна система, безпека, електрика, водопостачання та природний газ, супроводжуються центральною системою. В екстрених випадках ці технології можуть бути активовані.
- Жодні дані, згенеровані в лікарні, не втрачаються, і до всіх даних можна отримати доступ з будь-якого місця і в будь-який час.
- Оскільки папір не використовується, економляться стаціонарні витрати.
- Послуги лікарні можуть надаватися швидко і ефективно завдяки інтелектуальному програмному забезпеченню.

Практики, перераховані вище, є вимогами для стадії 7 в класифікації «Цифрова безпаперова лікарня». Крім того, Державна лікарня Гіресун Тіреболу в Туреччині, що отримала сертифікат «Стадія 6», була перевірена і проінформована про те, що всі процеси (відстеження ліків, прийом пацієнтів і т.д.) повинні виконуватися в цифровому середовищі принаймні в одній клініці лікарні, щоб отримати сертифікат 6-ої стадії. Тому педіатрична клініка лікарні була оснащена цифровою системою і строго перевірена HIMSS [18].

1.4 Висновки до першого розділу

Цифрові лікарні підвищують швидкість і ефективність бізнес-процесів і зводять до нуля витрати на папір і документацію. З точки зору робочого персоналу, помилки, допущені людиною, усуваються, і дані можуть бути отримані уповноваженими підрозділами, іншими установами охорони здоров'я та пацієнтами негайно і ретроспективно в будь-який час. Процесами діагностики та лікування можна керувати не тільки в стінах лікарні, але і з великих відстаней. Деякими процесами можна керувати за допомогою сенсорів, камер і систем раннього попередження без необхідності контролю з боку людей.

Завдяки системі керування ліками із замкнутим циклом між аптекою і палатою пацієнта, яка є однією з послуг, що надаються цифровими лікарнями, після того, як ліки призначаються лікарем в електронному вигляді, вони доставляються пацієнтові по каналу з інтелектуальним програмним забезпеченням і приймаються для управління відповідним персоналом.

Пандемія Covid-19 вплинула на розвиток охорони здоров’я по всьому світу. В Україні цифровізація тільки набирає оберти і може взяти приклад з Туреччини, яка вивела свої лікарні на новий рівень.

2 АРХІТЕКТУРА ТА СХЕМИ ІСНУЮЧИХ ЦИФРОВИХ ЛІКАРЕНЬ

Інтернет речей (IoT) – це мережа фізичних пристроїв та інших предметів, вбудованих електронікою, програмним забезпеченням, датчиками та мережевим підключенням, що дає змогу цим об’єктам збирати й обмінюватися даними [19]. Його вплив на медицину буде, мабуть, найважливішим і особистим ефектом. До 2022 року 40% технологій, пов’язаних з Інтернетом речей, будуть пов’язані зі здоров’ям, більше, ніж будь-яка інша категорія, що становитиме ринок у 117 мільярдів доларів [20]. Зближення медицини та інформаційних технологій, таких як медична інформатика, змінить охорону здоров’я, яку знаємо, обмежуючи витрати, зменшуючи неефективність та рятуючи життя.

На рисунку 2.1 проілюстровано, як ці зміни в медицині будуть виглядати у типовій лікарні IoT на практиці.

Рисунок 2.1 – Зміни в медицині в типовій лікарні Інтернету речей (IoT) на практиці

Пацієнт з цукровим діабетом матиме ідентифікаційну картку, яка під час сканування зв'язується із захищеною хмарою, в якій зберігаються життєво важливі дані його електронної медичної картки та результати лабораторних досліджень, медичні приписи та рецепти. Лікарі та медсестри можуть легко отримати доступ до цього запису на планшеті чи настільному комп'ютері.

Звучить досить просто, але прийняття електронних медичних карт змінило правила. Менш ніж за десятиліття чорнильно-паперова система управління записами, яка налічує тисячі років, буде оцифрована та замінена [21]. Переваги очевидні і багато. Паперові записи, часто написані сумнівним автором, можуть бути запхані в картотеки, поза досяжністю дослідників чи інших медичних працівників. Замість цього, зберігаючи всю важливу інформацію в одному місці та легко ділитися, електронні медичні картки (ЕМК) усуне багато неефективності та врятує життя.

Одна з головних проблем для впровадження IoT пов'язана з комунікацією. Хоча зараз багато пристроїв мають давачі для збору даних, вони часто обмінюються із сервером за відповідними протоколами. Кожен виробник має свої власні протоколи, що означає, що давачі різних виробників не обов'язково можуть спілкуватися один з одним.

Інженерні імітаційні рішення роблять медицину персоналізованою, прогнозною та профілактичною через медичний Інтернет речей (IoMT) [22].

2.1 Інтернет речей та розумна система охорони здоров'я.

Системи IoT складаються з давачів і пристроїв, підключених через мережу хмарних екосистем за допомогою високошвидкісного підключення між кожним модулем. Неопрацьовані дані, зібрані на цих пристроях/давачах, надсилаються безпосередньо до величезного сховища, яке пропонує хмарні сервіси. Ці дані додатково очищаються, а потім аналізуються, щоб отримати подальше уявлення про них. Для цього потрібне додаткове програмне

забезпечення, інструменти та додатки, які додатково допоможуть у візуалізації, аналізі, обробці та управлінні даними [60].

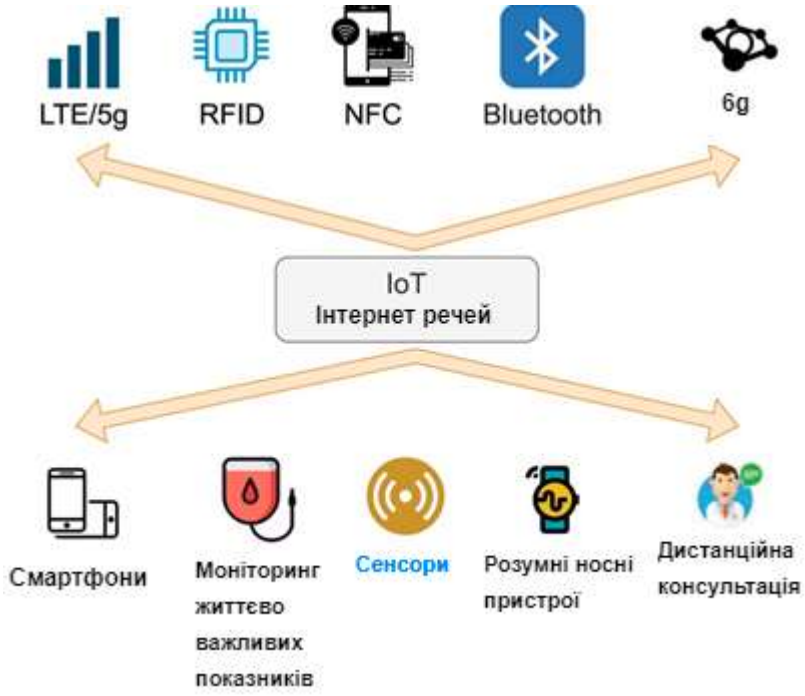

Рисунок 2.2 – Інтернет речей, технології та пристрої

На рисунку 2.2 показано декілька бездротових технологій, таких як RFID, NFC, Bluetooth, LTE і 5G/6G пов'язані з кількома пристроями, такими як смартфони, пристрої моніторингу, давачі, розумні носії та інші медичні пристрої. В даний час використання 5G/6G або вище поширене в IoMT через їхню високу пропускну здатність і наднизькі переваги затримки [23].

2.2 Розумна електронна медична допомога

Розумні лікарні – це лікарні, які створені на основі інтелектуальних автоматизованих та оптимізованих модулів на інфраструктурі інформаційних та комунікаційних технологій (ІКТ), щоб покращити процедури догляду за

пацієнтами та додати нові можливості. Існує кілька застосувань розумних лікарень, таких як телемедицина, дистанційна хірургія роботів.

Телемедицина – це надання клінічної допомоги на віддаленому місці. У дистанційній хірургії роботів медичні роботи виконують операцію за вказівками лікаря, який знаходиться далеко.

На рисунку 2.3 показано приклад розумної системи охорони здоров'я, в якій спочатку збираються вхідні дані з різних джерел (наприклад, шляхом віддаленого або фізичного збору) та надіслано до EHR (системи електронних медичних записів) [24].

Рисунок 2.3 – Приклад інтелектуальної електронної системи охорони здоров’я

Дані можуть бути класифіковані як неструктуровані, якщо вони збираються в автономному режимі на папері як медичні довідки персоналом. Якщо дані збираються у структурованій формі з пристроїв і давачів за допомогою попередньо визначених полів даних, які користувачі можуть вводити, їх буде легко обробляти в інших системах, таких як CRM (Customer Relational Management) System. CRM дозволяє використовувати інструменти для аналізу даних, а потім призначати їх попередньо визначеній цілі в екосистемі.

Основні дані та інформація з систем EHR надсилаються в систему CRM, і вона опрацьовує ці дані пацієнта. Ці опрацьовані дані генерують додаткові

тригери для пацієнтів та медичного персоналу в екосистемі. Пацієнти отримують вихідну комунікацію від лікарень та експертів у сфері охорони здоров'я у вигляді індивідуальних режимів здоров'я. Лікарі та інший медичний персонал отримують сповіщення про нагадування та інші сповіщення від того самого програмного забезпечення CRM в екосистемі [25].

2.3 Архітектура для IoMT

Архітектура IoMT складається з трьох рівнів (див. рис.2.4). Існує три шари: (1) шар речей, (2) шар туману та (3) шар хмар. Це модифікована версія архітектури, представленої в [26].

Рисунок 2.4 – Операції всередині шарів у IoMT

У цій архітектурі експерти з охорони здоров'я можуть також спілкуватися безпосередньо через маршрутизатор між рівнем Thing і Fog, а також через локальні сервери обробки на шарі туману. Кожен шар описаний нижче:

- Рівень речей складається з пристроїв моніторингу пацієнтів, давачів, приводів, медичних записів, засобів контролю аптек, генератора режиму живлення тощо. Цей шар безпосередньо контактує з користувачами екосистеми. На цьому рівні збираються дані з таких елементів, як носимі пристрої, дані моніторингу пацієнтів, дані віддаленого догляду Пристрої, які використовуються при цьому, повинні бути надійно розміщені, щоб забезпечити цілісність зібраних даних. За підключення цих пристроїв до шару туману відповідають локальні маршрутизатори в екосистемі. Дані далі опрацьовуються у відповідних шарах для отримання значущої інформації. Крім того, щоб зменшити затримку, експерти з охорони здоров'я можуть отримати дані пацієнта через маршрутизатор [27].
- Шар туману діє між хмарою і шаром речей. Цей рівень складається з локальних серверів і пристроїв шлюзу для слаборозподіленої мережі туманної мережі. Локальна обчислювальна потужність використовується пристроями нижнього рівня для реагування в реальному часі своїм користувачам. Ці сервери також використовуються для керування та адміністрування безпеки та цілісності системи. Пристрої шлюзу на цьому рівні відповідають за перенаправлення цих даних з цих серверів на хмарний рівень для подальшої обробки. Крім того, щоб зменшити затримку, експерти з охорони здоров'я можуть отримати дані пацієнта через цей маршрутизатор.
- Хмарний рівень складається з ресурсів зберігання даних і обчислень для аналізованих даних і створення на їх основі систем прийняття рішень. Хмара також пропонує широкі можливості для об'єднання величезних медичних систем і систем охорони здоров'я, щоб з легкістю виконувати свої повсякденні операції. Цей рівень складається з хмарних ресурсів, де будуть зберігатися дані, згенеровані медичною інфраструктурою, і аналітична робота може виконуватися, якщо це буде необхідно в майбутньому [28].

2.4 Нові технології в IoMT

2.4.1 Технологія блокчейн

Блокчейн (Blockchain) – розподілена база даних, що зберігає структурований ланцюжок записів (так званих блоків), що постійно довшає. Блокчейн складається з блоків або вузлів, які з’єднані через мережу, в якій записується інформація, якою обмінюються будь-який з вузлів мережі, і її можна використовувати для перехресних посилань. Ці блоки містять інформацію з попередніх блоків, і ця методологія допомагає визначити точне джерело зловмисників у мережі. Блоки, які не ідентифіковані в мережі, таким чином відкидаються, що відкриває шлях для того, щоб блокчейн розглядався як стратегія довіри в системах обміну інформацією, таких як IoMT [29].

Блокчейн дозволяє суб'єктам взаємодіяти один з одним без присутності централізованого органу в мережі. Записи даних у блокчейні зберігаються як блоки даних. Ці блоки, як було зазначено раніше, містять інформацію про найближчі блоки в ланцюжку з протоколами криптографії для їх безпечного використання. Ці блоки та їх дані можуть бути прочитані іншими користувачами, але дані в цих блоках залишаються захищеними від несанкціонованого доступу. Блокчейн також забезпечує плавне опрацювання смарт-контрактів, які не потребують жодного центрального органу для їх запуску [30].

Візуальне представлення різних елементів охорони здоров’я на платформі блокчейн показано на рисунку 2.5.

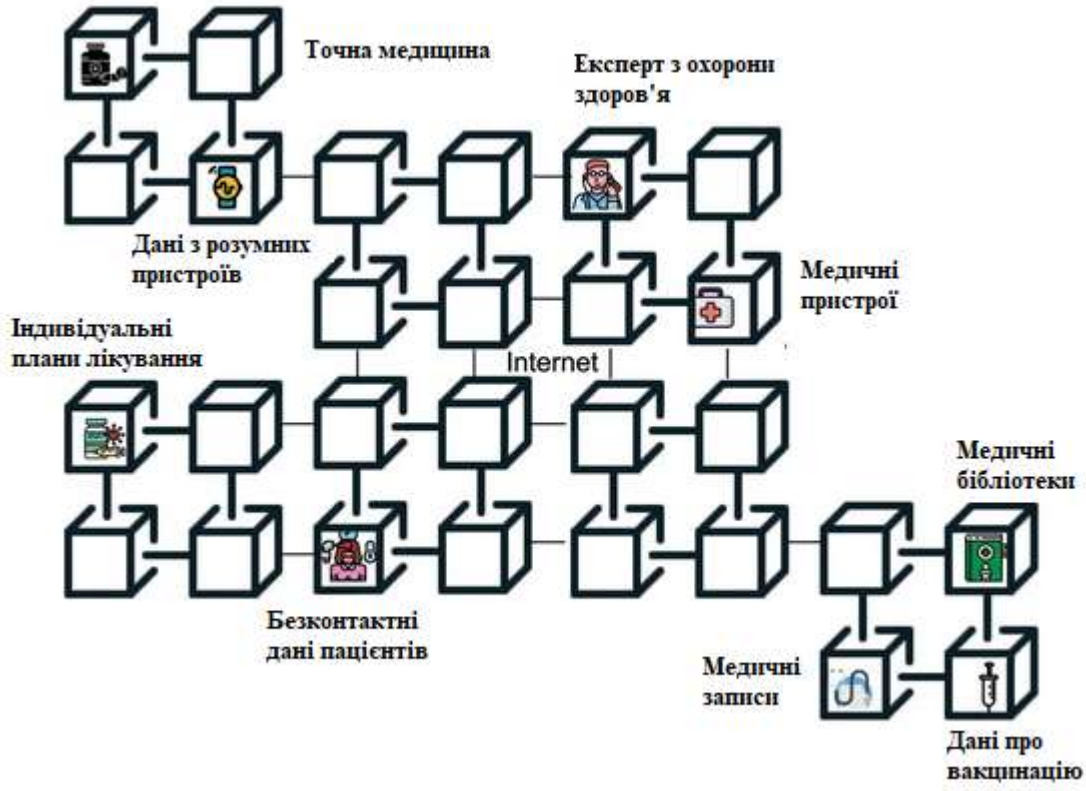

Рисунок 2.5 – Використання блокчейну в IoMT

Роль блокчейну в секторі охорони здоров’я для прийняття рішень, побудованих на його основі, вимагає розділення інфраструктури на менші модулі. Ці модулі потім можна інтегрувати з відповідними пристроями в структуру IoMT. Отримана система буде розподілена в природі і дозволить децентралізувати владу в мережі. Перевага розгортання блокчейн-систем пов’язана з фактором довіри, тоді як приплив даних в екосистему охорони здоров’я постійно зростає.

Блокчейн обіцяє задовольнити постійно зростаючий попит на обмін даними через інфраструктуру охорони здоров’я. Використання блокчейну в даний час тестується для систем EHR в лікарнях, після чого проводяться деякі клінічні випробування у всьому світі [31].

2.4.2 Пристрої з фізичною неклонованою функцією (PUF)

Пристрої PUF генерують унікальний відбиток пальців для вразливих елементів в екосистемі IoMT. Ці унікальні відбитки пальців/підписи

виникають внаслідок різниць у виготовленні цих пристроїв. Ці відбитки пальців можна використовувати для генерації секретних ключів (ключів криптографії) для захисту пристроїв та їхніх даних в екосистемі IoMT, де кінцеві пристрої (давачі) піддаються ризику атак апаратного втручання [33].

На рисунку 2.6 показано відображення пристроїв PUF з архітектурою, представленою в попередньому підрозділі.

Рисунок 2.6 – IoMTs, увімкнення пристроїв PUF

Пристрої PUF знаходяться в шарі речей у нашому відображенні. Ці пристрої відіграють важливу роль, коли справа доходить до аутентифікації пристроїв IoMT в екосистемі. Як показано на рис. 2.6, після шару туману безпека забезпечується більш спеціалізованими рішеннями безпеки підприємства, що пропонуються постачальниками послуг в архітектурі (наприклад, на основі AI/ML) [33].

2.4.3 Штучний інтелект та IoMT

На рис. 2.7. представлено кілька застосувань IoMT для штучного інтелекту, включаючи машинне навчання (ML) та обробку природної мови (NLP) в електронній охороні здоров’я. Точна медицина вимагає розширеної діагностики та індивідуальних схем із швидким часом доставки. Штучний інтелект (ШІ) є вагомими аргументами для цього, пропонуючи рішення в режимі реального часу для визначення нових шляхів лікування певних станів на основі історичних даних і даних реального часу. Різні функції в екосистемі

охорони здоров’я можна змінити за допомогою рішень на основі штучного інтелекту [34].

Рисунок 2.7 – IoMT з підтримкою машинного навчання та NLP

Це включатиме методи штучного інтелекту для створення класифікаторів, таких як автоматичний збір інформації про пацієнтів, планування прийомів пацієнтів, визначення лабораторних тестів, планів лікування, ліків, хірургічного лікування тощо. Ці класифікатори можна буде додатково навчати та підтримувати процеси прийняття рішень. Для інших класифікаторів, які не можуть бути записані в цифровому вигляді, NLP пропонує методи вилучення інформації з таких неструктурованих точок даних в інфраструктурі. Вони можуть бути у формі лабораторних звітів, записів фізичного огляду, оперативних записів та іншої інформації про виписку пацієнтів [35]. Крім того, машинне навчання прогнозує майбутні умови на основі історичних даних. Воно застосовує контрольоване, неконтрольоване або посилене навчання для прогнозування майбутніх умов.

2.4.4 SDN в IoMT

Частину мережі в IoMT можна розділити на дві частини:

- площина даних
- площина керування.

Площина даних перенаправляє трафік до місця призначення, тоді як

площина керування виконує необхідні завдання, які дозволяють площині даних приймати рішення щодо пересилання [36].

Програмно-конфігурована мережа (SDN) забезпечує стандартний спосіб зв'язку між площиною даних і площиною керування. Прикладами стандартних протоколів SDN є OpenFlow, Open vSwitch Database Management protocol і OpenFlow Configuration protocol (OF-CONFIG) [29]. Оскільки інтерфейс між площиною даних і площиною керування може бути стандартним за допомогою стандартного протоколу SDN, багато різних даних площини даних можна зібрати із зовнішнього сервера (може бути розташований в хмарі) за допомогою стандартного протоколу OpenFlow. Це дає змогу розробляти різні програми електронної охорони здоров’я, оскільки вони можуть розташовуватися в хмарному шарі [37].

На рисунку 2.8 показано запропоновані нами IoMT з підтримкою SDN, де пристрої IoMT підключені до програм електронного здоров’я, які можуть бути розташовані в хмарі, через площину керування SDN (вона може бути в шарі туману).

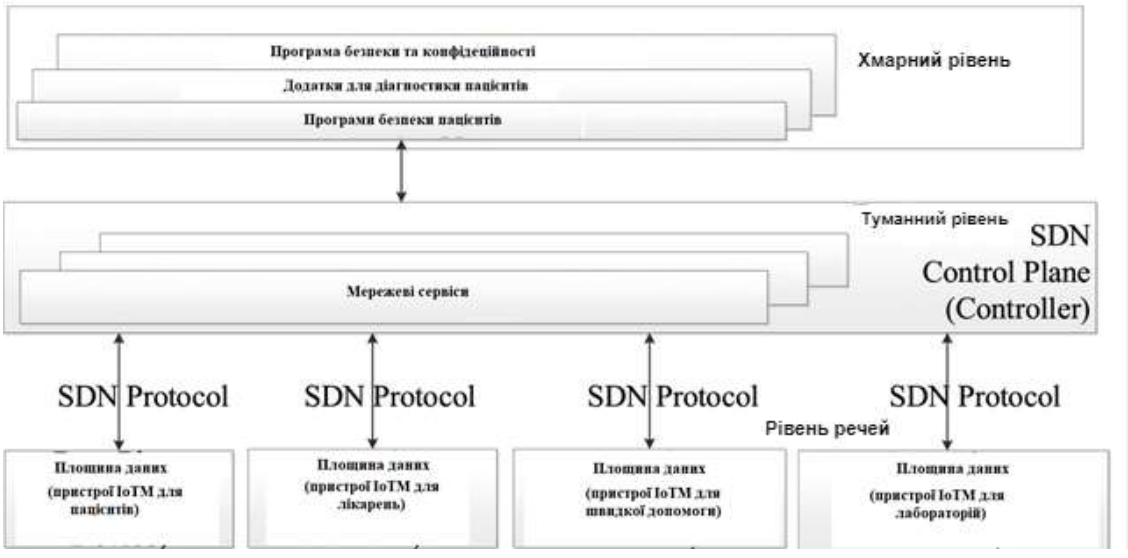

Рисунок 2.8 – IoMT з підтримкою SDN

Площина керування SDN збирає дані з пристроїв IoMT і надає їх до програми електронного медичного обслуговування. Додаток для електронної

медичної допомоги може бути програмою безпеки та конфіденційності, програмою для діагностики пацієнтів або програмою безпеки пацієнтів. Запропонована архітектура є модифікованою версією архітектури, запропонованої для Інтернету транспортних засобів із включеною SDN [38].

2.5 Різноманітні давачі

Використання давачів для збору даних з таких параметрів, як температура, ЕКГ, кров'яний тиск, пульс і серцебиття, змінило точність даних і в кінцевому підсумку призвело до того, що пацієнти отримають краще обслуговування, ніж раніше [39]. Системи моніторингу пацієнтів також покращили реакцію експертів із охорони здоров'я.

Основними компонентами IoMT є давачі. IoMT має застосування як у клінічних, так і в доклінічних сценаріях. У клінічному контексті IoMT використовується для моніторингу життєво важливих показників пацієнта, таких як температура, ЕКГ, кров'яний тиск, насичення крові киснем тощо. Це дозволяє постійно контролювати життєво важливі показники здоров'я пацієнтів, а також допомагає лікарям за допомогою панелей інструментів візуалізувати дані. Давачі можна розгортати та контролювати дистанційно, тим самим дозволяючи дистанційно надавати медичні послуги. У неклінічному контексті IoMT можна використовувати для відстеження активів, відстеження місцезнаходження лікаря, дотримання гігієнічних стандартів, визначення місцезнаходження машин швидкої допомоги під час надзвичайних ситуацій та ефективності роботи шляхом відстеження активів, людей у лікарні та надання інформації в реальному часі для логістики [40].

Пристрої для носіння або носіння – це розумні електронні пристрої, які містять різні давачі, які можна використовувати для моніторингу життєво важливих показників здоров'я. Датчики, які використовуються в носимих пристроях для збору даних, відомі як датчики для носіння. Ці речі можна носити на тілі або вставляти в одяг. Деякі з прикладів носимих пристроїв –

Fitbit, Apple Watch і Samsung Galaxy Gear. Використання носимих пристроїв різноманітне. У сфері охорони здоров’я носні пристрої можуть використовуватися в основному для моніторингу активності та моніторингу здоров’я, де відстежуються кілька життєво важливих показників здоров’я пацієнта, а дані передаються віддаленим лікарям або лікарям для прийняття відповідних рішень. Деякі з давачів, які використовуються для відстеження життєво важливих показників здоров’я: давачі пульсу, давачі частоти дихання, давачі температури тіла, давачі артеріального тиску, давачі пульсоксиметрії [41].

Давачі пульсу зчитують пульс людини, що можна використовувати для моніторингу надзвичайних станів, таких як зупинка серця та емболія легеневої артерії. Пульс можна зчитувати з зап’ястя, мочки вуха, грудей, кінчиків пальців тощо.

Показання мочки вуха та кінчиків пальців є високоточними, але їх не зручно носити. Давачі на зап'ясті, як правило, розглядаються як довгострокова система носіння. Деякі з комерційно доступних носних пристроїв, пов’язаних з фітнесом, які підтримують функцію моніторингу пульсу, це HRM-Tri від Garmin, H7 від Polar, FitBit PurePulse і TomTom Spark Cardio. Але всі виробники цих пристроїв заявили, що вони не придатні для виявлення захворювань. Іншими давачами, які можна використовувати для вимірювання пульсу, є давачі тиску, фотоплетизмографічний (ФПГ) давач, ультразвуковий давач і радіочастотний (РЧ) давач [42].

Давачі частоти дихання зчитують частоту дихання або кількість вдихів, які пацієнт робить за хвилину, що може допомогти визначити критичні стани, такі як напади астми, туберкульоз, гіпервентиляція, рак легенів тощо. Для вимірювання частоти дихання було розроблено кілька давачів, таких як назальний давач на основі термістора, ЕКГ-дихання, мікрофон, волоконно-оптичний давач, давач тиску. На ці давачі має вплив шум, що виникає через рух. Для відповідності WBAN настійно рекомендується використовувати датчики розтягування [43].

Давачі температури тіла використовуються для зчитування температури тіла людини, за допомогою яких можна виявити лихоманку, тепловий удар, гіпотермію тощо. Більшість сучасних дослідницьких робіт показують що давачі на основі термісторів зазвичай використовуються.

Давачі артеріального тиску використовуються для зчитування загального та часто контролюваного життєво важливого значення для здоров'я – артеріального тиску (АТ). Вимірювання артеріального тиску може привести до виявлення гіпертонії, яка призводить до серцево-судинних захворювань, таких як серцевий напад [44.

Давачі пульсоксиметрії зчитують рівень кисню в крові, що є ще одним важливим параметром, який може допомогти в діагностиці таких станів, як гіпоксія. Ці давачі вимірюють кисень крові шляхом отримання сигналів PPG. Давач PPG зазвичай містить два світлодіоди, один червоний і інший інфрачервоний, які фокусуються на шкірі. Більшість світла поглинається гемоглобіном крові. Кисень у крові розраховується фотодіодами, вимірюючи світло, яке не поглинається [45].

Дані, зібрані з давачів, в основному обробляються пристроями в шарі туману, що забезпечує підтримку невідкладної допомоги а потім зберігається в хмарі для тривалого зберігання даних або подальшої обробки.

2.6 Висновки до другого розділу

У розділі детально розглянуто архітектуру та схеми існуючих цифрових лікарень, а саме:

- Інтернет речей та розумну систему охорони здоров'я.
- Розумну електронну медичну допомогу.
- Архітектуру для IoMT.
- Нові технології в IoMT (PUF, SDN, блокчейн та штучний інтелект).
- Різноманітні давачі.

3 ЕНЕРГОЕФЕКТИВНА АВТЕНТИФІКАЦІЯ НА ОСНОВІ PUF ПРИСТРОЇВ В ІНТЕРНЕТІ МЕДИЧНИХ РЕЧЕЙ (IOMT)

Розумна лікарня, заснована на технології IoT і побудована за допомогою вектора різноманітних прикладних сервісних систем, є концентрованим відображенням IoT, що використовується в спеціальному місці лікарні, і це новий вид лікарні, об'єднаний з функцією діагностики, лікування, управління, і рішення.

Завдяки впровадженню розумної лікарні можна реалізувати систему прикладних програм, засновану на цифровому середовищі, і пацієнти можуть швидко та точно отримувати відповідну службову інформацію, таким чином він може реалізувати інформатизацію діагностики, стандартизацію управління та наукове рішення. У той же час, завдяки інтеграції та об'єднанню сервісу додатків, можна реалізувати отримання інформації, обмін і обслуговування в лікарні, щоб сприяти процесу впровадження в розумній діагностиці, розумному лікуванні, розумному управлінні, розумних рішеннях та розумному обслуговуванні [46].

Індустрія охорони здоров’я та розумної лікарні стрімко розвивається та бере всі можливості, які пропонує сучасний світ. Розроблено багато методів як можна застосувати IoT. В даний час дані про хворого можуть бути зібраними на відстані і вже потім відправлені лікареві для діагностики. Це навіть в деяких випадках допомагає поставити пацієнту діагноз та вилікувати його. Проте такий аспект роботи має і свої мінуси, такі як безпека та захищеність даних. Тому що дистанційність робить їх вразливими до атак, таких як підміна ідентичності або імітація діагнозу [47].

3.1 Автентифікація пристрою на основі PUF

На рисунку 3.1 продемонстровано небезпеки які можуть спіткати так званих користувачів електронних систем. Наприклад, впровадившись в

налаштування подачі кисню чи навіть в банальне дозування препаратів, можна налаштувати конфігурацію таким чином що та доза для людини буде смертельною.

Рисунок 3.1 – Атаки на електронні системи

Фізичні неклоновані функції (PUF) використовуються для генерації криптографічних ключів [48]. PUF використовує виробничі варіації, які вводяться в інтегральну схему (IC) під час її виготовлення. Варіації непередбачувані, неконтрольовані, неминучі і природні [49]. Отже, ключі, які генеруються за допомогою модуля PUF, також природно випадкові і унікальні для відповідного модуля PUF. Різні архітектури PUF були запропоновані дослідниками по всьому світу для інтеграції в різні середовища. Арбітер гібридного осцилятора PUF [50], використовується для протоколу аутентифікації пристрою на основі PUF. На рисунку 3.2 показана загальна концепція безпеки на основі PUF в парадигмі граничних обчислень [61].

Рисунок 3.2 – Запропонована безпека на основі PUF в парадигмі граничних обчислень Інтернету речей.

У данному підході кожен пристрій у мережі матиме вбудований в нього модуль PUF. Вони відповідають за створення унікальних ідентифікаторів для пристроїв Інтернету речей і серверів, присутніх в мережі. Протокол автентифікації пристрою включає в себе два етапи: етап реєстрації та етап автентифікації [51].

3.1.1 Етап реєстрації та автентифікації

Фаза реєстрації протоколу відбувається, коли в мережу потрібно ввести новий пристрій. Під час цієї фази сервер буде отримувати доступ до модуля PUF в кінцевому пристрої, а ключі надійно зареєстровані. Спочатку вхід C1 виклику надходить модулю PUF на сервері, і генерується відповідь R1.

Ця відповідь (R1) подається як вхід виклику до модуля PUF на кінцевому пристрої, а відповідь від нього генерується R2. Потім R2 передається модулю PUF на сервері і вводиться як вхід для виклику протягом другого часу. Після генерації відповіді R3 обчислюється його хеш, $X = H(R3)$. Цей хеш X і вхід виклику C1 зберігаються в захищеній базі даних. Цей процес повторюється, а відповідні вхідні дані та хеші зберігаються в базі даних для автентифікації в більш пізній період часу. Після завершення етапу реєстрації пристрій можна безпечно автентифікувати, виконавши аналогічні дії під час етапу реєстрації.

Під час автентифікації збираються виклик C1 і відповідний X із захищеної бази даних. Вхід Challenge подається як вхід PUF на сервері, а процес генерується для створення хешу X для запиту пристрою. Якщо хеш відповідає X, що зберігається в базі даних, пристрій проходить автентифікацію.

3.1.2 Імплементація прототипу

На рисунку 3.3 показана експериментальна установка для прототипу. Модуль PUF був розроблений на PMsec. Бортовий комп'ютер був сервером, а мікроконтролер – кінцевим пристроєм. Одноплатний комп'ютер був пристроєм з низьким енергоспоживанням і міг виконувати основні криптографічні функції, такі як хешування, які необхідні для протоколу PMsec. Мікроконтролер підключений до прототипу для ключів, що генеруються модулем PUF. На рисунку 3.4 показані вихідні дані одноплатного комп'ютера і мікроконтролера на етапах реєстрації та автентифікації.

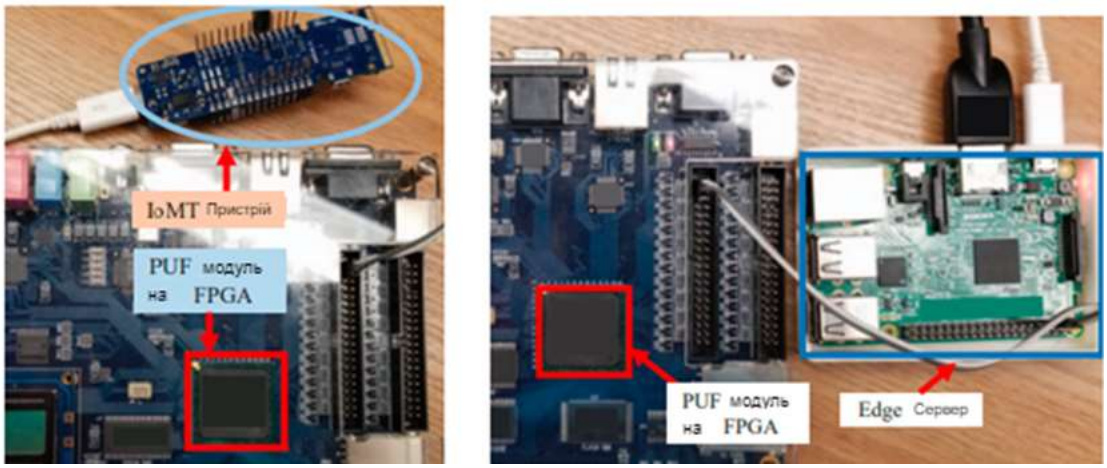

Рисунок 3.3 – Перевірка прототипу в середовищі побутової електроніки

Рисунок 3.4 – Перевірка правильності запропонованої схеми автентифікації

Результати, отримані в під час прототипування плати, зведені в таблицю 3.1. Час, необхідний для автентифікації пристрою, становить 1.5 секунди, а частота помилок становить 10%. Загальне енергоспоживання системи може бути знижено за рахунок інтеграції в протоколи більш енергоефективних конструкцій PUF. З пристроєм або модулем PUF на стороні сервера в руках виконання різних атак на систему буде складним завданням.

Таблиця 3.1 – Характеристика запропонованого прототипу

Параметри	**Значення**
Сервер	Одноплатний комп'ютер
Кінцевий пристрій	Плата розробки на базі 32-розрядного мікроконтролера
Час генерації ключа на сервері	800 ms
Час генерації ключа на пристрої IoMT	800 ms
Час для автентифікації пристрою	1.2 с. -1.5 с.
Частота помилок	10%

Оскільки жодна інформація про пристрій безпосередньо не зберігається в базі даних сервера, це додає додатковий рівень безпеки в середовище.

3.2 Автентифікація на основі PUF для E-Healthcare

На рисунку 3.5 представлено огляд запропонованої системи

автентифікації на основі PUF, де інфраструктура електронного здоров'я, що містить пристрої IoMT PUF, підключена через супутникову широкосмугову мережу з ISP (постачальником послуг Інтернету) та мобільними мережами. Використовуючи цю структуру, бачимо, що пристрої IoMT можуть бути віддалено автентифіковані та доступні медичним працівникам на дистанційному пристрої за допомогою механізму на основі PUF. Детальний вигляд підключених пристроїв можна побачити на рисунку 3.6. У цьому прикладі використовуємо засіб відстеження пакетів Cisco (інструмент моделювання) для імітації платформи.

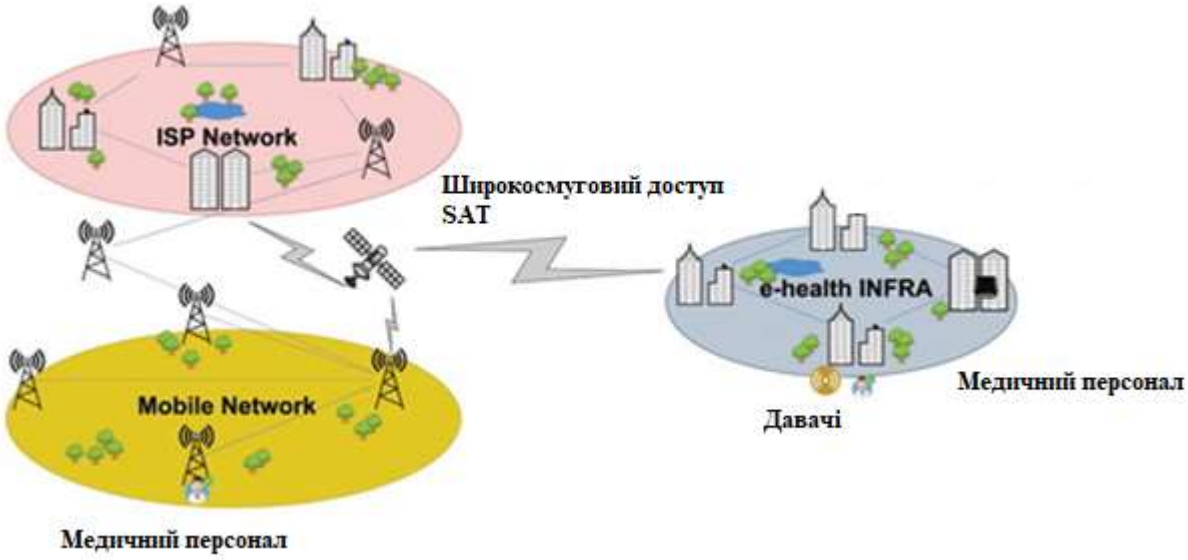

Рисунок 3.5 – Огляд автентифікації на основі PUF

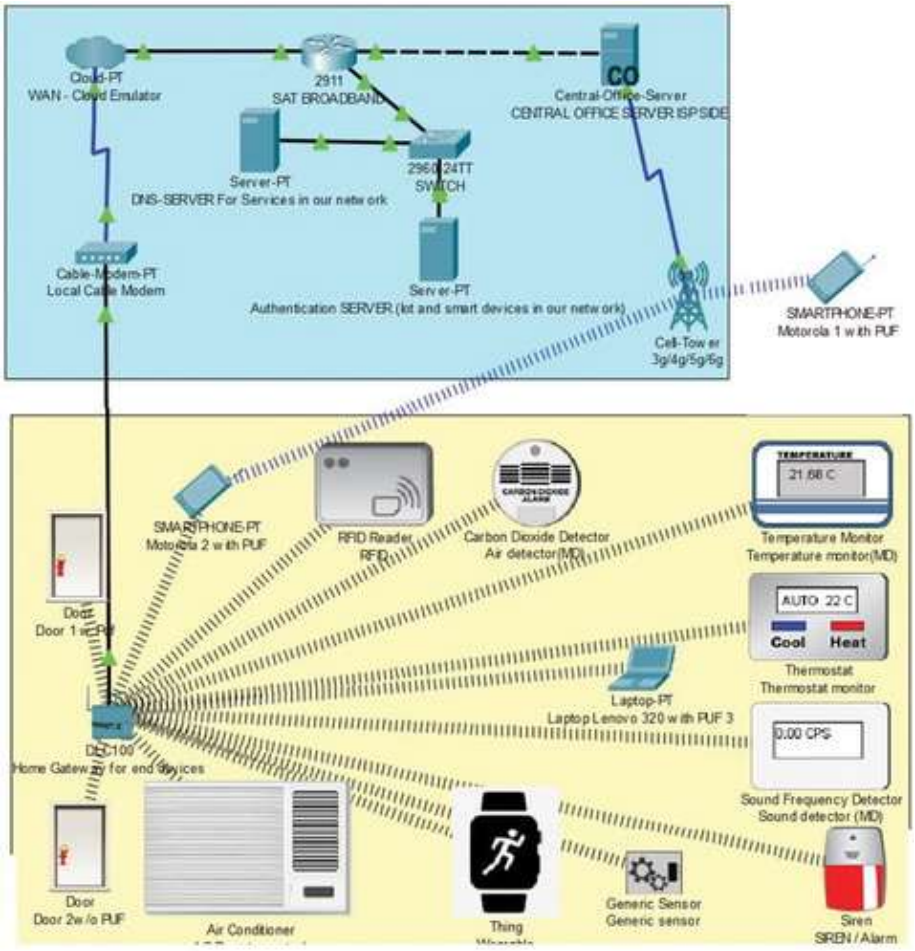

Рисунок 3.6 – Детальна змодельована топологія над системою трасування пакетів Cisco

На рисунку 3.6 показано всі пристрої IoMT, розташовані в інфраструктурі. Топологія створюється шляхом налаштування супутникового широкосмугового маршрутизатора (SAT), який діє як опорна точка для автентифікації пристроїв, які намагаються підключитися в архітектурі хмари. Додано хмарний емулятор WAN (Wide Area Network) для підключення кінцевих пристроїв до служб, які контролюються з далекого імітованого пристрою в мережі. Домашній шлюз DLC100 додано в топологію для з'єднання кінцевих пристроїв з провайдером через кабельний модем-CT, який служить кабельним модемом для перенаправлення трафіку вперед і назад. Елементи вуличної мережі можна побачити у вигляді вежі стільникового зв'язку, яка служить точкою 3G/4G/5G для підключення смартфонів.

Для представлення процесу автентифікації змоделювали 13 кінцевих пристроїв, які знаходяться в екосистемі електронного здоров'я. Для налаштування кінцевих пристроїв використовували конфігурації DHCP IP. Симуляція спрямована на підключення пристрою IoT, включаючи пристрої IoMT в нашому середовищі, до різних інших кінцевих пристроїв на основі механізму децентралізованого сервера автентифікації.

Таким чином, встановлено топологію, яку можна використовувати для безпечного підключення пристроїв по дискретному каналу, такому як супутниковий широкосмуговий канал. З цією метою створено наші DNS-сервери та сервер автентифікації IoT на супутниковому широкосмуговому каналі, який може дискретно служити каналом автентифікації.

Для цього прикладу створено сервер автентифікації IoMT на основі 10.0.0.253. Саме тут кожен пристрій у нашій інфраструктурі електронного здоров'я пройде автентифікацію на основі його облікових даних та пов'язаного підпису PUF.

Створено обліковий запис адміністратора для реєстрації та віддаленого керування пристроями. Для пристрою Motorola 1 з PUF-адресою IPv4, його DNS-сервер (10.0.0.254) і шлюз за замовчуванням для пакетної передачі налаштовані та представлені на рис.3.6.

Аналогічно, для інших кінцевих пристроїв у екосистемі, таких як SmartPhone-PT Motorola 2 з PUF, ноутбук-PT Lenovo 320 з PUF, пристрій IoT DOOR з PUF, носний пристрій, сирена, вимірювач температури (термометр) та моніторинг звуку, зчитувач RFID і детектор якості повітря, використовували подібні конфігурації для генерації IP. Станом цих пристроїв можна керувати дистанційно за допомогою інших кінцевих пристроїв, таких як SmartPhone-PT Motorola 2 з PUF, Laptop-PT Lenovo 320 з PUF, SmartPhone-PT Motorola 1 з PUF.

На рисунку 3.7 зображено підключення до віддаленого сервера автентифікації за IP-адресою 10.0.0.253, де розміщено сервер реєстрації для наших пристроїв Інтернету речей в інфраструктурі електронного здоров'я. Це

добре видно, оскільки всі інші кінцеві пристрої підключені в одну мережу. Таким чином, створено структуру, яку можна використовувати для безпечного підключення пристроїв через дискретний супутниковий широкосмуговий канал

Для автентифікації в середовищі, змодельованому IoMT, у нас є подія «IoT TCP», відфільтрована зі списку змодельованих подій у нашій представленій структурі. Зафіксували цю подію під час моделювання протягом 0,5 секунди і представили приклад для обробки часу автентифікації на рисунку 3.7 і рисунку 3.8.

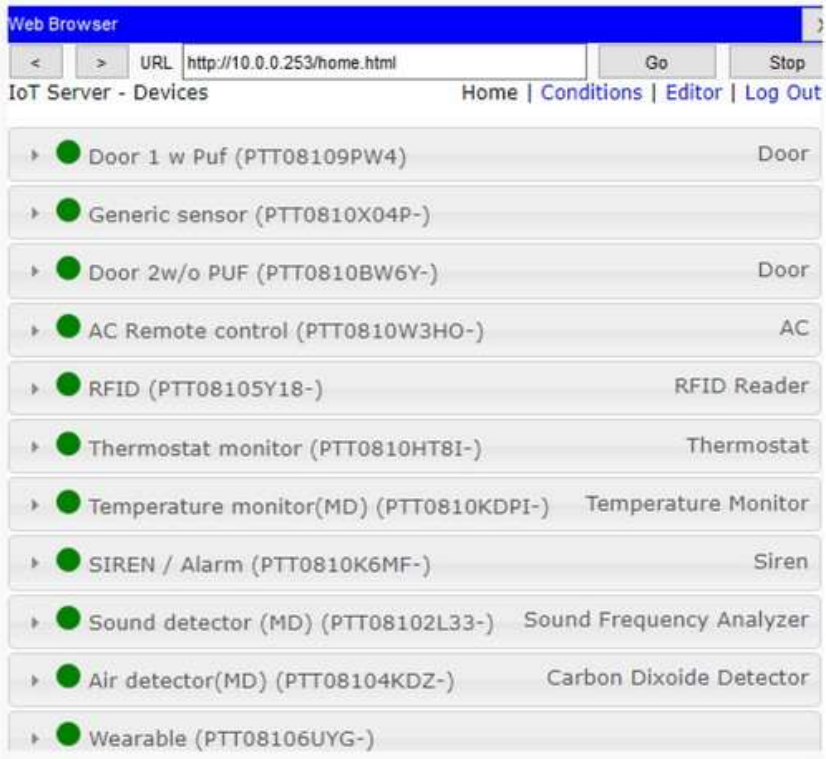

Рисунок 3.7 – Автентифікація віддаленого сервера

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.242	Home Gateway for end devices	Temperature monitor	IoT TCP
	0.242	Home Gateway for end devices	RFID	IoT TCP
	0.242	Home Gateway for end devices	AC	IoT TCP
	0.242	Home Gateway for end devices	CO2 detector	IoT TCP
	0.242	Home Gateway for end devices	Sound Detector	IoT TCP
	0.242	Home Gateway for end devices	Wearable	IoT TCP
	0.242	Home Gateway for end devices	Sensor	IoT TCP
	0.242	SWITCH	Authentication SERVER (Iot a...	IoT TCP
	0.256	--	Authentication SERVER (Iot a...	TCP
	0.257	Authentication SERVER (Iot a...	SWITCH	TCP
	0.258	SWITCH	SAT BROADBAND	TCP

Рисунок 3.8 – Час завершення автентифікації

На рис. 3.7, знаходимо ініціацію процесу автентифікації на 0,236-й секунді для події «IoT TCP», а на рис. 3.8 знаходимо той самий запит для пристрою «термометр», який обслуговується на 0,242-й секунді.

Термометр був зафіксований на панелі моделювання, спочатку запитуючи сервер на 0,236 секунди та на 0,242, і запит було виконано. Час, зафіксований для цієї події, становить близько 0,006 секунди для всіх інших розглянутих пристроїв в інфраструктурі електронного здоров’я.

3.3 Висновки до третього розділу

У третьому розділі розглянуто та досліджено інформаційну технологію PUF для різних аспектів IoMT, таких як безпека, конфіденційність, діагностика та лікування.

Представлено протокол автентифікації пристроїв на основі PUF, здатний автентифікувати пристрої, не вимагаючи високої обчислювальної потужності від кінцевих пристроїв. Цей протокол може використовуватися незалежно від протоколу зв'язку між кінцевим пристроєм і сервером. Ніяка інформація про кінцевий пристрій безпосередньо не зберігається на сервері, що додає додатковий рівень безпеки для навколишнього середовища.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Юридична відповідальність медичних працівників за порушення законодавства про охорону праці

Право на здоров'я в нашій країні отримує кожен громадянин. Відповідальність за це беруть на себе суспільство та держава, та несуть її перед теперішніми і майбутніми поколіннями за рівень здоров'я і збереження генофонду народу України, збереження пріоритету охорони здоров'я в державі, покращення умов праці, освіти, побуту і відпочинку, вирішення екологічних проблем, покращення охорони здоров'я та впровадження здорового способу життя.

Відповідальність за вчинення правопорушення є дійсно першочерговим питанням, що розглядаються теорією права. З точки зору того, що юридична відповідальність – це застосування заходів державного примусу до особи, яка вчинила правопорушення, слід зазначити, що такий підхід застосовується і до громадської охорони здоров'я [1].

Велика кількість медичних працівників, а також і керівників медичних установ мають поверхневе уявлення про юридичну відповідальність, встановлену чинним законодавством за правопорушення в галузі охорони здоров'я. У той же час знання підстав, видів і наслідків юридичної відповідальності, з одного боку, дисциплінує медичних працівників, а з іншого – знижує ймовірність необґрунтованого судового переслідування.

Враховуючи збільшення кількості судових позовів, поданих громадянами з приводу неналежного надання медичної допомоги, проблемам юридичної відповідальності лікарів за професійні правопорушення необхідно приділяти набагато більше уваги [1].

Правові, організаційні, економічні та соціальні засади охорони здоров'я в Україні визначають Основи законодавства України про охорону здоров'я (далі – Основи). [2]

Таким чином, відповідно до статті 80 Основ, особи, винні в порушенні закону Про охорону здоров'я, підлягають цивільній, адміністративній або кримінальній відповідальності відповідно до Закону.

Однак слід зазначити, що відповідно до частини третьої статті 34 Основ лікар не несе відповідальності за здоров'я пацієнта у разі відмови останнього від медичних призначень або порушення встановленого пацієнтом режиму.

Кримінальна відповідальність є найсуворішим типом юридичної відповідальності медичних працівників за правопорушення, вчинені ними в ході своєї професійної діяльності.

Згідно з частиною першою статті 2 Кримінального кодексу України (далі – Кримінальний кодекс) [54], підставою кримінальної відповідальності є вчинення особою суспільно небезпечного діяння, яке становить злочин, передбачений цим Кодексом.

Медичні працівники несуть відповідальність за вчинення злочинів на загальних підставах, крім того, в Кримінальному кодексі передбачено ряд складів злочинів, що мають відношення до професійної діяльності лікарів.

Злочини, вчинені медичними працівниками у зв'язку з їх професійною діяльністю, можна розділити на наступні:

- злочини проти життя і здоров'я людини (пацієнта);
- злочини проти прав особистості (пацієнта);
- злочини у сфері економічної діяльності в медичній практиці;
- злочини у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів;
- інші злочини, вчинені медичними працівниками у зв'язку з їх професійною діяльністю.

Переважна більшість «медичних» злочинів зосереджена в розділі II Кримінального кодексу «Злочини проти життя і здоров’я особи». До них відносяться, зокрема:

- неналежне виконання професійних обов'язків, що спричинило зараження людини вірусом імунодефіциту людини або іншим невиліковним інфекційним захворюванням (стаття 131 Кримінального кодексу);
- розголошення інформації про медичне обстеження з метою виявлення зараження вірусом імунодефіциту людини або іншим невиліковним інфекційним захворюванням (стаття 132 Кримінального кодексу);
- незаконний аборт (стаття 134 Кримінального кодексу) – якщо медичний працівник не має спеціальної медичної освіти;
- незаконна медична діяльність (стаття 138 Кримінального кодексу) – медична діяльність без спеціального дозволу, здійснювана особою, яка не має належної медичної освіти;
- ненадання медичної допомоги пацієнту медичним працівником (стаття 139 Кримінального кодексу);
- неналежне виконання професійних обов'язків медичним або фармацевтичним працівником (стаття 140 Кримінального кодексу);
- порушення прав пацієнта (стаття 141 Кримінального кодексу);
- незаконне проведення експериментів на людях (стаття 142 Кримінального кодексу);
- порушення встановленого законом порядку трансплантації органів або тканин людини (стаття 143 Кримінального кодексу);
- примусове донорство (стаття 144 Кримінального кодексу);
- незаконне розголошення лікарської таємниці (стаття 145 Кримінального кодексу) [54].

Слід зазначити, що випадки судового переслідування медичних працівників, а тим більше засудження їх в Україні відносно нечасті. Однак керівники охорони здоров'я повинні бути інформовані про те, які дії або бездіяльності підпадають під заборону кримінального законодавства і яку поведінку підлеглих слід використовувати для їх запобігання.

Адміністративна відповідальність – вид юридичної відповідальності, що виникає за правопорушення, передбачені Кодексом України Про адміністративні правопорушення (далі – КпАП) [55].

Таким чином, відповідно до статті 9 Кодексу про адміністративні правопорушення, адміністративне правопорушення (проступок) – це незаконна, винна (умисна або необережна) дія або бездіяльність, яка посягає на громадський порядок, власність, права і свободи громадян, встановлений порядок управління і за яке законом передбачена адміністративна відповідальність.

Адміністративна відповідальність за правопорушення, передбачені цим Кодексом, настає, якщо ці порушення за своїм характером не тягнуть кримінальної відповідальності відповідно до Закону.

Адміністративні правопорушення в галузі охорони здоров'я включають, зокрема:

- порушення санітарно-гігієнічних і санітарно-протиепідемічних правил і норм (стаття 42 КпАП);
- незаконне виробництво, придбання, зберігання, перевезення, пересилання наркотичних засобів або психотропних речовин без мети збуту в невеликих кількостях (стаття 44 КпАП);
- порушення встановленого порядку прийому, обробки, зберігання, реалізації та використання донорської крові і (або) її компонентів і лікарських засобів (стаття 451 КпАП) [55].

Особи, які вчинили адміністративні правопорушення, підлягають адміністративному покаранню, передбаченому санкціями статей, що встановлюють відповідальність за такі правопорушення. Слід зазначити, що в основному це штрафи в розмірі, що визначається неоподатковуваним мінімумом доходів громадян.

На сучасному етапі розвитку українського суспільства та медико-правової науки цивільно-правова відповідальність виходить на перший план щодо відповідальності медичних працівників за професійні правопорушення.

Відповідно до частини першої статті 1 Цивільного кодексу України (далі – ЦКУ) [56] цивільне право регулює особисті немайнові та майнові відносини (цивільні відносини), засновані на правовій рівності, свободі волі, майновій незалежності їх учасників.

Цивільно-правова відповідальність у сфері медичної діяльності – це вид юридичної відповідальності, що виникає в результаті порушення майнових або особистих нематеріальних активів громадян у сфері охорони здоров'я і полягає в основному в необхідності відшкодування шкоди. До особистих нематеріальних благ громадян, які безпосередньо пов'язані з медичною діяльністю, відносяться, перш за все, життя і здоров'я. З цієї причини можна стверджувати, що цивільно-правова відповідальність є своєрідним засобом захисту особистих немайнових прав (життя і здоров'я) пацієнтів при наданні медичної допомоги.

Варто зазначити, що більшість медичних працівників здійснюють свою професійну діяльність у трудових відносинах з медичними установами. Згідно з частиною першою статті 1172 ЦКУ, юридична або фізична особа відшкодовує шкоду, заподіяну їх працівником при виконанні ним трудових (службових) обов'язків.

Переважна більшість позовів, поданих пацієнтами проти медичних установ (у тому числі фізичних осіб-господарюючих суб'єктів, що займаються медичною практикою), є позовами про відшкодування матеріальної та моральної шкоди, заподіяної здоров'ю, спричиненої неякісною медичною допомогою. Компенсація за такий збиток проводиться відповідно до положень глави 82 ЦКУ [56].

Однак слід зазначити, що передумовою для відповідальності за шкоду є причинно-наслідковий зв'язок між протиправною поведінкою і заподіяною шкодою. Наприклад, якщо шкода не є результатом протиправної поведінки винного, а сталася з інших причин (через недотримання пацієнтом медичних рекомендацій або через індивідуальні особливості пацієнта), винний не несе відповідальності за шкоду.

Для того щоб понести цивільну відповідальність за заподіяння шкоди здоров'ю, необхідно, щоб такий збиток був заподіяний з вини особи, яка заподіяла шкоду. Вина медичних працівників зазвичай проявляється у формі недбалості. Щоб бути звільненим від обов'язку відшкодувати шкоду здоров'ю, особа, яка заподіяла шкоду, повинна довести, що це було не з його вини.

4.2 Підвищення стійкості роботи об’єктів медичної галузі в воєнний час

Переведення медичної служби на воєнний стан - один з найвідповідальніших і складних періодів її діяльності. При цьому порядок і послідовність виконання всіх медичних заходів здійснюються відповідно до встановленого ступеня готовності ЦО, які заздалегідь визначаються в мирний час. В Україні встановлено такі ступені готовності ЦО:

- «Повсякденний»;
- «Пріоритетні заходи Центрального комітету першої групи»;
- «Пріоритетні заходи Центрального комітету другої групи»;
- «Загальна готовність цивільної оборони».

Приведення Медичної служби цивільної оборони (далі МСЦО) в готовність і переведення її з мирного часу на воєнний стан забезпечує стійке управління медичними силами у воєнний час, скорочення втрат населення і персоналу служби за рахунок вжиття заходів з медичного захисту, підвищення стійкості медичних установ у воєнний час і підготовку медичних сил і обладнання для медичної підтримки нападу противника [57].

Приведення ЦО в деяку ступінь готовності може здійснюватися або послідовно, або, в залежності від ситуації, відразу в найвищому ступені готовності, з обов'язковим виконанням заходів, передбачених на попередніх етапах готовності. Для своєчасного збільшення сил ЦО і підготовки їх до виконання завдань в особливих випадках рішенням президента України

частина органу управління ЦО може бути заздалегідь приведена у вищий ступінь готовності.

Для скорочення часу переведення МСЦО на воєнний стан, ще до введення планів цивільної оборони, передбачається реалізація першочергових заходів Центрального комітету першої та другої груп, підвищення готовності медичної служби Цивільної оборони. Ці заходи повинні проводитися приховано, під виглядом навчань, тренувань і ремонтних робіт.

При систематичному переведенні системи цивільної оборони з мирного стану на воєнний, з наказом про проведення регулярних заходів першої групи, керівник МСЦО повідомляє і збирає керівництво МСЦО, розподіляє керівний склад служби відповідно до штатного розпису і заходів. Безпосередньо в пункті постійної дислокації органу управління охороною здоров'я організовується цілодобова зміна керівного складу МСЦО, члени якого приступають до виконання своїх обов'язків відповідно до штатного розпису. Головними фахівцями органу управління охороною здоров'я та співробітниками МСЦО відповідно до їх функціональних обов'язків є зазначені розділи плану медичної допомоги у воєнний час [58].

В ході заходів «Загальної готовності ЦО» здійснюється підготовка ЛПЗ категоризованих міст до евакуації в приміську зону, що вимагає великої уваги з боку МСЦО:

- необхідно підготуватися до виписки деяких пацієнтів на амбулаторне лікування;
- визначити групи нетранспортабельних пацієнтів та пацієнтів, які підлягають евакуації;
- визначити порядок вилучення майна з урахуванням його потреби в медичній допомозі;
- направити оперативні групи до місця дислокації ЛПЗ МСЦО в приміській зоні з метою отримання виділених приміщень і організації адаптивної роботи;

● вказати кількість транспортних засобів, необхідних для евакуації в лікарню.

Враховуючи можливість раптового нападу противника, важливим заходом в цей період є розгортання в приміській зоні додаткових лікарняних ліжок МСЦО силами закладів охорони здоров'я сільської місцевості і некатегоризованих міст.

Проведення комплексу санітарно-протиепідемічних заходів при ступені готовності «Загальна готовність ЦО» спрямоване на збереження здоров'я населення і персоналу формувань і установ ЦО, а також на запобігання виникненню і поширенню масових інфекційних захворювань. Ці заходи здійснюються Центрами державного санітарно-епідеміологічного нагляду і створеними на їх базі санітарно-протиепідемічними формуваннями по всій області, включаючи райони, призначені для розселення робітників, службовців і евакуйованого населення. в місцях дислокації евакуаційних органів [59].

Після отримання відповідних інструкцій МСЦО організовує медичне забезпечення для часткової евакуації населення і виведення медичних підрозділів підвищеної готовності в приміську зону.

В умовах неповного забезпечення захисними спорудами та медичними засобами індивідуального захисту робітників, службовців і населення категоріальних міст евакуація населення цих міст в передмістя є основним способом захисту його від сучасних засобів ураження.

Безпосередня підготовка та здійснення заходів з організації, підготовки та проведення евакуаційних заходів покладена на органи з евакуації, які працюють у співпраці з відповідними органами та службами ЦО. До складу евакуаційних і приймальних комісій з евакуації повинен входити представник МСЦО, який повинен взаємодіяти з іншими службами ЦО з питань евакуації медичних установ, а також надання медичної допомоги евакуйованому населенню. Евакуація населення супроводжується його масовим переселенням з категоріальних міст в приміські райони, що може привести до травм і загострення хронічних захворювань серед населення, погіршення

санітарно-епідеміологічної обстановки в регіоні, спалахів інфекційних захворювань. Тому в цей період на МСЦО покладено дуже важливі завдання щодо всебічного медичного забезпечення евакуаційних заходів [59].

Медичне забезпечення евакуації населення з категоріальних міст організовується на територіальній і виробничій основі і здійснюється відповідними керівниками органів охорони здоров'я адміністративно-територіальних утворень.

Медичне забезпечення евакуації населення включає проведення органами охорони здоров'я організаційних, медико-санітарних та протиепідемічних заходів, спрямованих на охорону здоров'я евакуйованого населення, своєчасне надання медичної допомоги пацієнтам та особам, які отримали травми під час евакуації, та запобігання поширенню та розповсюдженню.

При проведенні евакуаційних заходів перед МСЦО постають наступні завдання:

- Організація медичної допомоги населенню на всіх етапах евакуації та переселення.
- Евакуація медичних установ з міст в приміську зону.
- Виведення медичних формувань Центрального управління в приміську зону.
- Організація притулку та лікування нетранспортабельних пацієнтів.
- Розгортання ліжкової мережі в приміській зоні за рахунок евакуйованих лікарень.
- Організація медичної допомоги робітникам і службовцям установ, які продовжують працювати у воєнний час.
- Захист медичного персоналу та пацієнтів від вражаючих факторів зброї масового знищення та звичайних засобів ведення війни [59].

Успішне виконання завдань, пов'язаних з медичною евакуацією населення, досягається за рахунок чіткого планування заздалегідь. Для планування медичної підтримки евакуаційних заходів штаб-квартира МСЦО

повинна мати у своєму розпорядженні певними вихідними даними, які вони отримують від відповідного керівного органу центру. Вихідні дані повинні містити наступну інформацію:

- кількість евакуйованого населення (включаючи дитячі установи та дітей) в місті в цілому і окремо в його районах;
- розташування, кількість і добова пропускна здатність збірних пунктів евакуації (ЗЕП);
- маршрути і методи оцінки чисельності населення;
- розташування пунктів посадки (ПП) і кількість евакуйованого населення в кожній колоні або залізничному поїзді (судні);
- розміщення проміжних пунктів евакуації (ППЕ) і пунктів висадки, районів розселення і населення, що підлягає евакуації.

4.3 Висновки до четвертого розділу

У розділі розглянуто питання юридичної відповідальності медичних працівників за порушення законодавства про охорону праці. Можна зробити висновок, що знання керівниками закладів охорони здоров'я та їх співробітниками чинного законодавства про відповідальність медичних працівників та вжиття заходів щодо забезпечення його дотримання є ключем до належного функціонування закладів охорони здоров'я.

Також розглянуто питання підвищення стійкості роботи об’єктів медичної галузі в воєнний час. Ґрунтуючись на отриманих вихідних даних, відповідний штаб МСЦО визначає потребу в різних категоріях медичного персоналу, медичних установах і машинах швидкої допомоги для обслуговування населення поетапно і за маршрутами евакуації.

ВИСНОВКИ

1. У кваліфікаційній роботі детально описаний Інтернет медичних речей (IoMT) та представлено архітектуру для IoMT.

2. Розглянуто та досліджено нові інформаційні технології – PUF, штучний інтелект та інші для різних аспектів IoMT, таких як безпека, конфіденційність, діагностика та лікування.

3. Результати досліджень показують застосовність цих технологій в системі електронного здоров'я для автентифікації, безпеки, продуктивності або часу збору даних.

4. Системи охорони здоров'я наразі стикаються з проблемами, пов'язаними з критичною нестачею медичних працівників, тривалим часом очікування, зростанням попиту на послуги та фінансовими обмеженнями. IoMT може допомогти пом'якшити деякі обмеження, скоротивши час, який експерти з охорони здоров'я витрачають на повторювані дії, дозволяючи їм зосередитися на інших видах діяльності, наприклад, на прийомі більшої кількості пацієнтів.

5. Запропоновано розділити процес автентифікації на три етапи:

- на першому етапі визначено процес аутентифікації на основі підпису PUF на основі облікових даних, а потім продовжено аутентифікацію.
- на другому етапі все зроблено на фактичній точці повороту в структурі та використано топологію розподіленої мережі.
- на третьому етапі порівняно фактичні обчислювальні витрати процесу автентифікації та розгорнуто такий механізм всюди, де це можливо в IoMT.

6. Як результат, таке впровадження покращує захист інформації та зменшує ризик випадкового або навмисного втручання, а також запобігає створенню помилок або нещасних випадків під час передачі даних кінцевими девайсами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цифровизация медицины: быстрее, чем ожидалось https://www.iksmedia.ru/articles/5852600-Czifrovizaciya-mediciny-bystree-che.html

2. Цифровізація медичних послуг під час пандемії може врятувати життя https://blog.liga.net/user/yunazarov/article/39636

3. Songur, H., Saygın, T., Şifahaneden Hastaneye: Sağlık Kuruluşlarının Değişimine Genel Bir Bakış, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 19, (2014), 1

4. Mercy Virtual Care Center, www.mercyvirtual.net, 2016

5. Bilişim Zirvesi, Akıllı Hastane, http://saglikbilisimzirvesi.org/dijitalhastane, 2016

6. Wei-dong, W.A.N.G., The digital hospital in future: understanding and management of our future hospital, Information of Medical Equipment, 7 (2004)

7. Della Mea V., What is e-Health (2): The death of telemedicine?, Journal of Medical Internet Research, 3 (2001), 2, e22. doi:10.2196/jmir.3.2.e22.

8. Allen A., Morphing Telemedicine - Telecare - Telehealth - eHealth. Telemed Today, Special issue: 2000 Buyer's Guide and Directory, 1 (2000), 43.

9. Holland,M., The Digital Hospital of Tomorrow: The Time Has Come Today, https://h41368.www4.hp.com/h41111/rfg_formprocessor/digital_hospital/uk/en/pdf/DH-IDC-PAPER-HI216948.pdf , 2009

10. Global strategy on digital health 2020-2025 https://apps.who.int/iris/bitstream/handle/10665/344249/9789240020924-eng.pdf

11. Завдяки цифровізації система охорони здоров’я України змогла швидше реагувати на виклики, пов’язані з COVID-19 – Юлія Соколовська https://www.president.gov.ua/news/zavdyaki-cifrovizaciyi-sistema-ohoroni-zdorovya-ukrayini-zmo-68521

12. Електронна система охорони здоров'я в Україні

https://ehealth.gov.ua/

13. Україна повністю перейшла на електронний лікарняний з 1 жовтня: як це працює https://moz.gov.ua/article/news/ukraina-povnistju-perejshla-na-elektronnij-likarnjanij-z-1-zhovtnja-jak-ce-pracjue

14. У лікарні швидкої допомоги встановили найсучаснішу систему моніторингу https://zaxid.net/u_likarni_shvidkoyi_dopomogi_vstanovili_naysuchasnishu_sistemu_monitoringu_n1527787

15. Chang, Zhanjun, et al. , Realization of integration and working procedure on digital hospital information system, Computer Standards & Interfaces 25 (2003), 5, pp. 529-537.

16. T.C. Sağlık Bakanlığı, Dijital hastane, http://saglik.gov.tr/DH/belge/1-34974/dijital-kagitsiz-hastane-nedir.html, 2016

17. Li, Jin-Song, and Xiao-Guang Zhang., Construction Goals and Development Trend of Digital Hospital, Yiliao Weisheng Zhuangbei 31 (2010), 2, pp.5-7.

18. European Comission, eHealth, http://ec.europa.eu/health/ehealth/policy/index_en.htm Sağlık, 2016

19. Koonin L. M. et al., Trends in the use of telehealth during the emergence of the covid-19 pandemic – united states, January-March 2020, Morb. Mortal. Wkly. Rep., Vol. 69, pp.1595–1599, 2020.

20. Wu J., Guo S., Huang H., Liu W. and Xiang Y. Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives. IEEE Commun. Surv. Tutor., Vol. 20, no. 3, pp.2389–2406, 2018.

21. Naresh V. S., Pericherla S. S., Rama Murty P. S. and Reddi S. Internet of things in healthcare: Architecture, applications, challenges, and solutions. Comput. Syst. Sci. Eng., Vol. 35, no. 6, pp.411–421,2020.

22. Singh A., Parizi R. M., Zhang Q., Choo K.-K. R. and Dehghantanha A. Blockchain smart contracts formalization: Approaches and challenges to address

vulnerabilities. Comput. Security, Vol. 88, p.101, 2020.

23. Wang Q., Zhu X., Ni Y., Gu L. and Zhu H. Blockchain for the IoT and industrial IoT: A review. Internet Things, Vol. 10, pp.100,2020.

24. Dilawar N., Rizwan M., Ahmad F. And Akram S. Blockchain: Securing internet of medical things (IoMT). Int. J. Adv. Comput. Sci. Appl., Vol. 10, p.1, 2019.

25. Shamsoshoara A., Korenda A., Afghah F. And Zeadally S. A survey on physical unclonable function (PUF)-based security solutions for internet of things. 183, p.759, 2020.

26. Ahmed Z., Mohamed K., Zeeshan S. And Dong X. Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. *Database*, Vol. 2020, p.345, 2020.

27. S. Sharma. Towards high quality and flexible future internet architectures. Ghent: Ghent University, Faculty of Engineering and Architecture, 2016.

28. Sharma S. Towards artificial intelligence assisted software defined networking for internet of vehicles. in Intelligent Technologies for Internet of Vehicles, Internet of Things, N. Magaia et al., Eds. Springer Nature Switzerland AG, 2021.

29. Lalmuanawma S., Hussain J. And Chhakchhuak L. Applications of machine learning and artificial intelligence for Covid-19 (SARS-CoV-2) pandemic: A review, Chaos Solitons Fractals, Vol. 139, p.159,2020.

30. Huang, X. Intelligent remote monitoring and manufacturing system of production line based on industrial Internet of Things. Comput. Commun. 2020, 150, 421–428.

31. Xiao, Y.; Zhang, H.; Yuan, C.; Gao, N.; Meng, Z.; Peng, K. The Design of an Intelligent High-Speed Loom Industry Interconnection Remote Monitoring System. Wirel. Pers. Commun. 2020, 113, 2167–2187.

32. Atamuradov, V.; Medjaher, K.; Camci, F.; Zerhouni, N.; Dersin, P.; Lamoureux, B. Machine Health Indicator Construction Framework for Failure Diagnostics and Prognostics. J. Signal Process. Syst. 2020, 92, 591–609.

33. Umair, K.; Guanghua, X.; Liu, F.; Chen, L.; Liang, R.; Ben, N.; Waqas, B.A. Machine Health Monitoring Using Artificial Intelligence (AI). In Advances in Asset Management and Condition Monitoring; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1359–1374.

34. Bragazzi, N.L. Digital Technologies-Enabled Smart Manufacturing and Industry 4.0 in the Post-COVID-19 Era: Lessons Learnt from a Pandemic. 2020. Int. J. Environ. Res. Public Health, 2020 17, 4785.

35. Fu Zheng, Liang MingHuI, Conspectus of digital medicine [M]. Beijing; People's Medical Publishing House, 2009.

36. Michael M, Darianian M. Architectural solutions for mobile RFID services for the internet of things [D].Helsink i, Finland; University of Helsinki, 2007.

37. Nasir Abbas, Yan Zhang, Amir Taherkordi and Tor Skeie, "Mobile Edge Computing: A Survey", IEEE Internet Of Things Journal, Vol. 5, No. 1, February 2018, pp. 450 – 465.

38. M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," IEEE Pervasive Computer, Vol. 8, No. 4, pp. 14–23, Oct./Dec. 2009.

39. Jianli Pan, Lin Ma, Ravishankar Ravindran and Peyman TalebiFard, "HomeCloud: An Edge Cloud Framework and Testbed for New Application Delivery", 2016 23rd International Conference on Telecommunications (ICT), 978-1-5090-1990-8/16, 2016 IEEE.

40. Durga Amarnath M. Budida and Dr. Ram S. Mangrulkar, "Design and Implementation of Smart HealthCare System Using IoT", 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 978-1-5090-3294-5/17 IEEE 2017.

41. Alexandru Archip, Nicolae Botezatu, Elena Serban, Paul Corneliu Herghelegiu and Andrei Zal, "An IoT Based System for Remote Patient Monitoring", 17th International Carpathian Control Conference, June 2016, pp.1-6

42. Dejana Ugrenovic, Gordana Gardasevic, "CoAP protocol for Web –

based monitoring in IoT healthcare applications", 23rd Telecommunications forum TELFOR 2015, Serbia, Belgrade, November 24 – 26, 2015, 978-1-5090-0055-5/15, IEEE 2015, pp.79 – 82.

43. F. Schwiegelshohn, M. Hubner, P. Wehner, and D. Gohringer,"Tackling the new health-care paradigm through service robotics: Unobtrusive, efficient, reliable and modular solutions for assisted-living environments", IEEE Consum. Electron. Mag., vol. 6, no. 3, pp. 34–41, Jul. 2017.

44. C. Dobbins, R. Rawassizadeh, and E. Momeni, "Detecting physical activity within lifelogs towards preventing obesity and aiding ambient assisted living," Neurocomputing, vol. 230, pp. 110–132, Mar. 2017.

45. M. W. Raad, T. Sheltami, and E. Shakshuki, "Ubiquitous tele-health system for elderly patients with Alzheimer's," Procedia Computer Science, vol. 52, pp. 685–689, Jun. 2015.

46. H. Thapliyal, V. Khalus, and C. Labrado, "Stress detection and management: A survey of wearable smart health devices," IEEE Consum. Electron. Mag., vol. 6, no. 4, pp. 64–69, Oct. 2017.

47. Alhazmi O (2018) A survivable internet of things scheme. J Adv Res Comput Appl 13(1):19–26

48. Zyrianoff I, Heideker A, Silva D, Kleinschmidt J, Soininen J-P, Salmon Cinotti T, Kamienski C (2020) Architecting and deploying IoT smart applications: A performance–oriented approach. Sensors 20(1):84

49. Khowaja SA, Setiawan F, Prabono AG, Yahya BN, Lee S-L (2016) An effective threshold based measurement technique for fall detection using smart devices. Int J Ind Eng Comput 23(5):332–348

50. Islam M, Usman M, Mahmood A, Abbasi AA, Song O-Y (2020) Predictive analytics framework for accurate estimation of child mortality rates for Internet of Things enabled smart healthcare systems. Int J Distributed Sens Netw 16(5):1550147720928897

51. Zhou X, Liang W, Kevin I, Wang K, Wang H, Yang LT, Jin Q (2020) Deep learning enhanced human activity recognition for internet of healthcare things.

IEEE Int Things J 7:6429–6438

52. ВІДПОВІДАЛЬНІСТЬ МЕДИЧНИХ ПРАЦІВНИКІВ [Електронний ресурс] – Режим доступу до ресурсу: https://minjust.gov.ua/m/str_35697

53. Основи законодавства України про охорону здоров'я [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2801-12#Text

54. КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2341-14#Text

55. Кодекс України про адміністративні правопорушення [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80731-10#Text

56. ЦИВІЛЬНИЙ КОДЕКС УКРАЇНИ [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/435-15#Text

57. Ступеня готовності цивільної оборони та їх коротка характеристика [Електронний ресурс] – Режим доступу до ресурсу: http://ni.biz.ua/12/12_14/12_144534_stepeni-gotovnosti-grazhdanskoy-oboroni-i-ih-kratkaya-harakteristika.html.

58. Медична служба цивільної оборони [Електронний ресурс] – Режим доступу до ресурсу: http://medical-enc.com.ua/msgo.htm.

59. МЕДИЧНИЙ ЗАХИСТ НАСЕЛЕННЯ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ В ЄДИНІЙ ДЕРЖАВНІЙ СИСТЕМІ ЦИВІЛЬНОГО ЗАХИСТУ / [В. П. Печиборщ, П. Б. Волянський, В. М. Якимець та ін.]. – Київ, 2019.

60. IX науково-технічна конференція «Інформаційні моделі, системи та технології – Тернопіль, 2021.

61. XIX міжнародна науково-практична конференція «Математичне та програмне забезпечення інтелектуальних систем (МПЗІС) – Дніпро, 2021.

ДОДАТКИ

Додаток А

Дніпровський національний університет імені Олеся Гончара

Інститут кібернетики ім. В.М. Глушкова НАН України

ННК «Інститут прикладного системного аналізу»
НТУУ «КПІ ім. І. Сікорського»

Київський національний університет ім. Т. Шевченка

IT Dnipro Community

XIX міжнародна науково-практична конференція

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ (МПЗІС-2021)

ТЕЗИ ДОПОВІДЕЙ

MATHEMATICAL SUPPORT AND SOFTWARE FOR INTELLIGENT SYSTEMS (MSSIS-2021)

ABSTRACTS

17-19 листопада 2021 року

Дніпро, Україна

ЦИФРОВА ЛІКАРНЯ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ

Дзюба Д.Ю., Дмитроца Л.П.

Тернопільський національний технічний університет імені Івана Пулюя

У процесі інформатизації, популярність і часткове використання лікарняної інформаційної системи дозволило лікарні досягти певного ступеня інформатизації. Тим не менш, він також має деякі недоліки, такі як ручне введення медичної інформації, фіксована інформаційна точка, фіксований мережевий режим, [1] тощо, що серйозно обмежує побудову інформатизації лікарні. Швидкий розвиток Інтернету речей дав нову ідею для вирішення згаданих вище проблем. IoT представляє собою мережу, що з'єднує будь-які предмети з Інтернетом для здійснення обміну інформацією та зв'язку, а також для реалізації інтелектуального розпізнавання, позиціонування, стеження, моніторингу та управління, за допомогою радіочастотної ідентифікації (RFID), інфрачервоних сенсорів вимірювання, GPS, лазерних сканерів та іншої інформаційно-чутливого обладнання, у відповідності зі звичайним протоколом [2]. Цифрова лікарня на основі Інтернет речей, заснована на технології IoT і побудована з вектором різних прикладних сервісних систем, являє собою новий вид лікарні, що інтегрує функції діагностики, лікування, управління та прийняття рішень. Функції Інтернету речей, такі як всебічне сприйняття, надійна передача, інтелектуальна обробка тощо, забезпечують технічну підтримку платформи для будівництва та впровадження цифрової лікарня на основі Інтернет речей.

База даних усіх пацієнтів повинна бути досить зручною. Також дані пацієнта повинні бути приватними [3]. Тому пропонується спосіб, коли пацієнт та лікарі можуть спілкуватися через мобільний додаток та веб-додаток. Сенсор вимірювання температури, ЕКГ та серцебиття підключені до плати Arduino. Значення від мікроконтролера передаються веб-серверу за допомогою підключення Wi-Fi (див. рис. 1).

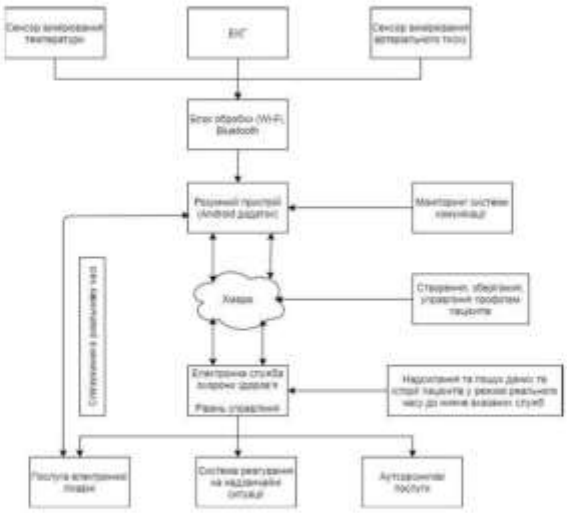

Рис 1. Структурна схема покращеної системи моніторингу

Значення параметрів можна переглянути за допомогою програми, встановленої у лікарів та смартфоні пацієнта.

Література

1. Yu Lei, Lu Yang, Zhu XiaoLing etc., Research advances on the technology of internet of things in medical domain [J], Applications and Research of Computer, 2012, 29 (1) , pp. 1-7

2. Gu JingJing, Chen SongCan, Zhuang YI, Wireless sensor network-based topology structures for the internet of things localization [J], Chinese Journal of Computers, 2010, 33 (9) , pp. 1548-1555

3. Real time wireless health monitoring application using mobile devices, International Journal of Computer Networks &Communications (IJCNC) Vol.7, No.3, May 2015, Amna Abdullah, Asma Ismael, Aisha Rashid, Ali Abou-ElNour, and Mohammed Tarique.

Додаток Б

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

ІХ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.6
Д.Ю. Дзюба, Л.П. Дмитроца, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРИСТРОЇ З ФІЗИЧНОЮ НЕКЛОНОВАНОЮ ФУНКЦІЄЮ (PUF)

UDC 004.6
D. Dziuba, L. Dmytrotsa, Ph.D., Assoc. Prof

DEVICES WITH PHYSICAL NON-CLONED FUNCTION (PUF)

Фізичні неклоновані функції (PUF) доцільно застосувати для генерації криптографічних ключів [1]. PUF використовує виробничі варіації, які вводяться в інтегральну схему (IC) під час її виготовлення. Варіації непередбачувані, неконтрольовані, неминучі і природні [2]. Отже, ключі, які генеруються за допомогою модуля PUF, також повністю випадкові й унікальні для відповідного модуля PUF.

Пристрої PUF генерують унікальний відбиток пальців для вразливих елементів в екосистемі IoMT. Ці унікальні відбитки пальців/підписи виникають внаслідок різниць у виготовленні пристроїв. Відбитки пальців можна використовувати для створення ключів криптографії, що захищають пристрої та їхні дані в екосистемі IoMT, де кінцеві девайси піддаються ризику атак апаратного втручання [3].

На рисунку 1 запропонована концепція безпеки на основі PUF для IoMT.

Рисунок 1. Безпека на основі PUF для IoMT.

Впровадження PUF в IoMT забезпечує захист інформації та охороняє від неконтрольованих дій. Також досліджено, що використання IoMT на основі PUF зменшує ризик випадкового або навмисного втручання і, як результат, запобігає створенню помилок чи нещасних випадків під час передачі даних кінцевими девайсами.

Література.

1. V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things," IEEE

2. V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Novel FinFET based Physical Unclonable Functions for Efficient Security in Internet of Things," in Proc. IEEE Int. Symp. Nanoelect. Inf. Sys. (iNIS), 2016, pp. 172–177
4. Ahmed Z., Mohamed K., Zeeshan S. And Dong X. Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. *Database*, Vol. 2020, p.345, 2020.