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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавра
(назва освітнього ступеня)

на тему: Захист інформації для використання IoT-пристроями в галузі охорони здоров'я

Виконав(ла): студент(ка) 4 курсу, групи СН-41
спеціальності 122 "Комп'ютерні науки"
(шифр і назва спеціальності)

(підпис) Старосілець В.А. (прізвище та ініціали)

Керівник (підпис) Мацюк О.В. (прізвище та ініціали)

Нормоконтроль (підпис) Шимчук Г.В. (прізвище та ініціали)

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

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2022

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

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

Кафедра Комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавра
(назва освітнього ступеня)

за спеціальністю 122 "Комп'ютерні науки"
(шифр і назва спеціальності)

студенту Старосілець Володимир Андрійович
(прізвище, ім'я, по батькові)

1. Тема роботи Захист інформації для використання IoT-пристроями в галузі охорони здоров'я

Керівник роботи Мацюк Олександр Васильович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « *16* » березня 2022 року № 4/7-161

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Науково-технічна література

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Вступ до IoT в охороні здоров'я та відповідні визначення розумних міст 1.1. Архітектура Інтернету речей 1.2. Компоненти Інтернету речей 1.3. Програми Інтернету речей 1.4. IoT в охороні здоров'я 2. Системи охорони здоров'я. 2.1. Рішення IoT для користувачів з обмеженими можливостями 2.2 Система моніторингу здоров'я пацієнтів 2.3 Проблеми безпеки 2.4 Рішення безпеки 2.5 Вирішення проблем конфіденційності 2.6 Розумна енергія 2.7 Питання безпеки для комунікаційних технологій 2.8 Проблеми безпеки для програм 2.9 Питання безпеки особистого захисту 3.Безпека життєдіяльності, основи хорони праці. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема роботи 2 Актуальність роботи
3-4. Рівні 5. IoT в охороні здоров'я 6. Об'єднання викликане Інтернетом речей
7. Архітектура систем медичного моніторингу
8. Аналіз систем захисту 9-10. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Гурик Олег Ярославович, к.т.н., доцент, доцент кафедри МТ		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2022	*Виконано*
2.	Підбір джерел по темі дослідження	04.01.2022-30.01.2022	*Виконано*
3.	Переклад та опрацювання джерел по темі дослідження	31.01.2022-06.02.2022	*Виконано*
4.	Виконання дослідження щодо захисту інформації в	12.06.2021-	*Виконано*
	галузі охорони здоров'я	13.06.2021	
5.	Оформлення розділу «Вступ до IoT в охороні здоров'я	14.02.2022-	Виконано
	та відповідні визначення»	06.03.2022	
6	Оформлення розділу «Системи охорони здоров'я»	07.03.2022-	*Виконано*
		03.04.2022	
7.	Виконання завдання до підрозділу «Безпека	04.04.2022-	*Виконано*
	життєдіяльності»	17.04.2022	
8.	Виконання завдання до підрозділу «Основи хорони	18.04.2022-	*Виконано*
	праці»	01.05.2022	
9.	Оформлення кваліфікаційної роботи	02.05.2022-15.05.2022	*Виконано*
10.	Нормоконтроль	16.05.2022-22.05.2022	*Виконано*
11.	Перевірка на плагіат		*Виконано*
12.	Попередній захист кваліфікаційної роботи		*Виконано*
13.	Захист кваліфікаційної роботи		

Студент _____ Старосілець В.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Мацюк О.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Захист інформації для використання IoT-пристроями в галузі охорони здоров'я// Кваліфікаційна робота// Старосілець Володимир Андрійович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СН-41 // Тернопіль, 2022 // сторінки ___-, рисунки ___, таблиць ____, джерел ___.

Ключові слова: цифрові міста, інтернет речей, захист інформації, великі дані, хмарні обчислення, інфраструктура.

Метою цієї кваліфікаційної роботи є дослідження систем охорони здоров'я IoT, щоб зрозуміти проблеми безпеки та визначити безпечні архітектури, які можуть допомогти вирішити ці проблеми.

У роботі досліджуються найпоширеніші застосування Інтернету речей в охороні здоров'я, наприклад моніторинг охорони здоров'я, а також детально досліджуються загрози, які виникають від використання цієї технології. Пояснюється, як загрози безпеці можуть впливати на системи охорони здоров'я та пацієнтів, а також досліджуються наслідки.

Розглядаються доступні рішення для протидії цим загрозам. Він також охоплює деталі деяких стандартів, які використовуються в Інтернеті речей системи охорони здоров'я для захисту, включаючи ISO CD 30141 та ISO AWI 21823.

ANNOTATION

Protection of information for the use of IoT devices in the field of health care// Qualification work // Starosilets Volodymyr Andriiovych// Ivan Puliyu Ternopil National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science, group. CH-41 // Ternopil, 2022 // pages ___, figures ____, tables ____, sources ___.

Key words: digital cities, the Internet of Things, information security, big data, cloud computing, infrastructure.

The aim of this qualification is to study IoT health systems to understand security issues and identify secure architectures that can help address these issues.

The paper examines the most common uses of the Internet of Things in health care, such as health care monitoring, and examines in detail the threats posed by the use of this technology. It explains how safety threats can affect health systems and patients, and the consequences are being investigated.

Available solutions to address these threats are being considered. It also covers details of some of the standards used on the Internet of Things for health protection, including ISO CD 30141 and ISO AWI 21823.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ШІ – штучний інтелект.

ПЗ – програмне забезпечення.

ІКТ – інформаційно-комунікаційні технології.

СС – Cloud Computing – хмарні обчислення.

IoT – Internet of Things – інтернет речей.

Saas – Software as a Service – програмне забезпечення як послуга.

POP – Post Office Protocol – протокол, що використовується клієнтом для доступу до повідомлень електронної пошти на сервері.

SMTP – Simple Mail Transfer Protocol – комунікаційний протокол для пересилання електронної пошти.

Зміст

Вступ

З моменту свого заснування технологія Інтернету речей (IoT) не спостерігала нічого, крім гіркого прогресу. Протягом останнього десятиліття загальна кількість підключених пристроїв стрімко зросла, і, за прогнозами, ці цифри зростуть і в майбутньому.

Метою цього дослідження є вивчення систем та архітектур охорони здоров'я Інтернету речей, щоб зрозуміти, які проблеми безпеки виникають у цих системах і які заходи можна вжити для їх подолання. Пристрої IoT включають фізичні об'єкти, до яких приєднані давачі, так що дані про поточну діяльність об'єкта або особи, до якої вони приєднані, можна відстежувати за допомогою давача та передавати на віддалений сервер для подальшого аналізу.

Пристрої Інтернету речей мають IP-адресу для бездротового підключення повсякденних об'єктів до Інтернету та забезпечення такого обміну інформацією надали дуже точне визначення медичної допомоги на основі Інтернету речей у своїй конференції «Впровадження Інтернету речей для охорони здоров'я», визначаючи її як платформу, на якій «різноманітні розподілені пристрої об'єднують, аналізують та передають медичну допомогу в режимі реального часу. інформацію в хмару, що дає змогу збирати, зберігати та аналізувати велику кількість даних у кількох нових формах та активувати сигнали на основі контексту.

Це дослідження описує системи охорони здоров'я та архітектури Інтернету речей, щоб зрозуміти проблеми надійності та безпеки даних, а також провести критичний аналіз рішень, які можуть допомогти подолати труднощі, які виникають через загрози безпеці.

1 ВСТУП ДО IoT В ОХОРОНІ ЗДОРОВ'Я ТА ВІДПОВІДНІ ВИЗНАЧЕННЯ

Інтернет речей (IoT) — це динамічна розподілена система мережі фізичних пристроїв, транспортних засобів та побутових приладів, яка може отримувати дані реального світу за допомогою давачів, обробляти їх для вироблення ідей та спілкуватися з іншими для обміну або обміну цими знаннями. IoT має певні ключові характеристики, які відрізняють їх від інших мереж, зокрема ідентифікацію, спілкування та взаємодію все, що може включати електронні пристрої, а також живих істот [1]. Пристрої IoT можуть підключатися до Інтернету в режимі реального часу. Підключення до Інтернету також дозволяє віддалено контролювати пристрої. Через нього в пристрій можна додати багато передових та інтелектуальних функцій.

1.1 Архітектура Інтернету речей

Архітектура Інтернету речей складається з чотирьох основних рівнів, які включають граничні технології, шлюз доступу, проміжне програмне забезпечення та прикладний рівень. Два нижніх рівні включають збір даних, а інші два використовують дані для аналізу та додавання [2]

Edge Technology: це перший рівень архітектури IoT, який містить апаратні компоненти збору даних, такі як давачі, системи радіочастотної ідентифікації (RFID), електронний обмін даними (EDI), глобальні системи позиціонування (GPS), камери та інтелектуальні термінали. Ці компоненти збирають інформацію, обробляють її та передають дані наступному шару.

RFID є портативними пристроями і мають мітку зчитування, а дані, які записуються, відповідають потребам у мітці RFID. RFID-мітки корисні для моніторингу даних у реальному часі. Дані, які передаються через мітку RFID,

можуть включати інформацію про пристрої та пацієнта у випадку системи моніторингу пацієнта, такі як рівень глюкози, кров’яний тиск та місцезнаходження. Системи IoT використовують бездротові сенсорні мережі (WSN), які мають величезну кількість вузлів, які сприймають результати [3]

Шлюз: шлюз доступу обробляє дані, отримані з граничного рівня, за допомогою таких технологій, як Wi-Fi, Ethernet, бездротова сенсорна мережа (WSN), WI-Max та глобальна система мобільного зв’язку (GSM) [4]. Шлюз дозволяє давачам підключатися до зовнішньої мережі за допомогою цих технологій. Апаратне забезпечення шлюзу попередньо обробляє дані давача (фільтрацію та агрегацію) перед відправкою їх у центр обробки даних [5].

Проміжне програмне забезпечення: проміжне програмне забезпечення є програмною платформою, яка надає різноманітні послуги даних, включаючи виявлення, фільтрацію, агрегацію, аналіз та управління доступом. Проміжне програмне забезпечення з’єднує рівень шлюзу доступу з верхнім рівнем, який є прикладним рівнем.

Рівень додатків: прикладний рівень з’єднує систему Інтернету речей з користувачами і має два підрівні, включаючи керування даними та службу додатків. Рівень керування даними надає такі послуги, як каталог, якість обслуговування, дані хмарних обчислень, обробка та M2M. Прикладний рівень включає інтерфейс між кінцевими користувачами та програмами, які використовуються на підприємствах [6].

1.2 Компоненти Інтернету речей

IoT містить безліч різних компонентів, які працюють разом. Одним з ключових компонентів системи є фізичний об'єкт, який використовується для збору та моніторингу інформації користувачів. Дані, які збирає цей об’єкт або пристрій, можуть включати життєво важливі ознаки здоров’я, такі як рівень глюкози, частота серцевих скорочень і кров’яний тиск.

Комунікаційні технології є ще одним компонентом, який служить сполучною ланкою між програмою охорони здоров'я та пристроями. Ці технології можуть бути ZigBee, Bluetooth, Light Fidelity або Wi-Fi.

ZigBee — це стандарт IEEE 802.15.4, який працює з низькою потужністю та на невеликій відстані. Технологія побудована на основі низькошвидкісної бездротової персональної мережі (LR-WPAN) і працює в діапазоні 2,4 ГГц ISM. Bluetooth, який також працює за стандартом IEEE 802.15.1, працює в тому ж діапазоні, але ZigBee коштує дешевше, ніж Bluetooth. Bluetooth створює з'єднання «точка-точка» або «точка-багатоточка» на основі бездротової персональної мережі (WPAN). Пристрої Bluetooth можуть працювати з низьким рівнем енергії і, таким чином, споживати менше енергії [7].

Light Fidelity (Li-Fi) — це система зв'язку з видимим світлом, яка використовує світло на відміну від Wi-Fi, який використовує радіохвилі. Швидкі світлові імпульси від 400 до 800 ТГц продовжують передавати через світлодіодну лампу, яка встановлена на трансивері. Ці світлодіоди передають дані у вигляді світла, тоді як фоторецептори отримують сигнали і перетворюють їх у цифрові дані. Однак у місцях, де є перешкоди, такі як стіни та дерева, Li-Fi не можна використовувати, оскільки передане світло може заважати іншим джерелам світла, таким як сонячне світло або лампочки. Технологія Li-Fi використовується для моніторингу пацієнта в кімнаті, наприклад, у випадку МРТ-сканера [8].

Технології Wi-Fi включають IEEE 802.11x Wireless LAN. Ці технології працюють на трьох взаємосумісних технологіях, включаючи Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum (FHSS) та Infrared (IR). Стандарти Wi-Fi, такі як IEEE 802.11n, добре працюють зі швидкістю передачі даних 600 Мбіт/с в діапазонах радіочастот 2,4 ГГц або 5 ГГц.

Технологія використовує множинний вхід і багато вихідних сигналів (MIMO) для максимального використання доступного діапазону. Для безпеки

доступні протоколи, такі як точки доступу, захищені Wi-Fi, захищені зони Wi-Fi, розширений стандарт шифрування та еквівалентна конфіденційність проводів.

Long Term Evolution (LTE) — це ще одна технологія бездротового широкосмугового доступу, яка використовує технологію 4G. Ця технологія забезпечує швидкість передачі даних висхідного зв'язку 75 Мбіт/с і швидкість передачі даних внизу 300 Мбіт/с.

LTE дуже рентабельний, особливо у випадках послуг M2M. Його можна використовувати в охороні здоров'я для моніторингу та відстеження пацієнтів та пристроїв, приєднаних до них. LTE-A – це фактичний стандарт зв'язку 4G, який забезпечує 3 Гбіт/с низхідного каналу та 1,5 Гбіт/с висхідного зв'язку з низькою затримкою. Ця технологія також забезпечила зворотну сумісність із мережами LTE, і, таким чином, служби можуть скористатися перевагами мереж LTE [9].

1.3 Програми Інтернету речей

Компонент програми в системі IoT піклується про організацію та форматування даних, які відбуваються між різними пристроями та додатками IoT. Розумні технології використовуються для надання допомоги користувачам, наприклад, у технології розумного дому, де мешканцям допомагає використання гаджетів та обладнання всередині будинку.

Розумні системи охорони здоров'я можна використовувати для допомоги людям з обмеженими можливостями, підключивши їх до медичних працівників через Інтернет за допомогою пристроїв IoT, підключених до їх тіла. Бездротові давачі можна помістити в одяг та інші предмети, які використовує пацієнт для забезпечення моніторингу через системи IoT, що дозволяє контролювати поведінку пацієнта на макроскопічному рівні та виявляти будь-які відхилення в поведінці, які можуть призвести до проблем зі здоров'ям пацієнта. У таких випадках можна вжити заходів дистанційно, а тривогу можна надіслати для початку процедури надання допомоги [10]

Користувачі системи Smart Healthcare, такі як лікарі та медичні працівники, можуть читати інформацію про пацієнта за допомогою розумних додатків. Входи можна надавати в режимі реального часу за допомогою сенсорів і RFID, підключених до пристроїв IoT.

Зібрані дані надсилаються в хмару для зберігання, а потім дані обробляються за допомогою хмарних програм. Хмарне сховище дозволяє отримувати доступ до даних з будь-якої точки земної кулі через Інтернет. З використанням хмарних обчислень зменшуються витрати на обробку та управління. Це пояснюється тим, що за наявності хмарних обчислень не потрібно купувати чи обслуговувати технологічне обладнання.

Система Інтернету речей може використовувати будь-яку з моделей розгортання з Software as a Service (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS).

IaaS включає програмне та апаратне забезпечення, яке приймає запити на обслуговування від користувачів.

Інструменти PaaS дозволяють використовувати хмарні програми для встановлення контролю.

SaaS може надавати користувачам такі послуги, як зберігання, обробка та виконання додатків [11]

1.4 IoT в охороні здоров'я

Різні сектори, включаючи промислові та непромислові, використовують пристрої Інтернету речей для покращення своєї інфраструктури, як-от телекомунікації, виробництво та охорона здоров’я. У секторі охорони здоров’я застосування IoT зростає.

На рис.1.1, наведено, що медична допомога на основі Інтернету речей поділяється на дві підкатегорії: послуги та програми. Він дає вичерпний огляд того, як IoT вплинув і надання допомоги у сфері охорони здоров'я.

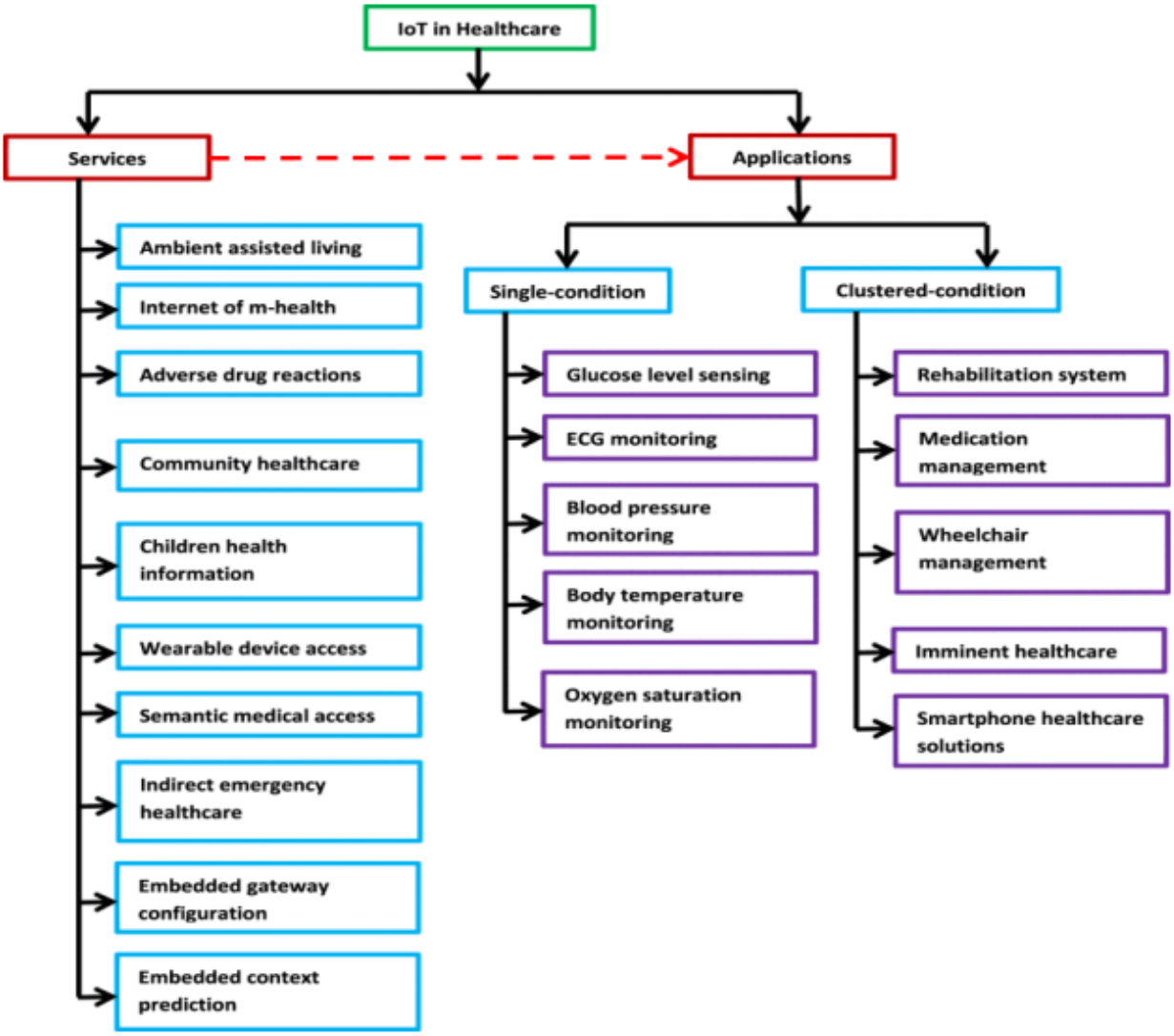

Рисунок 1.1 - IoT в охороні здоров'я

Послуги включають розумний спосіб життя, непряме надання медичних послуг у надзвичайних ситуаціях, мобільне здоров’я, усунення реакцій на ліки, забезпечення та надання доступу до інформації про здоров’я пацієнтів, пристрої, що носяться. Додатки далі поділяються на ті, що призначені для окремого пацієнта (одна умова), і ті, що призначені для обслуговування аудиторії (кластерні).

Додатки з одним умовою включають моніторинг рівня глюкози, ЕКГ, артеріального тиску, температури тіла та насичення киснем [12], тоді як

кластерні програми включають системи реабілітації, інвалідні візки та системи охорони здоров’я для смартфонів.

2 СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

Інтернет речей дозволив системам охорони здоров’я підвищити їхню ефективність у забезпеченні високої якості економічними способами, завдяки чому пацієнтам можна надавати якісні послуги та точніші діагнози. Пацієнти та медичні працівники встановлюють автоматизований зв’язок між ними, щоб практикуючий лікар залишався в курсі стану здоров’я пацієнта, а також міг використовувати створені інтелектуальні системи охорони здоров’я [13]. Ця комунікаційна технологія була інтегрована в носні пристрої, такі як ті, що використовуються для моніторингу рівня глюкози, артеріального тиску, рівня кисню та температури тіла [14]. Онлайн-портали охорони здоров’я пацієнтів також дозволяють обмінюватися інформацією про пацієнтів між різними сторонами, наприклад, пацієнтом та його/її лікарями.

Рисунок 2.1 – Об’єднання викликане Інтернетом речей

Розумні системи охорони здоров’я передбачають фіксацію параметрів здоров’я людини за допомогою біометричних датчиків. Спілкування між

пацієнтом і медичним працівником або опікуном відбувається через хмару Інтернету речей [12].

Дані збираються від пацієнтів за допомогою давачів, носимих пристроїв і додатків m-health і передаються в хмару IoT. Лікарі, практикуючі лікарі та страхові компанії отримують цю інформацію, щоб надавати ефективні медичні послуги як для лікування, так і для профілактики.

Переваги використання пристроїв Інтернету речей у хмарі включають захоплення даних у режимі реального часу та підвищення їх доступності для пацієнтів та постачальників медичних послуг.

Збір даних: давач використовується для збору даних від пацієнта або медичної установи. Прикладами таких датчиків є DS18B20, який використовується для фіксації значень серцевого ритму, і мікроконтролер Arduino Uno ATmega 328P, який фіксує дані про температуру тіла [17].

Хмарна система: дані, які збираються за допомогою сенсорних пристроїв, передаються на процесор, наприклад HLK-RM04 Serial, через модуль Wi-Fi і зберігаються на сервері MySQL. Це з'єднання встановлюється через протокол HTTP [18].

Портал охорони здоров'я в реальному часі: користувач через портал охорони здоров'я, який зазвичай написаний на Java і доступний через програми Android, доступні через кілька пристроїв, включаючи мобільні ноутбуки, планшети та персональні комп'ютери, може переглядати дані. Прикладом може бути програма для Android, яка сповіщає користувача мобільного телефону, якщо спостерігаються будь-які коливання у здоров'ї пацієнта [19].

2.1 Рішення IoT для користувачів з обмеженими можливостями

Рішення IoT використовуються в різноманітних медичних послугах, серед яких надання підтримки людям з обмеженими можливостями використовується для моніторингу пацієнтів, які страждають на хронічну хворобу або певну

інвалідність [20]. У цій області вже було проведено багато досліджень, і, таким чином, охорона здоров’я досягла багатьох успіхів у цій галузі. Розуміння того, як працюють ці системи, може допомогти дослідити можливі застосування медичної допомоги в цій галузі.

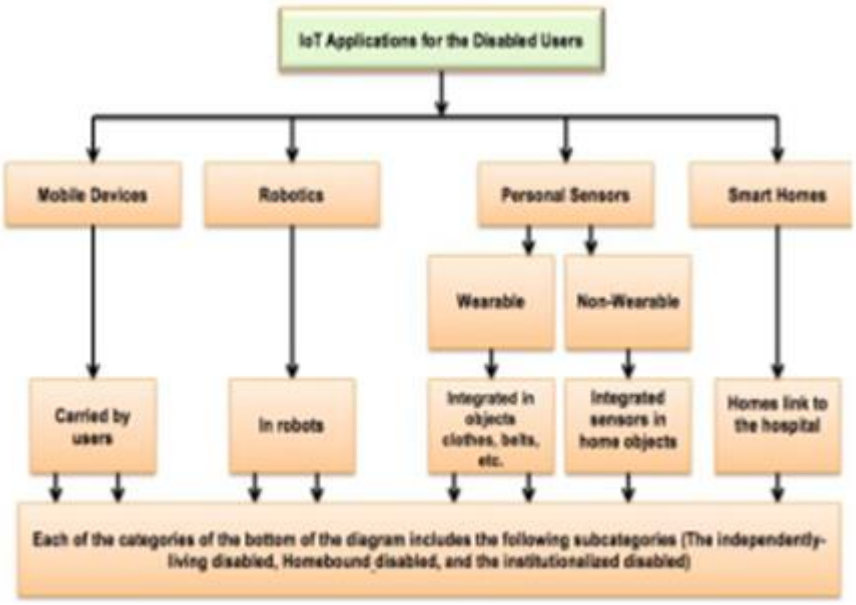

Рисунок 2.2 – Визначення людей з обмеженими можливостями

Рис.2.2 визначає людей з обмеженими можливостями як інвалідів, які проживають самостійно, інвалідів, які перебувають у домі, та інвалідів з обмеженими можливостями (інвалідів, розміщених у закладі) та класифікує способи, за допомогою яких IoT підтримує їх, щоб покращити свій спосіб життя.

Швидко зростаюча кількість старіння населення викликала все більше проблем зі здоров’ям, а витрати на охорону здоров’я зростали. У сільській місцевості медичних послуг недостатньо, т.к

не вистачає спеціалізованої медичної служби. Таким чином, інвалідам доводиться звертатися у великі лікарні та заклади охорони здоров’я, які коштують дорого. Інтернет речей може дозволити розширити номінальні медичні послуги від медичних працівників до сільського регіону і, таким чином, зробити медичне обслуговування економічно ефективним для них [21]. Ці завдання можуть включати заходи з технічного обслуговування як прийом їжі,

купання та одягання, інструментальна діяльність, як-от використання електронних пристроїв, як-от телевізор, телефон і посудомийна машина, та інші розширені види діяльності, як-от навчання, спілкування та заняття хобі [22].

Люди з обмеженими можливостями можуть бути класифіковані на основі їхніх типів інвалідності, включаючи фізичні вади та когнітивні розлади, або на основі компетенції, включаючи інвалідів, які живуть самостійно, інвалідів, прив'язаних до дому, та інвалідів, які перебувають у закладі. Люди з обмеженими фізичними можливостями мають розумові або сприйнятливі порушення, які найчастіше зустрічаються у людей похилого віку старше 59 років, оскільки їм не вистачає сили та витривалості. Когнітивні розлади виникають через психічні порушення, що спричиняють погану роботу в нормальному функціонуванні. Самостійно проживаючий інвалід може бути рухомим або нерухомим. Мобільних людей можна відстежувати за допомогою GPS та інших датчиків, таких як датчики наближення акселерометра та відеокамери, які можна підключити через Bluetooth, Wi-Fi або мобільний Інтернет.

Інваліди, прив'язані до дому, залишаються вдома та потребують спеціальної допомоги, якщо їм потрібно вибратися. Для такої людини вдома можна встановити сенсорні системи для надання допомоги вдома з такими пристроями, як носимі пристрої, які можуть полегшити їхнє життя. Інституціоналізовані інваліди потребують медичних установ для тривалого спеціалізованого догляду [23].

Інтернет речей може допомагати інвалідам різними способами, наприклад, запобігати захворюванням, запобігати інвалідності та боротися з хронічними захворюваннями. Віддалений моніторинг можна здійснювати за допомогою пристроїв IoT для виявлення життєво важливих показників у пацієнтів, щоб особа, яка доглядає, могла вжити негайних заходів, щоб принести користь пацієнту. Три доступні недорогі системи моніторингу для захоплення таких дані та складні алгоритми можна використовувати для даних, які збираються для

надсилання повідомлень медичним працівникам. Завдяки такому моніторингу можлива рання профілактика захворювання системи, оскільки ті, хто страждає деякими захворюваннями, як-от цукровий діабет, можуть контролюватися і, таким чином, запобігати виникненню надзвичайних ситуацій [24].

2.2 Система моніторингу здоров'я пацієнтів

Давачі IoT є потужним інструментом для сектору охорони здоров'я, оскільки вони дають змогу віддалено контролювати здоров'я пацієнтів, щоб лікарі та практикуючі лікарі могли стежити за станом здоров'я своїх пацієнтів та давати їм відповідні поради щодо покращення охорони здоров'я [17].

Система дистанційного моніторингу здоров'я пацієнтів зазвичай складається з трьох рівніархітектури. Мережевий рівень, який є першим рівнем архітектури, містить давачі, які можна носити, які діють як джерела для збору даних і даних, які можуть бути зібрані, включаючи останні стани здоров'я пацієнта, такі як кров'яний тиск і температура тіла.

Другий рівень архітектури IoT включає послуги, які дозволяють спілкуватися та обмінюватися даними між давачами та іншими вузлами в мережі. Верхній рівень архітектури має вузли, які використовуються для обробки та аналізу даних, які збираються для дослідження [19]. Ця трирівнева структура проілюстрована на рис.2.3 нижче.

Рисунок 2.3 – Архітектура систем медичного моніторингу

Пацієнтам з обмеженими можливостями можна надати допоміжне життя в навколишньому середовищі, щоб вони не були самотні, коли стикаються з проблемою здоров’я. Допомога може бути надана такому хворому навіть для щоденної рутинної роботи за допомогою систем зондування, обчислень, зв'язку та розвідки, пов'язаних із звичайними об'єктами. Деякі давачі також можуть бути вбудовані в тіло, як-от стимулятор серцевого ритму, або вбудований у меблі вдома. Ці різні типи давачів, вбудованих в різні об’єкти, з’єднані таким чином, що отримані дані формуються в одному місці в хмарі, а аналіз надається особам, які здійснюють догляд, або медичним працівникам. Ці пристрої також можуть включати біометричні дані, які можуть вимірювати ЕКГ, або інші системи тривоги, які дозволяють віддалений моніторинг і догляд [25].

2.3 Проблеми безпеки

Сьогодні існує величезна кількість пристроїв, які використовуються в мережах IoT, і ці пристрої представляють різноманітні сценарії електронного здоров’я, прикладом яких є віддалений моніторинг здоров’я пацієнтів [26]. Однак ці програми посилюють залежність систем від технологій ідентифікації пацієнта та стану здоров’я. Це може призвести до певних ризиків для пацієнтів, якщо зібрані дані не достовірні, а інформація про пацієнтів не достовірна. У відкритому та взаємопов’язаному середовищі систем IoT цілісність цих даних може бути під загрозою, оскільки дані під час передачі можуть бути піддані хакерам, які можуть використати дані, щоб скористатися ними та почати атаки на пацієнтів. Наприклад, злодій, який дізнається, що людина, яка живе в будинку, має слабке серце або хворобу, як-от астма, може використати інформацію та атакувати її слабкість, щоб вкрасти фізичні речі з дому [27].

Кібератаки на охорону здоров’я можуть бути дуже небезпечними для пацієнтів і навіть небезпечними для життя. Відповідно до Міжнародної організації зі стандартизації (ISO); організація, яка публікує міжнародні стандарти, охорона здоров’я стикається з великою кількістю випадків

порушення даних, і в 2014 році в системі охорони здоров'я Великобританії кількість випадків подвоїлася порівняно з попереднім роком.

У 2013 році медичні компанії зіткнулися з 183 витоками даних і 91 зломом, тоді як у 2014 році рівень безпеки даних зріс на 44%. Через такі атаки організаціям, можливо, доведеться сплатити штрафи в розмірі до 1,5 мільйона доларів США за один сингл порушення. Крім того, вони повинні повідомити пацієнтів та інших постраждалих протягом 60 днів з моменту порушення. Про порушення також слід повідомити ЗМІ, якщо це може вплинути понад 500 осіб відповідно до нормативу. У 2015 році понад 12,3 мільйона американців постраждали від 270 порушень безпеки даних у сфері охорони здоров'я. Сектору охорони здоров'я бракує достатньо ресурси, необхідні для захисту кібербезпеки, тому вони є привабливою мішенню для кіберзлочинців [28].

Існують онлайн-додатки, які використовуються для керування системами охорони здоров'я, які дозволяють обмінюватися інформацією про пацієнтів через Інтернет між лікарнею та пацієнтом або медичною установою. Це включає дані, зібрані за допомогою давачів у режимі реального часу, і включає відстеження їхньої регулярної діяльності [29].

Такі додатки необхідно мати потужні механізми авторизації. Якщо механізм аутентифікації недостатньо сильний, зловмисники можуть використати слабкість. Якщо таким чином під'єднано до пацієнта давач, це може мати жахливі наслідки і навіть призвести до смерті пацієнта.

Тому дуже важливо, щоб ці пристрої були в безпеці. Давачі IoT, що використовуються в медичних системах для підтримки пацієнтів, постійно збирають дані про відвідування лікарні, стан здоров'я пацієнта, і аналізує те ж саме в режимі реального часу. Вони здебільшого інтегровані з традиційною IT-інфраструктурою, що використовується в лікарні, і, таким чином, матиме більше проблем із безпекою.

Крім того, системи Інтернету речей зазвичай децентралізовані, що ще більше ускладнює передбачення та пом’якшення загроз безпеці та захист людей від зловмисників [30]

Критична інфраструктура лікарень і систем охорони здоров’я покладається на сенсорні пристрої та системи керування, які вразливі до загроз безпеці. Якщо ці загрози не врахувати належним чином, це може мати серйозні наслідки для пацієнтів. Критична інфраструктура організації включає виробництво електроенергії, телекомунікаційні мережі, фінансові послуги та медичні послуги. Кіберзагрози можуть спричинити відключення електроенергії та несправність систем догляду за слухом, що спричинить медичні нещасні випадки. Якщо зловмисник отримає доступ до системи моніторингу пацієнтів, зловмисник зможе контролювати медичні пристрої, що може вплинути на безпеку пацієнта [31].

Використання рішень кібербезпеки в Інтернеті речей у сфері охорони здоров’я є складним завданням.

Останні досягнення розробили вбудовані системи безпеки, виявлення вторгнень і захист давачів PLC як деякі з рішень для захисту медичних послуг IoT. Проте факт залишається фактом, що протоколи IoT все ще не мають достатніх функцій, необхідних для захисту систем від складних кіберзагроз. Оскільки GSM є домінуючою технологією, яка використовується в мережах IoT, вразливість є значною.

Алгоритм A5/3 або KASUMI, що використовується в Інтернеті речей, має деякі серйозні недоліки, якими можуть скористатися зловмисники. Протокол IPv6, розроблений для додатків із великим обсягом даних, використовується на пристроях з низьким енергоспоживанням і вразливий до атак DOS. Зловмисник може надсилати фрагментовані пакети фальшивим цілям через систему IoT, блокуючи тим самим послуги для справжніх користувачів під час атаки DOS [32].

Хоча протоколи IoT розроблені з використанням високоякісних технологій надання послуг, коли дані шифруються за допомогою слабкіших алгоритмів, рівень безпеки знижується.

Хмарна база даних забезпечує легкий доступ до систем зберігання, таких як бази даних NoSQL Mongo. Велика кількість даних, які формуються в режимі реального часу може оброблятися цими системами баз даних через один сервер. Ці бази даних містять конфіденційну інформацію про пацієнтів. Вплив може бути руйнівним для всієї бази даних і навіть для хмарної системи керування вмістом [32].

Медичні працівники можуть використовувати онлайн-системи для доступу до записів пацієнтів, а також для обміну ними з іншими спеціалістами. Дані, які передаються таким чином, можуть бути дуже чутливими та конфіденційними. Порушення цих даних може мати негативні наслідки як для пацієнта, так і для медичного закладу. Якщо систему охорони здоров'я необхідно захистити від таких загроз, важливо мати передові алгоритми обліку та авторизації.

Лікарні також повинні дотримуватися певних юридичних процедур.

2.4 Рішення безпеки

Безпека медичних пристроїв на основі IoT надзвичайно важлива, оскільки одиночне порушення або несправність може коштувати комусь життя. Існують різноманітні рішення безпеки, які використовуються для захисту систем охорони здоров'я на основі IoT. Проектування та впровадження більшості систем безпеки є складним і складним через їх низькі обчислювальні ресурси.

Проте всі ці системи рішень повинні мати деякі спільні основні риси. По-перше, що стосується фізичного простору, рішення має бути невеликим і зручним. Це пов'язано з тим, що більшості медичних пристроїв на основі Інтернету речей бракує потужності для великих водіїв. Тому очікується, що

рішення буде легким з точки зору як пристрою, на якому вони призначені для роботи, так і реалізованої кодової бази. Крім того, він повинен мати високу обчислювальну потужність, щоб він міг працювати ефективно й ефективно навіть на малопотужному пристрої [34].

Використання аутентифікації для доступу до даних через медичні портали на смартфонах є одним із поширених методів забезпечення безпеки. Аутентифікація заснована на криптографії, так що дані шифруються і можуть бути розшифровані лише за умови належної аутентифікації.

Аутентифікація може забезпечити безпеку, запобігаючи входу в систему неавтентичних користувачів, наприклад хакерів. Однак, оскільки системи є складними з використанням пристроїв Інтернету речей та інтернет-додатків, необхідні високоякісні рішення безпеки, і просто базової аутентифікації може бути недостатньо як забезпечення безпеки [35].

Зі збільшенням підключення та трильйонами об’єктів користувача, які приєднуються до мережі, кількість необхідних унікальних ключів аутентифікації зростає. Більшість розробників використовують технологію RFIP, оскільки вона споживає менше ресурсів, а також менш затратна. Фактично, Aggarwal and Das (2012) створили один такий легкий протокол для інтеграції з існуючою системою безпеки, яка також підтримувала ефективність системи. Продовжуючи свою роботу, [36] представили засоби перевірки під час виконання в системі безпеки, відому як ASSET.

Ці розробники також представили такі функції, як динамічний моніторинг контексту та адаптація. Захищені протоколи ініціалізації також дозволили медичним пристроям на основі IoT бути додатково захищеними. Одна з таких методик була розроблена Хоу, Лі та Гуттманом (2013) під назвою Chorus для безпечної ініціалізації групи бездротових пристроїв. Цей дворівневий протокол захищав пристрої від зовнішніх кібератак за допомогою внутрішньосмугової аутентифікації групових повідомлень та угоди групового автентифікованого

ключа. Система також мала додаткові можливості масштабованості через низькі вимоги до обладнання та обчислень.

Інший спосіб забезпечити безпеку пристроїв Інтернету речей, пов'язаних із охороною здоров'я, — це створити окрему мережу, яка дозволяє централізовано відстежувати пристрої через агреговані концентратори. Необхідно також суворо контролювати тип даних, з якими взаємодіють пристрої. Це виключає шанси хакерів проникнути в мережу.

2.5 Вирішення проблем конфіденційності

Можуть виникнути проблеми з конфіденційністю, оскільки багато даних, які є приватними для пацієнта, зберігаються в базі даних, яка заповнена даними, отриманими за допомогою пристроїв IoT. Медичні картки пацієнта зберігаються в базах даних, які мають бути конфіденційними, для чого може бути використана техніка ABE, яка передбачає шифрування даних за допомогою таких алгоритмів, як MD5 і AES, перед тим, як будуть збережені в базі даних. Система охорони здоров'я працює у двох доменах безпеки, включаючи публічний домен і особистий домен, так що два домени можуть мати різні вимоги безпеки. У публічних доменах можуть бути такі користувачі, як лікарі, медсестри, практикуючі лікарі чи дослідники, тоді як особистий домен матиме пацієнтів.

Схема вимірювання може використовуватися для виявлення конфіденційності вмісту, зібраного з давачів, і чи його слід зберігати у загальнодоступному або приватному доступі, відповідно до якого права доступу до зібраних даних можуть надаватися відповідним ролям у відповідних доменах [37].

Атаки на конфіденційність також можуть включати помилкове введення даних, що може завдати шкоди додатку охорони здоров'я або Інтернету речей. Протистояти такій атаці в IoT важко, оскільки пристрої мають обмеження у використанні ресурсів, так що стандартні рішення безпеки не можуть бути

реалізовані всередині них. Щоб подолати ці проблеми, потрібна розподілена система виявлення кібератак [37].

Про прослуховування даних і збереження конфіденційності через бездротовий зв’язок можна подбати за допомогою криптографічних протоколів з рухомим кодом або за допомогою зв’язку, пов’язаного з тілом. Для захисту зображень можна використовувати техніку біполярного приховування даних, що дозволить лікарям додати цифрову печатку до зображення в документі про стан здоров’я пацієнта. Шифрування з відкритим ключем може допомогти покращити конфіденційність даних за допомогою ефективного механізму шифрування даних [38].

Крім того, стандарт IEEE 802.15.4 надає рекомендації щодо захисту різних рівнів доступу архітектури IoT і може використовуватися як інструмент для додавання функцій безпеки в систему [39].

2.6 Вирішення проблем безпеки фізичних об'єктів

Фізичні об’єкти, такі як давачі, також можуть зіткнутися з проблемами безпеки, оскільки вони мають обмежені ресурси і не можуть запускати складні алгоритми безпеки. Для цих об’єктів може використовуватися більше традиційних архітектур, і, таким чином, несанкціонований доступ може стати легшим для зловмисників. Система IoT складається з чотирьох ключових компонентів, які включають людину, інтелектуальний об’єкт, процес і технологічну екосистему. Всі ці компоненти взаємодіють один з одним і, таким чином, впливають на такі фактори безпеки, як ідентифікація, надійність конфіденційності, безпека, довіра та відповідальність.

Фізичні пристрої, такі як RFID-мітки, які також мають такі різні взаємодіючі компоненти можуть зіткнутися з різноманітними атаками безпеки, такими як відмова в обслуговуванні, клонування, підробка, відмова від обслуговування, а також атака посередині, зловживання тощо.

Певні методи захисту безпеки можуть допомогти захистити RFID-мітки, такі як системне ланцюжок для уникнення несанкціонованого зчитування, шифрування за допомогою алгоритму AES або MD5 тощо. Ці рішення допомагають забезпечити безпеку, конфіденційність та цілісність системи охорони здоров'я для її користувачів [40].

2.7 Питання безпеки для комунікаційних технологій

Комунікаційні технології можуть зіткнутися з проблемами безпеки, такими як атаки DOS, затоплення, атаки чорної діри та атаки самонаведення. Ці технології дуже схильні до поєднання безпеки і можуть бути використані для атак за допомогою відстеження, крадіжки даних, охоплення, атак «посередині» та ін'єкції шкідливого коду.

Методи виявлення вторгнень можна використовувати для захисту систем зв'язку, оскільки вони можуть виявляти шкідливі дії, забезпечувати брандмауер та можливості запобігання перешкодам. Шифрування можна використовувати для збереження конфіденційності даних, які передаються по бездротовій мережі. Деякі алгоритми шифрування, які можна використовувати для цього, включають DES (Стандарт шифрування даних), AES (Розширений стандарт шифрування) і EES (Стандарт шифрування з умовним договором). Пристрої LTE захищені за допомогою таких методів, як синхронізація порядкових номерів (SQN) і протокол повторної аутентифікації [41].

2.8 Проблеми безпеки для програм

Проблеми з безпекою також можуть виникати в програмах, які використовуються в хмарі для керування мережею IoT. Щоб забезпечити безпеку програм, загальним заходом, який необхідно вжити, є захист точок доступу до

даних. Це можна зробити за допомогою механізмів захисту в точках, де дані про стан здоров’я пацієнтів передаються через хмару.

У цей момент зловмисник може отримати доступ до збережених медичних даних і змінити їх, щоб вплинути на пацієнта. Таким чином, дуже важливо підтримувати точки доступу найбільш безпечними в системі. Деякі з методів, які використовуються в системах Інтернету речей охорони здоров’я для такого захисту, включають використання алгоритмів безпеки, таких як шифрування на основі атрибутів шифрування політики (CPABE), яке використовує шифрування на основі атрибутів (ABE), працює над криптографією кривої Elliptc (ECC).), і використовує білінійне відображення [42].

2.9 Питання безпеки особистого захисту

Захист даних і конфіденційність осіб є двома взаємопов'язаними проблемами інформаційної безпеки. Мережі IoT передбачають захоплення та передачу великої кількості даних, які можуть включати особисту та конфіденційну інформацію. Пристрої Інтернету речей також можна модернізувати за межі простого збору даних, щоб з’явились нові можливості. Ці нові можливості також створюють нові ризики для безпеки осіб. Давачі IoT можуть збирати велику кількість даних про фізіологію та навколишнє середовище користувача за допомогою розумних пристроїв, таких як а ноутбуки, смартфони та цифрові носії. Ці розумні речі після оновлення можна керувати таким чином, щоб впливати на фізичні дії. Зв’язок може відбуватися між об’єктами, які під’єднані до мережі IoT автоматично, щоб вони обмінювалися даними один з одним і діяли відповідно до того ж [43].

Ця автоматична взаємодія та дії можуть вплинути на конфіденційність, конфіденційність та цілісність інформації, якою обмінюється. Особиста інформація, яку містять пристрої IoT, може містити дані не тільки особи, яка використовує пристрій, але й інших людей, які можуть бути пов’язані з

користувачем або якимось чином пов’язані з ним. Дані можуть містити деталі соціальної особистості, такі як ім’я, адреса, номер мобільного телефону тощо. Пристрої IoT містять багато даних, але недостатньо розвинені, щоб реалізувати всі рівні безпеки, які можуть захистити ці особисті дані, що може вимагати дотримання різноманітних політик конфіденційності, які можуть залежати від ситуації або контексту. Більший обсяг збору персональних даних може викликати проблеми незаконної обробки, профілювання, відстеження, призначення, виконання місії та багато інших проблем. Правозастосування у цьому контексті необхідно розуміти як захист прав користувачів, принципи галузі даних, право власності на дані, процедури контролю, порушення конфіденційності та середовище IoT характеристики. Можуть виникнути занепокоєння щодо крадіжки особистих даних, якщо дані відкрито доступні через мережі IoT. Наприклад, безконтактні кредитні картки можна прочитати без аутентифікації, що може дати можливість хакерам або зловмисникам володіти ідентичністю користувачів на банківському рахунку [44].

Шкідливі атаки на пристрої Інтернету речей можуть призвести до компрометації пристрою, а контроль переходить в руки зловмисника, завдяки чому отримується несанкціонований доступ до персональних даних, що підвищує ризик для користувачів. Частіше користувачі обмежені певним постачальником послуг і не можуть вільно переходити до іншого, що накладає обмеження, які можуть зашкодити безпеці. У секторі охорони здоров’я це може мати значні ризики для безпеки та конфіденційності, піддаючи ризику цілісність даних пацієнтів. Програма охорони здоров’я може розкрити зловмиснику дані про хворобу, яку має особа, що може бути використано для початку фізичного нападу, створюючи таким чином особисті ризики для здоров’я та життя пацієнта. Оскільки системи IoT автоматизують процес прийняття рішень, контроль над даними та рішеннями, які ініціюють конкретні дії з пристроїв втрачені. Це хвилює більшість людей, тому в усьому світі існує кілька законів про захист даних для захисту даних, які використовуються таким чином [34].

3 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ХОРОНИ ПРАЦІ

3.1 Порядок надання домедичної допомоги постраждалим при раптовій зупинці серця

Наше життя залежить не тільки від медичного працівника. Коли раптом людина перестала дихати, дати їй шанс вижити може будь-яка особа, яка опинилася поруч. І якщо розпочати надавати допомогу вперші 5 хвилин, ще до приїзду бригади екстреної медичної допомоги, Ви можете врятувати чиєсь життя. Не будьте байдужими! Проте слід знати, як це робити правильно.

1. Перед тим, як почати надавати допомогу, переконайтесь у відсутності небезпеки.

2. Визначте наявність свідомості: необхідно обережно потрясти постраждалого за плече та голосно звернутися до нього, наприклад: «З Вами все гаразд? Як Ви себе почуваєте?».

3. Якщо постраждалий реагує:

а) коли хворому нічого не загрожує, потрібно залишити його в попередньому положенні;

б) з’ясувати характер події, що сталася;

в) викликати бригаду екстреної медичної допомоги;

г) повідомити диспетчеру інформацію про постраждалого відповідно до його запитань та виконати його вказівки;

д) забезпечити нагляд за постраждалим до приїзду бригади екстреної (швидкої) медичної допомоги.

4. Якщо постраждалий не реагує:

а) звернутися до осіб, які поряд, за допомогою;

б) якщо постраждалий лежить на животі, повернути його на спину, фіксуючи шийний відділ хребта, та відновити прохідність дихальних шляхів, очистити ротову порожнину серветкою або

одягом хворого. Якщо механізмом травми було падіння з висоти, дорожньо-транспортна пригода, повішення або утоплення, допускати, що у постраждалого можлива травма в шийному відділі хребта;

в) при відсутності травми в шийному відділі хребта відновити прохідність дихальних шляхів методом закидання голови та розкрити ротову порожнину. За підозри на травму в шийному відділі хребта використовують метод висування нижньої щелепи вперед та розкриття ротової порожнини. Необхідно також визначити наявність дихання за допомогою прийому: «чути, бачити, відчувати». Суть цього прийому: нахилити своє обличчя максимально близько до рота та носа постраждалого, водночас боковим зором спостерігати за рухами грудної клітини хворого. За допомогою цього маневру Ви маєте змогу бачити рухи грудної клітки, вухом чути шум дихання, шкірою щоки вловлювати рух повітря під час дихання (відчуття тепла). Наявність дихання визначати протягом 10 секунд. У нормі за 10 секунд повинні почути 2 вдихи. Якщо вдихи відсутні чи лише один вдих, або виникли сумніви, чи є дихання, можна вважати, що дихання відсутнє.

5. Якщо постраждалий дихає, при відсутності свідомості:

а) перемістити постраждалого у стабільне положення (на боці), якщо не йдеться про травму хребта;

б) викликати бригаду екстреної (швидкої) медичної допомоги;

в) забезпечити нагляд за постраждалим до приїзду бригади екстреної (швидкої) медичної допомоги;

6. Якщо дихання відсутнє:

а) викликати бригаду екстреної (швидкої) медичної допомоги;

б) розпочати проведення серцево-легеневої реанімації:

– скласти руки в «замок», розмістити на середину грудини;

– виконати 30 натискань на грудну клітку глибиною не менше 5 см (не більше 6 см), з частотою 100 натискань (не більше 120) за хвилину;

– виконати 2 вдихи з використанням маски-клапану, дихальної маски тощо. За відсутності захисних засобів можна не виконувати штучне дихання, а проводити тільки натискання на грудну клітку.

Виконання двох вдихів повинно тривати не більше 5 секунд:

– після двох вдихів продовжити натискання на грудну клітку відповідно до наведеної схеми;

– змінювати особу, що проводить натискання на грудну клітку, кожні 2 хвилини;

– при відновленні у постраждалого дихання, рухової активності до прибуття бригади екстреної (швидкої) медичної допомоги припинити проведення серцево-легеневої реанімації.

Отже, кожна людина повинна володіти навичками з надання першої медичної допомоги, адже у ваших руках може бути чиєсь врятоване життя.

3.2 Вимоги охорони праці при виконанні робіт на персональному комп'ютері

Робочі місця офісних працівників, обладнані персональними комп'ютерами, повинні відповідати вимогам «Правил охорони праці під час експлуатації електронно – обчислювальних машин», затверджених Наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду від 26.03.2010 року №65 та «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно – обчислювальних машин», затверджених постановою Головного державного санітарного лікаря України від 10.12.1998 року №7 (ДСанПіН 3.3.2-007-98). Правила поширюються на всіх суб'єктів господарювання незалежно від форм власності, які у своїй

діяльності здійснюють роботу, пов’язану з персональними комп’ютерами, у тому числі на тих, які мають робочі місця, обладнані персональними комп’ютерами і периферійними пристроями.

Вимоги щодо розміщення і планування приміщень для роботи з комп’ютером:

Робочі місця, обладнані персональними комп’ютерами, заборонено облаштовувати у підвальних або цокольних приміщеннях будівель. При обладнанні приміщень забороняється використання полімерних матеріалів, що виділяють шкідливі хімічні речовини.

Також слід приділити увагу забезпеченню достатнім для здійснення роботи рівнем освітлення (природного та штучного – у темну пору доби) та звукоізоляції. Для регуляції рівня освітлення природним світлом бажано застосовувати жалюзі. Окрім того, у приміщеннях, де здійснюється робота з комп’ютерами, щодня має здійснюватися вологе прибирання з метою недопущення запиленості підлоги та меблів.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), мають бути надійно захищені діелектричними щиткам або сітками з метою недопущення потрапляння людини під напругу.

Особливої уваги заслуговують заходи дотримання протипожежної безпеки. Так, у всьому офісі лінії електромережі мають бути захищені від виникнення короткого замикання, а також від перепадів мережевої напруги, що може спричинити збої в роботі електронно–обчислювальної техніки. Приміщення (окрім тих, де розташовуються сервери) мають бути оснащені системою автоматичної пожежної сигналізації та вогнегасниками. Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, застосовувати негорючу ізоляцію.

У приміщенні, де одночасно експлуатуються понад п'ять комп’ютерів, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

Вимоги щодо організації та обладнання робочих місць. Площа, відведена на одне робоче місце має становити не менше 6 кв.м., а об’єм – не менше 20 куб.м. Конструкція робочого місця повинна забезпечувати підтримання оптимальної робочої пози, тобто такої, яка дозволяє працівникові виконувати роботу з мінімальним напруженням тіла, і яка дозволяє уникнути перевтоми в ході і після закінчення робочого процесу. Раціональна робоча поза має важливе значення для збереження здоров’я працівника, оскільки тривале перебування його в незручній і напруженій позі може призвести до таких захворювань, як сколіоз (викривлення хребта), варикозне розширення вен, плоскостопість тощо. Установлено, що робота в зігнутому положенні збільшує затрати енергії на 20%, а при значному нахиленні – на 45% порівняно з прямим положенням корпуса.

За потреби особливої концентрації уваги під час виконання робіт суміжні робочі місця операторів необхідно відділяти одне від одного перегородками висотою 1,5 – 2 м.

Робочі місця слід розташовувати відносно джерела природного світла (вікон) таким чином, щоб світло падало збоку, переважно зліва. Також робоче місце має відповідати сучасним вимогам ергономіки [52]:

- стіл повинен мати висоту поверхні 680 – 800 мм, ширину 600 – 1400 мм і глибину 800 – 1000 мм. Такі параметри забезпечують можливість виконання операцій в зоні досяжності працівника;
- робочий стілець має бути підйомно – поворотним, з можливістю регулювання висоти, бажано зі стаціонарними або змінними підлікотниками і напівм’якою нековзкою поверхнею сидіння, що легко чиститься і не електризується;

- екран комп’ютера має розташовуватися на оптимальній відстані від користувача, що становить 600 – 700 мм, але не менше 600 мм з урахуванням літерно – цифрових знаків і символів;
- відстань між бічними поверхнями персональних комп’ютерів повинна бути не менше 1,2 метри;
- відстань від тильної поверхні одного персонального комп’ютера до екрана іншого – 2,5 метри.
- персональний комп’ютер та його комплектуючи (монітор та інші периферійні пристрої) не повинні потрапляти під прямі промені сонячного світла та під дію інших джерел тепла (батареї опалення та інші прилади для обігріву приміщень).

*Вимоги безпеки під час роботи з комп’ютером***.** Щодня перед початком роботи оператор повинен:

- оглянути своє робоче місце: про виявлення ознак пошкодження обладнання інформувати свого безпосереднього керівника;
- відрегулювати освітленість на робочому місці, переконатися в відсутності відблисків на екрані комп’ютера, відсутності зустрічного світла;
- перевірити правильність підключення обладнання ЕОМ до електромережі;
- очистити екран комп’ютера від пилу та інших забруднень;
- перевірити правильність організації робочого місця й за необхідності провести відповідні коригування.

Оператор під час роботи зобов’язаний:

- виконувати тільки ту роботу, яку йому було доручено;
- підтримувати порядок і чистоту на робочому місці;
- тримати відкритими всі вентиляційні отвори обладнання;
- коректно закрити всі активні завдання у разі припинення роботи з комп’ютером;

- негайно відключити комп’ютером від електричної мережі у разі виникнення аварійної ситуації.

ВИСНОВОК

Незважаючи на низку загроз безпеці та конфіденційності, які створює технологія IoT, системи та протоколи одночасно були розроблені для запобігання та подолання цих порушень та забезпечити безпечне зберігання персональних даних про здоров'я.

Більше користувачів є синонімом збільшення обсягу даних, обробка яких зрештою стане надзвичайно складною. Це може поставити під загрозу безпеку особистої інформації. Інтерпретація результатів з такої великої кількості даних – це виснажлива робота, яка вимагає більш складних аналітичних програм і експертів з даних, ніж те, що існує зараз.

Інтеграція кількох пристроїв є ще одним недоліком, над яким зараз працюють виробники. Тому вкрай важливо створити набір протоколів і стандартів, які дозволяють легко групувати пристрої та швидкий обмін інформацією. Це може значно прискорити процес лікування та надати медичним працівникам повну вичерпну інформацію.

Важливо розуміти, що там, де безпека є серйозною проблемою в інших областях, пов’язаних з Інтернетом речей, у медицині це може бути питанням життя і смерті.

Дослідження та висновки, отримані в рамках цієї кваліфікаційної роботи, можуть бути використані та проаналізовані для розробки подальших рішень щодо управління та безпеки інформаційних систем у галузі охорони здоров’я. Очікується, що результати дослідження прокладуть шлях до подальшого визначення рішень, а також проблем, пов’язаних із забезпеченням безпеки інформаційних систем.

Результати дослідження можуть бути використані медичними працівниками для того, щоб покращити безпеку інформаційної системи. Крім того, висновки дослідження також можуть бути використані для того, щоб отримати додаткові знання щодо способів забезпечення безпеки інформації про

системи охорони здоров’я. Тому можна стверджувати, що результати дослідження будуть буде корисним для пацієнтів, постачальників медичних послуг, а також для дослідників у майбутньому.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kodali, R., Swamy, G. and Boppana, L. (2017). An implementation of IoT for healthcare. In: Conference: 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS). [online] Warangal: IEEE. Available at: https://www.researchgate.net/publication/305284960_An_implementation_of_IoT_fo r_healthcare [Accessed 16 Apr. 2022].
2. Bilal, M. (2012). A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers. Zhejiang University Hangzhou.
3. Garg, A. (2016). The Internet of Things: Impacts on Healthcare Security and Privacy. Litmos.
4. Canteaut, A., Lauradoux, C. and Seznec, A. (2006). Understanding cache attacks. [online] Institut National de Recherche en Informatique et en Automatique. Available at: https://www.rocq.inria.fr/secret/Anne.Canteaut/Publications/RR-5881.pdf [Accessed 23 May. 2022].
5. CityPulse. (2014). Real-Time IoT Stream Processing and Large-scale Data Analytics for Smart City Applications. CityPulse.
6. Collins, K. (2015). Know your real-time protocols for IoT apps. [online] InfoWorld. Available at: https://www.infoworld.com/article/ 2972143/internet-of-things/real-time-protocols-for-IoT-apps.html [Accessed 16 May. 2022].
7. Davidavičienė, V. (2018). Research Methodology: An Introduction. Progress in IS, pp.1-23.
8. Dasgupta, A., Mehta, R., & Raha, D. (2012). Healthcare Infrastructure and Services Financing in India: Operation and Challenges. PWC.
9. Denzin, N. and Lincoln, Y. (2000). Handbook of qualitative research. Thousand Oaks: Sage.

10. Dhar, M., Monangi, S., Setlur, R., Ramanathan, R. and Bhasin, S. (2018). Analysis of functioning and efficiency of a code blue system in a tertiary care hospital. Saudi Journal of Anaesthesia, 12(2), p.245.
11. Dlodlo, N. (2013). Potential applications of the internet of things technologies for South Africa's health services. Meraka Institute.
12. Hou, Y., Li, M. and Guttman, J. (2013). Chorus. Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks - WiSec '13.
13. H.Weber, R. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), pp. 23-30.
14. Human Kinetics Europe. (n.d.). Steps of the research process. [online] Available at: https://uk.humankinetics.com/blogs/excerpts/steps-of-the-research-process [Accessed 21 May. 2022].
15. infisim, V. (n.d.). What are the main benefits of IoT in healthcare? | InfiSIM. [online] InfiSIM. Available at: https://www.infisim.com/main-benefits-IoT-healthcare/ [Accessed 16 MAY 2022].
16. Internet of Things (IoT). (2017).This will help the Internet of Things growing faster.... [online] Available at: http://nicolaswindpassinger.com/IoT-standardization-care [Accessed 21 Mart 2022].
17. IoT Agenda. (n.d.). What is IoT devices (internet of things devices)? - Definition from WhatIs.com. [online] Available at: https://internetofthingsagenda.techtarget.com/definition/IoT-device [Accessed 16 Mart 2022].
18. Mallick, M. R. (2016). A Comparative Study of Wireless Protocols with LI-FI Technology: A Survey. International Journal of Advanced Computational Engineering and Networking, 4(6), pp. 123-127.
19. Milovanovic, D., & bojkovic, Z. (2017). Cloud-based IoT healthcare applications: Requirements and recommendations. International Journal of Internet of Things and Web Services, Volume 2, pp. 60-65.

20. Mishra, R. k., & Pandey, R. (2013). Aspects of Network Architecture for Remote Healthcare Systems. F.G.I.E.T .
21. Mohammed, J., Lung, C., Ocneanu, A., Thakral, A., Jones, C. and Adler, A. (2014). Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing. 2014 IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom). MS, A. (n.d.). Elliptic Curve Cryptography. [ebook] MIT University. Available at: https://ocw.mit.edu/courses/mathematics/18-704...elliptic-curves.../asarina.pdf [Accessed 21 Mart 2022].
22. Munir, A., Kansakar, P., & Khan, S. U. (2017). IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things. ARXIV.
23. Narendra, P., Duquennoy, S., & Voigt, T. (2015). BLE and IEEE 802.15.4 in the IoT: Evaluation and Interoperability Considerations. SICS.
24. Nath, S., & Som2, S. (2017). Security and Privacy Challenges: Internet of Things. Indian Journal of Science and Technology, 10(3), pp 2-5.
25. Niewolny, D. (2013). How the Internet of Things Is Revolutionizing Healthcare. Freescale Semiconductor.
26. Paavola, M. (2007). Wireless Technologies in Process Automation - Review and an Application Example. University of Oulu.
27. Patel, S., Singh, N., & Pandya, S. (2017). IoT based Smart Hospital for Secure Healthcare System. International Journal on Recent and Innovation Trends in Computing and Communication, 5(5), pp. 404-408.
28. Pathak, A. K. (2017). Security Challenges in Internet of Things (IoT). International Journals of Advanced Research in Computer Science and Software Engineering, 7(6), 648-652.
29. Preethi, 1. S., & J Senthil Kumar. (2017). IoT based Secure Healthcare System using BSN. IJRSET, 4(4), pp. 40-46.

30. Schorer, M., & Spier, M. (2017). IoT Business Brief – Healthcare Business. VMWare.
31. Sermakani, V. (2014). Transforming healthcare through Internet of Things. Project Management Practioners Conference (pp. 3-26). Bangalore: NIMHANS.
32. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, pp. 1-25.
33. Shen, W., Xu, Y., Xie, D., Zhang, T. and Johansson, A. (2011). Smart Border Routers for eHealthCare Wireless Sensor Networks. 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing.
34. Sidhu, B., Singh, H., & Chhabra, A. (2007). Emerging Wireless Standards - Wi-Fi, ZigBee and WiMAX. International Journal of Electronics and Communication Engineering, pp. 43-48.
35. Snieder, R. and Larner, K. (2013). The art of being a scientist. Cambridge: Cambridge Univ. Press.
36. Stolbikova, V. (2016). Can Elliptic Curve Cryptography be Trusted? A Brief Analysis of the Security of a Popular Cryptosystem. ISACA Journal, [online] 3. Available at: https://www.isaca.org/Journal/archives/2016/volume-3/Pages/can-elliptic-curve-cryptography-be-trusted.aspx [Accessed 23 May 2022].
37. Wind. (2015). Security in the Internet of Things: Lessons from the Past for the Connected Future. Wind River Systems, Inc.
38. Zarghami, S. (2013). Middleware for internet of things. University of Twente.
39. Zhou, W., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. University of Chinese Academy of Sciences.
40. Zhou, X., & Lutfiyya, H. (2016). IoT Stream Analytics Platform. The University of Western Ontario. Maleh, Y. and Ezzati, A. (2016). Towards an Efficient Datagram Transport Layer Security for Constrained Applications in Internet of Things. International Review on Computers and Software (IRECOS), 11(7), p.611.

41. Mallick, M. R. (2016). A Comparative Study of Wireless Protocols with LI-FI Technology: A Survey. International Journal of Advanced Computational Engineering and Networking, 4(6), pp. 123-127.
42. Mukherjee, S., Dolui, K., & Datta, S. K. (2013). Patient Health Management System using e-Health Monitoring Architecture. Kolkata, India: St. Thomas‟ College of Engineering and Technology.
43. Munir, A., Kansakar, P., & Khan, S. U. (2017). IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things. ARXIV.
44. Narendra, P., Duquennoy, S., & Voigt, T. (2015). BLE and IEEE 802.15.4 in the IoT: Evaluation and Interoperability Considerations. SICS.