НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Радіотехнічний факультет
Кафедра радіоприймання та оброблення сигналів

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ А.В. Мовчанюк
(підпис) (ініціали, прізвище)
“___”_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності апаратура радіозв’язку радіомовлення і телебачення
(код і назва)

на тему: Особливості оброблення даних медичних пристроїв та систем за концепцією Інтернету Речей

Виконав: студент VI курсу, групи РА-51м

Резніченко Антон Володимирович _____
(підпис)

Науковий керівник *к.т.н. доц. Мосійчук В.С.* _ _____
(підпис)

Консультант *з охорони праці к.т.н., доц. Каштанов С.Ф.* _____
(підпис)

Рецензент *д.т.н професор Шарпан О.Б.* _ _____
(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2017 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Інститут (факультет) Радіотехнічний факультет

Кафедра радіоприймання та оброблення сигналів

Рівень вищої освіти – другий (магістерський)

Спеціальність апаратура радіозв'язку радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ А.В. Мовчанюк
(підпис) (ініціали, прізвище)
«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Резніченку Антону Володимировичу

1. Тема дисертації Особливості оброблення даних медичних пристроїв та систем за концепцією Інтернету Речей,

науковий керівник дисертації Мосійчук Віталій Сергійович к.т.н. доцент,

затверджені наказом по університету від «22» березня 2017 р. №1173–с

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження: дані медичних пристроїв та систем

4. Предмет дослідження: телеметричні медичні системи, що працюють за концепцією Інтернету Речей

5. Перелік завдань, які потрібно розробити здійснити огляд сучасних систем біотелеметрії; розробити апаратну та програмну частину пристрою-приставки до вже існуючого біотелеметричного пристрою

6. Орієнтовний перелік ілюстративного матеріалу електронна презентація ____
_____
_____

7. Орієнтовний перелік публікацій не менше 2х публікацій за темою _____ дисертації

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	к.т.н., доцент Каштанов С.Ф.		

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Огляд сучасних біометричних систем	09.02.2017 – 23.02.2017	
2	Реалізація апаратної частини роботи	23.02.2017 – 30.03.2017	
3	Реалізація програмної частини роботи	30.03.2017 – 02.05.2017	
4	Розгляд питань охорони праці	02.05.2017 – 18.05.2017	
5	Оформлення роботи і презентації	18.05.2017 – 20.06.2017	

Студент _____ А.В. Резніченко
(підпис)

Науковий керівник дисертації _____ В.С. Мосійчук
(підпис)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Загальний обсяг магістерської дисертації складає 87 сторінок. Робота містить 15 рисунків, 10 таблиць. Список використаної літератури включає в себе 36 джерел, на які робляться посилання.

В роботі запропоновано реалізацію пристрою-приставки до вже існуючого медичного пристрою – вимірювача біоімпендансу ТОР-М1. Пристрій-приставка реалізований за концепцією Інтернету Речей. Було реалізовано апаратну та програмну частину. Пристрій-приставка має можливість використовувати хмарні сервіси для зберігання та візуалізації медичних даних пацієнтів. Також можливим є подальший аналіз великої кількості біомедичних даних пацієнтів для виявлення трендів та нових взаємодій між біомедичними показниками пацієнтів. Запропонований пристрій-приставка дозволяє значно покращити процес передачі, зберігання та візуалізації біомедичних показників пацієнтів.

Ключові слова: *пристрій-приставка, біотелеметрія, Інтернет Речей, хмарний сервіс, медичні дані.*

РЕФЕРАТ

Общий объем магистерской диссертации составляет 87 страниц. Работа содержит 15 рисунков, 10 таблиц. Список литературы включает в себя 36 источников, на которые делаются ссылки.

В работе предложено реализацию устройства-приставки к уже существующему медицинскому прибору – измерителя биоимпенданса ТОР-М1. Устройство-приставка реализовано по концепции Интернета Вещей. Были реализованы аппаратная и программная части. Устройство-приставка имеет возможность использовать облачные сервисы для хранения и визуализации медицинских данных пациентов. Также возможен дальнейший анализ большого количества биомедицинских данных пациентов для выявления трендов и новых взаимодействий между биомедицинскими показателями пациентов. Предлагаемое устройство-приставка позволяет значительно улучшить процесс передачи, хранения и визуализации биомедицинских показателей пациентов.

Ключевые слова: *устройство-приставка, биотелеметрия, Интернет Вещей, облачный сервис, медицинские данные.*

ABSTRACT

The total content of the master's dissertation is 87 pages. The work contains 15 figures, 10 tables. The list of references includes 36 sources, for which references are made.

In this dissertation, the implementation of an add-on device is proposed to an already existing medical device – the bioimpedance meter TOR-M1. The add-on device is based on the Internet of Things concept. The hardware and software parts were implemented. The add-on device is able to use cloud services for storing and visualization medical data of the patient. It is also possible to conduct further analyse of large number of patients' biomedical data to identify trends and new interactions between the biomedical indicators of the patient. The proposed add-on device allows to significantly improve the process of transmission, storage, and visualization of biomedical indicators of patients.

Keywords: *add-on device, biotelemetry, Internet Things, cloud service, medical data.*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 9
ВСТУП 10
РОЗДІЛ 1. АНАЛІЗ ТЕНДЕНЦІЙ РОЗВИТКУ СИСТЕМ БІОТЕЛЕМЕТРІЇ 12
1.1 Особливості розвитку систем телеметрії медичного спрямування 12
1.2 Алгоритми роботи систем біотелеметрії 16
1.3 Огляд існуючих медичних систем телеметрії 20
1.3.1 Безпека передачі даних 23
1.3.2 Відповідність сучасним стандартам та правилам зберігання та обробки медичних даних 23
1.3.3 Моніторинг та аналіз даних 25
1.3.4 Сумістність з існуючою медичною апаратурою 26
1.3.5 Висновки 27
1.5 Цифрові технології в охороні здоров'я 28
1.6 Особливості власного варіанту системи біотелеметрії 30
РОЗДІЛ 2 АПАРАТНА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ПРИСТРОЮ-ПРИСТАВКИ ЗА КОНЦЕПЦІЄЮ ІНТЕРНЕТУ РЕЧЕЙ 33
2.1 Структурна схема дослідної моделі пристрою-приставки 33
2.2 Стикування пристрою-приставки з вимірювачем біоімпедансу 34
2.3 Обґрунтування вибору програмного забезпечення серверу і бази даних 37
2.3.1 Обгрунтування вибору сервера 38
2.3.2 Обґрунтування вибору бази даних 39
2.4 Структура бази даних 41
2.4.1 Структура таблиць бази даних 42
2.4.2 Структура зв’язків таблиць бази даних 45
2.5 WEB-інтерфейс 47
2.5.1 Фреймворк Yii2 47
2.5.2 Інтерфейс користувача 48
Висновки 51
РОЗДІЛ 3 ОСОБЛИВОСТІ ПЕРЕДАЧІ ТА ОБРОБЛЕННЯ ДАНИХ З ПРИСТРОЇВ-ПРИСТАВОК 52

3.1 Вимоги до приватності та конфіденційності даних пацієнтів 52
3.1.1 Дотримання рекомендацій HIPAA у разі зберігання даних у хмарному сервісі 53
3.1.1 Контроль над даними 54
3.1.2 Рівні контролі різних моделей хмарних сервісів..... 55
3.2 Приймання та оброблення запитів до хмарного сервісу з пристроїв біотелеметрії 55
3.3 Оброблення медичних даних з пристрою-приставки 58
3.4 Розподіленні обчислення через API спеціалізованих обчислювальних платформ 60
3.5 Можливість впровадження та використання загального формату даних для біомедичних сигналів 62
РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 64
4.1 Визначення основних потенційних шкідливих та небезпечних факторів при виконанні науково-дослідних робіт. 64
4.2 Технічні рішення та організаційні заходи з безпеки і гігієни праці та виробничої санітарії. 65
4.2.1 Організація робочих місць користувачів ВДТ ПЕОМ..... 65
4.2.2 Санітарні норми приміщення 67
4.2.3 Мікроклімат у лабораторії 68
4.2.4 Склад повітряного середовища 70
4.2.5 Електробезпека..... 71
4.3 Заходи щодо поліпшення умов праці в науково-дослідній лабораторії 73
4.3.1 Перевірка та заземлюючого пристрою 74
4.4 Безпека в надзвичайних ситуаціях 75
4.4.1. Вимоги щодо організації ефективної роботи систем оповіщення персоналу у разі виникнення небезпечної ситуації..... 75
4.4.2. Обов’язки та дії персоналу у разі виникнення надзвичайної ситуації. 78
4.4.3 Пожежна безпека 79
ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ..... 81
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 83

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface/Прикладний програмний інтерфейс

ЕРНІ – Електронна медична особиста інформація

HTTP – Hyper Text Transfer Protocol/ протокол передачі даних, що використовується в комп'ютерних мережах

HTTPS – HTTP over SSL /

IoT – Internet of Things / Інтернет Речей

IP – Internet Protocol / ротокол мережевого рівня для передавання датаграм між мережами

MVC – Model-View-Controller/Модель-Представлення-Контролер

PHP – Hypertext Preprocessor / скриптова мова програмування

SSL – Secure Sockets Layer / криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером

URL – Uniform Resource Locator / стандартизована адреса певного ресурсу в інтернеті

БТ – Біотелеметрія

СКБД – Система керування базами даних

Хмарний сервіс – технологія, що передбачає віддалену обробку та зберігання даних.

ВСТУП

Нові досягнення в області інформаційних технологій створюють передумови трансформації системи охорони здоров'я і дають можливість кожному контролювати стан свого здоров'я на основі аналізу накопичених фактичних даних. Важливу роль в цьому відіграють системи біотелеметрії, за допомогою яких є можливим накопичення великої кількості даних.

Проте на сьогодні ще існує багато пристроїв, у яких функції реєстрації біосигналів реалізовані добре, а сукупний аналіз сигналів може бути виконаний лише вручну. Це майже унеможливлює аналіз даних великого об’єму з метою побудови певних закономірностей заснованих на зміні біологічних параметрів пацієнтів.

Також слід зазначити, що практично всі існуючі біотелеметричні системи працюють автономно одна від іншої, а деякі з них не зберігають біомедичні дані пацієнтів після вимірювання. Перспективним напрямком вирішення цієї проблеми є створення допоміжних пристроїв-приставок до вже існуючих біомедичних пристроїв з метою автоматизації передачі та зберігання медичних даних пацієнтів для подальшого аналізу та обробки.

Метою даної роботи є розробка пристрою-приставки до медичних пристроїв за концепцією Інтернету Речей для автоматизації бізнес процесів накопичення та машинного аналізу біомедичних даних пацієнтів.

Для досягнення мети було поставлено наступні задачі:

- Оцінити можливості технології Інтернету Речей (IoT) та сучасних телеметричних систем;
- розробити пристрій-приставку до медичного пристрою і програмне забезпечення для зберігання і подальшої обробки отриманих даних;
- проаналізувати особливості передачі та оброблення даних медичних пристроїв у разі впровадження технології Інтернету Речей у вигляді пристрою-приставки;

- розглянути питання охорони праці стосовно виготовлення дослідного зразка пристрою-приставки для передачі біомедичних даних.

Наукова новизна одержаних результатів полягає у наступному:

Висунуті та практично підтверджені гіпотези щодо можливості автоматизації передачі медичних даних з вже існуючих медичних пристроїв та зберігання і візуалізації медичних даних.

Практична цінність отриманих результатів:

Виконано аналіз існуючих рішень біотелеметричних систем, що працюють за концепцією Інтернету Речей і розроблено пристрій-приставку до вже існуючого біотелеметричного пристрою.

Апробація результатів. Основні положення і результати цієї роботи обговорювалися на науково-технічній конференції студентів, аспірантів та молодих вчених "РАДІОЕЛЕКТРОНІКА У XXI СТОЛІТТІ" [1].

Структура роботи

Робота складається зі вступу, чотирьох розділів, висновків і списку використаних джерел.

РОЗДІЛ 1.
АНАЛІЗ ТЕНДЕНЦІЙ РОЗВИТКУ СИСТЕМ БІОТЕЛЕМЕТРІЇ

1.1 Особливості розвитку систем телеметрії медичного спрямування

Телемедицина є галуззю сучасної медицини, яка забезпечує дистанційне надання медичної допомоги та обмін спеціалізованої медичної інформацією на основі використання сучасних телекомунікаційних технологій. Поява і розвиток телемедицини безпосередньо пов'язано з винаходом і вдосконаленням технічних засобів зв'язку (телефонія, радіо, телебачення), однак до появи сучасних комунікаційних технологій телемедична практика обмежувалась проведенням дистанційних медичних консультацій по телефонії або радіозв'язку, телеметрії фізіологічних показників у військовій або космічної медицини, в рідкісних випадках - передаванням медичних зображень по телевізійним каналам. Розробка і вдосконалення комп'ютерних технологій в практичній медицині в поєднанні з мережними технологіями сучасного цифрового зв'язку уможливили реалізацію телемедицини в її сучасному розумінні. В еволюції телемедичних систем до теперішнього часу можна виділити п’ять основних етапів:

Телемедичні системи першого покоління (1940-1990) спочатку телефонні лінії передач, системи мали просту конфігурацію, передавали лише сигнали без їх зберігання та обробки.

Телемедичні системи другого покоління (1990-1996) розроблялися на базі відеоконференцій і забезпечували передачу якісних статичних та динамічних медичних зображень з функціями архівування медичної інформації.

Третій етап розвитку (1999-2005) пов'язаний з впровадженням багатоканальної передачі медичної інформації, спільної роботи віддалених користувачів з медичними зображеннями, появою можливостей роботи з будь-якими каналами зв'язку; відбувається поступове злиття телемедичних та

медичних інформаційних систем в єдині функціональні комплекси.

Четверте покоління телемедичних систем (2005-2010) характеризується розвитком каналів зв'язку, які забезпечують можливості віддаленого обміну медичною інформацією в обсязі, достатньому для повноцінного надання якісної медичної допомоги відповідно до сучасних вимог.

П’ятий етап розвитку (2010-тепер. час) характеризується розвитком технології Інтернету Речей, яка передбачає автоматизацію бізнес процесів цифрових технологій охорони здоров’я. Наприклад передачу, обробку біомедичних сигналів, зберігання інформації в хмарах та ін..

Мета телемедицини – надання якісної медичної допомоги будь-якій людині незалежно від його місцезнаходження та соціального становища.
Предмет телемедицини – передача за допомогою телекомунікацій і комп'ютерних технологій всіх видів медичної інформації між віддаленими один від одного пунктами (медичними установами, пацієнтами та лікарями, представниками охорони здоров'я і т.д.).

Надання телемедичної допомоги характеризується переважно двома ознаками:

1. Види переданої інформації (опис історії хвороби, відеозображення ендоскопічної і УЗ-картини, рентгенівських знімків, мікроскопічних мазків, дані лабораторних аналізів і т.п.);

2. Спосіб передачі інформації (телефонні лінії, супутниковий і стільниковий зв'язок і т.п.) [4].

Телемедицина має наступні предметні області [7]:

- технології (вимірювальні прилади, системи моніторингу, канали зв'язку і комунікації, відеосистеми, робочі станції, бази даних, експертні системи і ін.);
- медична наука (робоче місце фахівця науково-дослідної установи; відомчі, міжвідомчі та державні інформаційні та бібліотечні бази даних; відомчі, міжвідомчі, державні та міжнародні наукові програми);

- охорона здоров'я (робоче місце фахівця, програми консультативної медичної допомоги, міжнародні консультативно-діагностичні центри);
- спеціальні галузі знань і діяльності (космічна біомедицина і медицина, екомедицина, медицина катастроф, медицина надзвичайних ситуацій, військова телемедицина та ін.);
- суміжні галузі знань і діяльності (вітчизняні та зарубіжні вчені, організації, міністерства і відомства, чия діяльність пов'язана з теоретичними і прикладними аспектами здоров'я людини).

Телемедична процедура - це стандартна послідовність спільних дій абонента, консультанта, координатора, пацієнта і допоміжного персоналу, яка відбувається за шаблонним сценарієм з використанням комп'ютерної та телекомунікаційної техніки і має строго певну мету [1].

Раніше виділяли наступні основні види телемедичних процедур:

– віддалене консультування та інструктаж;

– дистанційне навчання;

– моніторинг (біорадіотелеметрія);

– дистанційне маніпулювання.

Планувалося, що в процесі надання медичної допомоги з використанням телемедичних технологій будуть взаємодіяти лікуючий лікар, координатор, віддалений лікар, пацієнт, технічний і допоміжний персонал.

Але на сьогодні нагальною проблемою є нестача висококваліфікованих медичних кадрів і тому слід вилучити з цього алгоритму максимальну кількість задіяних осіб. В сучасних умовах максимальна кількість діючих осіб – дві: лікар та пацієнт, або сервіс/додаток та пацієнт.

Цікавим викликом на сьогоднішній день є автоматична обробка та побудова максимально точних прогнозів і трендів, а можливо і постановка діагнозу на основі великої кількості медичних даних заздалегідь зібраних за допомогою біомедичних пристроїв, що працюють за концепцією Інтернету Речей.

Інтеграція з Інтернетом має на увазі, що пристрої будуть використовувати IP-адресу як унікальний ідентифікатор. Проте, через обмежені адресні простори в IPv4 (що дозволяє використовувати 4,3 мільярда унікальних адрес), об'єктам IP доведеться використовувати IPv6, який забезпечує унікальними адресами мережевого рівня не менше 300 млн пристроїв на одного жителя Землі. Об'єктами в IP будуть не тільки пристрої із сенсорними можливостями, але також пристрої, які виконують дії (наприклад, лампочки або замки, якими керують через Інтернет). Значною мірою, майбутнє Інтернету Речей не буде можливим без підтримки IPv6, отже, глобальне впровадження IPv6 у найближчі роки буде мати вирішальне значення для успішного розвитку IP в майбутньому.

Для бездротової передачі даних особливо важливу роль в побудові Інтернету Речей відіграють такі характеристики, як ефективність, відмовостійкість, адаптивність, можливість самоорганізації. Основне зацікавлення в цьому сенсі представляє стандарт IEEE 802.15.4, що управляє доступом для організації енергоефективних персональних мереж, і є основою для таких протоколів, як ZigBee, WiFi, Bluetoot, 6LoWPAN.

ZigBee — це комунікаційна технологія, заснована на протоколі IEEE 802.15.4 для реалізації низькошвидкісних бездротових приватних мереж. ZigBee володіє такими характеристиками, як низьке енергоспоживання, низька швидкість передачі даних, низька вартість і висока пропускна здатність. В даний час ZigBee використовується в основному при передаванні інформації між різними речами електронного обладнання, які знаходяться в межах короткої відстані і швидкості передачі даних не дуже висока [27].

Wi-Fi — це локальна бездротова технологія, яка використовує 2,4 ГГц надвисокої частоти або 5 ГГц супер-високочастотної радіохвилі. Ця технологія дуже добре підходить для передавання великих обсягів даних по бездротовій мережі між пристроями, але це також вимагає багато енергії для роботи і має невеликий рівень пропускної здатності даних.

Bluetooth — це бездротова технологія, яка використовується для

передачі даних в персональних мережах. Він передає дані по смузі частот від 2,4 до 2,485 ГГц і працює на коротших відстанях, ніж Wi-Fi. За допомогою Bluetooth можна синхронізувати пару пристроїв, таких як телефони, навушники, колонки, комп'ютери і багато іншого. З розвитком Bluetooth v4.0 з'явилася можливість реалізувати функцію низького енергоспоживання і збільшений радіус дії до декількох десятків метрів.

Серед провідних технологій важливу роль у поширені Інтернету Речей відіграють рішення PLC — технології побудови мереж передачі даних по лініях електропередач, оскільки у багатьох додатках присутній доступ до електромереж (наприклад, торгові автомати, банкомати, інтелектуальні лічильники, контролери освітлення спочатку підключені до мережі електропостачання). 6LoWPAN, який реалізує шар IPv6 як над IEEE 802.15.4, так і над PLC, будучи відкритим протоколом, стандартизованих IETF, є особливо важливим для розвитку Інтернету Речей.

1.2 Алгоритми роботи систем біотелеметрії

Розглянемо алгоритми роботи телеметричних систем біотелеметрії різних етапів розвитку.

Перший етап.

У 40-50-ті роки у зв'язку з успіхами радіотехніки біотелеметричні методи лікарського контролю і физіологічних досліджень стали широко використовуватися в авіаційній, космічній та інших галузях медицини. Великий вплив на розвиток біотелеметрії в частині вдосконалення методів отримання біологічної інформації, вдосконалення датчиків, електронних вимірювальних пристроїв, методів кодування, передачі, запису та автоматичної обробки результатів вимірювання зробила космонавтика.

Біотелеметрія дозволила отримувати кількісну інформацію безпосередньо з досліджуваного об'єкта і реєструвати динаміку зміни фізіологічних процесів безперервно протягом тривалого часу в реальному навколишньому середовищі, характерної для його виробничої або іншої

діяльності, як в нормі, так і в патології. Тому з’явилася можливість застосування біотелеметрії для вивчення реакцій найважливіших фізіологічних систем здорового організму на різні зовнішні впливи при мінімальному порушенні комфортності і рухливості, а також для діагностики і динамічного контролю за станом хворих.

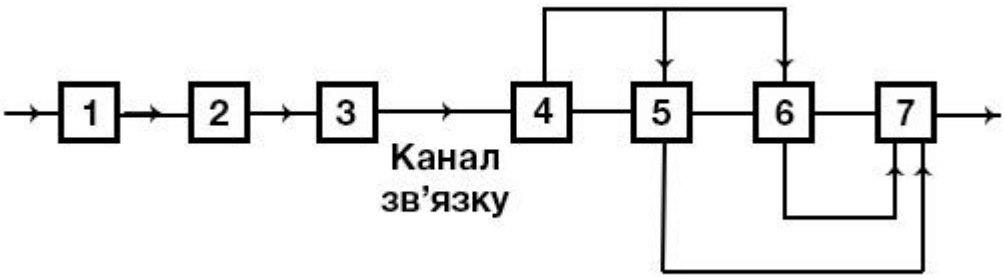

Рис. 1. 1 – Спрощена структурна схема біотелеметричної системи: 1 – сенсори біологічної інформації; 2 – електронні перетворюючі пристрої; 3 – телеметричний передавач; 4 – телеметричний приймач; 5 – пристрої запису інформації; 6 – вимірювальні пристрої автоматичної обробки; 7 – пристрої автоматичної обробки.

Спрощена структурна схема біотелеметричної системи першого покоління зображена на малюнку рис. 1.1 біотелеметрична система складається з двох частин. Перша, передавальна частина встановлюється на об'єкті досліджень або в безпосередній близькості від нього. Передавальна частина може вводитися також всередину об'єкта, наприклад у разі застосування ендорадіозонда.

До складу другої приймально-вимірювальної (стаціонарної) частини входять телеметричний приймач лінії зв'язку, пристрої запису інформації по каналах, вимірювальні пристрої та пристрої автоматичної обробки результатів вимірювання, включаючи комп’ютер. Залежно від призначення біотелеметричної системи можуть бути введені або виключені окремі ланки системи. Інформація з датчиків і перетворювачів послідовно проходили через кілька передавачів і приймачів (ретрансляція інформації).

Передавальна частина біотелеметричної системи може також включати в себе пристрої первинної обробки інформації з метою зменшення її надмірності і пристрої для зберігання даних в залежності від умови експлуатації і технічних особливостей системи.

Передача інформації від об'єкта досліджень до вимірювальних пристроїв здійснювалася за різними високо- або низькочастотних лініями зв'язку. Використовували телефон, а також високочастотні радіолінії з застосуванням ультракороткого хвильового діапазону. Для передачі інформації в водному середовищі знаходять застосування гідроакустичні, електромагнітні або оптичні лінії зв'язку. Під час першого етапу сенсори постійно модернізували. З'явилася можливість перетворювати біологічну інформацію і передавати її у відповідних одиницях виміру, наприклад величину артеріального і венозного тиску - в мм рт. ст., тони серця – в акустичних одиницях, механічні переміщення – в сантиметрах, електрокардіографічні, електроенцефалографічні електричні сигнали – в мікровольтах, мілівольтах. З виходу датчиків електричний сигнал у вигляді амплітуди струму або напруги, пропорційних вищенаведеній біологічній величині, надходить на вхід перетворючого електронного пристрою каналів з телеметричним передавачем лінії зв'язку.

Для забезпечення можливості передачі інформації про декілька виміряних величин за радіолінією зв'язку в біотелеметричних системах застосовували частотне або часове розділення каналів.

Основними медико-технічними вимогами до передавальної частини біотелеметрії було: надійне перетворення вимірюваної величини в сигнал, що передається і надійне виділення в сигналі вимірюваного параметра з безлічі інших сигналів шуму (сигнал / шум> 1/50), похибка телевимірювання 1 - 10%, забезпечення мінімальних габаритів, ваги і енергоспоживання. Стаціонарна приймальна частина системи біотелеметрії мала менш жорсткі обмеження по вазі, габаритам і енергоспоживання [8].

Другий та Третій етапи характеризувалися передачею і архівуванням

медичних зображень, під час третього етапу почалося поступове злиття телемедичних та медичних інформаційних систем в єдині багатофункціональні комплекси (рис. 1.2).

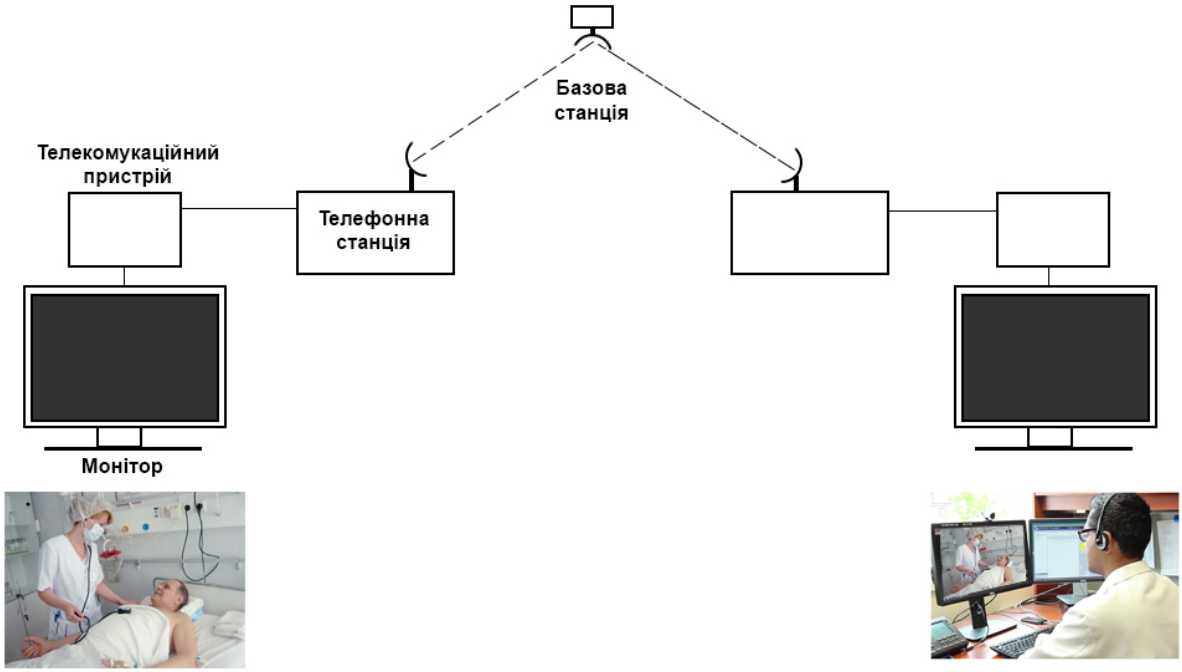

Рис.1.2 – Структурна схема телемедичної системи третього покоління

П’ятий етап характеризується доповненням і частково заміною звичайних технологій телемедицини інтернет технологіями, а саме технологією Інтернету Речей. Також розширилась мета телемедицини: з’явилася ціль і можливість структурно та автоматично зберігати та обробляти велику кількість медичних даних і в подальшому аналізувати їх та будувати точні прогнози. В основному за концепцією Інтернету Речей інформація зберігається в хмарних середовищах. Такі нововведення характеризуються підвищеними вимогами. Наприклад, є вимоги та стандарти по зберіганню та обробці медичних даних пацієнтів.

Рис.1.3 - Структурна схема телемедичної системи п'ятого покоління

1.3 Огляд існуючих медичних систем телеметрії

Згідно зі звітом компанії «Allied Market Research» [9], ринок медичних IoT-гаджетів і IoT-додатків з 2014 до 2021 року зросте до $ 136,8 млрд. Середньорічний темп зростання ринку медичного Інтернету речей складе 12,5%.

Лідером на ринку стануть програми, що дозволяють здійснювати спостереження за пацієнтами віддалено. Так, в 2021 році ця частина ринку медичного Інтернету речей в грошовому обчисленні дорівнюватиме $ 72,7 млрд. Крім цього, в найближчому майбутньому в сфері охорони здоров'я відбудеться зростання кількості високотехнологічних сервісів і систем.

Драйверами ринку стануть: підвищення доступності високошвидкісного Інтернету, зниження цін на сенсори, поширення медичних гаджетів і зростання інформованості користувачів про інновації в медицині [9].

Розглянемо декілька прикладів готових IoT-рішень в медицині:

1) MySignals – це нове покоління електронної медицини і медичної продукції, спеціально орієнтоване на дослідника, розробника і виробника. MySignals – це повноцінна медична система моніторингу най поширених біологічних показників людини, таких як електрокардіографія, температура тіла, дихання, кількість цукру в крові, кров'яний тиск та ін.. Загальна кількість сенсорів, що можна підключити – 16. Платформа має відкриту конфігурацію, власні додатки для Android та iOS, а також хмарне сховище для зберігання та аналізу даних [10]

Рис. 1.4 – MySignals SW

2) AdhereTech ставить за мету вирішити звичайну проблему в сфері охорони здоров'я: пацієнтам часто важко самим налаштувати засоби контролю за прийомом ліків, і введення необхідної інформації для багатьох скрутний.

Ця компанія з Нью-Йорка випускає «розумні» пігулниці з бездротовим зв'язком і акумулятором, термін служби яких до п'яти років. Вони автоматично в режимі реального часу посилають інформацію про дотримання часу прийому ліків. У разі якщо пропущено прийом ліків, то пацієнт отримає персональне текстове повідомлення або автоматичний

дзвінок на телефон.

Смарт-пігулниці відповідають вимогам HIPAA (Закон про охорону та відповідальність за інформацію медичного страхування в США), FDA (Федеральне управління з нагляду за якістю харчових продуктів і медикаментів) і сертифікації CE, вказує компанія [11].

Рис. 1.5 – AdhereTech Smart Wireless Pill Bottle

3) Проект Blue Sky є колаборацією між Pfizer і IBM, що включає планове клінічне дослідження з використанням системи сенсорів, мобільних пристроїв та машинного навчання, щоб забезпечити цілодобове спостереження за пацієнтами в режимі реального часу, та повідомлення результатів пацієнтам та лікарям.

Мета полягає в тому, щоб контролювати прогресування та лікування хвороби Паркінсона.

Pfizer має намір розвивати систему до 2019 року, коли один з його експериментальних препаратів лікування хвороби Паркінсону увійде в третій етап розробки. Однак, третя фаза випробування, як правило, сувора і забирає багато часу, а це означає, що може бути якийсь час, перш ніж ми бачимо

тестувальну систему IBM [12].

Порівняльна характеристика розглянутих платформ буде проводитися по наступним критеріям:

- безпека передачі даних;
- можливість розширення та масштабування системи;
- моніторинг та аналіз даних;
- сумісність з існуючою медичною апаратурою.

Критерії розташовані в довільному порядку. Важливість кожного з критеріїв буде встановлена далі.

1.3.1 Безпека передачі даних. Основні запропоновані методи забезпечення безпеки інформації, що передається з сенсорів та з клієнтських програм управління/адміністрування – це SSL з’єднання, аутентифікація сесії, з’єднання через логін та пароль, унікальний ідентифікатор кожного пристрою.

MySignals не виділяє унікальний ідентифікатор на кожен сенсор. Натомість, він видає ідентифікатор лише на головний пристрій, до якого приєднано всі сенсори одного пацієнта. Натомість всі сенсори в Blue Sky мають окремі ідентифікатори. Не зважаючи на деякі відмінності усі три системи відповідають вище представленим вимогам.

1.3.2 Відповідність сучасним стандартам та правилам зберігання та обробки медичних даних. Медична інформація відображає дані та результати медичних наукових досліджень й медичної практики. З одного боку, вона відображає процеси та явища в системі охорони здоров'я (тобто є засобом, що використовується лікарями під час медичної практики), з іншого боку, вона може бути результатом роботи інформаційно-обчислювальних центрів, спеціалістів оргметодвідділів тощо.

Згідно HIPAA, певна інформація вважається інформацією про здоров'я, що охороняється (protected health information - PHI). PHI - це дані про фізичне

і психічне здоров'я пацієнта в минулому, сьогоденні і майбутньому, про надання пацієнтові медичної допомоги, про платежі пацієнта за медичні послуги в минулому, сьогоденні і майбутньому, а також дані (ідентифікатори), що ідентифікують особу. PHI включає в себе персональну ідентифікаційну інформацію (PII), таку як імена, адреси, пов'язані з пацієнтом дати (дата народження або дата обслуговування), номери телефонів, номери факсів, адреси електронної пошти, URL-адреси, IP-адреси, номери соціального страхування , номери рахунків, номери ліцензій, номери медичних карт, номери планів медичного страхування, ідентифікатори пристроїв і їх серійні номери, ідентифікатори і серійні номери транспортних засобів, біометричні ідентифікатори і фотографії. Іншими словами, до PHI відносяться будь-які унікальні ідентифікаційні номери, коди або характеристики, за якими можна простежити пацієнта.

Електронна інформація про здоров'я, що охороняється (EPHI) - це фактично та ж PHI або персонально ідентифікаційна інформація про здоров'я, що створюється, отримується, обслуговується і передається в електронному вигляді. Якщо стандарт конфіденційності застосовується до будь-якого виду PHI (письмова, друкована, електронна і усна), то стандарт безпеки застосовується тільки до EPHI.

Платформа MySignals була розроблена Cooking Hacks (відкритий апаратний підрозділ Libelium), щоб допомогти дослідникам та розробникам вимірювати дані біометричних сенсорів для експериментів та тестування. Але, так як платформа не має медичних сертифікатів, вона не може використовуватись для моніторингу критичних пацієнтів, котрим потрібен точний медичний моніторинг.

AdhereTech на відміну від попередньої платформи має сертифікати по захисту медичних даних користувачів від різних установ:

- FDA – Управління з санітарного нагляду за якістю харчових продуктів та медикаментів (США). Воно відповідає за регуляцію та нагляд над

безпечністю харчових продуктів, біологічно активних добавок, ліків, вакцин, медичних приладів, ветеринарної продукції та косметики;

- HIPAA – (Закон про переносиміть та підзвітність даних медичного страхування від 1996 року) - це закон Сполучених Штатів, в якому містяться положення про конфіденційність і безпеку даних для захисту медичної інформації. Закон, який був підписаний в серпні 1996 року, оновлений в 2013 році, містить п'ять розділів;
- CE – Європейська комісія описує знак CE як «паспорт», який дозволяє виробникам вільно поширювати промислові товари на внутрішньому ринку ЄС;
- USP – Фармакопейна конвенція США;
- ISO – Міжнародна організація зі стандартизації.

Платформа Blue Sky на сьогоднішній день має тільки сертифікацію HIPAA (оновлену від 2013 року), тому що на сьогодні цей проект проходить лише фазу попереднього тестування лише на території США.

Таким чином можна зробити висновок, що дані користувачів AdhereTech найбільш захищені, а дані, що будуть збирати, обробляти та зберігати за допомогою пристроїв та сервісів MySignals можуть потрапити третій стороні, так як MySignals – це не сертифікований медичний пристрій, а відкритий апаратний продукт для досліджень.

1.3.3 Моніторинг та аналіз даних. В «MySignals HW» передача даних може відбуватися за допомогою різних каналів:

- Bluetooth
- Wi-Fi
- 3G
- 4G
- GPRS
- Zigbee / 802.15.4

Канал передачі даних залежить від вибору передавального модуля користувачем, але в стандартному «MySignals SW» передача даних відбувається через Wi-Fi з’єднання. Аналіз даних відбувається в хмарі [10].

В «AdhereTech» передбачений тільки один канал передачі даних – це Wi-Fi. Інформація опрацьовується в хмарі, а потім у разі необхідності сервіс комунікує як з пацієнтом так і з лікарем.

За проект «Blue Sky» відомо, що сенсори комунікують з мобільними пристроями користувачів-пацієнтів через Wi-Fi та Bluetooth, а зберігання та обробка даних буде відбуватись у хмарі компанії IBM.

Таблиця 1.1 – Оцінка каналів передачі та місць зберігання та обробки даних

Назва	Канал передачі даних	Місце зберігання та обробки даних
MySignals	Bluetooth, Wi-Fi, 3G, 4G, GPRS, Zigbee / 802.15.4	Хмарне середовище
AdhereTech	Wi-Fi	Хмарне середовище
Blue Sky	Bluetooth, Wi-Fi	Хмарне середовище IBM

1.3.4 Сумістність з існуючою медичною апаратурою. Часткова сумісність існуючих медичних сенсорів можлива лише з MySignals, тому ця платформа має відкритий структуру, яку розробники та виробники мають можливість конфігурувати виходячи із своїх нагальних потреб. Тобто є можливість використовувати сенсори та прилади власної розробки або використовувати сигнали з повноцінних старих медичних пристроїв. Можна сказати, що платформа MySignals майже повністю замінює декілька важких стаціонарних медичних приладів.

«AdhereTech», навідміну від «MySignals», пропонує використовувати власні пристрої та власний сервіс і не передбачає можливості роботи із вже існуючими медичними пристроями.

Оскільки в системі «Blue Sky» використовуються тільки бездротові сенсори, то використання старої медичної апаратури є неможливою. Але ціль

проекту є не безпосереднє лікування, а накопичення корисних даних пацієнтів з хворобою Паркінсона, для подальшої оптимізації та автоматизації лікування цієї хвороби.

1.3.5 Висновки. У ході дослідження були проаналізовані медичні IoT-платформи, такі як MySignals, AdhereTech та Blue Sky за чотирма параметрами:

- Безпека передачі даних
- Можливість розширення та масштабування системи
- Моніторинг та аналіз даних
- Сумісність з існуючою медичною апаратурою

В аспекті безпеки передачі даних всі три платформи виявилися однаково надійними, реалізуючи передові технології в шифруванні даних та аутентифікації користувачів та пристроїв.

В аспекті відповідності сучасним стандартам та правилам зберігання та обробки медичних даних домінує платформа AdhereTech, так як має усі необхідні сертифікації на території США, а також в Європі. Платформа MySignals не має жодних сертифікацій, які стосувалися б стандартів та правил зберігання та оброблення медичних даних, так як це насамперед інструмент для досліджень і розробки, а не повноцінний медичний прилад. Платформа Blue Sky, на сьогодні, має лише сертифікацію в США, тому що вона ще проходить тестування.

В аспекті моніторингу та аналізу даних усі три платформи використовують хмарні сервіси для зберігання та обробки даних, але лише MySignals має можливість використовувати для передачі даних такі канали як 3G, 4G, GPRS, Zigbee / 802.15.4, у той час як Blue Sky може використовувати Bluetooth та Wi-Fi, а AdhereTech лише Wi-Fi.

В аспекті сумісності з існуючою медичною апаратурою усі три платформи програють, оскільки жодна з них не може комунікувати із вже існуючими медичними пристроями. Лише MySignals в теорії може використовувати сенсори від старих медичних пристроїв.

1.4 Цифрові технології в охороні здоров'я

Експонентні досягнення в області науки і техніки трансформують здоров'я і медицину і дають хворим контроль над своїм здоров'ям. Здатність розшифровувати людський геном за доступною ціною революціонізує нашу здатність розуміти ризики захворювання і налаштовувати лікування. Це, поряд з поліпшенням діагностичного сканування і візуалізації, означає, що тепер ми знаємо більше про анатомію людини, відкриваючи шлях для точних ліків і заснованих на фактичних даних підходів до профілактики і самоврядуванню[13].

Middleware - це ім'я, дане технології, яка дозволяє ефективно використовувати дані, створені на персональних комунікаційних пристроях (наприклад, смартфонах), в системі охорони здоров'я. Вона була розроблена у відповідь на виклик управління величезним обсягом даних, що генеруються аварійними сигналами і попередженнями. Middleware полегшує обмін даними і даними, що дозволяє додаткам ефективно взаємодіяти. Вона автоматизує клінічну документацію і виконує віддалене спостереження і агрегацію даних.

Портативне цифрове обладнання для візуалізації трансформує поставку медичних послуг, починаючи від машини швидкої допомоги і завершаючи операційним залом, що робить передову візуалізацію доступною для пацієнтів у віддалених районах. Наприклад, до недавнього часу використання ультразвуку було обмежено його розміром, вартістю і потребою в електроенергії. Тепер, менші, доступні, ультразвукові машини, деякі здатні розміститися в долоні, можуть видавати зображення з високою роздільною здатністю працюючи на акумуляторній батареї. Використання поширюється по всьому світу, забезпечуючи сучасну мобільну візуалізацію медичних клінік у віддалених сільських районах.

Інноваційні цифрові сенсори

Широкий спектр нових цифрових датчиків розробляється на основі інноваційних рішень, в тому числі:

• новий липкий датчик на основі гелю, який контролює електричну активність в органі, що не сповзаючи

• патч-подібний датчик, який переміщається разом зі шкірою, записує і відправляє інформацію про здоров'я на синхронізовані смартфони і комп'ютери

• датчик «Електронна шкіра», який вдягають на зап'ясті, який контролює і лікує м'язові розлади у людей, які страждають паркінсонізмом або на епілепсію, виявляючи поштовхи і вивільняючи лікарські засоби, вбудовані в патч, який поглинається через шкіру

• проковтуючий датчик від Proteus Digital Health, який контролює, коли пацієнт приймав або не приймав ліки, а також надає біометричні дані, такі як частота серцевих скорочень, сон, фізична активність і рівень стресу

Цикл зрілості цифрових технологій охорони здоров'я

З огляду на широкий спектр нових технологічних розробок, прогнозування того, як ринок буде розвиватися і які технології вплинуть на постачання медичних послуг, є складним завданням. Gartner, ведуча науково-дослідницька та консультаційна компанія з інформаційних технологій, відома своїм графічним методологічним інструментом «Цикл зрілості технологій» створила таку модель і для цифрової медицини [14] (рис 1.6).

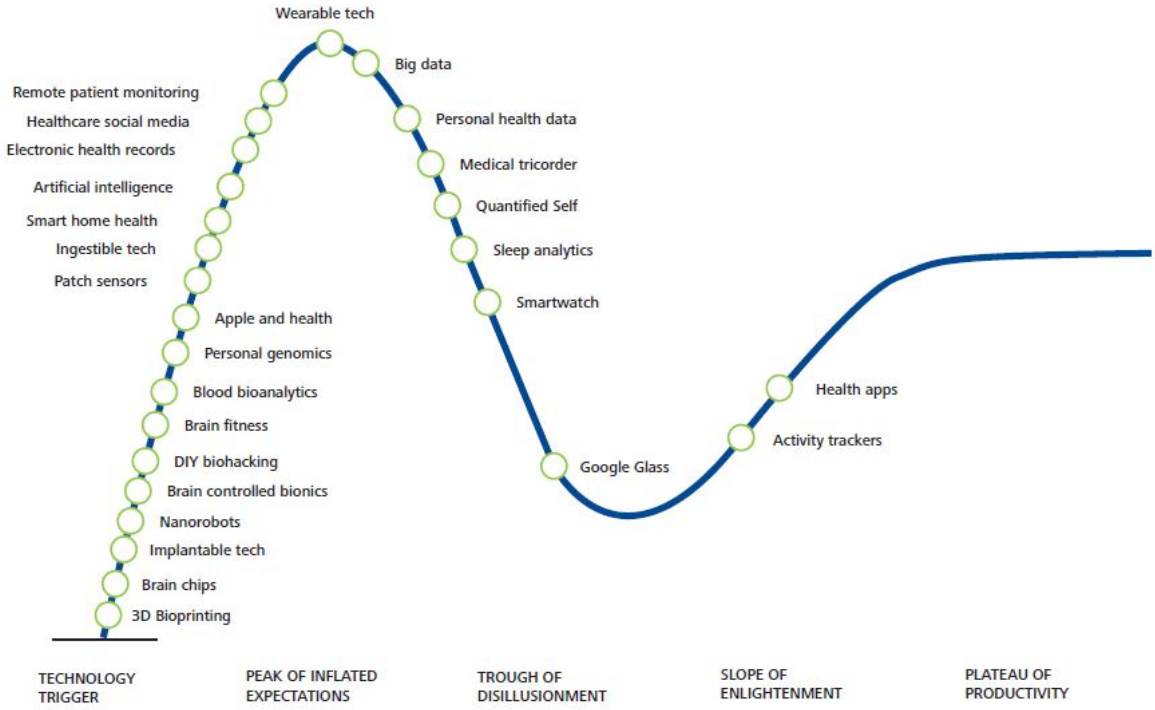

Рис. 1.6 - Цикл зрілості цифрових технологій в медицині [15]

Важливе місце в подальшому розвитку медицини займають великі дані (Big Data). Маючи великі обсяги структурованих даних пацієнтів можна прогнозувати вплив тих чи інших ліків, лікування та ін.. А перехід від великої кількості неструктурованих даних в паперових носіях до структурованих та оцифрованих даних може забезпечити саме технології Інтернету Речей.

1.5 Особливості власного варіанту системи біотелеметрії

Перспективним для розвитку та впровадження цифрових технологій охорони здоров’я (Digital Health) є розробка пристроїв та систем за концепцією Інтернету речей (IoT). Інтернет речей передбачає можливість підключення до мережі ряду фізичних пристроїв медичного призначення з електронікою, програмним забезпеченням, сенсорами з метою збору та обміну даними [16].

Більшість наявних медичних діагностичних систем працюють автономно та не надають можливості аналізувати дані та результати у

сукупності [17]. Зазвичай оператору (лікарю) необхідно проводити вимірювання безпосередньо на пацієнті і заносити дані в базу даних вручну. А у разі використання застарілого обладнання результати обстеження можуть взагалі зберігатися на паперових носіях, що значно ускладнює можливість аналізу їх у сукупності та значно обмежує можливості структурованого накопичення значної кількості діагностично-цінних даних. Робота оператора також потенційно створює передумови появи додаткових помилок в базі даних. Таким чином, перспективним є розробка IoT- пристроїв приставок для вже існуючих пристроїв реєстрації біосигналів та для медичної апаратури з метою автоматизації процесів накопичення діагностично-цінних даних та аналізу їх у ретроспективі та у сукупності з іншими показниками.

Реалізація таких пристроїв приставок вимагає проробки як апаратної частини стикування з медичною апаратурою за наявними в ній інтерфейсами та проколами, так і програмної частини, що буде розміщена на сервері хмарного сервісу. У разі простого варіанту реалізації необхідно реалізовувати IoT-пристрій приставку індивідуально під кожен конкретний пристрій реєстрації біосигналів. Більш складний варіант реалізації передбачає створення універсального програмно-апаратного рішення з можливістю переналаштування під конкретний варіант медичної апаратури.

Для опрацювання описаного вище підходу виконано розробку пристрою-приставки до вимірювача біоімпендансу ТОР-М1 [18]. Призначення цього IoT-пристрою приставки є реєстрація та автоматичне зберігання у хмарному сервісі вимірювань імпедансу (модуль та фаза) на трьох частотах 20, 100 та 500 кГц для пацієнтів, що проходять періодичні процедури гемодіалізу [19]. Передбачається використання отриманих даних для уточнення динаміки та змін гідратації тканин пацієнтів хронічного гемодіалізу та прогнозування і передбачення змін «сухої ваги», що є критичним параметром для таких пацієнтів. Відображення даних виконується через Web-додаток.

Апаратно пристрій-приставка реалізована на основі радіомодуля

ESP8266 з підтримкою підключення до Wi-Fi мереж, хмарний сервіс реалізований на основі PHP фреймворку Yii2. Головною перевагою рішення на ESP8266 є низька вартість та простота реалізації апаратної частини. Перспективним надалі є удосконалення хмарного сервісу шляхом впровадження стандарту HIPAA [20] для можливості забезпечення персонального моніторингу параметрів біосигналів. Також перспективним є розробка пов’язаного з хмарним сервісом мобільного додатку.

РОЗДІЛ 2
АПАРАТНА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ПРИСТРОЮ-ПРИСТАВКИ ЗА КОНЦЕПЦІЄЮ ІНТЕРНЕТУ РЕЧЕЙ

Не дивлячись на відносну простоту запропонованого рішення проблеми автоматизації передачі, зберігання та обробки біомедичних даних, треба детально опрацювати наступні питання: інтерфейс стикування пристрою-приставки з вже існуючими біомедичними пристроями діагностики, метод передачі даних у хмарне сховище, архітектуру бази даних та WEB-додаток для візуалізації результатів вимірювання.

2.1 Структурна схема дослідної моделі пристрою-приставки

Реалізуючи простий приклад реалізації біомедичної системи діагностики за концепцією Інтернету Речей було обрацьована апаратна та програмна частина. Апаратна частина складається з плати NodeMCU з відповідною прошивкою, а програмна з серверу, бази даних і WEB-додаткудля відуалізації і керування. Програмна частина знаходиться у хмарному сервісі (рис. 2.1).

Рис. 2.1 – Алгоритм роботи пристрою-приставки до вимірювача біоімпендансу TOP-M1

Розглянемо принцип роботи досліджуваної системи. Біомедичні дані вимірювань у вигляді вже числових значень передаються з вимірювача біоімпендансу TOP-M1. Вимірювач біоімпендансу має вихідний COM-порт. Дані з цього порту кабелем передаються на UART вхід плати NodeMCU. Після накопичення масиву даних вимірювання одного пацієнта вони передаються через радіомодуль ESP8266 у базу даних хмарного сервісу. Після чого відбувається візуалізація біомедичних даних у вигляді таблиць та графіків у WEB-додатку. Подальший аналіз даних можливий з будь-якої точки світу, при умові, що у дослідника-аналітика буде відповідний доступ до бази даних.

2.2 Стикування пристрою-приставки з вимірювачем біоімпедансу

Схема побудована на базі мікроконтролера NodeMCU v3 з вбудованим Wi-Fi модулем ESP8266 [Рис. 2.1, 2.2]. Даний контролер, попри свою низьку ціну, є дуже зручним засобом розробки цифрових схем пристроїв-приставок за концепцією Інтернету Речей.

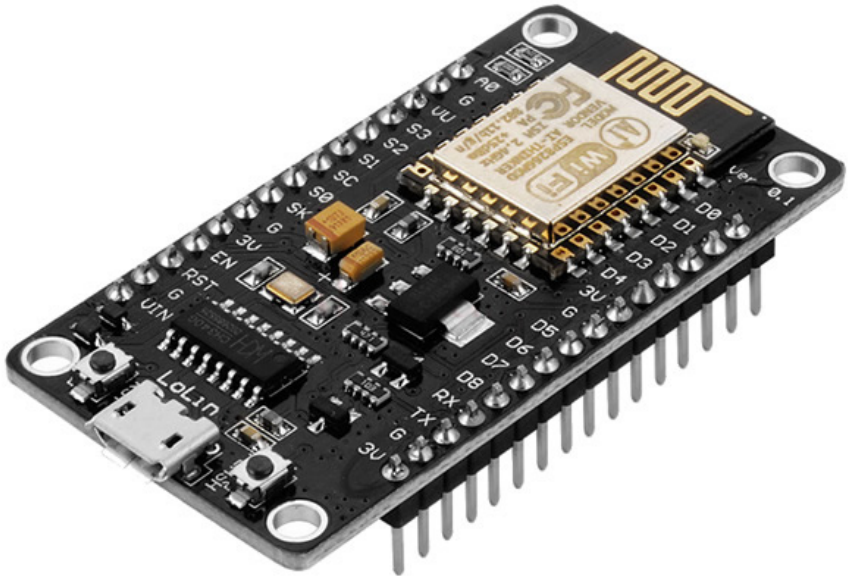

Рис. 2.2 – Мікроконтролер NodeMCU v3

NodeMCU – відкритий безкоштовний проект на основі скриптової мови програмування Lua. Прошивка досить потужна і дозволяє дуже швидко і просто реалізовувати різні типові проекти. Прошивка вміє виконувати Lua-скрипти як з послідовного UART порту (аналогічно AT-командам) так і з внутрішньої flash пам’яті (виконуючи скрипти). Lua скрипти зберігаються у Flash у внутрішній файловій системі. Файлова система пласка, спрощена. Тобто без підкаталогів. Варто пам’ятати, що ESP8266 – це тільки мікроконтролер. Скриптами можна отримати доступ до власних файлів, читати і зберігати різну інформацію. NodeMCU модульна. Що з одного боку дозволяє нарощувати функціонал, а з іншого зібрати прошивку тільки з необхідних модулів і не витрачаючи даремно пам’ять.

Основні переваги NodeMCU:[23]

- Простота програмування;
- Асинхронна івентова модель програмування;
- 40+ вбудованих модулів;
- Прошивка доступна з або без підтримки плаваючої точки (цілочисленні використовують менше пам'яті)
- Проект постійно оновлюється, як і його документація[10]
- Підтримка програмування на декількох мовах, в тому числі C

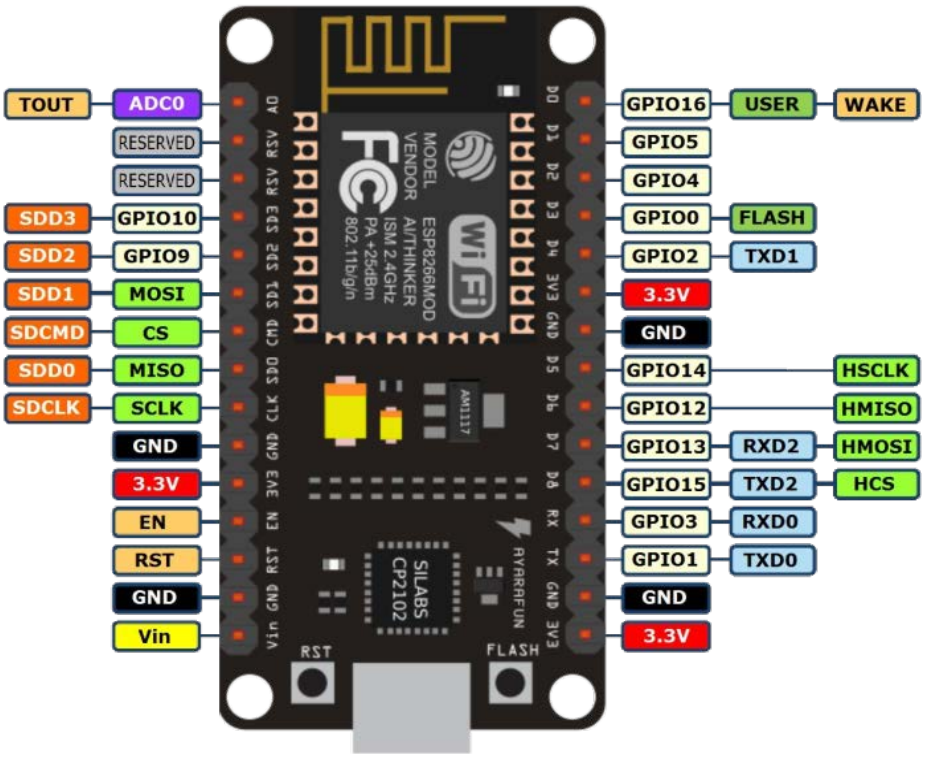

Рис. 2.3 – Схема мікроконтролера NodeMCU v3

Програмування виконується в середовищі розробки Arduino IDE на мові програмування C. Мікроконтролер підключається до комп'ютера через microUSB, що забезпечує його живленням. Також через microUSB виконується його програмування.

Вимірювач біоімпендансу TOP-M1 передає спочатку номер сесії, потім через кожні 6 секунд усереднене значення амплітуди, фази біоімпендансу та струму. Тобто одне вимірювання проходить протягом однієї хвилини. Відповідно ESP8266 передає дані одного повного вимірювання на сервер після його завершення.

ESP8622 має один повноцінний UART порт. NodeMCU дозволяє використовувати ще один UART порт, який може тільки передавати дані, але нас цікавить повноцінний порт. Невелика складність використання UART порту виникає через те, що з цього ж порт відбувається програмування плати NodeMCU. Коли запускається скрипт, який використовує UART, скрипт перехоплює весь введення по порту UART, і NodeMCU не виконуватиме ніяких команд, поки скрипт не «відпустить" UART. Щоб уникнути

блокування NodeMCU і забезпечити можливість відправляти команди, застосуємо наступний скрипт.

```
print("Waiting ...")
tmr.register(0, 5000, tmr.ALARM_SINGLE, function(t)
tmr.unregister(0); print("Starting..."); dofile("uart1.lua")
end)
tmr.start(0)
```

Таким чином зробимо автозапуск скрипта з затримкою.

За замовчуванням швидкість порту 115200bps. NodeMCU автоматично підбирає коректну швидкість роботи UART. Це дуже зручно, оскільки різні модулі можуть працювати на різних швидкостях. Автоподбор швидкості порту позбавляє від необхідності зберігати налаштування порту. Проте, можна чітко вказати параметри роботи UART порту за допомогою функції:

```
uart.setup (id, baud, databits, parity, stopbits [, echo])
```

Для читання даних з порту UART виконується реєстрація callback функції, якою як параметр передається прийняті символи. callback функція "чіпляється" на подію "data". Інших подій поки що немає. При реєстрації можна вказати, коли викликати функцію. При отриманні певної кількості символів або коли буде отримано вказаний символ, наприклад, символ кінця рядка. Коли така подія виникає, викликається функція і їй як параметр передається вся рядок, яка була прийнята.

Для уникнення проблеми з UART можна використовувати новіший модуль ESP32, але у зв’язку із тим, що платформа NodeMCU не сумісна з ним, виникає потреба власноруч будувати схожу платформу, що несе більші незручності ніж відсутність другого повноцінного UARTу.

2.3 Обґрунтування вибору програмного забезпечення серверу і бази даних

В реалізації програмної частини основне місце займає питання вибору серверу та бази даних. В цьому підрозділі розглянуті основні аргументи вибору серверу та типу бази даних. Було прийнято рішення використовувати

відносно прості рішення для тестового дослідження.

2.3.1 Обгрунтування вибору сервера. Сервер баз даних виконує обслуговування та управління базою даних та відповідає за цілісність та збереження даних, а також забезпечує операції введення-виведення при доступі клієнта до інформації.

Архітектура клієнт-сервер складається з клієнтів та серверів. Основна ідея полягає в тому, щоб розміщувати сервери на потужних машинах, а додаткам, що використовують мовні компоненти СКБД, забезпечити доступ до них з менш потужних машин-клієнтів за допомогою зовнішніх інтерфейсів.

В якості сервера баз даних для зберігання та обробки біомедичних даних отриманих з пристрою-приставки використовується MySQL. Для експерементальних досліджень треба було обрати оптимальне рішення, що містило б у собі веб-сервер та зручну систему керування базами даних. Також важливим фактором вибору серверу була вартість. Тому було вирішено використовувати для тестових досліджень XAMPP.

XAMPP — безкоштовна багатоплатформова збірка веб-сервера з відкритим початковим кодом, що містить HTTP-сервер Apache, базу данних MariaDB, MySQL й інтерпретатори скриптів для мов програмування PHP та Perl, а також додаткові бібліотеки, що дозволяють запустити повноцінний веб-сервер.

Для повноцінного промислового рішення XAMPP має ряд недоліків, тому що від самого початку він створювався як інструмент для розробників, дозволяючи веб-дизайнерам і програмістам тестувати свою роботу, не використовуючи Інтернет. Для спрощення роботи деякі можливості і налаштування безпеки відключені за замовчуванням, і в цілому XAMPP рекомендується до використання тільки в дуже дружньому оточенні. Тому для подальшого промислового використання треба буде використовувати інші платні рішення.

Повний пакет XAMPP містить:

- Web-сервер Apache с поддержкой SSL
- СУБД MySQL
- PHP
- Perl
- FTP-клиент FileZilla
- POP3/SMTP сервер
- утилиту phpMyAdmin.

XAMPP працює з усіма 32-х розрядними ОС Microsoft (98 /2000/XP/2003/Vista/7/8/8.1/10), а також з Linux, Mac OS X і Solaris. Програма вільно поширюється згідно ліцензії GNU General Public License .

2.3.2 Обґрунтування вибору бази даних. База даних (англ. database) – сукупність даних, організованих відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами; ця сукупність підтримує щонайменше одну з областей застосування (за стандартом ISO/IEC 2382:2015[**Ошибка! Источник ссылки не найден.**]).

Існують наступні види архітектури баз даних:

- Архітектура «файл-сервер»

Ця архітектура передбачає виділення однієї з машин мережі як головної (сервер). На такій машині зберігається спільна централізована БД. Усі інші машини мережі виконують функції робочих станцій, за допомогою яких підтримується доступ користувацької системи до бази даних. Файли бази даних відповідно до призначених для користувача запитів передаються на робочі станції, де в основному і проводиться обробка даних. При великій інтенсивності доступу до одних і тих же даних продуктивність інформаційної системи різко падає.

- Архітектура «клієнт-сервер»

Ця архітектура передбачає, що в мережі розміщується сервер баз даних. Ним виступає комп'ютер (або комп'ютери), який містить бази даних, СКБД та

пов'язане з ними програмне забезпечення, і налаштований для надання користувачам інформаційної системи доступу до бази даних. Клієнти, які працюють із даними (вони можуть бути розташовані на різних комп'ютерах мережі), надсилають відповідні запити серверу. Сервер їх отримує, опрацьовує, та надсилає відповідь клієнту.

За моделлю організації даних розрізняють наступні бази даних:

- Ієрархічна. Може бути представлена у вигляді дерева, що складається з об'єктів різних рівнів. Між об'єктами існують зв'язки типу «предок-нащадок».
- Мережна. Така база даних подібна до ієрархічної, за винятком того, що кожен об'єкт може мати більше одного предка.
- Реляційна. Ця база даних зберігає дані у вигляді таблиць.
- Об'єктно-орієнтована. У цій базі даних дані оформлюють у вигляді моделей об'єктів.

Виходячи із вищенаведених характеристик баз даних було прийнято рішення використовувати реляційну систему керування базою даних з відкритим кодом MariaDB типу «клієнт-сервер».

Типом таблиць було обрано MyISAM, що має наступні характеристики

- макс. диск: 256Тб;
- повнотекстовий пошук;
- наявна реплікація;
- макс. індексів: 64;
- макс. записів: 2^{32};
- макс. довжина ключа 1000 байт;
- ключі займають місце на диску до (макс.): (key_length + 4) /0.67;
- є можливість зберігати файли даних і індексів на різних пристроях;
- кожен стовпець може мати свою систему кодування;
- максимальна сума довжин VARCHAR і CHAR: 64k.

2.4 Структура бази даних

Структура бази даних повинна бути зрозумілою і лаконічною, щоб адміністратору було легко керувати даними в ній. Оскільки ми будемо використовувати реляційну базу даних, то в її структуру будуть входити таблиці і зв'язки, що визначені зовнішніми ключами. Також потрібно врахувати вимоги захисту особистої медичної інформації пацієнтів та типи доступів різних користувачів, що ускладнить структуру бази даних.

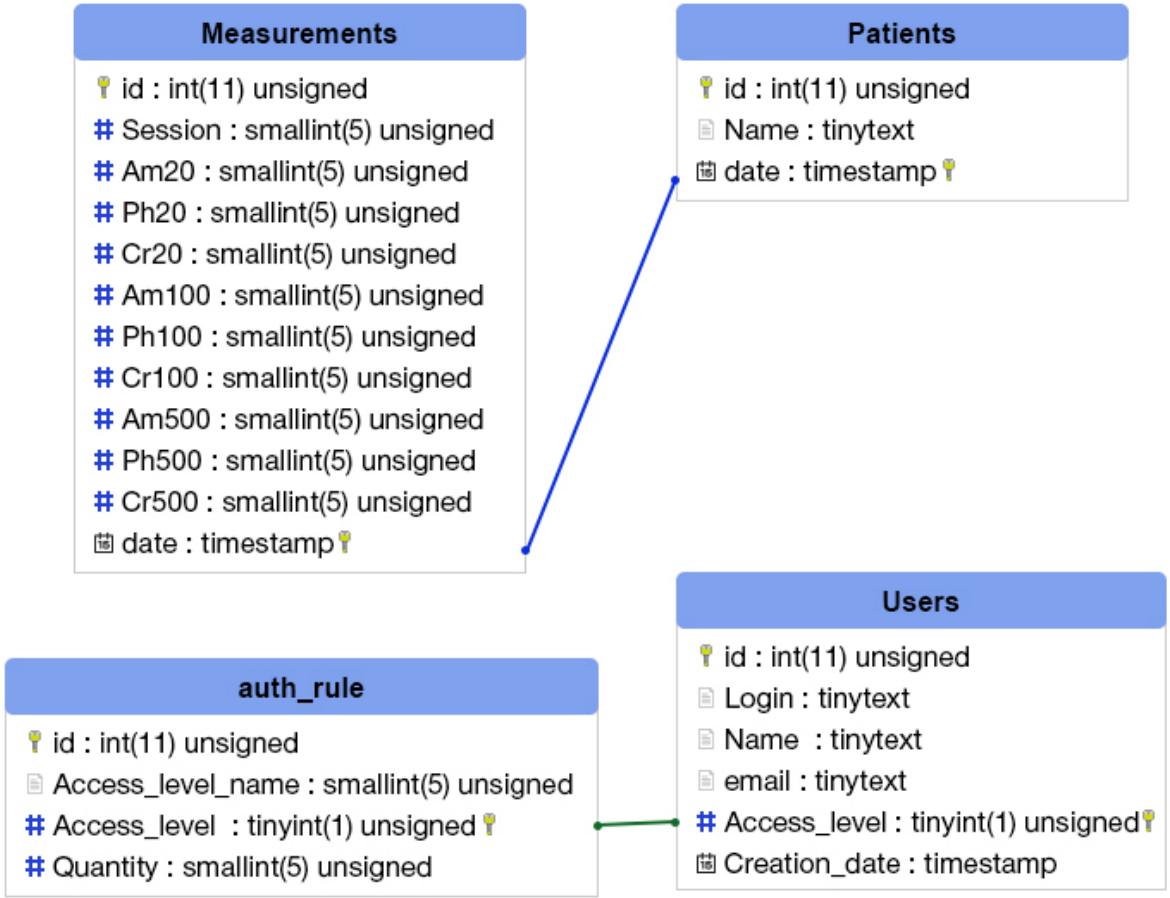

Рис. 2.4 – Загальна структура бази даних

2.4.1 Структура таблиць бази даних. Розглянемо випадок коли з вимірювача біоімпендансу в хмару передаються вже числові значення вимірів (рис.2.4). Тоді в таблицю вимірувань *Measurements* будемо записувати унікальний ідентифікаційний номер *id*, номер сесії *Session*, значення амплітуди та фази біоімпедансу та струму на трьох частотах – 20, 100 та 500 кГц, відповідно *Am20, Ph20, Cr20, Am100, Ph100, Cr100, Am500, Ph500, Cr500* та. дату запису вимірювання *date*. Таким чином, в цій таблиці буде 12 стовпців (таблиця 2.1).

Розглянемо більш детально структуру таблиці у розрізі типів даних, ключів та інших властивостей. Для числових полів стовпця *id* обрано тип даних int, що для натуральних чисел має максимальне числове значення 4294967295, з атрибутом unsigned та з функцією автоінкременту. Поле *id* має індекс unique. Для числових полів стовпців *Session, Am20, Ph20, Cr20, Am100, Ph100, Cr100, Am500, Ph500, Cr500* обрано тип даних smallint, так як ці значення чотиризначні, а цей тип має максимальне значення для натуральних чисел 65535, з атрибутом unsigned. Поля стовпця *Date*, у яких буде зберігатись дата, мають тип даних datatime, за замовченням поле має властивість current_timestamp та індекс unique.

Таблиця 2.1 Приклад таблиці *Measurements*

Id	Session	Am20	Ph20	Cr20	Am100	Ph100	Cr100	Am500	Ph500	Cr500	Date
1	0001	2638	0887	0005	2348	0887	0000	2150	0887	0000	2017-05-30 10:45

Через вимоги конфіденційності потрібно зберігати особисті дані пацієнтів в іншій таблиці. Тому було створено таблицю *Patients*. Вона має стовпці *id* – унікальний ідентифікаційний номер, *name* – ім’я та прізвище пацієнта, *date* – дата запису вимірювання. Також в перспективі можна буде розширити таблицю іншими даними пацієнтів. Таким чином, в цій таблиці буде 3 стовпця (таблиця 2.2).

Таблиця 2.4.2 Приклад таблиці *Patients*

Id	Name	Date
1	Anton Reznichenko	2017-05-30 10:45

В цій таблиці поля *id,* та *date* мають ті самі параметри, що і в таблиці *Measurements*. Текстові поля стовпця *name* мають тип даних tinytext, який має максимальну довжину 255 символів, що є достатнім для того, щоб помістилося ім’я та прізвище пацієнта. Також тип tinytext, а не, наприклад, char, був обраний тому, що довжина в байтах рядка типу char буде 255•K+1, а довжина в байтах рядка типу tinytext буде L•K+1 де L – кількість символів в рядку, K – байт на символ. Тобто чим коротшим буде рядок типу tinytext, тим менше він буде займати місця на жорсткому диску сервера.

Крім таблиць безпосередньо пов’язаних із біомедичними даними у базі даних також присутні таблиці з інформацією про користувачів системи та їх рівні доступу до інформації та керування системою.

Таблиця рівнів користувачів системи *auth_rule* має чотири стовпці(таблиця 2.3): *id* – унікальний порядковий номер, *access_level_name* – назва рівня доступу користувача, *access_ level* – рівень доступу, *quantity* – кількість користувачів кожного рівня . Комірки стовпця *id* мають такий самий тип даних, що і в таблиці *Measurements.* Поля стовпця *access_level_name* мають тип даних tinytext, а *access_level* – tinyint unsigned. Поля стовпця *quantity* мають тип даних smallint unsigned. Стовпець *access_level* має властивість Primary Key та значення комірок цього стовпця повинні бути унікальними.

Табл. 2.3 – Приклад таблиці *auth_rule*

Id	Access_level_name	Access_level	Quantity
1	Admin	1	2
2	Analyst	2	3
3	Doctor	3	10

4	Viewer	4	5

На першому етапі база даних буде мати чотири рівня доступу. Розглянемо усі рівні більш детально:

- Admin – рівень повного доступу до всіх дій системи. Кількість адміністраторів повинна бути якомога меншою. Це потрібно для того, щоб зменшити ймовірність помилкового впливу людського фактору в роботу системи.
- Analyst – рівень доступу тільки до зчитування даних медичних досліджень. Аналітик не має доступу ні до запису, видалення біомедичних даних ні до особистих конфіденційних даних пацієнтів.
- Doctor – рівень доступу тільки до запису біомедичних даних пацієнтів, особистих даних пацієнтів, а також до WEB-додатку для візуалізації даних.
- Viewer – найобмеженіший рівень доступу в системі. Користувач з таким типом доступу скоріш за все – пацієнт, дані якого використовуються в системі. Цей користувач має доступ тільки до своїх візуалізованих, у вигляді таблиць чи графіків, даних.

Таке розділення рівнів доступів зумовлений вимогами до конфіденційності та безпеки особистих біомедичних даних пацієнтів.

Розглянемо структуру таблиці користувачів *Users* (рис.2.4). Таблиця має наступні стовпці: *id* – унікальний порядковий номер, *login* – унікальне ім'я користувача в системі, *Name* – реальне ім’я користувача, *emal* – електронна адреса користувача, *access_ level* – рівень доступу користувача, *creation_date* – дата створення користувача.

Поля стовпців *login, Name* та *email* мають тип даних tinytext. Поля стовпців *id* та *access_ level* мають типи даних такі як в таблиці *auth_rule*. Крім того стовпець *access_ level* має унікальний індекс, що пов’язує його з одноіменним стовпцем у таблиці *auth_rule.* Поля стовпця *creation_date* має такий самий тип даних, як і поле *date* в таблиці *Patients.*

Табл. 2.4 – Приклад таблиці *Users*

Id	Login	Name	email	Access_level	Creation_date
1	RezAV	Anton Reznichenko	rezavua@gmail.com	1	2017-05-17 05:18
2	DocVas	Vasyl Kopychuk	vaskop@i.ua	3	2017-06-17 15:20
3	Joe45	Joe Brown	joe45brown@yahoo.com	4	2017-06-19 16:00
4	Frank1	Frank Moretti	frank.moretti@gmail.com	2	2017-06-20 11:03

В подальшому, із розширенням системи з огляду на інтеграцію інших медичних діагностичних пристроїв, потрібно буде розширювати і структуру бази даних. Насамперед, потрібно буде створити інші таблиці типу *Measurements*, також потрібно буде змінити алгоритм доступів до бази даних. Треба буде ввести параметр, що пов’язував би тип доступу і тип вимірювання. Також необхідно у разі дослідження пацієнта декількома діагностичними пристроями надати йому можливість відслідковування усіх медичних показників. Подібну інтеграцію потрібно буде провести для лікарів-терапевтів, яким потрібно знати різні біомедичні показники пацієнтів. Можливо для цього потрібно буде ввести ще один тип доступу до таблиці доступів бази даних.

2.4.2 Структура зв’язків таблиць бази даних. Зв'язок працює шляхом зіставлення даних в ключових стовпцях; зазвичай це стовпці з одним і тим же ім'ям в обох таблицях. У більшості випадків зв'язок зіставляє первинний ключ однієї таблиці, що є унікальним ідентифікатором кожного рядка цієї таблиці, із записами зовнішнього ключа іншої таблиці.

Існує чотири типи зв'язків між таблицями. Тип створюваного зв'язку

залежить від того, як визначені пов'язані стовпці:

- Зв'язки «один до багатьох»
- Зв'язки «багато до одного»
- Зв'язки «багато до багатьох»
- Зв'язки «один до одного»

В нашому випадку використовується тип зв'язку «один до одного». Тому що ми пов’язуємо стовпцю *date* в двох таблицях, щоб по даті вимірювання можна було визначити такі дані пацієнта як ім’я та прізвище.

Щоб зв’язати таблиці в базі даних між собою при їх створенні повинні бути зроблені наступні налаштування. При створенні таблиці *Measurements* в налаштуваннях стовпця *date* вибрати індекс Index з назвою *measure_date* (назву обирає творець бази даних), потім при створенні таблиці *Patients* налаштуваннях стовпця *date* зробити такий самий індекс, як у попередній таблиці. Потім при написанні запитів до бази даних можна буде групувати дані вищеописаних таблиць саме за індексом *measure_date*. Наприклад якщо аналітику чи розробнику потрібно буде витягнути з бази даних ім’я пацієнта, номер сесії, та дату вимірювання, треба буде написати наступний запит:

```
SELECT m.name, p.session, p.data FROM Measurements m, Patients p
ORDER BY measure_date;
```

Схожі налаштування були зроблені у таблицях *auth_rule* та *Users* для того, щоб пов’язати між собою користувачів сервісу та їх рівні доступу.

Таким чином не дивлячись на те, що база даних вийшла не великою і розгалудженою. Вона є простою функціональною й оптимізованою з точки зору типів даних та керування нею в подальшому. Також її ресурс достатній для використання з одним пристроєм біотелеметрії. Для більшої кількості пристроїв, або цілих систем потрібно буде використовувати інші більш потужні, можливо платні, рішення.

2.5 WEB-інтерфейс

Веб-інтерфейс - це сукупність засобів, за допомогою яких користувач взаємодіє з веб-сайтом або будь-яким іншим додатком через браузер. Веб-інтерфейси набули широкого поширення в зв'язку з ростом популярності всесвітньої павутини і відповідно – розповсюдженям скрізь веб-браузерів. Одною з основних вимог до веб-інтерфейсів є їх однаковий зовнішній вигляд і однакова функціональність при роботі в різних браузерах.

Основною перевагою веб-інтерфейсів є відсутність необхідності встановлення додаткового програмного забезпечення, тому що популярні операційні системи поставляються із вже установленим браузером.

2.5.1 Фреймворк Yii2. Yii2 – об'єктно-орієнтований компонентний фреймворк, написаний на PHP і реалізуючий парадигму MVC. Yii – це універсальний фреймворк і може бути задіяний у всіх типах веб-додатків, що використовують PHP. Фреймворк має наступні особливості:

- висока продуктивність щодо інших фреймворків, написаних на PHP [35]
- парадигма Модель-Представлення-Контролер
- інтерфейси DAO і ActiveRecord для роботи з базами даних
- підтримка інтернаціоналізації
- кешування сторінок і окремих фрагментів
- перехоплення і обробка помилок
- введення та валідація форм
- аутентифікація і авторизація (RBAC і ACL)
- використання AJAX і інтеграція з jQuery, підтримка Bootstrap
- генерація базового PHP-коду для CRUD-операцій (скаффолдинг)
- підтримка тем оформлення для їх легкої зміни
- можливість підключення сторонніх бібліотек
- міграції бази даних

- автоматичне тестування
- підтримка REST

Yii випущений під новою ліцензією BSD. Це означає, що цей фреймворк можна використовувати безкоштовно для розробки як відкритих, так і пропрієтарних веб-додатків. Текст, що міститься в Офіційною документації Yii, ліцензується для громадськості відповідно до ліцензії GNU Free Documentation License (GFDL).

Були розроблені відповідні моделі зв’язку бази даних та веб-додатку.

2.5.2 Інтерфейс користувача. Інтерфейс користувача, (UI - англ. User interface) – інтерфейс, що забезпечує передачу інформації між користувачем-людиною і програмно-апаратними компонентами комп'ютерної системи (ISO / IEC / IEEE 24765-2010) [36].

Стартова сторінка сайту – вікно входу у WEB-додаток (рис 2.5). Доступ до даних з вимірювача біоімпендансу, а також керування ним стороннім особам не допускається. Тільки авторизовані користувачі з певним рівнем доступу мають доступ до будь-яких маніпуляцій та моніторингу.

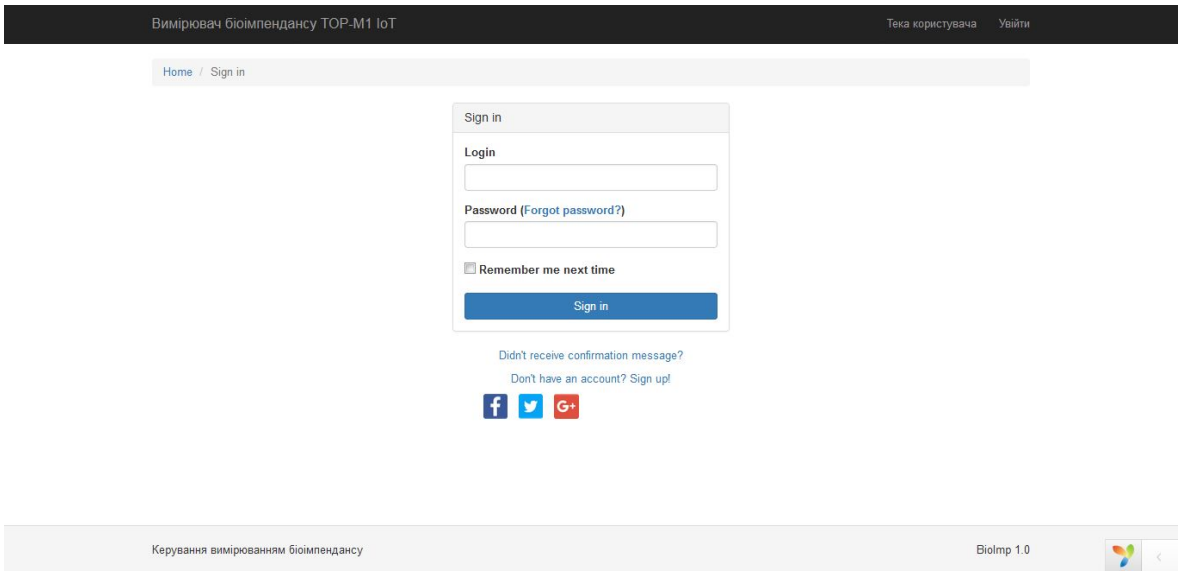

Рис. 2.5 – Сторінка входу до веб-додатку

Був розроблений веб-інтерфейс для моніторингу біопоказників пацієнтів, а саме біоімпендансу. Також є можливість спостерігати за динамікою показників кожного пацієнта. У лікаря є можливість дистанційно

ввімкнути або вимкнути запис біомедичних даних до бази даних, що передаються з вимірювача біоімпендансу. Інтерфейс кабінета користувача показаний на рис. 2.6.

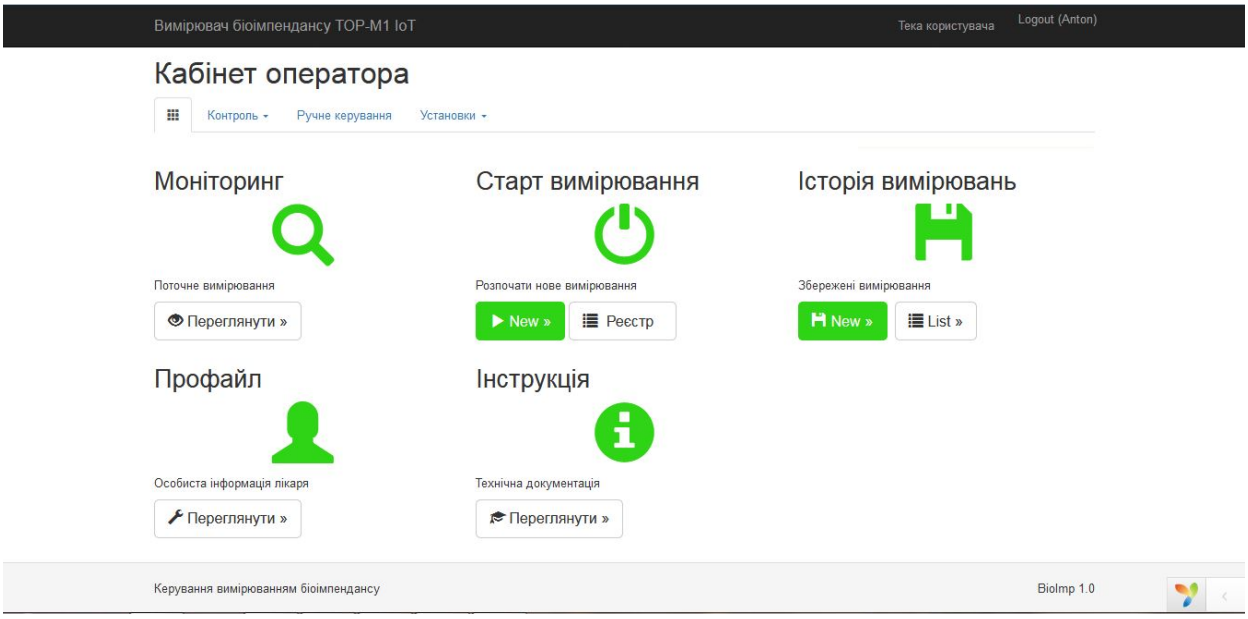

Рис. 2.6 – Сторінка кабінету лікаря-оператора

Інтерфейс сторінки результатів вимірювань також виконаний у мінімалістичному стилі (рис 2.7). Для побудови сторінки результатів вимірювання широко використовувалася мова програмування Javascript, а саме для побудови графіків виміряних показників. Для побудови графіків використовується бібліотека *plotly.js*, яка надає широкі можливості для вибору типів графіків. Також для побудови графіків даних із цією бібліотекою можна використовувати такі мови програмування, як Python, Pandas та R.

У цілому для розробки візуальної частини WEB-додатку була використана мова розмітки веб-сторінок HTML5, каскадна таблиця стилей CSS3, скриптова мова програмування Javascript, її бібліотека jQuery та клієнтський фрейворк Bootstrap 3.

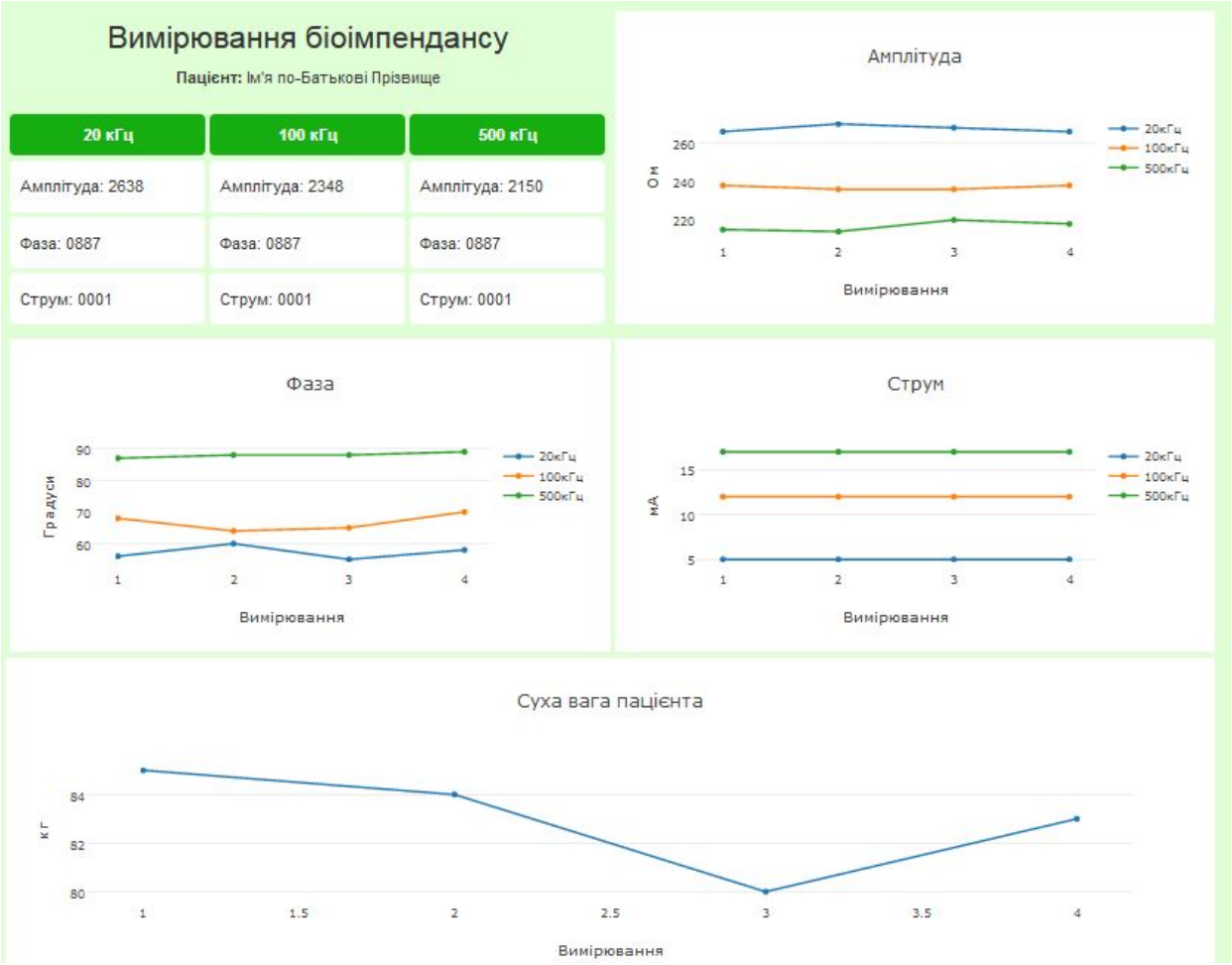

Рис. 2.7 – Сторінка результатів вимірювання

Висновки

Розробка програмної частини пристрою-приставки до вимірювача біоімпедансу стосувалася саме хмарного сервісу. Для тестового запуску розробка програмної частини охопила вибір і налаштування серверу, розробку архітектури бази даних, її безпосереднє створення, налаштування зв’язків у ній та створення веб-інтерфейсу користувача.

Для тестової роботи сервісу було прийнято рішення використовувати сервер XAMPP, але для реального продукту потрібно розробляти рішення на реальних апаратних потужностях, або, можливо, використати готове платне рішення, яких на сьогоднішній день пропонують багато кампаній.

Структура бази даних і зв’язків між таблицями у ній доволі не складна. Це добре, тому, що складність зв’язків може призвести до появи помилок при розширені та доповненні сервісу. Безумовно, база даних та структура додатку із ростом системи буде ускладнюватись, але необхідно не допустити плутанини при цьому.

WEB-інтерфейс користувача є мінімалістичним та адаптивним, що дуже добре для кросбраузерного та кросплатформенного використання цього додатку як лікарями так і пацієнтами.

При розробці програмної частини використовувались наступні технологій:

SQL – для створення бази даних і її зв’язків

HTML5, CSS3 – для створення інтерфейсу користувача

JavaScript – для створення графіків у веб-додатку

PHP – для налаштування фреймворку Yii2

РОЗДІЛ 3
ОСОБЛИВОСТІ ПЕРЕДАЧІ ТА ОБРОБЛЕННЯ ДАНИХ З ПРИСТРОЇВ-ПРИСТАВОК

Оброблення медичних даних за концепцією Інтернету Речей має характерні особливості. На першому плані стоять вимоги по приватності та конфіденційності медичних даних пацієнтів. Інколи ці вимоги навіть обмежують можливості і функції який можуть дати нові розробки. Наступними особливостями є приймання та оброблення запитів з пристроїв-приставок, а також оброблення прийнятих медичних даних вже у хмарному сервісі. Також існує питання: розробляти функціонал для оброблення медичних сигналів, чи використовувати існуючі готові напрацювання у вигляді API?

3.1 Вимоги до приватності та конфіденційності даних пацієнтів

Переваги впровадження мережевих технологій в сфері охорони здоров'я зачіпають чотири взаємопересічні області ризику, включаючи аварійний вихід пристроїв з ладу, як фактор, що знижує довіру до систем. У разі виникнення серйозних збоїв громадськість може заперечувати проти використання мережевих технологій в медицині, що відстрочить їх впровадження на роки і десятиліття. Другим за важливістю завданням є захист конфіденційної інформації про особу і здоров'я пацієнта, оскільки в середовищі хакерів медичні відомості вважаються особливо цінними. У проведеному компанією PricewaterhouseCoopers (PwC) опитуванні про глобальний стан інформаційної безпеки в 2015 році (Global State of Information SecURLty Survey 2015) відзначається, що, згідно з даними органів фінансування охорони здоров'я та постачальників медичних послуг, число збоїв у безпеці в 2014 році зросла на 60%, що майже вдвічі перевищує приріст в інших галузях [24].

Нові технології, такі як електронна медична документація та медичні

пристрої, мобільні і Web-додатки, дозволяють лікарям покращувати стан здоров'я пацієнтів і рятувати життя. Лікарям ці технології дозволяють збирати більше інформації для вивчення історій хвороби пацієнтів. Ці технології і пов'язані з ними дані постійно взаємодіють, обмінюючись інформацією про здоров'я за допомогою все більш складних систем, що збільшує ризики і уразливості. Сьогодні не лише лікарі відповідають за збереження медичних даних пацієнтів, особи, що керують зберіганням даних, також несуть відповідальність за її збереження.

Усвідомлюючи вразливість інформації про здоров'я, уряд США прийняв закони Health Information Portability and Accountability Act (HIPAA) в 1996 році і Health Information Technology for Economic and Clinical Health (HITECH) Act в 2003 році. Ці закони вимагають від організацій, що мають справу з інформацією про здоров'я, виконання певних заходів щодо забезпечення конфіденційності і безпеки, а також інформування пацієнтів в разі, коли конфіденційність і безпека їх особистих даних знаходиться під загрозою.

В умовах, коли споживачі переходять на хмарні сервіси і повідомляють конфіденційні подробиці про своє здоров'я, розуміння цих стандартів і вимога суворого їх дотримання стає основою відповідальної поведінки організації і довіри пацієнтів.

3.1.1 Дотримання рекомендацій HIPAA у разі зберігання даних у хмарному сервісі. Перенесення даних в хмару призводить до ряду проблем, які ускладнюють дотримання HIPAA медичними організаціями, бізнес-партнерами і самими постачальниками хмарних сервісів. Це проблеми контролю, доступу, доступності, загальних багатокористувацьких середовищ, готовності до інцидентів і реагування на них, а також захисту даних. Хоча зберігання приватної електронної медичної інформації в хмарі має багато переваг, споживачі і постачальники хмарних сервісів повинні знати, як кожна з цих проблем впливає на дотримання вимог рекомендацій HIPAA і HITECH. Рекомендації HITECH стосуються зберігання, обміну та обробки саме EPHI,

на відміну від HIPPA які стосуються використання медичних даних в усіх можливих середовищах.

3.1.1 Контроль над даними. Доручаючи постачальникам хмарних сервісів зберігання своїх даних, споживачі відмовляються від прямого контролю над цими даними, починаючи з рівня додатків. Таким чином передбачається делегування контролю над приватними даними електронної медичної інформації. Щоб зрозуміти, як будуть дотримуватися вимоги, необхідно знати, хто має контроль над даними і несе за них відповідальність. Внаслідок змін у контролі над даними, що виникають у разі перенесення персональних медичних даних до хмарного сервісу, споживачі і постачальники хмарних сервісів повинні укласти договір (до початку надання послуг), зокрема з визначенням сторони, що бере відповідальність за конфіденційність і безпеку даних на себе.

3.1.2 Рівні контролі різних моделей хмарних сервісів. Моделі рівнів сервісу хмарних обчислень таких як програмне забезпечення як сервіс (SaaS), платформа як сервіс (PaaS) і інфраструктура як сервіс (IaaS)) надають споживачам різні рівні контролю, найчастіше пропонують відповідний компроміс в безпеці. Споживачі і постачальники повинні знайти баланс для своїх організацій і визначити ризик, який вони готові взяти на себе, втрачаючи контроль над даними. Жодна з цих моделей не надає споживачам контроль над базовою хмарною інфраструктурою, але споживачі мають більший контроль над інфраструктурою у разі використання IaaS і менший контроль у разі використання PaaS і SaaS. Залишається невирішеним питання: якщо угода укладається на рівні додатку або інфраструктури, передається відповідальність за дані постачальнику хмари частково або в повному обсязі? З точки зору виконання вимог рекомендацій HIPAA і HITECH той, хто має контроль над EPHI, бере на себе підвищену відповідальність за безпеку доступу, моніторинг витоків, аудит, управління ризиками і т.д. [25,25].

3.2 Приймання та оброблення запитів до хмарного сервісу з пристроїв біотелеметрії

Сучасні веб-ресурси не просто надають інформацію відвідувачу, але і взаємодіють з ним. Для взаємодії з користувачем потрібно отримувати деяку інформацію від нього. Для отримання даних поширені методи GET і POST. В PHP є підтримка цих методів передачі даних GET і POST. Розглянемо детальніше, як працюють ці методи.

Дані методом GET передаються шляхом їх додавання до URL-адреси. Часто можна зустріти в браузері довгі і незрозумілі URL адреси. Наприклад: function.php?Login=Name&email=poshta. В даному випадку дані обробляються у function.php. Після знаку питання «?» йде перерахування переданих параметрів (параметри розділяються знаком «&») зі значеннями: параметру login присвоєно значення *Name*, а змінної email значення *poshta*.

Дані будуть зберігається в суперглобальному масиві $_GET. Приклад використання методу GET представлений нижче:

```
<html>
<body>
<form method="GET">
Login: <input type="text" name="login">
E-mail: <input type="text" name="email">
<input type="submit" value="Send">
</form>
<?php
echo "<br/>login = ". $_GET['login'];
echo "<br/>email = ". $_GET['email']; ?>
</body>
</html>
```

В результаті виконання цього коду до URL додається ?login=Name&email=poshta.

Метод POST призначений для відправки запиту нової сутності на сервер, так що вона буде зберігатися як підресурс ресурсу, ідентифікованого URL. Наприклад, для URL http://pryklad.com/clients за допомогою методу POST запитів можна додавати нових клієнтів, кожен з яких містить ім'я, адресу та контактні дані. Розробники сайтів відійшли від такої концепції з двох причин. Остання частина URL більш ймовірно опише сторінку обробки веб-додатку та його технології, наприклад http://pryklad.com/applicationform.php. Також, з огляду на природне обмеження більшості веб-браузерів роботи тільки методами GET та POST, розробники зрозуміли необхідність додавання додаткових можливостей в метод POST, включаючи зміну існуючих записів та їх видалення.

Тобто не можна сказати, що кожна веб-форма повинна містити метод POST у відкриваючому тезі. Чимало форм використовуються для отримання інформації з серверу, без зміни основних баз даних. Для таких форм пошуку ідеально підходить метод GET.

Бувають випадки, коли HTTP GET не підходить навіть для отримання даних. Прикладом є ситуація, коли велика кількість даних повинна бути записана в URL. Браузери і веб-сервери мають обмеження на довжину URL,

які вони обробляють без помилки. URL-кодування зарезервованих символів в адресі та рядку запиту може значно збільшити довжину, в той час як HTTP-сервер Apache може обробляти до 4000 символів в URL, Microsoft Internet Explorer обмежує довжину будь-якого URL 2048 символами.

Також HTTP GET запити не повинні використовуватися дляпедавання конфіденційної інформації, такої як імена користувачів і паролі, які повинні бути представлені разом з іншими даними для завершення запиту. У разі використання протоколу з шифруванням HTTPS, історія браузера і журнали веб-сервера, ймовірно, містять повні URL адреси у вигляді відкритого тексту, що можуть бути знайдені, якщо система буде зламана. Тому у разі передавання конфіденційної інформації використовується HTTP POST.

Таким чином обидва методи успішно передають необхідну інформацію з веб-форми до скрипта, тому у разі вибору того чи іншого методу, який буде найбільш підходити хмарному сервісу, потрібно враховувати наступні фактори:

- метод GET обмежує обсяг переданої скрипту інформації;
- метод GET відправляє скрипту всю зібрану інформацію у відкритому вигляді як частину URL, що зменшує безпеку сервісу;
- метод GET генерує веб-сторінки, що будуть завжди унікальні, їх можливо помітити закладкою;
- використовуючи метод GET можна передавати дані не через веб-форму, а через URL-сторінки, ввівши необхідні значення через знак &;
- при використанні методу GET існує ризик того, що пошуковий робот може виконати той чи інший відкритий запит;
- адреса сторінки а сторінку, що згенерувалася методом POST не можна (адреса сторінки залишається незмінною, так як дані в URL-адресі не підставляються)
- метод POST дозволяє передавати запиту файли.

І з огляду та вищеописані вимоги по приватності та конфіденційності даних пацієнтів в роботі над програмним забезпеченням пристрою-приставки

до вимірювання біоімпедансу для передачі даних у хмарне середовище було прийнято використовувати метод POST. Також метод POST треба використовувати у разі передачі безпосередньо біомедичних сигналів, метод GET в даному випадку взагалі не підійде через його обмеженості.

3.3 Оброблення медичних даних з пристрою-приставки

У разі обробки даних медичних пристроїв за допомогою обчислювальних систем постає питання: у якому вигляді передавати сигнал з медичного пристрою? Можливими варіантами може бути передача первинного біомедичного сигналу або його параметрів, наприклад амплітуди та фази. Кожен з цих варіантів має свої переваги та недоліки.

Розглянемо детальніше особливості передачі безпосередньо біомедичних сигналів. Більшість біомедичних сигналів мають електричну природу. Це біопотенціали мозгу, серця, м’язів. Біомедичні сигнали, що мають іншу природу, можуть бути перетворенні в електричні. Таким чином носієм інформації біооб’єкту до пристрою обробки та аналізу цієї інформації є електричні сигнали.

Застосування комп’ютерів для обробки біомедичних сигналів відкрило нові можливості по виявленню більш тонкої структури сигналу, що сприяє більш точному діагностуванню різних захворювань. У той же час існуючі методи обробки біомедичних сигналів за допомогою ком’ютерів часто є просто автоматизацією давно відомих «ручних» методів.

Біомедичні сигнали, як правило, змінюються у часі і за амплітудою неперервно, тобто є так званими аналоговими сигналами. Після обробки біомедичних сигналів засобами цифрової обчислювальної техніки інформація, що міститься в них повинна бути представлена хмарному сервісу. Людина (оператор, аналітик) краще сприймає візуально оформлену інформацію у вигляді графіків та таблиць. Тому необхідно робити зворотне перетворення сигналу з цифрового виду у неперервний, наприклад, будувати графіки у хмарному сервісі. Для цього спочатку цифровий сигнал за

допомогою ЦАП перетворюється у дискретний (імпульсний) сигнал, а потім з дискретного сигналу отримують неперервний сигнал. Перетворення дискретного сигналу в неперервний здійснюють за допомогою операцій інтерполяції або фільтрації. Фільтрація також використовується при нормалізації сигналів для підвищення відношення сигнал/шум.

Оскільки більшість біомедичних сигналів мають виражену періодичність, для вивчення загальних питань перетворення та обробки таких сигналів треба розглядати спектральне представлення періодичних сигналів в різних базисах.

Ціль обробки біомедичних сигналів – виявлення інформативних параметрів, зо характеризують функціональний стан контролюючих систем організму, запам’ятовування цих параметрів і представлення їх у вигляді, зручному для сприйняття, аналізу і прийняття рішення споживачем (лікуючим лікарем, діагностуючим лікарем).

Існуючі методи обробки сигналів: спектральні, кореляційні, структурні, згорткові, інформаційно-аналітичні, вейвлетні та ін. мають свої особливості як у використанні, так і по одержуваних результатах, що часто самі по собі потребують додаткового аналізу і оцінки.

Для обробки біомедичних сигналів у якості спрощеного варіанту можна використовувати готові API різних спеціалізованих обчислювальних засобів та систем, наприклад Mathematica [31].

Метод передачі та обробки безпосередньо біомедичного сигналу має наступні переваги:

- можливість діагностики та дослідження додаткових параметрів сигналів;
- більша точність дослідження та діагностики;
- простіша конфігурація медичного пристрою.

Недоліки:

- вищі вимоги до об’єму бази даних;
- вищі вимоги до обчислювальної спроможності серверу;

- ймовірність помилки при накопиченні та аналізу додаткових параметрів сигналу.

У разі приймання параметрів біомедичних сигналів вся обробка та перетворення сигналу відбувається в самому біотелеметричному пристрої.

Метод передачі та обробки вже числових значень показників біомедичного сигналу має наступні переваги:

- менші вимоги до об’єму бази даних та серверу;

Недоліки:

- у випадку помилки чи виходу з ладу системи, що перетворює сигнал у числові значення неможливо швидко наладити роботу усієї системи;
- неможливість діагностики та дослідження додаткових параметрів сигналів;
- додаткова система в медичному пристрої.

3.4 Розподіленні обчислення через API спеціалізованих обчислювальних платформ.

У якості прикладу використання спеціалізованої обчислювальної платформи як через API так і використовуючі готові IoT-рішення розглянемо платформу Mathematica.

В системі Mathematica 9 додана обробка і аналіз сигналів нового покоління, повністю інтегровані з великої підтримкою алгебраїчних операцій, безперервного і дискретного обчислення в системі Mathematica. Серед нових можливостей – функції з розрахунку аналогових і цифрових фільтрів, функції обробки сигналів, які можна використовувати з аудіо, зображеннями та іншими даними, а також нові функції візуалізації і дискретні перетворення. Також система Mathematica має спеціальні хмарні сервіси, які налаштовуються індивідуально під потреби користувача. Так приймаючи медичні дані на хмарний сервіс від Mathematica ми маємо можливість застосовувати складний символьний і цифровий аналіз, робити

візуалізацію (рис. 3.1) та створювати інтерактивні звіти. Це все можна робити в одній системі з одним інтегрованим робочим процесом.

Рішення bioinformatics Wolfram легко інтегрують спеціалізовані можливості, такі як вбудовані обчислювальні дані геному та білку та вирівнювання послідовностей, забезпечуючи при цьому максимально автоматизоване та надійне середовище для обчислювань, розробки та розгортання.

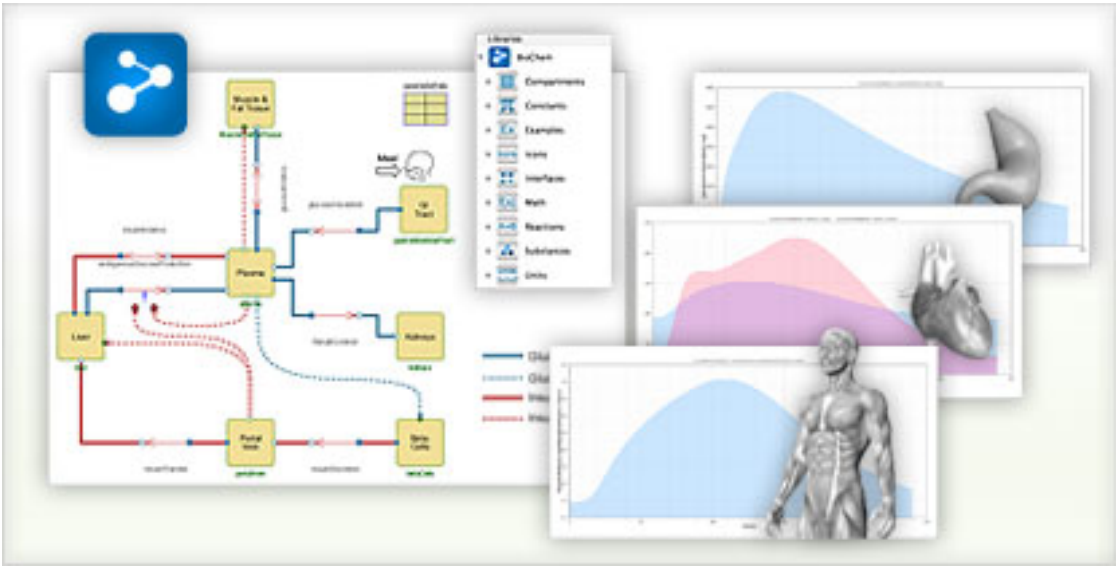

Рис. 3.1 – Аналіз процесів в глюкозно-інсулінній системі за допомогою Wolfram SystemModeler[31]

Wolfram Cloud по суті робить кожен аспект хмарних операцій програмованим, вносячи безпрецедентний рівень інтеграції, гнучкості, простоти і можливостей в нове покоління хмарних технологій. Обчислювальні можливості та програмні рішення Wolfram вже використовуються такими гігантами медичної індустрії як Abbot, Bayer, Amgen та ін.[31].

Головною особливістю і, в деяких випадках, недоліком програмного рішення Wolfram є використання спеціально розробленої мови програмування Wolfram. Перевагою цієї мови є її «математичність» – наявність великої кількості вбудованих математичних операторів та бібліотек. Недоліком є складність інтеграції рішень від Wolfram з іншими готовими хмарними сервісами. Також недоліком для деяких рішень є

небезкоштовність більшості програмних продуктів Wolfram Mathematica, але є обмежені у часі використання trial-версії. Скористувавшись trial-версією можна зрозуміти функціонал того чи іншого рішення.

3.5 Можливість впровадження та використання загального формату даних для біомедичних сигналів

Загальний формат даних для біомедичних сигналів (General Data Format for Biomedical Signals, GDF) – це науковий та медичний формат файлу. Метою GDF є об'єднання та інтегрування кращих рис всіх форматів файлів для зберігання біомедичних сигналів в одному форматі – GDF [32].

Первісна специфікація GDF була представлена в 2005 році як новий формат даних з метою подолання деяких обмежень популярного європейського формату даних для біомедичних сигналів (EDF). GDF був також розроблений, щоб об'єднати безліч форматів файлів, які були призначені для дуже специфічних застосувань (наприклад, окремо для ЕКГ і окремо для ЕЕГ). Первісна специфікація GDF версії 1.0 має бінарний заголовок і використовує таблицю подій, тобто дозволяє розмічати дані всередині файлу. Оновлена специфікація GDF була випущена в 2011 році, в якій були додані поля для додаткових відомостей про суб'єкта (стать, вік, та ін.), а також можливість зберігання даних по кожному відведенню (частоту семплювання, налаштування фільтрів і т.д.).

GDF часто використовується в проектах і дослідженнях розробок інтерфейсів мозок-комп'ютер. Однак, оскільки GDF забезпечує розширений набір функцій у порівнянні з іншими стандартами, він також може бути використаний у багатьох інших областях

Вільна поширювана бібліотека BioSig реалізує читання і запис даних в GDF для GNU Octave/MATLAB і C/C++ [33].

Незважаючи на всі переваги GDF, він не може бути зручним для всіх застосувань через бінарний формат зберігання. Цю задачу намагається вирішити розширений формат даних, що розробляється в даний час –

Extensible Data Format (XDF) з метою надання гнучкого формату для всіх видів даних, але в більшій мірі для біомедичних сигналів. Станом на 2015 рік, XDF знаходиться має статус бета-версії [34].

РОЗДІЛ 4.
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Основною метою даного розділу дипломної роботи є визначення потенційно небезпечних та шкідливих виробничих факторів, які пов’язані з проектуванням, виготовленням та експлуатацією пристрою-приставки до вимірювача біоімпендансу. Необхідно перевірити відповідність цих факторів вимогам санітарних норм та електробезпеки і запропонувати відповідні технічні рішення та організаційні заходи щодо зменшення або повного усунення їх впливу на робочий персонал і навколишнє середовище. Також необхідно розглянути питання безпеки в надзвичайних ситуаціях. При проектуванні пристрою-приставки передбачається виконання усіх вимог ГОСТ 12.1006-84 та ДСНІП №476 і ДСНІП №239 щодо захисту від негативних дій ЕВМ.

4.1 Визначення основних потенційних шкідливих та небезпечних факторів при виконанні науково-дослідних робіт.

Оброблення сигналів проводиться за допомогою персонального комп’ютера (ПК). При роботі на ПК людина піддається впливу іонізуючого, інфрачервоного й ультрафіолетового випромінювань екрана монітора, рівні яких повинні відповідати вимогам ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з ВДТ ПЕОМ».

При проведенні повного циклу робіт з проектування потенційно – небезпечними та шкідливими факторами можуть бути:

- можливість ураження електричним струмом;
- електростатичне поле, В ДТ ПЕОМ;

- механічні шуми, які пов’язані з роботою принтера і вентиляційної системи комп’ютера;
- значна напруга зорових органів і пов’язане з цим перевтомлення користувача ПЕОМ;
- значне навантаження на пальці і кисті рук, що при відсутності профілактики і медичного контролю, може викликати професійні захворювання,
- тривале перебування в одному й тому ж самому положенні сидячи, що викликає застійні явища в організмі людини;
- наявність іонізуючого рентгенівського випромінювання (НРВ) ВДТПЕО;
- випромінювання оптичного діапазону (ультрафіолетове, інфрачервоне і випромінювання видимого діапазону) ВДТПЕО;
- відблиски на екрані монітора.

Розглянемо вплив цих факторів детальніше.

4.2 Технічні рішення та організаційні заходи з безпеки і гігієни праці та виробничої санітарії.

4.2.1 Організація робочих місць користувачів ВДТ ПЕОМ

ДСанПіН 3.3.2.007-98 "Державні санітарні норми і правила роботи з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин" встановлює норми щодо забезпечення охорони праці користувачів ПК. Дотримання вимог цих правил може значно знизити наслідки несприятливої дії на працівників шкідливих та небезпечних факторів, які супроводжують роботу з відеодисплейними матеріалами, зокрема можливість зорових, нервово-емоційних переживань, серцево-судинних захворювань.

Для того щоб забезпечити точне та швидке зчитування інформації в зоні найкращого бачення, площина екрана монітора виставлена перпендикулярно нормальній лінії зору. При цьому передбачена можливість переміщення монітора навколо вертикальної осі в межах ±30° (справа наліво) та нахилу вперед до 85° і назад до 105° з фіксацією в цьому положенні. Клавіатура розміщена на поверхні столу на відстані 100…300 мм від краю. Кут нахилу клавіатури до столу обрано в межах від 5° до 15° так, що зап'ястя на долонях рук розташовуються горизонтально до площини столу. Таке положення клавіатури зручне для праці обома руками.

Робочі місця з ПК розташовано відносно від стіни з вікнами на відстані не менше 1,5 м, від інших стін — на відстані 1 м, відстань між собою - не менше ніж 1,5 м. Причому так, щоб природне світло падало збоку, переважно зліва. Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски з поверхні екранів ПК передбачені сонцезахисні жалюзі.

Штучне освітлення робочого місця, обладнаного ПК, здійснюється системою загального рівномірного освітлення. Як джерело штучного освітлення мають застосовуватись люмінесцентні лампи ЛБ.

Вимоги до освітлення приміщень та робочих місць під час роботи з ПК:

- освітленість на робочому місці повинна відповідати характеру зорової роботи, який визначається трьома параметрами: об'єктом розрізнення - найменшим розміром об'єкта, що розглядається на моніторі ПК; фоном, який характеризується коефіцієнтом відбиття; контрастом об'єкта і фону;
- необхідно забезпечити достатньо рівномірне розподілення яскравості на робочій поверхні монітора, а також в межах навколишнього простору;
- на робочій поверхні повинні бути відсутні різкі тіні;
- в полі зору не повинно бути відблисків (підвищеної яскравості поверхонь, які світяться та викликають осліплення);
- величина освітленості повинна бути постійною під час роботи;

Тривалість регламентованих перерв під час роботи з ЕОМ становить 10 хвилин через кожну годину роботи .

Для зниження нервово-емоційного напруження, втомленості зорового аналізатора, для поліпшення мозкового кровообігу і запобігання втомі доцільно деякі перерви використовувати для виконання комплексу вправ, які передбачені ДСанПіН 3.3.2.007-98.

4.2.2 Санітарні норми приміщення

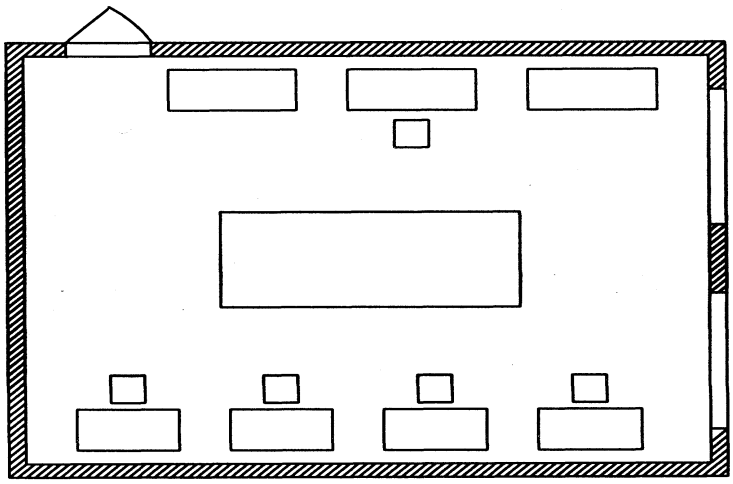

Рис 4.1 – План приміщення лабораторії.

Приміщення лабораторії має форму паралелепіпеда з наступними параметрами: висота - 3,5 м , ширина – 8 м, довжина - 6 м і розділена шафою-перегородкою на дві частини: конструкторську і технологічну (рис 4.1).

У лабораторії може працювати одночасно 5 чоловік. Меблі в лабораторії розставлені таким чином, щоб ширина проходів між робочими місцями була не менш 1 метра, і ці проходи були постійно вільні.

Загальна площа лабораторії, займана шафами:

S1 = 5 м2, а відповідний об’єм: V1 = 10 м3.

Сумарна площа, займана столами, включаючи стелажі з полками і стільців складає :

S2 = (1,2 • 0,6) • 4 + (1,5 • 0,6) • 3+(0,4•0,4)•5 = 6,38 м2,

займаний ними об’єм складає:

V2 = (1,2 • 0,6) • 4 • 0,75 + (1,5 • 0,6) • 3 • 0,75+(0,4•0,4)•5•0,45 =

= 2,16 + 2,025+0,36 = 4,544 м3

Тоді загальний об’єм і площа меблів, що знаходяться в лабораторії, буде:

Sзаг. = S1 + S2 = 5 + 6,38 = 11,38 м2;

Vзаг.= V1 + V2 = 10 +4,544 = 14,544 м3.

Об’єм і площа вільного простору, що приходиться на одного робітника в лабораторії:

Sна1. = (Sпов. – Sзаг.) / 5 = (6 • 8 - 11,38) / 5 = 7,324 м2;

Vна1. = (Vна1 – Vзаг.) / 5 = (6 • 8 • 3,5 – 14,544) / 5 = 30,691 м3.

У досліджувальному приміщенні здійснюється проектування, розрахунок, зборка і передексплуатаційна перевірка пристроїв промислової електроніки. По основних параметрах досліджуване приміщення відповідає санітарнотехнічним нормам СН245-82, що приведені в таблиці 4.1

Таблиця 4.1

Нормована величина	Приміщення без обчислювальної техніки	Приміщення з обчислювальною технікою
Площа лабораторного приміщення на 1 чоловіка	≥4,5м^2	≥6, 3м^2
Об’єм приміщення лабораторії на 1 чоловіка	≥15м^3	≥19м^3
Висота приміщення від підлоги до виступаючих поверхонь перекриття	2,8 м	

4.2.3 Мікроклімат у лабораторії

Відповідно до ДСН 3.3.6.042-99 установлені параметри виробничого мікроклімату, дотримання, яких забезпечує нормальні умови праці персоналу.

Роботу, виконувану інженерами в процесі розробки, налагодження і зборки даного пристрою, можна віднести до категорії 1а - легкі фізичні роботи (роботи, виконувані сидячи і не потребуючі фізичного напруги), при яких енерговитрати людини не перевищують 138 Вт (до 120 ккал/ч).

Для підтримки оптимальних умов праці лабораторія обладнана кондиціонером, що підтримує наступні параметри повітря робочої зони:

• температура повітря Т °З = 22°С;

• відносна вологість повітря Q = 60 %.

Контрольні виміри відносної вологості і температури повітря проводились в теплий і холодний час року, а також проводились виміри швидкості руху повітря в лабораторії. Мікроклімат у приміщенні лабораторії залежить від температури повітря навколишнього середовища, потужності джерел тепловиділяючих і теплопоглинальних, котрі знаходяться в приміщенні. Дані вимірів зведені в таблицю 4.2.

Таблиця 4.2 Мікролімат в лабораторії.

Період року	Категорія праці	Температура °С	Відносна вологість, %	Швидкість руху повітря, м/с
		Оптм.	Оптм.	Оптм.
Холодний і перехідний	Легка 1а	22-24	40-60	0,1
Вимірювання	Легка 1а	12-14	65-68	0,1
Теплий	Легка 1а	23-25	40-60	0,1
Вимірювання		24-26	60	0,15

З таблиці 4.2 видно, що в лабораторії всі параметри мікроклімату знаходяться в припустимих межах, крім температури повітря в холодний час року. Для того, щоб підвищити температуру і забезпечити оптимальні умови праці були проведені ряд заходів: утеплення вхідних дверей і віконних прорізів, а також у лабораторію був поставлений масляний електрообігрівач, що автоматично підтримує температуру повітря в лабораторії +22 °С.

4.2.4 Склад повітряного середовища

Періодично в лабораторії проводиться пайка для електричного контакту електронних компонентів. Для цих цілей використовується олов'яно-свинцевий припій ”ПОС 61”, а також рідкий каніфольно-спиртовий флюс, що не містить кислот. Для знежирення контактів, що спаюються, і видалення залишків флюсу, використовується етиловий спирт. У процесі пайки припій і флюс виділяють шкідливі для організму людини пари, ГДК який встановлений ГОСТ 12.1.005-88.

При проведенні санітарно-гігієнічної перевірки були встановлені наступні концентрації шкідливих речовин у робочій зоні (табл. 4.3):

Таблиця 4.3

Найменування речовин	Клас небезпеки	Кількість речовини, що знаходиться в повітрі, мг/м^3	ПДК, мг/м^3
Олово	3	5	10
Свинець	1	0,008	0,01
Спирт етиловий	4	150	>10

Як видно з таблиці 4.3 концентрація етилового спирту перевищує ПДК, тому робочі місця, де здійснюється пайка, обладнані витяжкою, що включається під час пайки і виключається за10 хв після закінчення пайки.

У лабораторії використовується природна і механічна вентиляція. Природна вентиляція здійснюється через відкриті кватирки під дією градієнта температур повітря лабораторії і зовнішнього повітря. Примусова вентиляція здійснюється вбудованим у віконний проріз, кондиціонером і двома витяжками, установленими над робочими місцями, де здійснюється пайка.

4.2.5 Електробезпека

Лабораторія, у якій відбуваються роботи з монтажу і налагодження пристрою, згідно з ПУЕ відносяться, по небезпеці поразки персоналу електричним струмом – до приміщень без підвищеної й особливої небезпеки.

При нормальному (неаварійному) режимі роботи пристрою , що розглядається в даному дипломному проекті, гранично припустимі рівні напруг дотику і струмів приведені в таблиці 4.5. (ГОСТ 12.1.038-88 ССБТ).

Таблиця 4.5 Норми напруг дотику і струмів у неаварійному режимі.

№ п/п	Рід струму	U, В	I, мА
1	Змінний 50 Гц, не більш	2	0,3
2	Постійний, не більш	8	1

При виникненні аварійного режиму, напруги і струми, що протікають через людину не повинні перевищувати значень представлених у таблиці 4.6.

Таблиця 4.6

Струм	Нормо-вана вели-чина	Гранично допустимі струми, мА, і напруги, В, при тривалості дії, с											
		0,01-0,08	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1	більше 1
Змінний 50 Гц	$I_д$	650	500	250	165	125	100	85	70	65	55	50	6
	$U_д$												36
Постійний	I	650	500	500	330	250	200	170	140	130	110	100	8
	U												36
Випрямлений двохнапів-періодний	I_a	6650	5500	4400	3300	2270	2230	2220	2210	2200	1190	1180	—
	U_a												—

Лабораторія оснащена електрощитом, що має центральний рубильник і три рубильники автоматами, що роблять відключення електроживлення від кожного робочого місця окремо. Також у лабораторії маються розетки під однофазну мережу 220 В і f = 50 Гц і трифазну мережу 380 В з глухозаземленою нейтраллю та з використанням автоматів захисту струму. Кожне робоче місце має щиток, що забезпечує живлення 220 В і 380 В, f = 50 Гц, а також миттєве відключення живлення автоматом.

Розрахунок вимикаючої здатності.

Сила струму, при виникненні однофазного замикання на корпус приладу рівна:

$$I_{кз} = \frac{U_ф}{R_ф + R_0 + Z_T / 3} = \frac{220}{6 + 4 + 0{,}11} = 22 \text{ А},$$

де: $R_ф$ - активний опір фазового дроту, $R_ф$ =6 Ом

R_0 - активний опір опору нуля, R_0 =4 Ом

$U_ф$ - напруга фази, яка рівна $U_ф$ =220 В.

Максимальне значення напруги яка появиться на корпусі при аварійному режимі, В, рівна:

$U_{max} = I_{кз} \cdot R_0 = 22 \cdot 4 = 88$ В.

U_{max} <Uдоп , при t<0,1 – Uдоп=500В, згідно з ГОСТ 12.1.038-88.

Тому швидкість спрацювання автомата повинна бути меншою 0,1 сек., а струм спрацювання повинен бути рівний із умови:

$I_{кз} > I_{сп} \geq 1{,}41\ I_{ном}$.

Безпека експлуатації електричного устаткування і захист від поразки електричним струмом забезпечується застосуванням ряду захисних мір:

- персонал, що працює з приладами повинний бути технічно грамотним;
- неприступність і робоча ізоляція струмоведучих частин;
- ремонтний персонал, що виконує ремонтні роботи в електричних установках, повинний мати електромеханічну спеціальність, і групу допуску;
- необхідна перевірка знань ТБ і інструктаж з надання першої допомоги людині, ураженому струмом.

4.3 Заходи щодо поліпшення умов праці в науково-дослідній лабораторії

На підставі проведеного аналізу можна зробити висновок про доцільність застосування заземлюючого пристрою, що дозволяє зменшити напругу дотику, як при нормальному так і при аварійному режимах роботи електрообладнання.

4.3.1 Перевірка та заземлюючого пристрою

Правила улаштування електроустановок (ПУЕ) обмежують найбільші опори заземлення, $R_Д$: при сумарній потужності генераторів або трансформаторів в мережі живлення не більше 100 кВт або 100 кВА – 10 Ом;

в інших випадках – 4 Ом;

При використанні штучного заземлення повинна виконуватись умова $R < R_Д$.

Нехай тип заземлення – вертикальний електрод – стержень довжиною 4 м і діаметром d = 0.01 м. Питомий опір ґрунту ρ - 100$Ом \cdot м$ (для суглинку). З урахуванням кліматичного коефіцієнтаФ = 2, маємо:

$$\rho_{РОЗРАХ} = \rho \cdot Ф = 200\ Ом \cdot м$$

Визначимо опір розтікання струму заземлювачів:

$$R_{1в} = \frac{\rho}{2\pi L} \cdot \left[\ln\left(\frac{2L}{d}\right) + 0.5 \cdot \ln\left(\frac{4t + L}{4t - L}\right)\right] \qquad (4.6)$$

де $\rho = 200$ Ом · м; $L = 4$ м; $d = 0{,}01$ м; $t = 4$ м.

Підставивши числові значення, маємо:

$$R_{1в} = \frac{200}{2\pi 4} \cdot \left[\ln\left(\frac{2 \cdot 4}{0{,}01}\right) + 0.5 \cdot \ln\left(\frac{4 \cdot 4 + 4}{4 \cdot 4 - 4}\right)\right] = 55{,}2\ Ом$$

Таким чином, опір штучного заземлювача більше нормованого значення, тому необхідно паралельно з'єднати декілька однотипних заземлювачів:

$$R_{зв\Sigma} = \frac{R_1}{n \cdot \eta_E}, \qquad (4.7)$$

де $\eta_E \approx 0{,}5$– коефіцієнт, що враховує взаємне екранування заземлювача; п = 20; $L/a = 1$ (а– відстань між заземлювачами), заземлювачі розташовані по контуру.

$R_{зв} = 5{,}52$ Ом

Довжина сполучної смуги:

$$L_{спол} = a \cdot n = 4 \cdot 20 = 80 \text{ м}$$

Ширина смуги 0.02м, а відстань від смуги до поверхні землі 1м. Тоді опір розтікання струму сполучної смуги:

$$R_П = \frac{\rho}{2\pi \cdot L_{спол}} \cdot \ln\left(\frac{2 \cdot L_{спол}^{\ 2}}{B_{спол} \cdot H_{спол}}\right) = \frac{200}{2\pi \cdot 80} \cdot \ln\left(\frac{2 \cdot 80^2}{0.01 \cdot 1}\right) = 5.32 \text{ Ом}$$

З урахуванням коефіцієнта використання смуг $\eta_П = 0{,}8$:

$$R_П = \frac{R_П}{\eta_П} = 6{,}65 \text{ Ом}$$

Еквівалентний опір заземлювача складається з паралельно включених $R_П$ і $R_{зв}$:

$$R_{ЕКВ} = \frac{R_П \cdot R_{зв\Sigma}}{R_П + R_{зв}} = \frac{5{,}52 \cdot 6{,}65}{5{,}52 + 6{,}65} = 3{,}1 \text{ Ом}$$

Отримане значення опору заземлювача отримали менше гранично допустимого $R_Д$.

4.4 Безпека в надзвичайних ситуаціях

Безпека в надзвичайних ситуаціях регламентується ПЛАС (ДНАОП 0.00-4.33-99). Одними з основних складових ПЛАС є розробка технічних рішень та організаційних заходів з евакуації та оповіщення виробничого персоналу і його дій у разі виникнення надзвичайної ситуації, а також вирішення питань пожежної безпеки.

4.4.1. Вимоги щодо організації ефективної роботи систем оповіщення персоналу у разі виникнення небезпечної ситуації

Оповіщення виробничого персоналу у разі виникнення НС, наприклад при пожежі, здійснюється відповідно до вимог НАПБ А.01.003-2009.

Необхідність обладнання виробничих приміщень певним типом СО визначається згідно з додатком Е до ДБН В.1.1-7-2002 "Захист від пожежі. Пожежна безпека об'єктів будівництва".

При обладнані виробничих будівель системою оповіщення, їх необхідно поділяти на зони оповіщення з урахуванням об'ємно-планувальних рішень будинків, шляхів евакуації, поділення на протипожежні відсіки тощо, а також з урахуванням вимог, що наведені в примітці 1 таблиці Е.1 додатка Е до ДБН В.1.1-7-2002.

Розміри зон оповіщення, черговість оповіщення та час початку оповіщення людей в окремих зонах визначаються, виходячи з умов забезпечення безпечної та своєчасної евакуації людей у разі виникнення НС.

Оповіщення про НС та управління евакуацією людей здійснюється одним з наступних способів або їх комбінацією:

- поданням звукових і (або) світлових сигналів в усі виробничі приміщення будівлі з постійним або тимчасовим перебуванням людей;
- трансляцією текстів про необхідність евакуації, шляхи евакуації, напрямок руху й інші дії, спрямовані на забезпечення безпеки людей;
- трансляцією спеціально розроблених текстів, спрямованих на запобігання паніці й іншим явищам, що ускладнюють евакуацію;
- розміщенням знаків безпеки на шляхах евакуації згідно з ДСТУ ISO 6309;
- ввімкненням евакуаційних знаків "Вихід";
- ввімкненням евакуаційного освітлення та світлових покажчиків напрямку евакуації;
- дистанційним відкриванням дверей евакуаційних виходів;
- зв'язком оперативного (чергового) персоналу СО (диспетчера пожежного поста) із зонами оповіщення.

Як правило, СО вмикається автоматично від сигналу про пожежу, який формується системою пожежної сигналізації або системою пожежогасіння. Також з приміщення оперативного (чергового) персоналу СО (диспетчера пожежного поста) слід передбачати можливість запуску СО вручну, що

забезпечує надійну роботу СО не тільки при пожежі, а і у разі виникнення будь-якої іншої НС. Повинен бути забезпечений розподіл пріоритетів щодо повідомлень для виробничого персоналу у такій послідовності:

I (найвищий) – повідомлення оперативного (чергового) персоналу СО (диспетчера пожежного поста) під час пожежі, або у разі виникнення будь-якої іншої НС;

II – повідомлення, які записані на будь-якому носії та вмикаються автоматично від спрацювання систем пожежної автоматики, або за сигналом оперативного (чергового) персоналу СО (диспетчера пожежного поста);

III – службові повідомлення, що не стосуються організації та управління евакуацією людей.

У разі одночасного транслювання декількох повідомлень, що мають різні пріоритети, повідомлення, які мають нижчий пріоритет, повинні автоматично блокуватись.

СО повинна мати можливість одночасно передавати різні мовленнєві повідомлення в різні зони оповіщення.

Згідно з вимогами ДБН В.1.1-7-2002 необхідно забезпечити можливість прямої трансляції мовленнєвого оповіщення та керівних команд через мікрофон для оперативного реагування в разі зміни обставин або порушення нормальних умов евакуації виробничого персоналу.

У разі виникнення пожежі у багатоповерхових виробничих будівлях, СО повинна спрацьовувати у такій послідовності:

- в першу чергу, здійснюється оповіщення людей про пожежу на поверсі, де виникла пожежа;
- потім оповіщення людей про пожежу на поверхах, що розташовані вище поверху, де виникла пожежа;
- в останню чергу, оповіщення людей про пожежу на поверхах, що розташовані нижче поверху, де виникла пожежа.

Затримку часу оповіщення про НС/пожежу для різних поверхів будинку необхідно передбачати з урахуванням злиття потоків людей на

шляхах евакуації відповідно до розрахунків по ГОСТ 12.1.004 "ССБТ. Пожарная безопасность. Общие требования".

У багатоповерхових виробничих будівлях, які поділені на протипожежні відсіки по вертикалі, СО повинна вмикатися одразу для всього протипожежного відсіку, де виникла пожежа. Затримку часу оповіщення про НС /пожежу/ для інших вертикальних протипожежних відсіків будинку слід передбачати з урахуванням злиття потоків людей на шляхах евакуації відповідно до вимог додатка 2 згідно ГОСТ 12.1.004.

4.4.2. Обов’язки та дії персоналу у разі виникнення надзвичайної ситуації.

У разі виникнення надзвичайної ситуації (НС) працівник, який її помітив, повинен:

- негайно повідомити про це засобами зв’язку органи МНС та Державну пожежну охорону, вказати при цьому адресу кількість поверхів, місце виникнення НС, наявність людей, а також своє прізвище;
- повідомити про НС керівника, адміністрацію, пожежну охорону підприємства;
- організувати оповіщення людей про НС;
- вжити заходів щодо евакуації людей та матеріальних цінностей;
- вжити заходів щодо ліквідації наслідків НС з використанням наявних засобів.

Керівник та пожежна охорона установи, яким повідомлено про виникнення НС, повинні :

- перевірити, чи викликані підрозділи МНС та підрозділи Державної пожежної охорони;
- вимкнути у разі необхідності струмоприймачі та вентиляцію;
- у разі загрози життю людей негайно організувати їх евакуацію та їх рятування, вивести за межі небезпечної зони всіх працівників, які не беруть участь у ліквідації наслідків НС;

- перевірити здійснення оповіщення людей про НС;
- забезпечити дотримання техніки безпеки працівниками, які беруть участь у ліквідації наслідків НС;
- організувати зустріч підрозділів МНС та Державної пожежної охорони, надати їм допомогу у локалізації та ліквідації НС.

Після прибуття на пожежу підрозділів МНС та Державної пожежної охорони повинен бути забезпечений безперешкодний доступ їх до місця, де виникла НС.

4.4.3 Пожежна безпека

Будинок в якому знаходиться лабораторія, являє собою п'ятиповерхову будівлю з цегельними стінами, бетонними перекриттями між поверхами і дерев'яним дахом. Необхідний ступінь вогнестійкості даного будинку 1 чи 2. Для підвищення вогнестійкості будівлі застосоване оштукатурювання вапняно-цементною штукатуркою.

По вибухо-пожежонебезпеці, згідно НАПБ Б.03.002-2007 (Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою), приміщення лабораторії відносяться до категорії В, тому що в ній знаходяться горючі і тяжкогорючі рідини , речовини і матеріали. По пожежо-вибухобезпеці робоча зона відноситься до зони П-IIа – приміщення, в яких можливе утворення лише локальних вибухонебезпечних сумішей.

Причини виникнення пожежі можуть бути наступні:

1. електронагрівальні прилади, залишені без догляду ,а також паяльник;
2. коротке замикання в електромережі й устаткуванні;
3. запалення пальних матеріалів і предметів, що знаходяться в безпосередній близькості від споживачів електричної енергії;
4. перегрів місць з’єднання струмоведучих частин;
5. недотримання норм техніки безпеки;

Для того, щоб уникнути виникнення пожежі, у лабораторії прийняті наступні міри:

1. силовий щит з центральним рубильником виведений окремо, і прохід до нього знаходиться вільним;

2. все устаткування і прилади розміщаються на неспаленій підставці і на безпечній відстані від легкозаймистих рідин;

3. згідно до ГОСТ 12.4.009 – 83 та ISO3941-77 на 100 м2 треба розмістити 1-2 вогнегасники, тому в лабораторії з первинних засобів пожежегасіння маються один вуглекислотний вогнегасник “ОУ2”, для приведення в дію якого необхідно тільки відкрити вентиль;

4. кондиціонер, що знаходиться в лабораторії, обладнаний вибухобезпечним двигуном і вентилятором;

5. меблі розташовані таким чином, щоб не створювати перешкод при евакуації на випадок пожежі; розміри дверних прорізів відповідають усім вимогам СН и П 2.09.02 – 85 та ДБН; поруч з лабораторією вивішена план-схема евакуації на випадок пожежі;

6. при надходженні на роботу в лабораторію всі трудящі проходять вступний і первинний (безпосередньо на робочому місці) інструктаж.

7. для виявлення початкової стадії пожежі застосовуються установки пожежної сигналізації на базі автоматичних сигналізаторів типу “ДТЛ”.

Приміщення лабораторії відповідає НАПБ А.01.001-95.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

1) Було проведено аналіз першоджерел за напрямком біотелеметричних систем, сформульовано задачі автоматизації передачі та зберігання медичних даних з вже існуючих медичних пристроїв, які потребують вирішення.

2) Розроблено апаратну частину пристрою-приставки за концепцією Інтернету Речей. Пристрій-приставка реалізована на платі NodeMCU з радіомодулем ESP8266. Написаний програмний код у середовищі Arduino IDE.

3) Розроблено програмну частину пристрою-приставки, що відповідає за приймання, зберігання та обробку біомедичних даних з пристрою-приставки у хмарний сервіс. Для цього було створено базу даних власної структури, розроблені алгоритми взаємодії сервера та бази даних. Також було розроблено веб-додаток для зручної візуалізації даних вимірювань.

4) Розглянуті вимоги до сучасних біотелеметричних пристроїв, питання взаємодії хмарного сервісу і біотелеметричного пристрою. Також було розглянуто обчислювальні можливості хмарних сервісів для застосування у медицині.

5) Після проведення детального огляду існуючих сучасних медичних систем телеметрії, а також аналізу сучасних напрямків розвитку цифрових технологій в охороні здоров’я було зроблено висновок про актуальність розробки пристроїв-приставок до вже існуючих біотелеметричних пристроїв.

Під час розробки апаратної та програмної частини використовувались в основному безкоштовні програмні рішення, які мають певні обмеження. Найбільше це стосується серверу. Таким чином для реальних біотелеметричних систем, що працюють за концепцією Інтернету Речей потрібно використовувати платні і більш потужні рішення. Також при масштабуванні біотелеметричної системи і при значному збільшенні кількості даних для зберігання та обробки треба буде переходити на інший тип баз даних.

Передача, зберігання та обробка біомедичних даних мають свої особливості. Одними з них є вимоги до конфіденційності та приватності даних пацієнтів. Дотримування цих вимог призводить до ускладнення насамперед структури бази даних та рівнів доступу до неї. Під час оброблення вже чисельних даних з медичного пристрою є переваги у вигляді простоти обчислень в хмарному сервісі, але зберігання та обробка первинних медичних сигналів має більш вагомі переваги у вигляді масштабування хмарного сервісу, можливості більш гнучкого дослідження біомедичних сигналів та виявлення нових закономірностей та процесів у них.

Перспективним є впровадження та використання загального формату для біомедичних сигналів, що дозволить уніфікувати більшість біотелеметричних систем для сукупної обробки багатьох сигналів одночасно.

Наукові (теоретичні) результати магістерської дисертації можуть бути використані для подальшого теоретичного дослідження можливостей плати NodeMCU з радіомодулем ESP8266.

Прикладні (практичні) результати магістерської дисертації можуть бути використані під час розробки серійних зразків пристроїв-приставок до вже існуючих біомедичних діагностичних пристроїв, та накопиченні діагностично-цінних даних пацієнтів для їх аналізу у сукупності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Резніченко А. В. Особливості розробки iot-пристроїв приставок до медичної апаратури / А.В. Резніченко, В.С. Мосійчук // Радіоелектроніка у XXI столітті наук.-техн.-конф. студентів, аспірантів та молодих вчених. — Київ, 2017. – С. 109-110.

2. Григорьев А. И. Клиническая телемедицина / А. И. Григорьев, О. И. Орлов, В. А. Логинов, Д. В. Дроздов, А. В. Исаев, Ю. Г. Ревякин, А. А. Суханов. – М. : "Слово", 2001. – 144 с.

3. Кувакин В. И. Телемедицина: определение, основные направления и история развития / В. И. Кувакин. – Режим доступу: http://www.telemed.ru

4. Лях Ю. Е. Введение в телемедицину. Серия: Очерки биологической и медицинской информатики / Ю.Е. Лях, А.В. Владзимирский. – Донецк: ООО Лебедь, 1999. – 102 с.

5. Юсупов Р.М. Телемедицина – новые информационные технологии на пороге XXI века / под ред. Р.М. Юсупова, Р.И.Полонникова. – СПб, 1998. – с. 487.

6. Lacroix A. Final Report and Recommendations of The G-8 Global Healthcare Application Sub-Project / L. Lareng, D. Padeken // Телемедицина и проблемы передачи изображений.-Тез.докл.третьего ежегодного Московского международного Симпозиума по телемедицине. – М. : МАКС Пресс, 2000.– С.76-77.

7. Яценко В.П. Стратегия развития телемедицины / Валентин Порфирьевич Яценко // I Международная электронная научная конференция "Высокие технологии в медицине". – Донецк, 1999. – С. 39-40.

8. Парин В. В. Биологическая телеметрия / Василий Васильевич Парин. – М., 1971.

9. Internet of Things (IoT) Healthcare Market by Component (Implantable Sensor Devices, Wearable Sensor Devices, System and Software), Application (Patient Monitoring, Clinical Operation and Workflow Optimization, Clinical

Imaging, Fitness and Wellness Measurement) - Global Opportunity Analysis and Industry Forecast, 2014–2021. – Режим доступу: https://www.alliedmarketresearch.com/iot-healthcare-market

10. e-Health Sensor Platform V2.0 for Arduino and Raspberry Pi [Biometric / Medical Applications]. – Режим доступу: https://www.cooking-hacks.com/documentation/tutorials/ehealth-biometric-sensor-platform-arduino-raspberry-pi-medical#step1_1

11. Smart Wireless Pill Bottles. – Режим доступу: https://www.adheretech.com/

12. Ben Davis (2017) 10 examples of the Internet of Things in healthcare. – Режим доступу: https://econsultancy.com/blog/68878-10-examples-of-the-internet-of-things-in-healthcare/

13. Connected health How digital technology is transforming health and social. – Режим доступу: https://www2.deloitte.com/uk/en/pages/life-sciences-and-healthcare/articles/connected-health.html

14. Health on the 2014 Gartner Hype Cycle, Health Populi, September 2014. – Режим доступу: http://healthpopuli.com/2014/09/02/health-on-the-2014-gartner-hype-cycle/

15. The Digital Health Hype Cycle, Bionicly, December 2014. – Режим доступу: http://bonicly.com/digital-health-hype-cycle

16. Zanella A, Bui N, Castellani A, Vangelista L and Zorzi M. (2014) Internet of things for smart cities. IEEE Internet Things J., Vol. 1, Iss. 1, pp. 22-32

17. Kruse C. S. Adoption factors of the electronic health record a systematic review / K. Kothman, K. Anerobi, L. Abanaka // JMIR Med Inform. Vol. 4, No 2, el9.

18. Mosiychuk V.S. Wideband bioimpendance meter with an active electrodes / V.S. Mosiychuk, G. V. Timoshenko, O. B. Sharpan // Wideband bioimpendance meter with an active electrodes. 2015 IEEE 35th International Conference on Electronics and Nanotechnology. – Київ, 2015. DOI: 10.1109/ELNANO.2015.7146896

19. Mosiychuk V.S. Bioimpendance monitoring of dialysis patients dURLng ultrafiltration / V.S. Mosiychuk, G. V. Timoshenko, O. B. Sharpan, B. V. Tkachuk, R.S. Tomashevskyi // 2016 IEEE 36th International Conference on Electronics and Nanotechnology. – Київ, 2016. – DOI: 10.1109/ELNANO.2016.7493056

20. Health Information Privacy – Режим доступу: https: //www.hhs.gov/hippa

21. Методичні рекомендації з застосування телемедицини в Україні, що затверджені МОЗ України. – Режим доступу: http://www.moz.gov.ua/ua/portal/mttm_method_recomm/

22. Казаков В. Н. Телемедицина / В.Н. Казаков, В.Г. Климовицкий, А.В. Владзимирский. – Донецк : Типография ООО «Норд», 2002. – 100 с.

23. NodeMcu Connect Things EASY. – Режим доступу: http://nodemcu.com/index_en.html

24. The Global State of Information SecURLty® Survey. 2017. – Режим доступу: https://www.pwc.com/gx/en/issues/cyber-secURLty/information-secURLty-survey.html

25. Privacy and secURLty of patient data in the cloud. – Режим доступу: https://www.ibm.com/developerworks/cloud/library/cl-hipaa/index.html

26. Public Law 104– 191 – Health Insurance Portability and Accountability Act of 1996. – Режим доступу: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html

27. Zigbee. – Режим доступу: http://www.zigbee.org/

28. Владзимирский А. В. Проблема формирования терминологии в телемедицине / Антон. Вячеславович Владзимирский // Арх. клин. эксп. мед. – Київ, 2001. – Т. 10, № 1. – С. 108-112.

29. ISO/IEC 2382:2015, Information technology – Vocabulary – Part 1. – Режим доступу: https://www.iso.org/standard/63598.html

30. GNU GENERAL PUBLIC LICENSE. – Режим доступу: https://www.gnu.org/licenses/gpl-3.0.ru.html

31. BioInformatics. – Режим доступу: http://www.wolfram.com/solutions/industry/bioinformatics/

32. Scientific data formats. – Режим доступу: http://pub.ist.ac.at/~schloegl/matlab/eeg/

33. The BioSig Project. – Режим доступу: http://biosig.sourceforge.net/

34. Xdf – Режим доступу: https://code.google.com/archive/p/xdf/

35. Performance of Yii. – Режим доступу: http://www.yiiframework.com/performance/

36. ISO/IEC/IEEE 24765:2010(en). – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:24765:ed-1:v1:en