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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: Система геолокації інфекційного хворого

Виконав(ла): студент(ка) 6 курсу, групи САм-61
спеціальності
124 «Системний аналіз»
(шифр і назва спеціальності)

(підпис) Головко О.В. (прізвище та ініціали)

Керівник (підпис) Кунанець Н.Е. (прізвище та ініціали)

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

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

Рецензент (підпис) Цуприк Г.Б. (прізвище та ініціали)

Тернопіль
2020

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)
« » 2020 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 124 «Системний аналіз»
(шифр і назва спеціальності)

студенту Головку Олександру Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Система геолокації інфекційного хворого

Керівник роботи д.н.с.к., професор кафедри КН Кунанець Н.Е.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20___ року № _____

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1 Аналіз наукових публікацій
2 Автоматизоване відстеження контактів інфекційних хворих
3 Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

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

7. Дата видачі завдання 21 вересня 2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.09.20-27.09.20	*Виконано*
2.	Підбір наукових джерел щодо системи геолокації	28.09.20-04.10.20	*Виконано*
	інфекційного хворого		
3.	Переклад та опрацювання наукових джерел щодо	05.10.20-11.10.20	*Виконано*
	системи геолокації інфекційного хворого		
4.	Виконання дослідження щодо системи геолокації	12.10.20-18.10.20	*Виконано*
	інфекційного хворого		
5.	Оформлення розділу «Аналіз наукових публікацій»	19.10.20-25.10.20	*Виконано*
6.	Оформлення розділу « Автоматизовавне відстеження »	26.10.20-01.11.20	*Виконано*
	Контактів інфекційних хворих»		
7.	Оформлення розділу «Охорона праці та безпека в	02.11.20-08.11.20	*Виконано*
	надзвичайних ситуаціях»		
8.	Виконання завдання до підрозділу «Охорона праці»	09.11.20-15.11.20	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	16.11.20-22.11.20	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	23.11.20-29.11.20	*Виконано*
11.	Нормоконтроль	30.11.20-05.12.20	*Виконано*
12.	Перевірка на плагіат	07.12.20	*Виконано*
13.	Попередній захист кваліфікаційної роботи	14.12.20	*Виконано*
14.	Захист кваліфікаційної роботи	21.12.20	

Студент _____ Головко О.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кунанець Н.Е.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Система геолокації інфекційного хворого // Кваліфікаційна робота освітнього ступеня «Магістр» // Головко Олександр Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група САм-61 // Тернопіль, 2020 // С. 97, рис. – 25, табл. – 9, додат. – 1, бібліогр. – 66.

Ключові слова: ГЕОЛОКАЦІЯ, COVID-19, ЗАСТОСУНКИ, ДОСЛІДЖЕННЯ

У кваліфікаційній роботі досліджено систему геолокації інфекційного хворого. Розглянуто застосунки для відстеження контактів хворих та заражених на COVID-19 і їх моніторинг.

Розглянуто існуючі системи телемедицини як у світі так і в Україні, закон «Про телемедицину». Їх вплив на систему охорони здоров'я, яку роль вони відіграють в час епідемії. Описано основні методи визначення місця розташування які використовуються у світі на даний час і їх основні недоліки та переваги.

Проаналізовано існуючі застосунки для відстеження контактів хворих на COVID – 19. Описані їхні архітектури які розділяються на: централізовану, децентралізовану та гібридну.

Описано моделі для відстеження контактів які складаються з певних етапів та кроків. Дві основних із них є модель яка використовує бездротові технології як NFC та Bluetooth, друга – GSM мережі.

Розглянуто систему IoT у діагностиці пацієнтів з COVID-19. Описано застосунок для моніторингу коронавірусу SDA-COVID-19.

ANNOTATION

IS for analytical data processing of psychometric tests // Qualifying work of the educational degree "Master"// Holovko Olexandr V. // Ternopil’ Ivan Pul’uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science, group SAm-61/ / Ternopil', 2020 // P. 97, Tables – 9, Fig. – 25, Annexes. – 1 , References – 66.

Keywords: GEOLOCATION, COVID -19 , APPS, RESEARCH

In the thesis the system of geolocation of an infectious patient is investigated. Applications for tracking the contacts of patients and infected with COVID-19 and their monitoring are considered.

The existing telemedicine systems both in the world and in Ukraine, the law "About telemedicine" are considered. Their impact on the health care system and the role they play in the epidemic. Describes the main methods of determining the location used in the world today and their main disadvantages and advantages.

The existing applications for tracking the contacts of patients with COVID - 19 are analyzed. Their architectures are described, which are divided into: centralized, decentralized and hybrid.

Describes models for tracking contacts that consist of certain steps and steps. The two main ones are a model that uses wireless technologies like NFC and Bluetooth, the second is GSM networks.

The IoT system in the diagnosis of patients with COVID-19 is considered. An application for monitoring coronavirus SDA-COVID-19 is described.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ГІС – геоінформаційна система.

ЕОМ – електронно-обчислювальна машина.

ПЕОМ – персональна електронно-обчислювальна машина.

ВДТ – візуально-дисплейний термінал.

БД – база даних.

ПЗ – програмне забезпечення.

НС – надзвичайна ситуація.

ЦО – цивільна оборона.

HUB – в загальному розумінні, вузол певної мережі.

BLE (англ. Bluetooth Low Energy) – є частиною специфікації Bluetooth 4.0, яка також включає протоколи класичного Bluetooth і протокол високошвидкісного Bluetooth (Classic Bluetooth and Bluetooth High Speed Protocols).

ПК – персональний комп’ютер.

LCS (Location Services) – це спеціальні послуги, що підтримуються бездротовими мережами, які використовують місцерозташування користувачів.

IoT (англ. Internet of Things) – це мережа фізичних об'єктів, які мають вбудовані технології, що дозволяють здійснювати взаємодію з зовнішнім середовищем, передавати відомості про свій стан і приймати дані ззовні.

XML (англ. Extensible Markup Language) – запропонований консорціумом World Wide Web Consortium (W3C) стандарт побудови мов розмітки ієрархічно структурованих даних для обміну між різними застосунками, зокрема, через Інтернет.

SSID (англ. Service Set Identifier) – унікальне найменування бездротової мережі, що відрізняє одну мережу Wi-Fi від іншої.

NFC (англ. Near Field Communication) – технологія бездротового високочастотного зв'язку малого радіуса дії.

GPS (англ. Global Positioning System) – сукупність радіоелектронних засобів, що дозволяє визначати положення та швидкість руху об'єкта на поверхні Землі або в атмосфері.

SOAP (англ. Simple Object Access Protocol) – протокол обміну структурованими повідомленнями в розподілених обчислювальних системах, базується на форматі XML.

ЗМІСТ

ВСТУП

*Актуальність теми роботи***.** Новий тип коронавірусу COVID-19 виявився найбільшим викликом через його постійну структурну еволюцію, а також відсутність належних антидотів для цього конкретного вірусу. Вірус в основному поширюється і розмножується серед людей завдяки тісному контакту, що, на жаль, може відбуватися різними непередбачуваними способами. Тому, щоб уповільнити поширення цього нового вірусу, єдиними важливими ініціативами є підтримка соціальної дистанції, здійснення відстеження контактів, використання належних засобів безпеки та запровадження карантинних заходів. Для контролю за розповсюдженням вірусу дослідники та органи влади розглядають можливість використання мобільних застосунків на основі смартфонів для ідентифікації ймовірних заражених людей, а також зони з високим ризиком зараження для підтримки заходів ізоляції. В даній роботі запропоновано новий метод відстеження контактів COVID-19 на основі даних геолокації користувачів мобільних телефонів.

Метою дослідження є огляд сучасних викликів та застосування застосунків для відстеження контактів у боротьбі з пандемією COVID-19.

Завданнями роботи є:

- Забезпечити актуальний огляд сучасних проблем та програм відстеження контактів у боротьбі проти COVID-19 в сучасному світі.
- Обговорити рекомендації щодо вирішення цих проблем.
- Дослідити сучасні наслідки використання цифрового відстеження контактів та майбутніх спалахів інфекційних хвороб.
- Дослідити методи визначення місця розташування.
- Обговорити роль телемедицини в час пандемії.

Об'єктом дослідження є огляд застосунків та програм відстеження контактів у боротьбі проти COVID-19.

Предмет дослідження – актуальний огляд сучасних проблем програм відстеження контактів у боротьбі проти COVID-19 в суспільстві.

Апробація результатів магістерської роботи. Окремі результати роботи представлені на такій науковій конференції:

1. VIII науково – технічна конференція «Інформаційні моделі, системи та технології» На тему « Using smartphones and wearable devices to monitor behavioral changes during covid-19» («Використання смартфонів та носимих пристроїв для моніторингу змін поведінки під час covid-19») та на тему « Telemedicine in the covid-19 era» (« Телемедицина в епоху Covid-19»).

1 АНАЛІЗ НАУКОВИХ ПУБЛІКАЦІЙ ПО ТЕМІ ДОСЛІДЖЕННЯ

1.1 Існуючі медичні системи телемедицини, охорони здоров'я

Завдяки вдосконаленій системі охорони здоров’я та високим рівнем життя тривалість життя постійно збільшується. Оскільки мобільність людей також зросла, члени сім'ї часто живуть далеко один від одного. Це означає, що турбота про старших переходить від молодого покоління до системи соціальної допомоги. Це додає додаткового навантаження на систему охорони здоров’я.

В даний час більшість країн постраждали від пандемії COVID-19, яка не тільки загрожує здоров’ю населення, але і змінює багато аспектів життя людей, зокрема світову економіку. Різні країни розглядали кілька заходів щодо боротьби з COVID-19 та контролю за ним. Послуги телемедицини – один із найефективніших способів боротьби з пандемією COVID-19 та боротьби з нею. З огляду на високий ризик передачі хвороби через контакт від людини до людини, телемедицина може бути корисною для контролю COVID-19 за рахунок зменшення прямого контакту. Одним з важливих застосувань телемедицини є спостереження за пацієнтами після виписки з лікарні, яке також може бути використане для пацієнтів з COVID-19. Відповідно, це може зменшити контакт між пацієнтами та лікарями, а також призведе до посилення нагляду за населенням.

Всесвітня організація охорони здоров'я визначає телемедицину як «надання медичних послуг усіма медичними працівниками з використанням інформаційно-комунікаційних технологій для обміну дійсною інформацією для діагностики, лікування та профілактики захворювань та травм "[1]. Тому, телемедицина може здійснюватися за допомогою таких засобів зв’язку тексту (електронна пошта, Facebook Messenger, WhatsApp), відео (Skype, Zoom, Microsoft Teams, Facetime тощо) або аудіо (телефон). Вона може бути синхронізованою (текст, відео чи аудіо в режимі реального часу) або

асинхронною (електронною поштою), і може залучати різних осіб (пацієнт-лікар, лікар-терапевт, медичний працівник-пацієнт або медичний працівник).

В Україні телемедицина почала розвиватися на початку 2000-х. Спочатку в Одеській області, Дніпропетровській та Харківській. Телемедичні мережі почали будувати приватні клініки. Тоді це відбувалося на рівні ініціативи окремих медичних закладів.

Був прийнятий законопроект «Про телемедицину» (№ 10196 від 14.03.2012 р.) який визначає її як комплекс організаційних, фінансових і технологічних заходів, що забезпечують надання дистанційної консультаційної медичної послуги, за якої пацієнт або лікар, що безпосередньо проводить обстеження та/або лікування пацієнта, отримує дистанційну консультацію іншого лікаря з використанням телекомунікацій[38].

Великим кроком для активного розвитку відео консультацій по всій країні стала телемедична мережа Medinet. Ця платформа почала функціонувати на базі Одеської області у 2019 році. Менш ніж за рік роботи лікарі надали понад 10 тис. телеконсультацій. В умовах боротьби з COVID-19 багато медичних закладів України долучаються до дистанційних відеоконсультацій, які дозволяють зберегти здоров'я лікарів і пацієнтів, а також взаємодіяти лікарям з колегами в особливо складних випадках.

Для здійснення телемедицини між пацієнтами та медичним персоналом потрібна усна згода, причина консультації, наявність медичної картки, рекомендації та запис часу, проведеного на консультації, та аналізу даних медичної карти [2].

Це можна полегшити за рахунок інтеграції IT-систем, призначених для літніх користувачів. Однак система телемедицини обмежена не лише соціальним доглядом, вона може використовуватися в будь-яких ситуаціях домашнього догляду для тих, хто потребує постійного нагляду або живе далеко від будь-якого медичного закладу. Використання системи повинно входити в повсякденний режим будь-якого користувача, і її застосування не повинно бути проблемою. Це

нещодавно розроблене рішення може бути застосоване від лікарень до клінік до будинків для престарілих. Ця система надає більшу свободу та впевненість у собі своїм користувачам.

Система телемедицини повинна мати веб-сайт, за допомогою якого можна вирішити вищезазначену проблему. Доглядачі можуть бачити виміри своїх пацієнтів у будь-який час і в будь-якому місці, оскільки послуги надаються цілодобово.

Користувач (пацієнт, лікар або медсестра) може опитати певні параметри здоров'я в своїх пацієнтів за датою та типом. Крім того, доглядачі можуть бачити деякі дані пацієнтів, на призначених пристроях можна змінювати межі вимірювання індивідуально. Пацієнти можуть лише переглядати власні виміри. Результати вимірювань відображаються на різних діаграмах у веб-клієнті. Однак дані, що відображаються на веб-сайті, мають звідкись надходити. В систему вбудовано чотири пристрої:

- Вимірювач артеріального тиску.
- Глюкометр крові.
- Термометр для тіла.
- Шкала балансу.

Жоден з них не може безпосередньо спілкуватися з веб-сервером. Оскільки вони мають лише модуль Bluetooth та модуль Wi-Fi. Тому потрібен комунікаційний пристрій, телефон, який виступає в ролі комунікаційного вузла, і програма, яка здатна взаємодіяти з пристроями та веб-сервером. Телефон отримує дані від пристроїв і додає до них деяку необхідну інформацію, наприклад, дату, час, місце вимірювання та контролер.

Документи, які надсилаються на веб-сервер, обробляються та зберігаються у базі даних. Для цього існує служба, де HUB надсилає дані, і ця служба також відповідає за обробку. Оброблені дані зберігаються в базі даних у форматі XML. Крім того, програма може ідентифікувати будь-якого зареєстрованого користувача. Кожен користувач повинен мати тег NFC, який ідентифікує їх.

Значення тегів NFC зберігається в базі даних, і базовий користувач запитує це за допомогою HUB. Таким чином, система може призначити вимірювання пацієнту та керівнику для нього / неї.

Життєво важливі параметри: артеріальний тиск, рівень глюкози в крові, температура тіла, маса тіла. Вони контролюються пацієнтами вдома за порадою лікаря. В рамках системи створено інструменти, які надсилають попереджувальні повідомлення лікарям або медсестрам, якщо вимірювання відхиляються від норми.

Смартфон із застосунком відповідає за передачу інформації від кінцевого обладнання (лічильник артеріального тиску, глюкометр, термометр тіла та ваги) до веб-служби телемедицини та ідентифікації користувачів шляхом сканування їх тегів NFC (Near Field Communication). HUB також створює XML-документ на основі інформації, яка надходить за шкалою балансу. Крім того, HUB відображає отриману інформацію.

З іншого боку, користувач може поєднувати нові пристрої з застосунком; тому існує вбудований посібник, який допоможе користувачам у цьому. Крім того, у HUB є прихований режим адміністратора, де можна встановити адресу веб-сервера, мобільний Інтернет або Wi-Fi із SSID та паролем (рис 1.1).

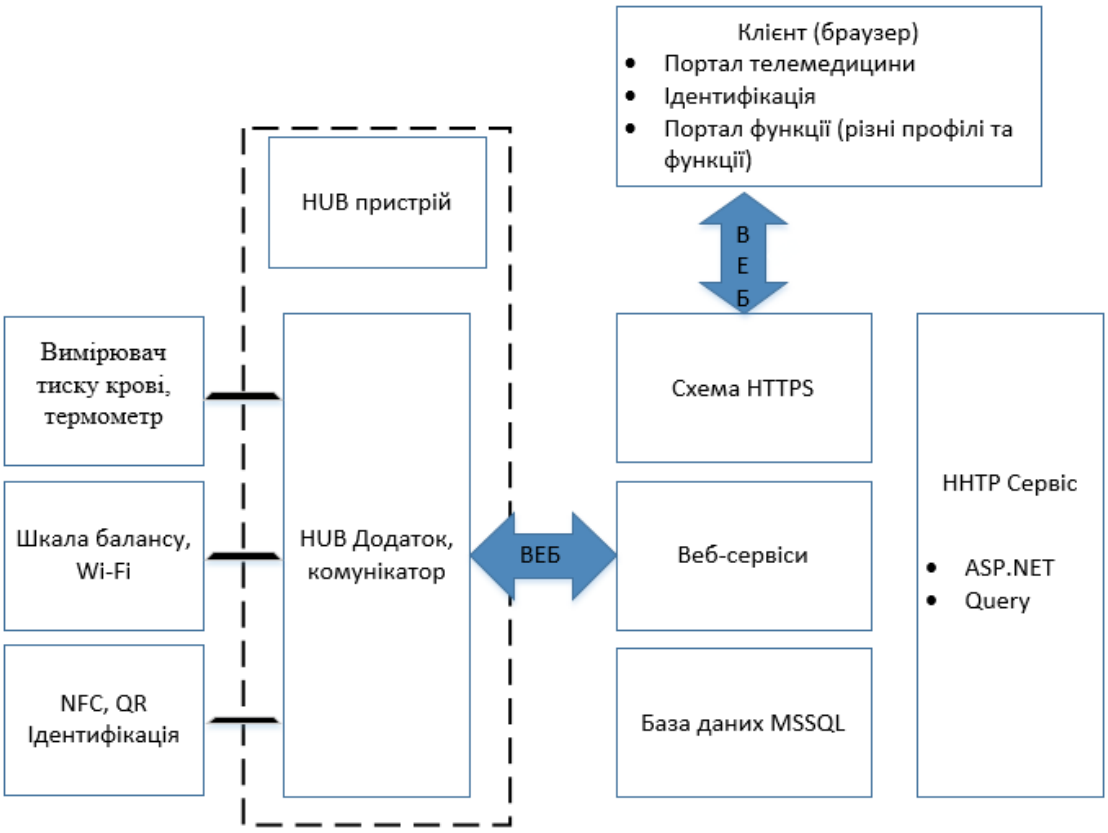

Рисунок 1.1 – Схема передачі даних

В майбутньому планується включити в телемедичну систему більше функціональних можливостей. З цього можна дійти до висновку, що система має велике майбутнє у галузі охорони здоров'я [3].

1.2 Існуючі застосунки для відстеження контактів з COVID-19

Вірус, який викликає нову хворобу COVID-19, поширився головним чином завдяки тісній взаємодії або контакту з людиною, яка вже уражена вірусом і все ще несе ознаки вірусу. З грудня 2019 року вже розпочато роботу над потенційною вакциною розвитку, однак до приходу вакцини єдиним можливим рішенням захисту є відстеження та ізоляція заражених людей та відстеження людей, які останнім часом тісно контактували з ними. З цією метою декілька країн працювали над розробкою застосунків для смартфонів для відстеження та інформування своїх громадян про можливу небезпеку, коли вони перебувають у

тісному контакті з хворою особою. Для різних платформ, а саме для Android, Windows та IOS, було розроблено велику кількість державних та недержавних програм для відстеження контактів.

Розроблені застосунки для відстеження контактів в значній мірі розроблені національними або державними регуляторами охорони здоров'я. Щоб забезпечити надійне та ефективне рішення, розроблені застосунки для прийняття рішення використовують інформацію з різних давачів смартфонів (GPS, Bluetooth), а також імена, адреси, стать, вік, контактні дані, історію журналу викликів та історію контактів тощо. Ці програми або взаємодіють автоматично з національними системами охорони здоров’я для результатів тестування громадян або громадяни вручну надають результати тесту для організації охорони здоров'я.

Використання цих застосунків, як правило, є добровільним і розглядається як засіб для контролю за поширенням вірусу. Розроблена програма запитує дозвіл приватних даних користувачів, наприклад контактні дані, історія дзвінків, пошук в Інтернеті, дозволи камери, доступ до записів викликів, повідомлень та мобільних носіїв інформації (відео та фотографії). Конфіденційність користувачів може бути захищена за допомогою використання різних механізмів, наприклад анонімізація даних, диференціальна конфіденційність та децентралізована розробка застосунків.

Структурний дизайн застосунків для відстеження контактів в основному використовує дані користувачів, тому виникають деякі проблеми конфіденційності, які спонукають розробника до створення рішень для збереження конфіденційності. Конфіденційність користувачів може бути вирішена за допомогою централізованої та децентралізованої установки системи. Централізовані та децентралізовані програми повністю мають різну архітектуру та властивості, показані на (рис 1.2) та пояснені нижче.

1) Централізовані моделі: у централізованому режимі смартфон користувачів, які мають конкретні програми відстеження контактів, відправляє

випадковий ідентифікатор до централізованої довіреної системи. Централізована система в цій установці зберігає інформацію від усіх користувачів програми. Якщо результат перевірки на вірус COVID-19 у даного користувача позитивний, ідентифікатор інших користувачів, які в минулому обмінялися ідентифікаторами, може бути надісланий на централізований сервер разом з іншою інформацією, наприклад час надсилання даних, час обміну ідентифікаторами тощо. Централізована система розшифровує ідентифікатори та автоматично сповіщає взаємодіючі телефони, пропонуючи або інформуючи користувачів про самоізоляцію чи вжиття інших запобіжних заходів. Централізована система також може використовувати наявну інформацію для подальшого аналізу та політики щодо розміщення блокування у важко наближених районах.

2) Децентралізовані моделі: у децентралізованому режимі немає надійної централізованої системи, яка б обробляла дані користувача та відповідала ідентифікатору смартфонів. Якщо людині встановлено позитивний діагноз COVID-19, ідентифікатор його телефону та результат тестування завантажується в централізовану систему. Інші смартфони, які мають застосунок, можуть отримувати доступ до цих звітів і локально перевіряти, був користувач поруч із зараженою людиною чи ні. Якщо смартфон наштовхується на особу, яка має COVID-19, то попередження надсилається користувачеві смартфона з метою обережності та самоізоляції. Місце та близькість людини не відомі централізованій системі, що забезпечує конфіденційність користувачів, які використовують застосунок. Організація охорони здоров’я чи уряд все ще використовували спільні дані для розуміння поширення вірусу в громаді, але не мали б детальної інформації про користувачів.

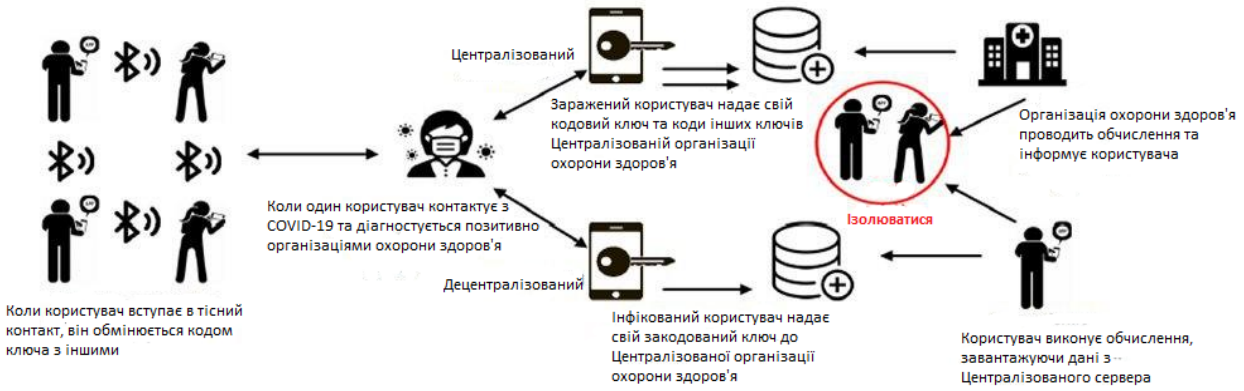

Рисунок 1.2 – Архітектурне налаштування програм для відстеження контаків

Централізована архітектура, базується на протоколі Bluetrace [4]. ROBERT [5] – подібний протокол, який базується на централізовану архітектуру. TraceTogether (Сінгапур) [6] та CovidSafe [7], (Австралія), які базуються на протоколі Bluetrace, та програми StopCovid (Франція) [8], яка реалізує протокол ROBERT. Aarogya Setu (Індія) – це зразок централізованої архітектури що використовує як Bluetooth, так і GPS.

3) Гібридна модель. У централізованій архітектурі сервер виконує всі складні завдання, наприклад, обчислення TempID, шифрування, дешифрування, аналіз ризику та сповіщення про сповіщення для контактів з атакою. З іншого боку, всі ці функції делеговані пристроям децентралізованої архітектури, зберігаючи сервер лише як дошку оголошень для цілей пошуку. Гібридна архітектура пропонує розділити ці функції між сервером і пристроями. Більш конкретно, генерація і управління TempID залишаються децентралізованими (тобто обробляються пристроями) для забезпечення конфіденційності та анонімності, в той час як аналіз ризику та повідомлення повинні нести відповідальність за централізований сервер. Існує три основні причини виконання процесу відстеження на сервері: 1) У децентралізованій архітектурі серверу невідомо про кількість користувачів групи ризику, оскільки пристрої роблять цей аналіз ризику, не враховуючи сервер. Таким чином, сервер не має статистичної інформації і не в змозі запустити будь-яку аналітику даних для ідентифікації кластерів експозиції. 2) Аналіз ризиків та повідомлення

вважаються чутливим процесом, тому це прерогатива влади, зважаючи на наявні інфраструктурні ресурси та стан пандемії. 3) Завантажена інформація про зустрічі від заражених користувачів не надається для інших користувачів, а зберігається лише на сервері. Це дозволяє уникнути атак деанонімізації користувачів, можливих у децентралізованій архітектурі. На (рис 1.3) показана послідовність взаємодії в гібридній архітектурі на основі протоколу «Desire protocol».

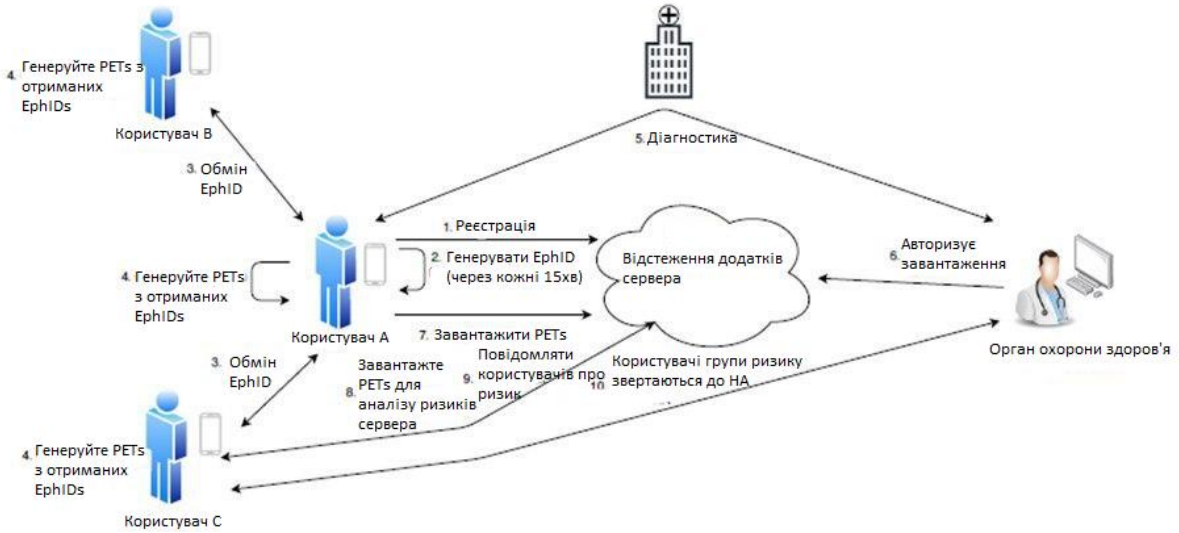

Рисунок 1.3 – Гібридне відстеження додатків

Цей протокол вимагає, щоб у процесі реєстрації програми користувач призначив унікальний ідентифікатор пристрою без запису PII. Потім пристрої криптографічно генерують та обмінюються тимчасовими ідентифікаторами EphID з іншими пристроями через BLE. Для кожного отриманого EphID два непов’язаних токени приватної зустрічі (PET Private Encouncer Tokens) генеруються та зберігаються. Після того, як користувач перевірив свій результат, на локальний сервер завантажується список локально генерованих PET. Тепер будь-який пристрій може надсилати свої другі генеровані маркери PET на сервер, який потім виконує аналіз ризику та повідомлення, сервер не може виводити

будь-яку ідентифікаційну інформацію з PET, і вся комунікація між сервером і пристроями здійснюється шляхом проксі-мережі або мережі анонімізації.

1.2.1 Застосунки/протоколи які базуються на централізованій архітектурі

1) TraceTogether

Застосунок TraceTogether, запущений урядом Сінгапуру в березні 2020 року, був одним з перших програм відстеження контактів, розгорнутих для громадськості [8]. OpenTrace, був опублікований у вигляді відкритого коду. Деталізовано лише одну додаткову функцію протоколу BlueTrace, яка була реалізована в застосунку TraceTogether, але пропущена в централізованому описі архітектури. Сервер видає попередні TempID на кожен пристрій замість одного TempID. Це потрібно для того, щоб кожен пристрій постачав дійсні TempID, навіть якщо Інтернет-з'єднання нестабільне.

2) CovidSafe (AU)

CovidSafe був випущений австралійським урядом 26 квітня 2020 року, вихідний код для клієнтів Android та iOS був опублікований 8 травня 2020 року [9]. Covid-Safe працює за протоколом Bluetrace і демонструє багато подібних характеристик для програми TraceTogether, включаючи вразливість до різних типів атак, перелічених у (табл 1.1).

Таблиця 1.1 – Можливі атаки на програми для відстеження та протоколи

Розділ №	Відстеження програм та протоколів	Відтворення / зміна	Бездротове відстеження	Підтвердження місцезнаходження	Перераховування	DoS	Зв’язок	Перенесення
VI-A1	Trace Together (BlueTrace)	+	+	+	-	+	+	+

Продовження таблиці 1.1

VI-A2	CovidSafe (AU) (BlueTrace)	+	+	+	-	+	+	+
VI-A3	StopCovid (ROBERT)	+	+	-	-	+	+	-
VI-A4	Aarogya Setu	+	+	+	+	+	○	○
VI-B2	PACT (East Coast)	Обмежений повтор +зміна	+	-	+	+	+	+
VI-B3	CovidSafe(UoW) (PACT-West Coast)	Обмежений повтор +зміна	+	-	+	+	+	-
VI-B4	SwissCovid – DP-3T (low cost)	+	+	-	+	+	+	+
VI-B5	DP-3T (unlinkable)	+	+	-	-	+	-	+
VI-B6	CovidWatch (TCN)	+	+	-	-	+	+	-
VI-B7	Pronto-C2	+	+	-	-	+	+	○
VI-B8	Hamagen	-	-	-	-	-	+	-
VI-B9	COVID Safe Paths	-	-	-	-	-	+	-
VI-C1	DESIRE	+ Тільки зміна	+	-	-	+	-	-
VI-C2	ConTra Corona	+	+	-	-	+	-	-
VI-C3	EpiOne	+	+	-	-	+	+	+

Ці дві програми відрізняються за часом існування TempID. Trace використовує значення 15 хвилин, як рекомендовано в специфікаціях протоколу BlueTrace, тоді як CovidSafe працює 2 години. Це робить CovidSafe більш вразливим для атак. Відносна перевага CovidSafe перед TraceTogether полягає в тому, що пристрої не повинні часто завантажувати TempID. Ще одна відмінність між цими двома програмами полягає в інфраструктурі, що склалася. Хоча

TraceTogether використовує Google Cloud для надання сервісних програм, CovidSafe використовує сервери Amazon AWS, які розташовані в межах Австралії.

3) StopCovid – ROBERT

Протокол відстеження близькості від ROBUST і збереження конфіденційності (ROBERT) – це централізований протокол програми відстеження, який спільно розробляють дослідники INRIA (Франція) та Fraunhofer (Німеччина)[5]. Застосунок StopCovid, який розроблений у Франції став доступний у червні 2020 року і використовує протокол ROBERT. StopCovid має вихідний код.

Основна відмінність протоколів BlueTrace від ROBERT – це тип даних користувачів, які зберігаються на сервері. Хоча перші є зберігачами PII, останні зберігають лише анонімні ідентифікатори, які називаються EphID, таким чином забезпечуючи рівень конфіденційності. Протоколи також різняться в процесі сповіщення, тобто, як сповіщають користувачів, що входять до групи ризику. ROBERT вимагає від усіх користувачів часто перевіряти використовувані EphID з сервером, щоб визначити, чи вони позначені як ризик. На противагу цьому, із BlueTrace органи охорони здоров’я могли б швидше повідомляти користувачів, які мають ризик захворіти. Процес сповіщення можливий, оскільки BlueTrace може зіставити TempID на зібрану особисту інформацію. У ROBERT позитивно ідентифікований користувач завантажує EphID в шахматному та випадковому порядку, на відміну від протоколу BlueTrace, де всі контакти завантажуються за один раз. Це робиться для того, щоб розірвати зв’язок контактів з тією ж людиною і не допустити сервер до проведення аналізу даних. Однак аналіз мережевого трафіку, який обмінюється пристроєм, потенційно може дозволити противнику зв’язувати звіти разом.

4) Aarogya Setu

Aarogya Setu – це програма, розгорнута в Індії на основі централізованої архітектури. Код застосунка для Android був випущений 26 травня 2020 року

[10]. Окрім збору даних PII та контактних даних, ця програма також збирає дані про місцерозташування (GPS координати) та дані про самооцінку (відповіді, надані особою на тест самооцінки) [11]. Він здійснює аналіз даних щодо зібраної інформації, щоб вказати, скільки позитивних випадків знаходиться в межах 500 м – 10 км від поточного місцезнаходження користувача. Користувачі можуть завантажувати дані про сліди, якщо вони позитивні на COVID-19 або не виконують тест самооцінки. На відміну від інших програм, уряд Індії зробив обов'язковим для всіх державних службовців та тих, хто живе в зонах стримування захворювань, встановлювати застосунок Aarogya Setu.

1.2.2 Застосунки/протоколи які базуються на децентралізованій архітектурі

1) Apple/Google Exposure Notification APIs

Apple і Google [12], [13] об'єдналися, щоб підтримати збереження конфіденційності для відстеження контактів, розробивши систему сповіщень. Запропонований ними механізм відстеження відповідає децентралізованій архітектурі, описаній раніше. Їх систему планували прокласти в два етапи. Під час першої фази, 20 травня 2020 року, було випущено API для підтримки програм, розроблених органами охорони здоров'я, призначених для безперебійної роботи на пристроях iOS та Android. Це розроблено, щоб допомогти керувати проблемами, пов’язаними зі скануванням BLE, з якими стикаються поточні програми [4]. Програми, засновані на нещодавно випущених API від Apple і Google, можуть використовувати запропоновані асоційовані зашифровані метадані (AEM) під час служби оповіщення. AEM – це зашифрована конфіденційність зашифрованих метаданих, що включає потужність передачі, щоб допомогти зібрати більш точні результати оцінки близькості. На другому етапі Apple / Google планують включити підтримку на рівні ОС, щоб сприяти більш широкій адаптації, усуваючи потребу в додатку для відстеження контактів. Застосунок під назвою SwissCoviD, було випущено 25

травня 2020 року для пілотного тестування командою DP-3T [14]. SwissCoviD базується на API Apple / Google. Аналогічно, 16 липня 2020 року в Німеччині було випущений застосунок з відкритим кодом під назвою Corona-Warn-App [15], який базується на цих API. Ще один проект під назвою Aurora [16] розробляється командою PathCheck для використання API, розробленого Apple / Google. Багато існуючих застосунків, у тому числі деякі з централізованої категорії, вже почали досліджувати способи міграції наявної кодової бази до API, випущеного Apple / Google.

2) PACT (East-coast)

Дизайн протоколу PACT був використаний як основа для пояснення децентралізованої архітектури, включаючи встановлення, обмін зустрічами та процес відстеження. Дослідницьке співробітництво під керівництвом MIT [17] розробило цей протокол.

На застосунок локально зберігаються «seed data» (використовуються для генерації) та «chirp data» (включаючи отриманий час та потужність сигналу), PACT (East-cost) також дозволяє користувачеві додатково зберігати додаткові метадані, наприклад інформацію про місцезнаходження, у своїх локальних файлах журналу під час отримання «chirp». Дані про місцезнаходження можуть допомогти визначити місце контакту, наприклад, ресторан або парк. Ці необов'язкові метадані можуть допомогти зменшити помилкові результати та підвищити точність системи, залучаючи більше контекстної інформації.

3) CovidSafe - PACT (West-coast)

Конфіденційні протоколи та механізми мобільного відстеження контактів – PACT (West-coast) [18] – протокол відстеження, запропонований дослідниками з Вашингтонського університету. Основна функція мобільного відстеження використовує дуже схожий процес, порівняно з базовою децентралізованою системою, що використовується в застосунку PACT East-coast, в якому всі особисті дані локально зберігаються (і шифруються) на телефоні, пристрої транслюють псевдовипадкові ідентифікатори, і користувач це добровільно

публікує / завантажує дані. PACT використовує інший механізм генерації на основі ключів для створення псевдовипадкового ідентифікатора, який використовується для шарингу. 128-бітний ключ спочатку подається в генератор псевдовипадкових випадків, і генерується 256-бітний вихід довжини (для прикладу можна взяти SHA-256). Половина довжини цього результату (128-бітна) використовується як тимчасовий псевдовипадковий ідентифікатор протягом визначеного періоду [t0 + dt i; t0 + dt (i + 1)], а інша половина використовується як вхід для наступного псевдовипадкового генератора. Ця конструкція дозволяє економити сховища, зберігаючи менше «seeds», ніж застосунок PACT (Східно-узбережжя). Після цього ці псевдовипадкові ідентифікатори транслюються та збираються, подібно до PACT (East-coast).

Як і всі децентралізовані протоколи, PACT (West-coast) також сприйнятливий до атак з перерахуванням, оскільки «seeds» заражених користувачів завантажується на сервер і в подальшому може бути поширений з усіма користувачами. Застосунок CovidSafe (UoW) [19], для якого бета-версія була випущена в травні 2020 року, базується на протоколі PACT (West-coast).

4) SwissCoviD - DP-3T

Децентралізоване відстеження збереження конфіденційності (DP-3T) [20] – специфікація протоколу, заснована на децентралізованій архітектурі, запропонована консорціумом університетів та організацій з Європи під керівництвом EPFL, Швейцарія. Пілотний застосунок під назвою SwissCovid [58] було випущено 25 травня 2020 р. У специфікаціях є дві версії, версія "низької вартості" та "незв'язна" версія. Протокол дуже схожий за функціоналом з базовою децентралізованою архітектурою. Щоденний ключ генерується кожним пристроєм, використовуючи хеш-ланцюг з попереднього щоденного ключа, а потім використовується для генерації EphID. Повідомлення обмінюються з іншими пристроями, які контактують через Bluetooth, що містять ці EphID, з інформацією про термін дії та приблизним часом (датою). Обмінювані дані залишаються у локальному сховищі, поки користувач не

перевірить позитивні результати. Чиновники охорони здоров'я визначають «заразне вікно», тобто, в який час позитивний випадок заразний і може заразити інших. Ідентифіковані користувачі завантажують лише свої щоденні ключі починаючи з цієї дати. Після завантаження даних заражений користувач змінює свій випадковий ключ для генерування майбутніх щоденних ключів, щоб запобігти відстеженню / ідентифікації в майбутньому. Інші користувачі завантажують щоденні ключі, завантажені зараженим користувачем, і порівнюють їх збережені EphID з EphID, реконструйовані з щоденних ключів зараженої людини. Таким чином, процес аналізу ризику здійснюється локально на окремих пристроях. Застосунок повідомляє користувача, якщо він знаходиться в тісному контакті, і просить дозволу завантажувати його щоденні ключі.

5) DP-3T Unlinkable

Документ із специфікацією DP-3T [20] також має другу версію, яка називається "Незв'язувальна" конструкція. Ця конструкція відповідає на твердження про те, що децентралізований дизайн піддається атакам зв’язків та перерахувань, оскільки щоденні ключі для заражених користувачів стають доступними для всіх інших пристроїв.

Основна зміна цього дизайну полягає в тому, що щоденні ключі, завантажені зараженими користувачами, перетворюються сервером у відповідні EphID. Сервер хешує ці значення у Cuckoo filter [21], перш ніж поширювати їх іншим користувачам. Користувачі все ще можуть перевірити, чи отримані ними EphID з криптографічним хешем і чи відповідають вони будь-яким записам у Cuckoo filter чи ні. Користувач не може отримати доступ до іншої інформації, включаючи, скільки або які інші EphID були закодовані у Cuckoo filter. Час обробки на сервері збільшується порівняно з версією DP-3T. Також Cuckoo filter повинен бути ретельно розроблений, щоб мінімізувати шанси на помилкові позитиви, тоді як помилкові негативи неможливі з цим фільтром. Цей дизайн також дозволяє користувачам вибірково завантажувати зустрічі (шляхом

придушення / редагування деяких зустрічей) у фазі завантаження. Ще одна запропонована особливість полягає у використанні передачі секретних k-out-n-n, щоб мінімізувати ймовірність збору EphID протягом коротких періодів контакту. Контакт повинен зібрати щонайменше k поширюваних оголошень для успішної реконструкції EphID. Це обмежує ефективні EphID контактами, які здійснюються протягом достатньої тривалості.

6) CovidWatch – TCN

Дослідники зі Стенфордського університету та Університету Ватерлоо розробили Covid-Watch [22]. Ця програма ще перебуває на пілотній фазі. Вихідний код є загальнодоступним [23], і він відповідає протоколу коаліції TCN (Тимчасовий контактний номер) [24]. Протокол TCN генерує «keychain», таким чином, що кожен ключ (seed), отриманий з головного ключа, генерує один унікальний тимчасовий контактний номер (chirp). Як і інші децентралізовані протоколи, TCN завантажує на сервер лише компактні seed data (головний ключ, термін придатності тощо), а не весь список TCN. Усі seeds, що належать до звіту, можуть бути перевірені / підтверджені сервером, оскільки вони генеруються та прив’язані до одного і того ж головного ключа. Зловмисні суб'єкти потенційно можуть запустити атаку на зв’язок, щоб дізнатись пов’язані TCN, спостерігаючи за кількома TCN із звітів, які використовують один і той же головний ключ. Тому можна проводити часті повороти головних ключів, щоб зробити TCN не пов'язуючими з різними звітами. Однак це збільшує кількість пунктів, які потрібно підтримувати, піднімаючи питання масштабованості. Таким чином, застосунку необхідно враховувати компроміс між масштабованістю та зв’язковістю під час вибору періоду обертання головного ключа.

7) Pronto-C2

Дослідники з університету Салерно, Італія, запропонували систему відстеження контактів Pronto-C2 [4]. Це децентралізована програма, яка дозволяє пристроям спілкуватися анонімно один з одним, ховаючи ці комунікації від центрального сервера, запобігаючи масовому спостереженню. В основі

протоколу лежать два криптографічні інструменти: обмін ключами Diffie Hellman (DH) [25] та сліпі підписи [26]. Таємний $sk_a \epsilon Z_p$ та ефемерний ідентифікатор $eph_A = g^{skA}$ генеруються в Alice's device та зберігаються на сервері. Адресат A відзначається пристроєм, де створений його ефемерний ідентифікатор який зберігається на сервері (це сховище також може бути реалізовано за допомогою blockchain). Пристрій транслює цю адресу та отримує адреси від інших пристроїв, що знаходяться поблизу. Це суперечить децентралізованим конструкціям, які поділяють ефемерні ідентифікатори. Alice зберігає рядок ($eph_{A,i}, sk_{A,i}, addr_A$,t), коли отримує eph_B від Bob. Тут $sk_{A,i}$ – секретний ключ з попереднього оновлення *i*, а *t* містить допоміжну інформацію, наприклад, силу сигналу BLE, час тощо. Якщо Alice тести позитивні, вона отримує ефемерний ідентифікатор кожного контакту зі свого списку контактів. Для контакту з Bob вона отримує eph_B за допомогою $addr_B$. Alice обчислює $K' = eph_B^{skA}$, що є ключем DH між собою та Bob, і ключ $K = H(K'||eph_A||eph_B)$. Потім вона надсилає (засекречену) інформацію *K* на сервер автентифікації, який додає сліду підпис до *K*. Підпис запобігає атакам DoS та забезпечує те, що сервер авторизації не може виконати аналіз соціальних графіків. Користувач Y, який бажає перевірити свій ризик, може завантажити ідентифікатори ефемерного списку зі свого списку контактів на адресу $addr_X$. Потім вони обчислюють ключ *DH K'* між собою та ефемерним ідентифікатором Eph_X у $addr_X$. Він обчислює $K = H(K'||Eph_X||Eph_Y])$. *Y* завантажує нещодавно доступні ключі (заражених осіб) з сервера і перевіряє, чи належить *K* до цього набору. Якщо відповідність знайдена, користувач в зоні ризику. Пристрої спілкуються із сервером за допомогою анонімних каналів, таких як TOR, щоб запобігти зв'язку ефемерних ключів із користувачами.

8) Hamagen

Застосунок Hamagen розроблено Міністерством охорони здоров'я Ізраїлю. Hamagen відрізняється від багатьох інших застосунків для відстеження контактів тим, що він не покладається на запис зустрічей з іншими телефонами в околицях

за допомогою Bluetooth. Він перевіряє історію GPS мобільного телефону з історичними географічними даними про виявлені випадки Міністерства охорони здоров'я. Перевірка проводиться локально на мобільному телефоні особи. Дані про місцерозташування кожного користувача не залишаються на його пристрої, а також не надсилаються третій стороні. Застосунок періодично (щогодини) завантажує файл, що містить анонімізований перелік місць, які за останні 14 днів відвідували люди, у яких діагностовано COVID-19. Цей файл отриманий в Міністерстві охорони здоров'я та заповнений даними, що показують людей, які пройшли епідеміологічне розслідування, використовуючи різні інструменти, доступні Міністерству. Потім програма оцінює перехресне посилання на ці місця (включаючи часові мітки) з даними про місцерозташування, які зберігаються локально на пристрої користувача.

Якщо програма виявить, що існує можливість того, що особа перебуває в тому самому місці і одночасно з діагностованим випадком, на телефоні відображається повідомлення із зазначенням даних про місцезнаходження та час перебування особи до позитивного випадку. Користувач телефону має можливість переглянути сповіщення. Якщо повідомлення вважається невірним, наприклад, якщо користувач не був у зазначеному місці в зазначений час, користувач може вказати, що інформація неправдива. Якщо користувач підтвердить свою присутність у контактному місці, він спрямовується на веб-сайт Міністерства охорони здоров’я для отримання інформації про те, що робити далі. Застосунок повинен мати доступ до історії локацій (GPS-даних) телефону та списку базових станцій стільникового зв'язку та Wi-Fi-точок доступу, що виникали протягом останніх двох тижнів. Ця інформація зберігається в SQLite, також вимагає доступу до Інтернету, щоб періодично завантажувати оновлений файл із сервера Міністерства охорони здоров'я. Вихідний код програми був розроблений за допомогою React Native і є відкритим кодом на GitHub [27].

9) COVID Safe Paths

Команда PathChecks [28] розробила цей застосунок та його вихідний код для Andriod і iOS та зробила його загальнодоступним [29]. Він схожий на Hamagen за функціональністю, оскільки він також використовує реєстрацію траєкторій розташування GPS. Також було випущено інструмент карт на основі браузера під назвою "Safe Places", який може взаємодіяти з застосунком Safe path. Діагностовані користувачі можуть добровільно поділитися своїми маршрутами розташування з органами охорони здоров'я, використовуючи інструмент карти безпечних місць. Інші користувачі можуть завантажити анонімізований а також узагальнені набори даних про загальнодоступні місця, щоб перевірити, чи контактували вони з ідентифікованою особою, не завантажуючи їх траєкторію.

1.2.3 Застосунки/протоколи які базуються на гібридній архітектурі

1) DESIRE

Гібридна архітектура базується на специфікації протоколу DESIRE [30]. Використання криптографічно генерованих PET дає користувачам більше контролю, зберігаючи ці відмінності від поширюваних EphID. Це дозволяє уникнути можливого збирання контактних даних для аналізу соціальних графіків. Усі дані, що зберігаються на сервері, шифруються ключами, які зберігаються на пристроях клієнтів. Це захищає клієнтські дані в разі порушення сервера даних. Аналіз ризиків та повідомлення обробляються сервером (замість клієнтів, як у випадку з децентралізованими версіями), що обмежує ймовірність запуску іншими користувачами атак перерахунку та зв’язку.

2) ConTra Corona

ConTra Corona [31] – це гібридний протокол, запропонований німецькими дослідниками з науково-дослідного центру інформаційних технологій FZI та Карлосруеського технологічного інституту. Contra Corona покращує захист конфіденційності, пом'якшуючи атаки зв’язків, які можна розпочати на

децентралізованих застосунках. Це досягається шляхом прийняття механізму обміну ключами DDH для перевірки процесу завантаження даних для людини з діагнозом COVID-19. Крім того Contra Corona, пропонує чітке розділення сервера, використовуючи три різні сервери; сервер подання, відповідальний сервер та сервер сповіщень. Пропозиція Contra Corona суттєво відрізняється від базової гібридної архітектури (на основі протоколу DESIRE). Однак основні припущення однакові. Пристрої генерують свої ідентифікатори, а централізований сервер відповідає за аналіз ризику та процес сповіщення. Кожен користувач генерує ідентифікатор попередження (WID) кожен день на основі свого реального ідентифікатора (наприклад, імені). Для кожного WID пристрій обчислює *sid* (розглядаються як seed ідентифікатори), зашифровані відкритим ключем та *pid* сервера подання (псевдовипадковий ідентифікатор, зашифрований та хешований на основі sid). *pid* і *sid* завантажуються на сервер подання. Спочатку сервер подання збирає пари всіх користувачів (sid; pid). Після того, як сервер подання накопичив достатню кількість клієнтських пар, він переміщує їх та потім відправляє на відповідний сервер (це допомагає зменшити перерахування). Якщо відповідальний сервер отримує *pid,* завантажений одним із заражених користувачів, він шукає відповідний *sid* усіх потенційно заражених користувачів та надсилає їх на сервер сповіщень. Нарешті, сервер сповіщень розшифровує *sid* для відновлення ідентифікатора попередження (wid) користувача та публікує список розширень. Усі користувачі регулярно отримують список віджетів із сервера сповіщень та порівнюють його з тими (зберігаються локально), якими вони користувалися протягом попередніх 28 днів.

Протокол Contra Corona використовує n-out-k-таємний обмін *pid* (n приймається як 15, та k як 45) і вибирає випадковий ідентифікатор m (наприклад, m може бути прийнятий як MAC-адреса Bluetooth). Одну таємну частку *pid* транслюють щохвилини. Користувачі, які отримали та накопичили 15 таких

передач того ж користувача m, можуть реконструювати номер цієї контактної події та надалі зберігати цю контактну подію на пристрої.

Поліпшення конфіденційності ConTra Corona базується на тому, що сервери не мають безпосереднього зв’язку між собою, а всі канали зв'язку анонімізовані або автентифіковані. Сервер подання вважається найбільш надійним компонентом, оскільки він зберігає всі відповідні (sid; pid) пари ідентифікаторів, які генеруються кожним користувачем. Додаткове шифрування та рандомізація використовуються для запобігання розголошенню статусу зараженого користувача іншим користувачам. Протокол також вимагає від органу охорони здоров'я перевірити цілісність звіту (завантажений зараженою особою), щоб зменшити помилкові результати захворюваності в системі (а також запобігти атаці DoS).

3)EpiOne

EpiOne [32] була запропонована групою дослідників під керівництвом Каліфорнійського університету в Берклі, щоб захистити від нападів та аналізів соціальних контаків. На момент написання джерела вихідний код не був доступний. В основі протоколу лежить криптографічна техніка, відома як Прямий набір перетину (PSI Private Set Intersection) [33,34].

На високому рівні пристрої генерують та обмінюються випадковими ідентифікаторами (tokens) за допомогою початкових даних. Кожен пристрій підтримує надіслані та отримані списки токенів. Якщо користувач тестує позитивні результати, вони завантажуються через працівників охорони здоров'я, які використовують сервер для побудови відправлених токенів. Користувач, який хоче перевірити його тісні контакти та сервер, повинен дотримуватися протоколу приватного встановленого перетину, щоб перевірити, чи є перетин між отриманими маркерами та тими, які підтримуються на сервері. Користувач отримує сповіщення про виявлення відповідності. Intersection protocol приватного набору гарантує, що ні користувач, ні сервер не знають повного набору токенів, тим самим запобігаючи небажному аналізу даних.

На більш фундаментальному рівні EpiOne складається з двох серверів, сервера збору з посадовими особами охорони здоров'я та непідтвердженого сервера перевірки. Перед початком роботи протоколу всі учасники, включаючи користувачів, медичних працівників та сервер підтвердження, спочатку погоджуються щодо параметрів безпеки. Сервер підтвердження генерує публічну / приватну пару секретних ключів і публікує відповідний відкритий ключ. Кожен користувач може вибрати випадкові seeds та отримати tokens використовуючи input seeds, протягом дня. Це корисно, оскільки сервер підтвердження може згодом реконструювати маркер, якщо він знає відповідне seed. Коли користувачі контактують між собою, вони обмінюються токенами. Список відправлених та отриманих токенів зберігається на мобільному пристрої. Коли користувач отримує позитивний результат, він завантажує зашифровані seed (зашифровані відкритим ключем сервера підтвердження) на сервер збору, який підтримують посадові особи охорони здоров’я. Служби охорони здоров’я, у свою чергу, переміщують зашифровані seed та відправляють їх на верифікаційний сервер, який може розшифрувати seed та реконструювати всі маркери. Користувач може з'ясувати, чи знаходився він у безпосередній близькості до позитивного випадку COVID, безпечно обчислюючи (використовуючи протокол перетину приватного набору), простоту перетину між двома наборами токенів. Сервер не розкриває набір токенів позитивних випадків (запобігання атаці нумерації), а також користувач не розкриває набір токенів, отриманих від інших користувачів.

1.3 Методи визначення місця розташування

Послуги визначення місцезнаходження (LCS Location Services) – це нові послуги, що підтримуються бездротовими мережами, які використовують розташування користувачів. Для служб, що базується на розташуванні, поточне місцезнаходження мобільного терміналу повідомляється в стандартному

форматі (наприклад, географічні координати) користувачеві, мережному оператору, постачальнику послуг та для внутрішніх операцій PLMN.

LCS використовує один або позиціонуючі методи позиціонування, щоб визначити місцерозташування користувацького обладнання (UE Custom equipment). Позиціонування цільового мобільного терміналу застосовує два основні принципи: вимірювання сигналу та обчислення місцезнаходження на основі виміряних сигналів.

Стандарти підтримують два варіанти реалізації LCS, які відрізняються мережевим об'єктом, який фактично обчислює позицію UE. У режимі, що підтримується UE (на основі мережі), UE вимірює різницю в часі надходження декількох комірок і передає результати вимірювань в мережу, де мережа обчислює позицію. У режимі, заснованому на UE (з підтримкою мережі), UE проводить вимірювання, а також здійснює обчислення положення. Технології визначення місцезнаходження, запропоновані в стандартах мереж доступу, GSM (ETSI) та UMTS (3GPP), є:

Cell ID + TA

Це найпростіший спосіб описати загальне розташування MS. Вимога до мережі: ідентифікація BTS, до якого повідомляється мобільний телефон, та місце розташування BTS. Оскільки мобільна станція може знаходитися в будь-якій точці комірки, точність цього методу залежить від розміру комірки, оскільки типова стільникова станція GSM знаходиться в діаметрі від 2 км до 20 км. Подальше зменшення площі клітини шляхом уточнення клітинного сектора є типовою стратегією, що використовується для підвищення точності (рис 1.4).

Позиціонування, як правило, більш точне в міських районах з щільною мережею менших осередків, ніж у сільській місцевості, де є менше базових станцій. Якщо використовувати мікроклітини, розмір комірок може бути значно зменшений – до діапазону декількох сотень метрів. Точність ідентифікатора комірки можна додатково підвищити, включивши міру TA. Ці вимірювання

можуть бути використані для визначення відстані від MS до BTS, додатково зменшуючи похибку позиції.

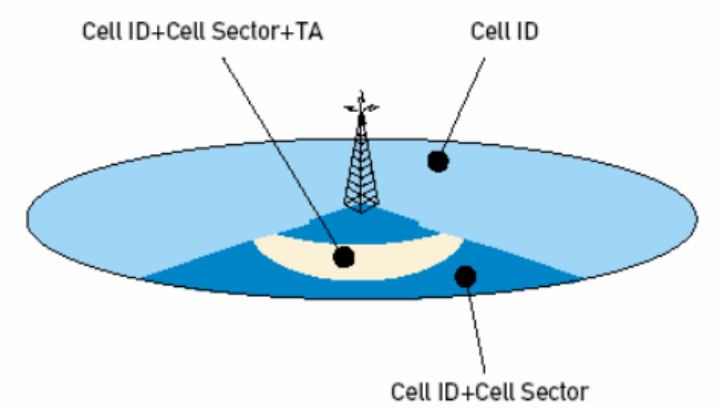

Рисунок 1.4 – Cell ID + Cell Sector + TA

Недоліки

- Низька точність від 100 до 1100 м.

Переваги

- Ніяких змін у пристрої немає. Потрібні лише MLC в мережі.
- Підтримка існуючого обладнання у мережах.
- Швидка реакція, приблизно 1 сек.

Розширена спостережувана різниця у часі (E-OTD)

Метод позиціонування E-OTD (рис 1.5) заснований на MS, що вимірює різницю у часі приходу між пакетами BTS поблизу в GSM. E-OTD вимагає модифікації мобільної станції. Сигнали щонайменше з трьох блоків BTS приймаються MS, а також одиницею вимірювання місця (LMU). LMU – еталонний приймач. Функція LMU полягає в обчисленні різниці часу приходу сигналів від BTS, знаючи положення LMU. Він вимірює так само, як і різниці в часі сигналу мобільного пілотного сигналу від базових станцій. З цих відмінностей у часі та відомого *x, y* координати сервера розташування можуть легко обчислити довідкові дані для E-OTD. Параметри різниці в часі

надходження сигналів використовуються при обчисленні положення мобільних терміналів на локальному сервері. На малюнку показаний принцип методу E-OTD [35].

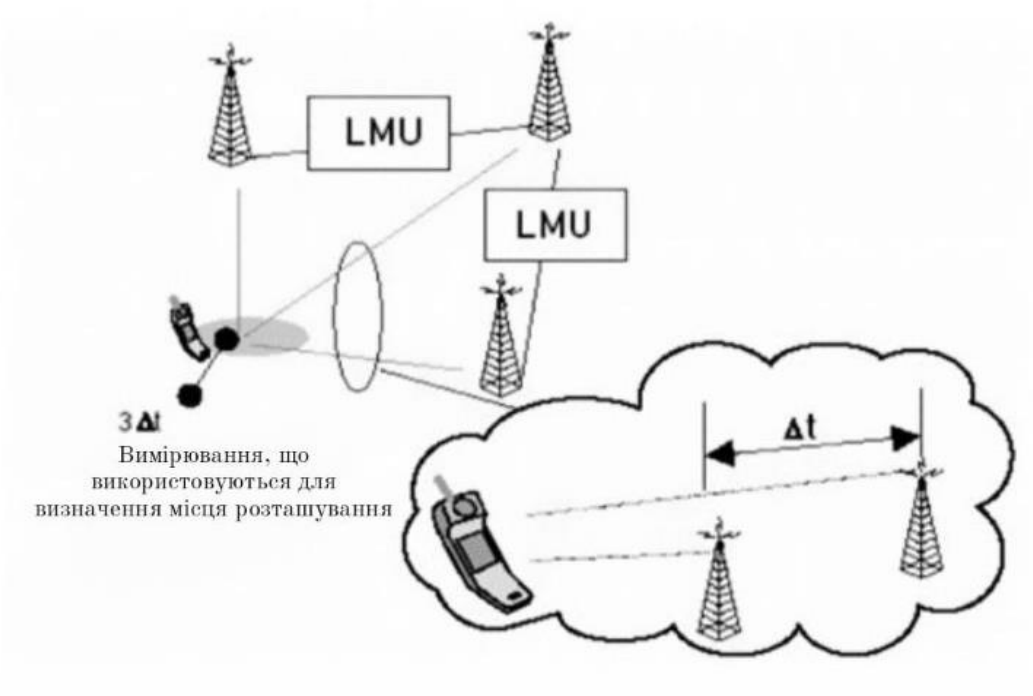

Рисунок 1.5 – Принцип методу E-OTD

Недоліки

- Середня точність між 50-200 м.
- Додане програмне забезпечення, і великий вплив на мережу - висока вартість.
- Для роумінгу впровадження E-OTD вимагає значної модифікації, оскільки роумінгова мережа повинна мати LMU.
- Не стійкий до багатопроменевого поширення.

Переваги

- Швидка реакція приблизно. 5 сек, залежно від затримки мережі.

Мережевий GPS (AGPS) або бездротовий GPS (WAG)

A-GPS використовує супутники в космосі як орієнтири для визначення місця розташування. Точно вимірюючи відстань від трьох супутників, приймач

тріангулює своє положення де-небудь на землі [36]. Приймач вимірює відстань, вимірюючи час, необхідний для передачі сигналу від супутника до приймача (рис 1.6). Для цього потрібна точна інформація про час, тому на практиці необхідні вимірювання з четвертого супутника, щоб допомогти усунути помилки вимірювання часу, створені неточностями недорогих ланцюгів синхронізації, які зазвичай використовуються в MS.

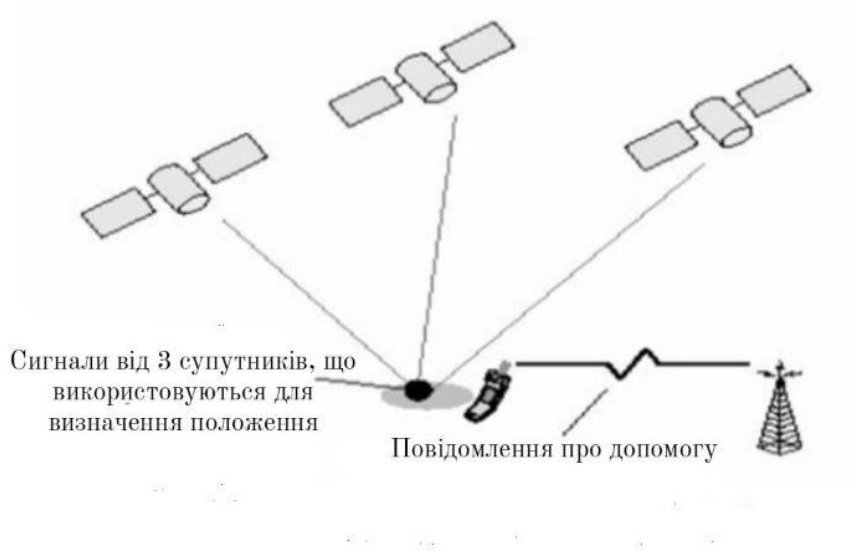

Рисунок 1.6 – Мережа AGPS

Недоліки

- Необхідний високоємнісний акумулятор.
- Час відгуку повільний порівняно з іншими технологіями.
- Потрібна інтеграція приймача CPS.

Переваги

- Висока точність (10-50 м).
- Перевірена технологія.
- Уникає дорогих модифікацій мережі.
- Легка підтримка роумінгу.

Кут прибуття (AOA)

Методи кута прильоту засновані на припущенні, що BTS можуть вимірювати кути надходження сигналів, що передаються MS (рис 1.7). Якби між MS та двома BTS була лінія зору (LOS), а вимірювання AOA були доступні, MS знаходилася б у перетині ліній, визначених кутами прибуття. Багатосторонність викликає серйозні помилки, особливо коли методи AOA використовуються в міських умовах. Цей метод вимагає, щоб BTS були обладнані антенами, які можуть вимірювати значення AOA [37].

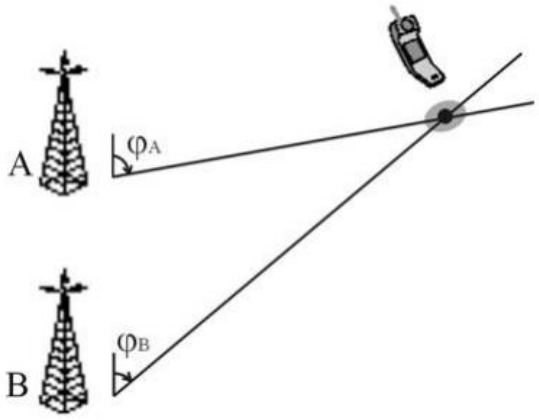

Рисунок 1.7 – Кут прибуття

Недоліки

- Відносно низька точність (приблизно 300 м).
- Сприйнятливий до багатопроменевих перешкод.
- Більші витрати на інфраструктуру для встановлення додаткових спрямованих антен.

Переваги

- Ніяких модифікацій слухавки не потрібно.
- Потрібно лише мінімум 2 осередки для визначення.

місцезнаходження користувача

Гібридна технологія

Гібридна технологія локації поєднує A-GPS з іншим розташуванням місця таким чином, що дозволяє сильним сторонам одного компенсувати слабкі місця іншого, щоб забезпечити більш надійне рішення щодо розташування. Найпоширенішою реалізацією гібридної технології для GSM є поєднання A-GPS з Cell-ID. Як правило, це області, де щільність комірок висока, тому Cell-ID буде на точнішому кінці діапазону точності, хоча він не буде таким точним, як A-GPS.

Для бездротових операторів або постачальників послуг, що базуються на розташуванні, слід ретельно продумати вибір найкращої технології визначення місцезнаходження, яка визначатиметься необхідним додатком, що базується на розташуванні. [37].

1.4 Висновок до розділу 1

В першому розділі було розглянуто телемедичну систему, яка містить в собі багато функціональних можливостей. Система є актуальною, адже надає послуги у боротьбі проти пандемії COVID-19. Вона має досить хороше перспективне майбутнє у сфері охорони здоров’я. Тому було розглянуто існуючі застосунки відстеження контактів з COVID-19. Вони базуються на трьох основних архітектурах: централізованій, децентралізованій, гібридній. Всі застосунки використовують найпопулярніші методи місцярозташування такі як: Cell ID + TA, E-OTD, мережевий та безмережеві GPS, AOA та гібридну технологію.

2 АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ КОНТАКТІВ ІНФЕКЦІЙНИХ ХВОРИХ

2.1 Автоматизоване відстеження контактів для управління розповсюдженням Covid-19 на основі даних геолокації з мобільних стільникових мереж

Коронавірус (COVID-19) виявився найбільшим викликом через його постійну структурну еволюцію, а також відсутність належних антидотів для цього конкретного вірусу. Вірус в основному поширюється серед людей завдяки тісному контакту, які відбуваються різними способами. Тому, щоб уповільнити поширення цього нового вірусу, важливими ініціативами є: підтримка соціальної дистанції, здійснення відстеження контактів, використання належних засобів безпеки та введення карантинних заходів. Для контролю за розповсюдженням вірусу дослідники та органи влади розглядають можливість використання мобільних застосунків для ідентифікації ймовірних заражених людей, а також зони з високим ризиком захворюваності. Однак ці методи в значній мірі залежать від передових технологічних особливостей і виявляють значні лазівки в конфіденційності.

Після оголошення ВООЗ (Всесвітня організації охорони здоров’я) в якості спалаху захворювання COVID-19 30 січня 2020 року [39, 40] та пандемії 11 березня 2020 року [41] надзвичайною ситуацією, що викликає міжнародне занепокоєння в галузі охорони здоров'я, багато країн розробили різні програми відстеження контактів для моніторингу та контролю розповсюдження вірусу в країні. Згідно з повідомленням CNN Cables News Network (Кабельна мережа новин), застоунок Health Code [42], який використовується у багатьох районах Китаю, працює наступним чином: застосунок запитує людей про їх симптом, а також історію подорожей, можливість контакту з COVID-19 позитивних пацієнтів, їхні робочі місця, адреси житла, номери телефонів, номери паспортів, національний ідентифікаційний номер тощо. Після перевірки на мобільний

телефон людини, буде надісланий «QR-код» в певного кольору в залежності від ризику. Користувачам з червоним кодом доведеться пройти державний карантин або самокарантин протягом 14 днів, користувачі з бурштиновим кодом – 7 днів, але користувачі із зеленим кодом вважаються безризиковими. Основна проблема в цьому застосунку полягає в тому, що людина навмисно надає неправильну інформацію щодо своєї інформації про поїздку чи симптому або знаходиться у тісному контакті з позитивним пацієнтом із COVID-19, тоді він отримає зелений код і, ймовірно, вплине на більшу кількість людей до того, як його ідентифікують.

У березні 2020 року Міністерство охорони здоров'я Сінгапуру вперше випустило програму відстеження контактів під назвою «TraceTogether» та протокол BlueTrace на основі BLE (Bluetooth Low Energy) [43], де відстеження буде здійснюватися за допомогою технології Bluetooth мобільних телефонів. Для відстеження людина повинна встановити програму, а Bluetooth повинен бути завжди ввімкнений. Під час встановлення на мобільному телефоні людини створюється унікальний маркер. Кожного разу, коли дві особи перебувають у безпосередній близькості, їх телефон обмінюється цим маркером через Bluetooth і зберігає цей номер маркера в пам'яті телефону [44].

Загальноєвропейський механізм відстеження близькості (PEPP-PT) [45], спільний проект між Німеччиною, Францією та Італією, запропонував централізований центр обробки даних на основі техніки відстеження на основі низьких енергій Bluetooth (BLE), де будь-який мандрівник, який подорожує в межах ЄС можуть використовувати єдиний застосунок, щоб повідомити уряд про список своїх контактів, не потребуючи додаткових застосунків для відстеження контактів.

Є кілька основних проблем у системах відстеження, що базуються на BLE, як за допомогою централізованого, так і децентралізованого підходів. По-перше, якщо людина не користується смартфоном із Bluetooth-підключенням, тоді її чи її неможливо простежити. Зрозуміло, що в першій світовій країні, як Сінгапур чи

Німеччина, більшість людей користуються смартфонами, але не обов'язково кожен постійно підтримує з'єднання Bluetooth у своєму пристрої. По-друге, хоча технологія Bluetooth розглядається як дешевий, надійний варіант з низьким енергоспоживанням, будь-який зловмисний користувач може отримати доступ до інформації, що зберігається у мобільних пристроях, за допомогою Bluetooth [46, 47, 48]. У роботі [47] Naveed et al. пояснив проблеми безпеки використання мобільної технології Bluetooth для пристроїв Android, а автори показали проблеми безпеки на платформі iOS [49]. Таким чином, конфіденційність даних є основною проблемою в застосунках на основі Bluetooth. Для будь-якої програми для відстеження контактів основною метою є інформування людини про те, чи вона зазнала впливу вірусу. Однак у програмах на основі Bluetooth, навіть якщо особа не контактувала з жодною зараженою особою, але знаходиться в межах досяжності Bluetooth, користувач телефону буде позначений як підозрюваний і може зазнати соціальних знущань. Це також може плутанину, якщо кількість таких помилкових тривог значно зросте. З іншого боку, якщо розглянути сценарій такої країни, що розвивається, як Бангладеш, Нігерія тощо, де коронавірус створює фобію серед людей, оскільки медичні заклади для підтримки великої кількості пацієнтів є недостатніми. Цей тип програми відстеження контактів створить масову паніку, а не обізнаність, і люди будуть стикатися з соціальними переслідуваннями.

Хоча більшість програм для відстеження контактів зараз використовують техніку відстеження на основі BLE, деякі дослідники також замислюються над збереженням інформації про мобільність користувачів і передачі в подальшому цієї інформацію лише тоді, коли COVID-19 виявляється позитивним [50]. Що стосується безпеки даних та конфіденційності, це більш безпечно. Програма відстеження контактів на основі Bluetooth „CONTAIN", де особа користувача буде повністю анонімною. Проведені експерименти в різний час включення Bluetooth (випадковий, децентралізований, централізований) для порівняння результатів [51]. У експериментальних результатах виявилено, що навіть якщо

Bluetooth увімкнено, лише коли користувач переходить на будь-яке публічне зібрання, продуктивність програми є кращою, ніж якщо вона увімкнена випадковим чином у різний час доби.

Виявлено, що більшість випущених до цього часу програм для відстеження контактів COVID-19 базуються на відстеженні контактів на основі розташування / близькості, звіту про точку доступу на основі місцезнаходження та самостійному відстеженні симптомів [43, 45, 52-53]. З іншого боку, якщо дані про місцезнаходження можна отримати з мереж стільникових мобільних телефонів, то проблеми, пов’язані з технікою відстеження на основі BLE, можна усунути, а також відмовитись від технологічних вимог (наприклад, телефонів з Bluetooth та розумними функціями). Існує методика відстеження місцезнаходження за межами приміщення для мобільних пристроїв у стільниковій мережі [54]. Показано, що запропонована методика майже на 88% точніша у порівнянні з аналогічними. У міських районах ефективність відстеження є найкращою із середньою точністю до 112 м. Також виявлено, що стільникові системи демонструють перспективні характеристики позиціонування і в приміщеннях [55]. У цій роботі запропоновано підхід до трасування контактів із використанням даних геолокації стільникових SIM-карт на відміну від методів трасування на основі BLE. У запропонованій моделі підтверджений номер мобільного телефону пацієнта COVID-19 буде переданий відповідному оператору мобільного зв’язку, щоб знайти інформацію про його мобільність за останні 7 днів. Оператор використовуватиме інформацію про геолокацію для відстеження мобільності, як показано на рис 2.1.

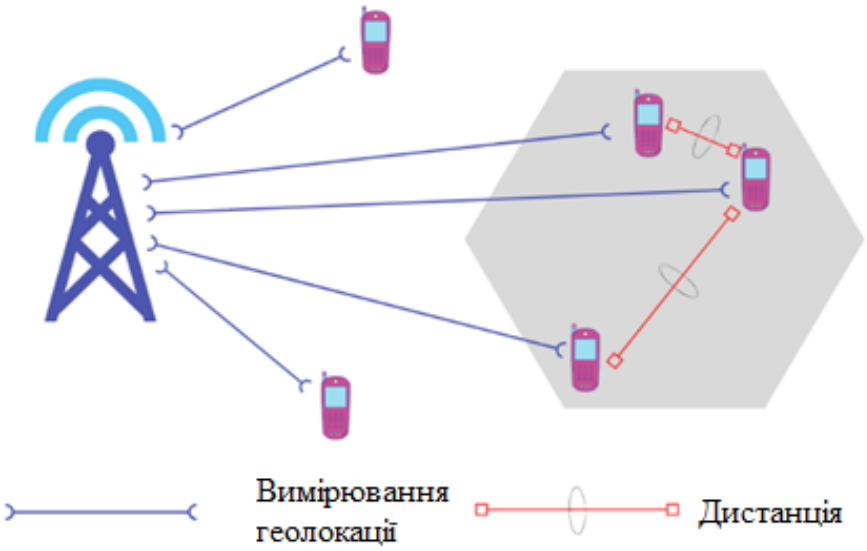

Рисунок 2.1 – Відстеження контактів через мобільну телефонну мережу з використанням даних геолокації

У запропонованій моделі не потрібен мобільний телефон із підтримкою Bluetooth / Wi-Fi / NFC, оскільки оператор використовуватиме підхід відстеження на основі геолокації, отримуючи дані про місцезнаходження безпосередньо з базової станції для ідентифікації ймовірних заражених людей. Цей метод дозволяє уникнути поширення паніки серед людей, оскільки він не вимагає постійного попередження про можливість зараження. Потім відповідальний орган може визначити найбільш ризикованих осіб на основі інтенсивності контакту з позитивними пацієнтами Covid-19 та доручити їм пройти ізоляцію / тест, якщо це необхідно. Крім того, якщо людина відчуває, що розвинув будь-які симптоми COVID-19, запропонований метод може також провести первинний скринінг, перевіривши, чи включений номер стільникового телефону до списку підозрюваних.

2.1.1 Пропозиція моделі відстеження контактів

У цьому пункті представлено запропоновану модель відстеження контактів на основі геолокації стільникового телефону. Загальна структура

складаться з трьох операційних фаз. Кожна фаза має певні заходи. Фази та їх операції показано нижче:

ЕТАП – I: Збір даних. На цьому етапі первинні дані для пацієнтів з COVID-19 будуть збиратися у призначених тестових центрах. Тоді заражені ділянки будуть показані за допомогою будь-яких картографічних служб (наприклад, Google map). Діяльність, яку слід виконати на цьому етапі, описана нижче, а процес зображений на рис 2.2.

Рисунок 2.2 – Діаграма потоку етапу – I

1) Крок 1

Щоразу, коли людина відвідує тест-центр COVID-19, дві основні відомості, такі як поточна адреса та активні номери мобільного телефону, повинні бути записані в місцевий реєстр тестового центру.

2) Крок 2

Якщо особа виявляється позитивною щодо COVID-19, то раніше записана інформація (тобто адреса та номери телефонів) повинна передаватися в центральну базу даних.

3) Крок 3

На цьому етапі буде підраховано кількість заражених осіб в окремій зоні (наприклад, у відділі, районі, місті, дорозі тощо).

4) Крок 4

Буде встановлено застосунок де кожен може здійснити просту реєстрацію за номером мобільного. Зареєстрований користувач може шукати певне

місцезнаходження та отримувати кількість заражених людей навколо нього за допомогою будь-яких картографічних служб (наприклад, Google map).

ЕТАП – II: Визначення ймовірних випадків. На другому етапі зосереджуємося на тому, як уряд може ідентифікувати ймовірно інфікованих. Номер стільникового телефону позитивних пацієнтів Covid-19 можна простежити, щоб з'ясувати можливі випадки, як показано на рис 2.3. Тут будь-який інший користувач стільникового телефону, який знаходився в безпосередній близькості (наприклад, 2 метри) від зараженої людини під час останні 7 днів перебуває у списку підозрюваних. Але усім людям не потрібно встановлювати будь-які застосунки, оскільки дані про місцезнаходження (широта та довгота) будуть збиратися з мережі мобільних телефонів. Отже, цей процес не обмежується використанням смартфонів, також можна отримувати дані для користувачів будь-якого типу стільникових телефонів (наприклад, функціональних телефонів). Покроковий процес проілюстровано нижче, а процес зображено на рис 2.4.

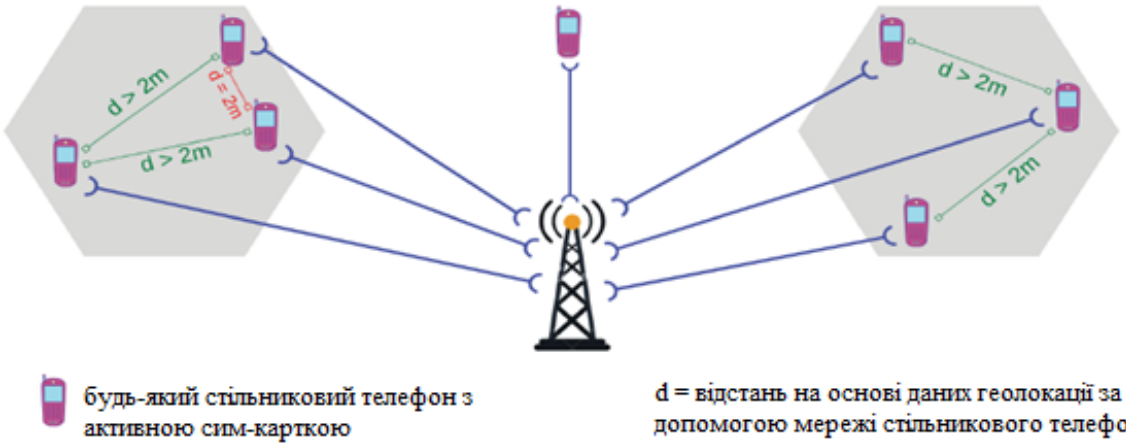

Рисунок 2.3 – Пошук можливих випадків за допомогою даних геолокації від операторів мобільних телефонів.

1) Крок 1

Після отримання даних (тобто списку заражених осіб) із центральної бази даних, кожен номер мобільного телефону буде надісланий відповідному оператору мобільного зв'язку, щоб отримати інформацію про мобільність (широту та довготу) відповідних користувачів стільникових телефонів протягом попередніх 7 днів. Одночасно з цим оператора також попросять надати мобільні номери активних користувачів стільникових телефонів у зонах мобільності заражених осіб на певній відстані.

2) Крок 2

Інформація про зону мобільності, отримана на попередньому кроці, потім буде надіслана всім іншим операторам для ідентифікації всіх активних користувачів стільникових телефонів, що знаходяться в зоні на той момент.

3) Крок 3

Усі номери стільникових телефонів (отримані з кроків 1 і 2) будуть зберігатися в центральній базі даних із позначкою "можливі заражені пацієнти / номери стільникових телефонів".

4) Крок 4

Якщо виявляється, що певний номер з'являється кілька разів у списку "можливі заражені пацієнти / номери стільникових телефонів", тоді користувачам мобільних телефонів буде запропоновано пройти тест на ізоляцію / COVID-19 відповідно.

Рисунок 2.4 – Діаграма потоку етапу – II

ЕТАП – III: Запит користувача. На цьому етапі, якщо людина відчуває фізичну незручність і хоче пройти тест, застосунок може допомогти прийняти рішення та передбачити можливість зворотного шляху. Для цього запропоновано такі дії, як описано нижче, поетапно, а процес зображено на рис 2.5.

Рисунок 2.5 – Діаграма потоку етапу – III

1) Крок 1

За допомогою програми будь-яка особа може здійснити пошук, чи вказати відповідний номер стільникового телефону у списку підозрюваних.

2) Крок 2

Якщо програма вже підозрює користувача мобільного телефону, особі буде запропоновано відповісти на деякі анкети, які можна взяти з собою [56, 57, 58]. Зразок набору запитань наведено в таблиці 2.1.

Таблиця 2.1 – Зразок анкети

Зразки запитань	**Користувацькі параметри**	
	Опція – 1	**Опція – 2**
Поява або погіршення кашлю	Так	Ні
Задишка	Так	Ні
Біль у горлі	Так	Ні
Нежить, чхання і закладеність носа	Так	Ні

продовження таблиці 2.1

Хриплий голос	Так	Ні
Набряки	Так	Ні
Нудота / блювота / діарея / живіт / біль	Так	Ні
Несподівана втома	Так	Ні
Лихоманка	Так	Ні

3) Крок 3

Відповіді буде перевірено та проаналізовано в режимі реального часу за допомогою заздалегідь визначеного набору.

4) Крок 4

Нарешті, після аналізу, якщо виявиться, що людина може бути інфікованою, їй буде наказано пройти тест на COVID-19. Ці три фази об'єднують, щоб сформувати запропонований спосіб відстеження контактів, а загальний потік зображений на рис 2.6.

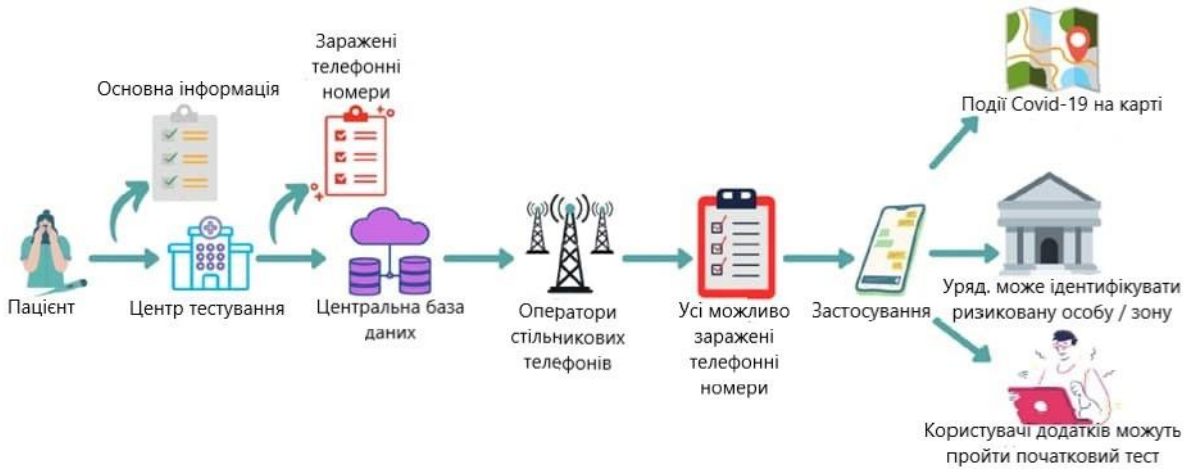

Рисунок 2.6 – Загальна блок-схема запропонованої системи

Запропонована модель використовує дані геолокації користувачів мобільних пристроїв безпосередньо від мобільних операторів. Таким чином загальна ефективність відстеження контактів значно покращується, зберігаючи конфіденційність користувачів.

2.1.2 Порівняння з іншими рішеннями

Найбільш сильним аспектом запропонованого методу відстеження контактів є те, що він не обмежується передовими технологічними вимогами (наприклад, смартфон, Bluetooth, Wi-Fi, NFC тощо). Єдина вимога – кожна людина повинна мати при собі мобільний телефон з активною сім-картою. З урахуванням 5,112 мільярда унікальних мобільних користувачів, 67% покриття у всьому світі (ще вище в міських районах, де COVID-19 має найгірший ефект), дані геолокації мобільних телефонів, здається, є найбільш життєздатним засобом відстеження контактів. Нещодавно кілька статей узагальнили різні підходи, запропоновані в літературі, для мінімізації поширення під час спалаху COVID-19 [59], [60]. Більшість підходів застосовуються за допомогою сучасних технологій. Загальноприйнятими підходами є шеринг, вибірковий шеринг, відмова від участі, спільний доступ за участю, приватний набір: безпечні шляхи тощо. Кожен із цих підходів має свої сильні сторони та обмеження. Раскар та ін. надали детальне резюме підходів, згаданих вище [59]. Розглянуто детальне порівняння, представлено [59] та проаналізувано різні аспекти кожного методу. Порівняння сильних сторін та обмежень існуючих та запропонованих методів викладено в таблиці 2.2. Коефіцієнти порівняння проілюстровані нижче відповідно до запропонованої моделі:

*Точність.*Оскільки інформація про мобільність буде збиратися у мобільних операторів, очевидно, що дані будуть точними.

*Прийняття.*Проблеми пристосованості не буде, оскільки людині не потрібно виконувати жодної заздалегідь визначеної діяльності.

*Конфіденційність.*Проблеми конфіденційності розглядаються з точки зору користувачів, місцевого бізнесу, користувачів запропонованої моделі та не-користувачів. Ці питання обговорюються нижче:

1) ризик конфіденційності для носіїв

Для користувачів не буде загрози конфіденційності, оскільки особиста інформація не буде оприлюднена. Оприлюднюватись будуть лише дані про

заражених через будь-які картографічні служби (наприклад, Google map). Під час ідентифікації сусідніх або конкретного користувача стільникового телефону інформація про місцезнаходження не буде оприлюднена. Запропонована модель працює централізовано. Дані про місцезнаходження будуть використовуватися лише для прогнозування ймовірності зараження відповідного користувача.

2) ризик конфіденційності місцевого бізнесу

Для місцевого бізнесу будуть дуже низькі ризики конфіденційності, оскільки місця відвідування, не будуть оприлюднені.

3) ризик конфіденційності для користувачів

Конфіденційність користувачів буде захищена, оскільки програма збиратиме дані про місцезнаходження від оператора SIM-карти, а не від місця розташування пристрою за допомогою Bluetooth або інших засобів.

4) ризик конфіденційності для «не користувачів» (non-users)

Можуть бути порушення конфіденційності для «*non-users»* оскільки «користувачі» та «*non-users*» якимось чином пов'язані через соціальні відносини, але це характерно і для інших методів відстеження контактів. Коли людину діагностують як COVID-19 позитивну, члени сім'ї або друзі можуть зазнати тих самих ненавмисних наслідків події.

Згода. Питання згоди розглядаються з точки зору носіїв, бізнесу та користувачів запропонованої моделі. Ці питання показано нижче:

1) згода носіїв вірусу

Вважається, що запропонована модель працює таким чином, що інформація про пацієнтів буде записана до тесту на COVID-19. Як результат, згодом неможливо буде приховати деталі носія вірусу. Тому згода не потрібна, оскільки це звичайна практика.

2) згода місцевого бізнесу

Згода місцевого бізнесу на запропоновану модель головним чином залежить від державної політики.

3) згода користувачів

Під час реєстрації користувачеві буде запропоновано надати номер стільникового телефону. Навіть коли користувач хоче перевірити, чи контактував він з яким-небудь пацієнтом COVID-19, номер стільникового телефону потрібно надіслати оператору для перехресної перевірки.

Таблиця 2.2 – Аналіз міцності та обмеження іншими запропонованими методами

Моделі	**Основна сила**	**Основні обмеження**
Шаринг	• відсутність питань громадського усиновлення • конфіденційність користувачів захищена • В основному доступний для всіх	• Значний ризик конфіденційності для носіїв covid -19 • питання точності даних • високий ризик дезінформації та масової паніки
Вибірковий шаринг	• Помірний ризик конфіденційності для носіїв covid-19 • масова паніка може бути обмежена	• питання точності даних • ризик дезінформації • обмежена технологічними вимогами
Одноадресний	• низький ризик масової паніки • точність даних висока	• відсутність конфіденційності для користувача • не корисний для масових людей
Участь	• Конфіденційність користувачів захищена від масових людей	• може бути шахрайська діяльність • масове прийняття користувачів низьке • Потрібна повна згода носія covid-19

продовження таблиці 2.2

Приватний комплект: Безпечний шлях	• загальна точність висока • низький ризик конфіденційності для носія covid-19	• обмежена технологічними вимогами • від носія covid-19 потрібна повна згода
Запропоноване рішення	• висока точність даних про місцезнаходження • користувачі стільникових телефонів не повинні бути смартфонами, а будь-якими телефонами з активною сим-карткою • для збору даних необхідна користувацька програма • менш помилково негативний випуск	• користувач повинен мати при собі стільниковий телефон

Системні виклики. Системні виклики розглядаються з точки зору носіїв вірусу, підприємств та користувачів запропонованої моделі. Проблеми описані нижче:

1) дезінформація

Існує дуже низький ризик дезінформації, оскільки дані про місцезнаходження не будуть братися з будь-якого вводу користувача. Швидше дані будуть збиратися у оператора SIM-картки.

2) паніка

Запропонована модель може певною мірою зменшити паніку, оскільки користувачі моделі можуть перевірити початковий статус, а також інтенсивність, перебуваючи вдома.

3) шахрайство та зловживання

Очікується, що не буде шахрайських дій, оскільки програма не потребуватиме жодного відкритого підключення (наприклад, Bluetooth, NFC тощо).

4) безпека інформації

Запропонована модель розроблена з урахуванням проблем безпеки та важливої інформації користувача. Оскільки для роботи із запропонованим методом потрібен лише номер стільникового телефону, існує дуже низький шанс появи проблем у безпеці.

5) рівний доступ

Рівний доступ – головна сила запропонованої моделі, оскільки вона не обмежується жодними технологічними вимогами (наприклад, смартфонами, акумулятором, певною ОС тощо), а потрібен лише мобільний телефон.

6) соціально-економічні фактори

Запропонована модель майже не має поганого впливу на соціально-економічні фактори. Іноді це залежить від практики уряду, якщо така існує.

2.2 Існуючі системи контролю

Оскільки технологічна інфраструктура продовжує розвиватися, світ навколо нас став більш зв’язаним, ніж будь-коли раніше, і все, що можна зв’язати, буде пов’язане. Розумні міста, розумні будинки, розумна роздрібна торгівля, підключені автомобілі та пристрої свідчать про те, як підключені пристрої порушують статус-кво, що веде до створення ефективної, автоматизованої планети.

Інтернет речей (IoT) об'єднує всі речі в мережі Інтернет з метою обміну інформацією для досягнення розумних розпізнавань, позиціонування, відстеження, моніторингу та адміністрування, використовуючи передбачені

протоколи за допомогою засобів зондування інформації для здійснення обміну інформацією та зв'язку.

2.2.1 Система IoT у діагностиці пацієнтів із Covid 19

У розпал пандемії вірусу коронавірусу розроблено специфікації системи, здатної виявляти хворих вірусом корони за допомогою системи IoT (рис 2.7).

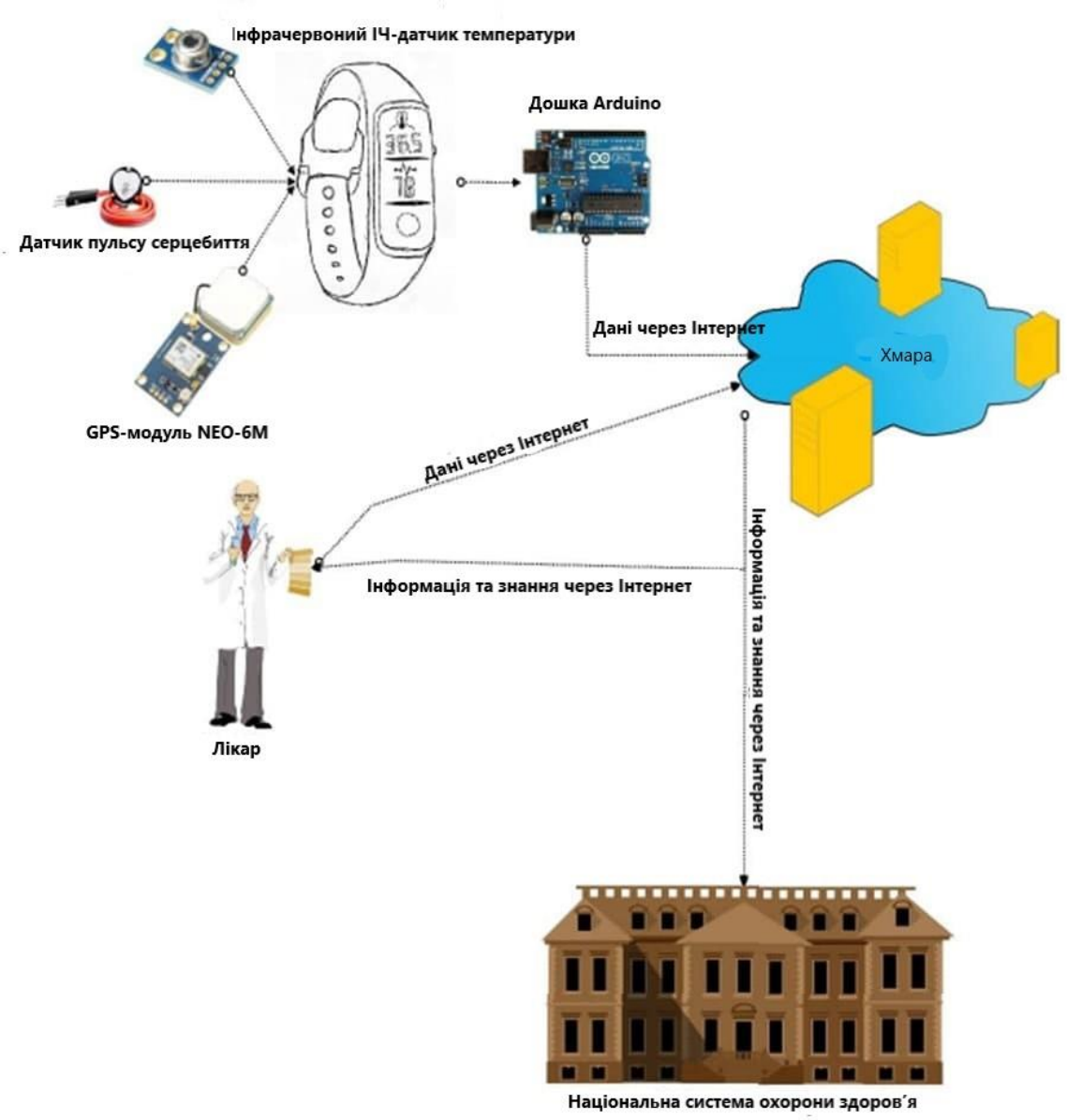

Рисунок 2.7 – Система IoT в умовах пандемії коронавірусу

Система IoT має багато переваг у телемедицині: профілактика та перша допомога людям, які сприйнятливі до серцевих нападів, моніторинг

епілептичних нападів, моніторинг людей, які страждають алкоголізмом, скринінг пацієнтів Covid 19 [63].

Найпомітніша апаратна частина системи складається з браслета, який носить людина (рис 2.8). Він має вбудований давач температури, монітор серцевого ритму та давачі розташування (GPS). Інформація, отримана від давачів через браслет, надсилається на плату Arduino, яка перетворює сигнали в цифрову інформацію. Ця інформація не зберігається на платі, оскільки місця для зберігання недостатньо для великого обсягу даних, необхідних для спостереження за людиною, що носить браслет.

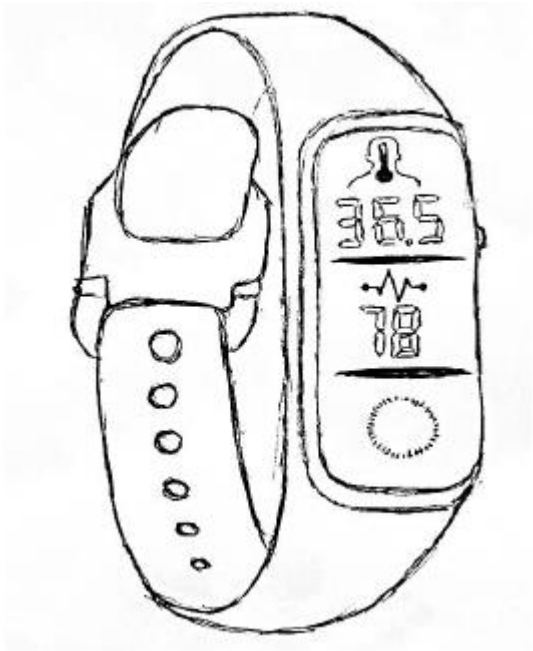

Рисунок 2.8 – Пристрій моніторингу

Для точного прогнозування людей із хворобою Covid 19 програмне забезпечення потребує узгодженої бази даних, яка буде збиратися у людей і зберігатися в хмарі. З хмари вони перейдуть як до лікарів, до яких призначені відповідні особи, та до Національної системи охорони здоров’я для аналізу з огляду на майбутні реформи системи охорони здоров’я, а також для макроекономічної статистики. Розглянемо дизайн прототипу постійного моніторингу здоров’я пристрою. Цей пристрій схожий на розумні годинники, які

зараз заповнюють ринок, але він орієнтований на показники здоров'я, а не на мультимедіа. Це також дуже схоже на фітнес-браслети, але спосіб обробки та використання даних, зібраних із давачів, дуже різний. Нижче представлені основні апаратні компоненти, орієнтовані на давачі (рис 2.9).

Рисунок 2.9 – Основні апаратні компоненти

Існують також інші обов'язкові елементи обладнання, такі як акумулятор, світлодіод, РК-дисплей тощо.

2.2.2 Обробка даних та специфікації програмного забезпечення

Система IoT (рис 2.10) має реальні переваги з точки зору швидкості, з якої дані отримуються від давачів, потім передаються в хмарні бази даних,

обробляються хмарним програмним забезпеченням і перетворюються на цінну інформацію для лікарів та системи охорони здоров’я.

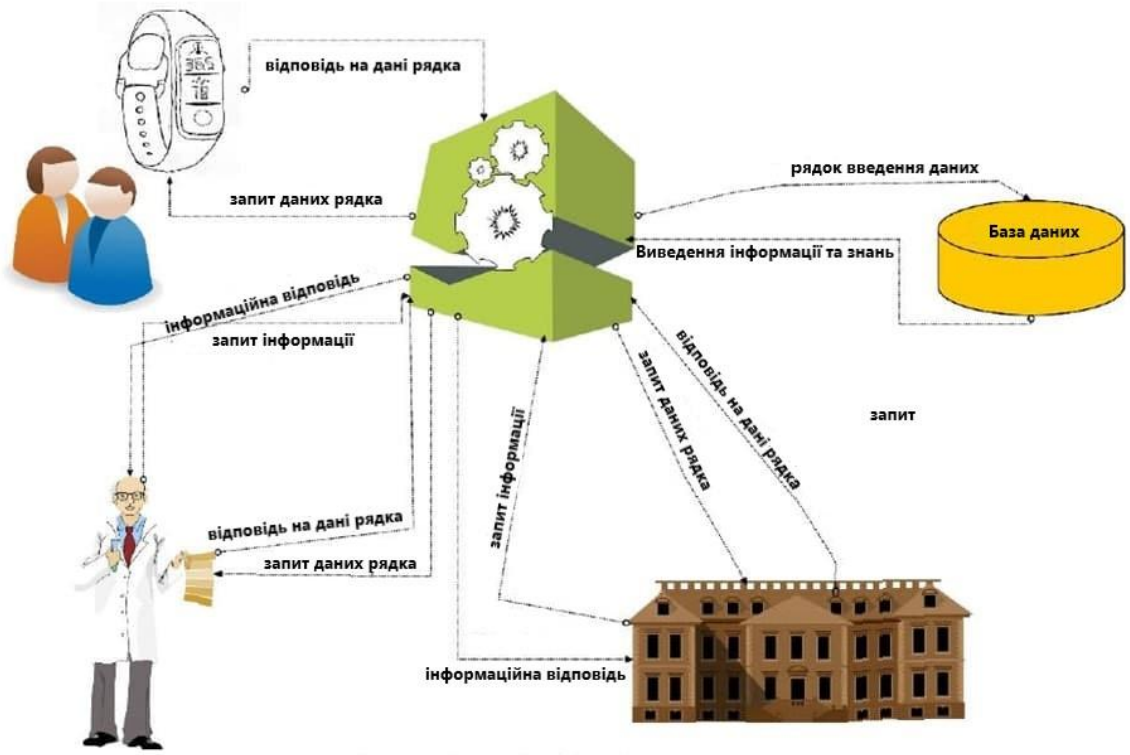

Рисунок 2.10 – Система охорони здоров’я IoT

Для категорії людей, в зоні підвищеного ризику до хвороби, сценарій наступний: деякі люди носять браслети з давачами. Інформація про давач надсилається до Oracle Cloud. Тут реалізується застосунок, який передбачає за допомогою алгоритмів машинного навчання людей, які страждають на Covid 19.

Вхідні дані надходять як від людей, які носять браслети з давачами, так і від їхніх лікарів, як результат – це інформація у вигляді високоякісних прогнозів, які надсилаються лікуючому лікарю та органам охорони здоров’я. У випадку, якщо особа, має «підтверджений позитивний» результат програмним забезпеченням, лікар, який отримує інформацію, зв’язується з органами охорони здоров’я для тестування особи. Однак слід піти на компроміс між уникненням збоїв системи через надзвичайно великий обсяг даних та виявленням пацієнтів

якомога раніше, було вирішено взяти дані з інтервалом у три години [63]. Цей інтервал часу вибирається довільно, навіть якщо система перевантажена через великий обсяг даних, а також численну обробку. Якщо буде виявлено, що ефективність профілактики не зменшується при збільшенні інтервалу, тоді інтервал буде здійснюватися невеликими кроками максимум на одну годину.

Дані не потрібно очищати, оскільки вони надходять із подібних джерел, відповідно з давачів, а також зі стандартних медичних карт осіб. Якщо у деяких випадках давачі не надсилають певні дані, поля, призначені для цих даних, заповнюються виразом N / A.

Потік даних базується на веб-сервісах SOAP (запит-відповідь). Застосунок вимагає ряд даних від давачів, а також від лікарів та органів охорони здоров'я, що вимагають інформації та знань із хмарного застосунку. Хмарний застосунок обробляє та моделює дані рядків, отримані з двох раніше згаданих джерел, і надсилає їх лікарям та органам охорони здоров'я.

Тому цікавить, який алгоритм може точно передбачити, які суб'єкти заражені. Дані отримуються з пристроїв, які носять люди. Характеристиками, які аналізуються і які можуть бути вирішальними для дослідження, є:

- розташування – щоб визначити, чи перебуває людина у вогнищі інфекції, чоловічої чи жіночої статі;
- пульсу, чи страждає пацієнт на серцево-судинні захворювання, діабет чи хронічні респіраторні захворювання, гіпертонію;
- температура та вік.

Дані очищені та підготовлені, щоб не було порожніх полів у базі даних (рис. 2.11).

```
RangeIndex: 300 entries, 0 to 299
Data columns (total 10 columns):
 #   Column                    Non-Null Count  Dtype
---  ------                    --------------  -----
 0   Outbreak                  300 non-null    int64
 1   Gender                    300 non-null    int64
 2   Heart_Rate                300 non-null    int64
 3   Cardiovascular_Disease    300 non-null    int64
 4   Diabetes                  300 non-null    int64
 5   Chronic_Respiratory_Disease  300 non-null    int64
 6   Hypertension              300 non-null    int64
 7   Temperature               300 non-null    float64
 8   Age                       300 non-null    int64
 9   Covid_19_Suspect          300 non-null    int64
dtypes: float64(1), int64(9)
memory usage: 23.6 KB
```

Рисунок 2.11 – Очищення даних

Температура та пульс є важливими факторами для створення моделі (рис. 2.12). Щоб отримати уявлення про те, як хворі (помаранчеві крапки) чи здорові (сині крапки) обстежувані розташовані залежно від температури та частоти серцевих скорочень. Помітно, що у пацієнтів нормальний артеріальний тиск (90), а температура висока (37,5-38).

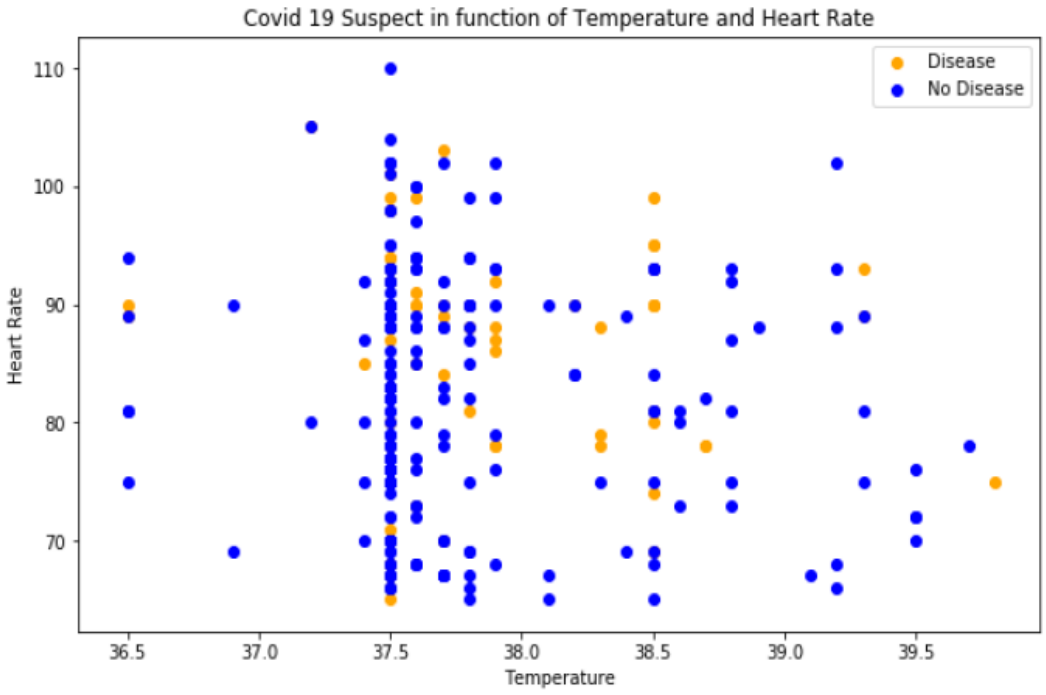

Рисунок 2.12 – Розсіяний графік підозр на хвороби та нехвороби

Відповідно до артеріальної гіпертензії (22 підозрюваних не мають гіпертонічної хвороби, 12 мають м’яку артеріальну гіпертензію, 19 мають середню гіпертензію та 13 мають серйозну гіпертензію), що свідчить про те, що гіпертонія не відіграє особливої ролі у впливі на прогноз. Натомість матриця кореляції чітко вказує, що кожен із факторів лише незначно впливає на інфекцію. Вони окремо відіграють слабку роль у прогнозуванні, але разом у сукупності відіграють особливу роль (рис. 2. 13).

Рисунок 2.13 – Кореляційна матриця

Алгоритми моделювання підходять в цьому випадку. Є 9 незалежних змінних (спалах, стать, частота серцевих скорочень, серцево-судинні хвороби, діабет, хронічна хвороба дихальних шляхів, гіпертонія, температура, вік), і можна з’ясувати, до якої категорії належить залежність до змінної (підозра на

Covid 19), тобто бачити для кожного суб'єкта підозру на Covid 19 (значення 1) чи ні (значення 0). Дослідження починаєтсья з таких алгоритмів: логістична регресія, KNN та Random Forest. При простому оцінюванні аналіз точності вказує для кожного: 72%, 67%, 73%. Що стосується логістичної регресії, якщо збільшити розмір тесту на 25%, можна отримати вищий коефіцієнт передбачуваності на 82% -83%, маючи лише 1 помилку на матриці. Із загальних даних вибирають 20% для тестування, а решту 80% для навчання моделі. Для випадкової моделі класифікатора - 72%, а для логістичної регресії оцінка на тестовій вибірці становить 81%. Навіть якщо збільшити кількість перевірених даних до 25%, відсоток залишається на рівні 74-75%.

Матриця у моделі дерева рішень відображає 10 помилок із 51 на даних тестування та 5 помилок з 9 на прогнозуванні даних.

Отримано хороший результат за допомогою алгоритму Support Vector Machine (SVM), який дає коефіцієнт передбачуваності 80%, а для ядра SVM отримано 80%, маючи 0 помилок на Confusion Matrix.

2.3 Застосунок для моніторингу коронавірусу SDA-COVID-19

COVID-19 є швидкопоширюваною та летальною хворобою. Соціальна дистанція – єдиний спосіб зупинити розповсюдження вірусу. Тому представлено застосунок соціального дистанціювання під назвою SDA-COVID-19. Запропонований застосунок (SDA-COVID-19) допоможе людям підтримувати соціальне дистанціювання шляхом обміну даними між телефонами про потенційно інфікованих або заражених людей COVID-19, з якими особа спілкувалася або контактувала, завдяки чому особа буде попереджена, якщо заражена людина знаходиться в безпосередній близькості.

2.3.1 Проблеми та випробування, що стоять перед SDA COVID-19

Приватність. Хоча багато хто стурбований розкриттям конфіденційності своїх даних, все-таки SDA-COVID-19 можна розглядати як інструмент перевірки для людей, які претендують на роботу, або поточний персонал, що підтримує робоче середовище. Крім того, всі дані зберігаються на власному телефоні людини, отже, ніхто не матиме доступу до таких даних. Крім того, дані, що вимагаються від власника телефону, не перевищують того, що людина зазвичай надає своєму лікарю при першому відвідуванні. У цьому контексті дослідники запропонували дві версії SDA-COVID-19.

Безпека. У SDA COVID-19 є багато аспектів проблеми безпеки. По-перше, крадіжка даних, дані кожного власника телефону розміщуються на його власному телефоні та шифруються.

Доступ до смартфона. Хоча багато хто не володіє смартфонами, що є особистим вибором для людей. Однак, згідно з [61], кількість власників смартфонів становить 3,5 мільярда чоловік, що "означає, що 45,12% населення світу володіє смартфоном" [62]. Крім того, SDA-COVID-19 може спонукати людей купувати смартфони, оскільки застосунок стане їхнім детектором здоров’я та системою раннього попередження про потенційний ризик піддатися пандемії.

Закон та нормативні акти. Фізична особа (вона ж власник смарт-телефону) є людиною, яка ризикує захворіти хворобою. Використання SDA-COVID-19 є найбільш корисним для людини, оскільки воно буде інформувати особу про стан її здоров’я. Крім того, питання нормативно-правових актів не застосовуватиметься, коли людина намагається виявити безпечне середовище та бути проінформованою про своє життя та здоров'я.

2.3.2 Робочі кроки службової версії SDA-COVID-19

Перша версія SDA-COVID-19 описана в цьому пункті. Ця версія SDA-COVID-19 орієнтована на сервіс і повинна обмінюватися даними для зв'язку з

постачальником послуг зв'язку через Інтернет-хмару. У цій версії SDA-COVID-19 дані передаються в базу даних COVID-19, і постачальник послуг зв'язку може маніпулювати ними та використовувати дані для відстеження заражених COVID-19 людей, див рисунок 2.14. Така система належним чином підключена до медичного центру. Медичними центрами можуть бути будь-які державні організації охорони здоров'я, такі як міністерство охорони здоров'я. Далі представлено основні 9 кроків SDA-COVID-19 наступним чином:

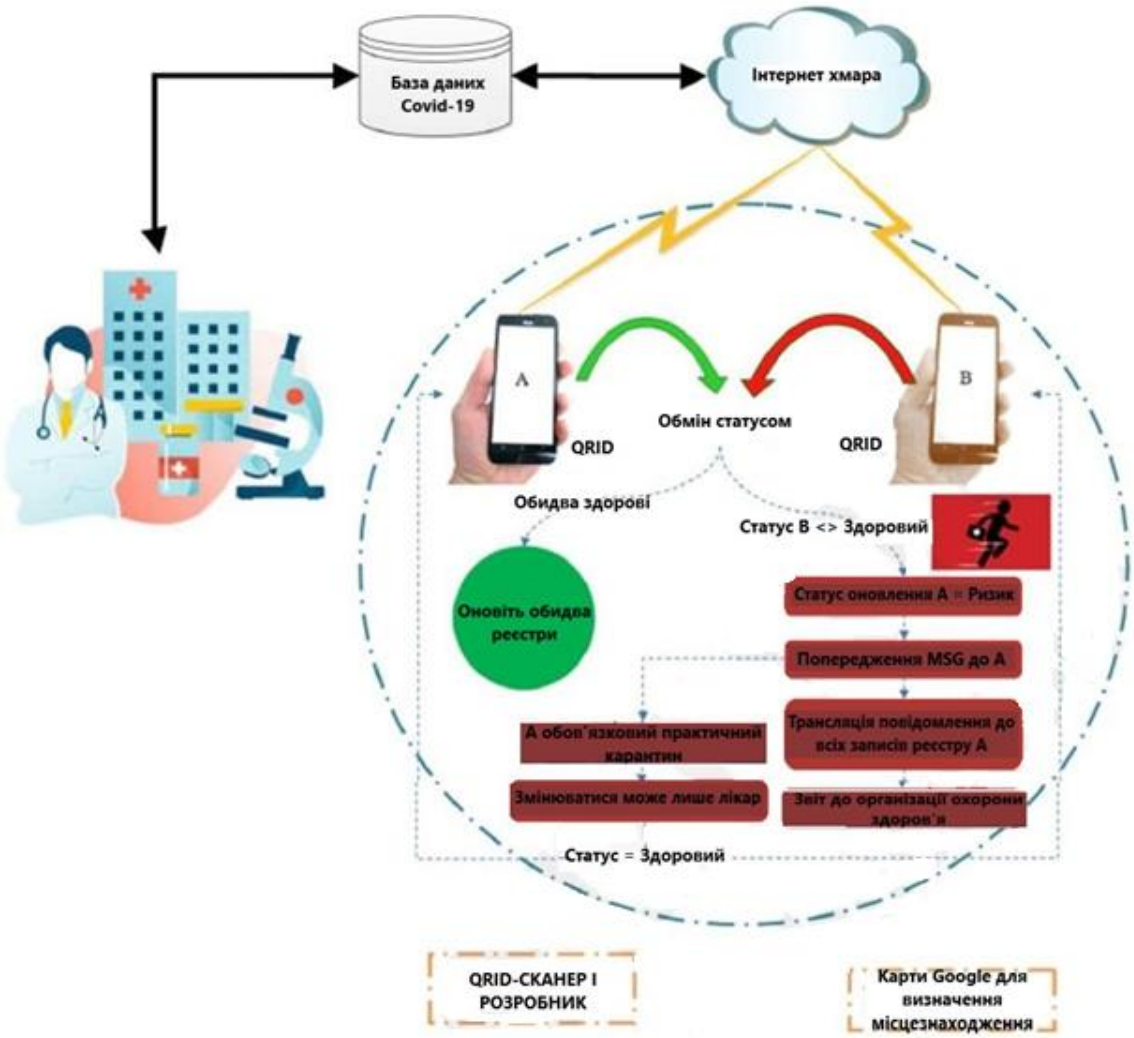

Рисунок 2.14 – Версія SDA-COVID-19 орієнтована на службу

1) Глобальна база даних COVID-19, доступ до якої здійснюється через інтернет, буде оновлюватися органами охорони здоров'я COVID-19, відповідальними за реєстрацію всіх випадків у кожній країні по всьому світу.

2) SDA-COVID-19 буде завантажено та встановлено на смартфоні з магазину додатків iPhone, Google play або Samsung Play Store. Кожен завантажений SDA-COVID-19 надасть смартфону номер (основний номер) на основі серійного номера та номера телефону смартфона.

3) Особа повинна зареєструватися в SDA-COVID-19, використовуючи ім'я, адресу, національний ідентифікатор, дату народження, стан здоров'я, як показано в розділі структури даних. Надалі дані будуть зашифровані за допомогою пароля власника телефону.

4) Використовуючи інтернет та GPS, SDA-COVID-19 буде відстежувати всі переміщення та розташування користувачів та реєструвати всі місця та людей, які постійно перебувають у безпосередній близькості від користувача.

5) SDA-COVID-19 не лише повідомить користувача про наявність зараженої або потенційно зараженої людини шляхом сканування людей навколо користувача, але також попередить систему охорони здоров'я у випадку, якщо користувач знаходився досить близько (менше 1,8 м.), і тому агенти охорони здоров'я будуть стежити за її / його справою, оскільки він / вона буде записаний як підозрюваний випадок у базі даних COVID-19, і йому буде повідомлено про перебування вдома протягом 14 днів.

6) Коли медичний працівник виявляє, що хтось інфікований COVID-19, всім людям, які протягом останніх 3-4 тижнів знаходились в безпосередній близькості від зараженого випадку, потрібно порадити пройти карантин та пройти тестування та переконатись, що вони не заражені COVID-19.

7) У випадку, якщо людина натисне спеціальну кнопку на смартфоні, що вона може бути заражена вірусом, SDA-COVID-19 надішле попереджувальне повідомлення всім людям, які були поруч протягом останніх 3-4 тижнів, щоб повідомити їх про це та вжити необхідних заходів.

8) Коли отримано попереджувальне повідомлення, стан телефону зміниться на статус "Ризик", отже, власник телефону повинен бути на карантині

протягом 14 днів і зв’язатися з найближчим закладом охорони здоров’я. Власник телефону повинен застосовувати запобіжні заходи, щоб не заразити інших. Телефон також надсилатиме повідомлення у своєму реєстрі у вигляді ланцюгового повідомлення.

9) Як тільки власник телефону вилікується, його / її статус зміниться лікарем з акредитованого медичного закладу. Лікар підпише власника телефону з його / її даними, використовуючи метод двосторонньої факторної автентифікації.

2.3.3 Робочі кроки Bluetooth версії SDA-COVID-19

Друга версія SDA-COVID-19 має Bluetooth. SDA-COVID-19 у цьому випадку є автономним застосунком з опцією, яка не підключена до бази даних COVID-19, отже, постачальник послуг зв'язку не має доступу до даних, див. рисунок 2.15. Дані в SDA-COVID-19 розподіляються, і кожен власник смартфона може добровільно надати свої дані до закладів охорони здоров’я. Така версія SDA-COVID-19 буде більш прийнятною для громадськості, і люди не матимуть проблем із конфіденційністю. Далі представлено основні 8 кроків SDA-COVID-19 наступним чином:

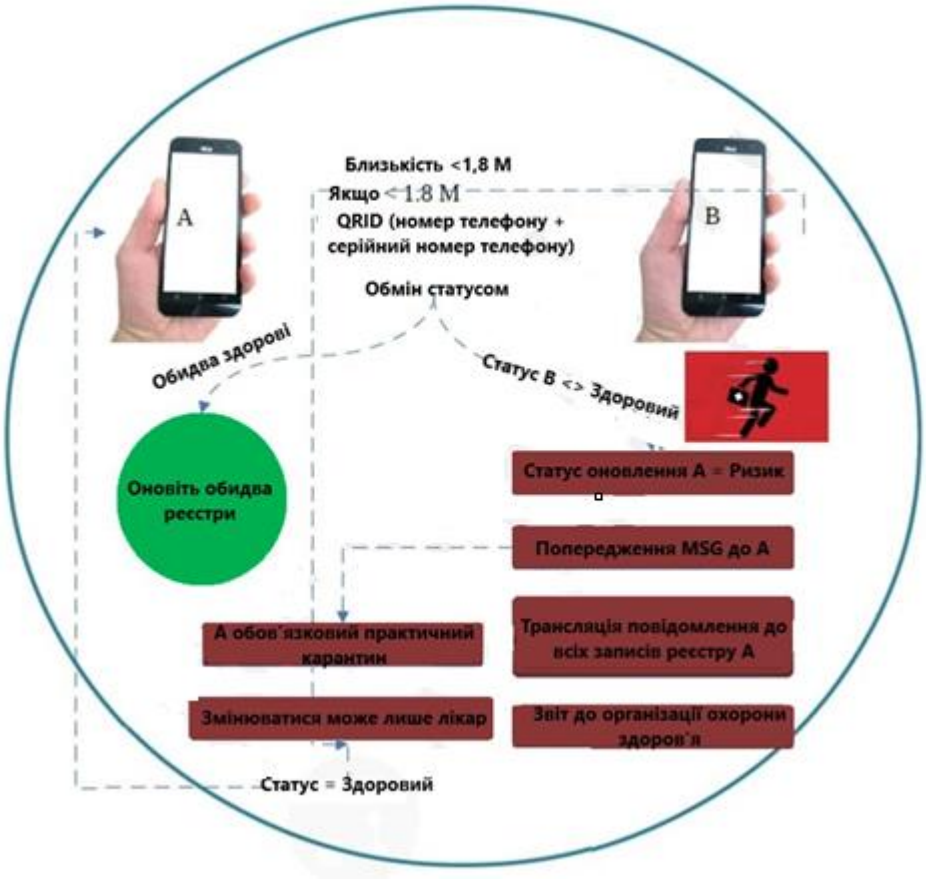

Рисунок 2.15 – Орієнтована на Bluetooth версія SDA-COVID-19

1) SDA-COVID-19 буде завантажено та встановлено на смартфоні з магазину додатків iPhone, Google play.

2) Кожен завантажений SDA-COVID-19 надасть смартфону номер (основний номер) на основі серійного номера та номера телефону.

3) Особа повинна зареєструватися в SDA-COVID-19, використовуючи ім’я, адресу, національний ідентифікатор, дату народження, стан здоров’я, як показано в розділі структури даних. Надалі дані будуть зашифровані за допомогою пароля власника телефону.

4) SDA-COVID-19 через телефон буде розшарювати свій номер на інші телефони радіусом 1,8 М (рис 2.16).

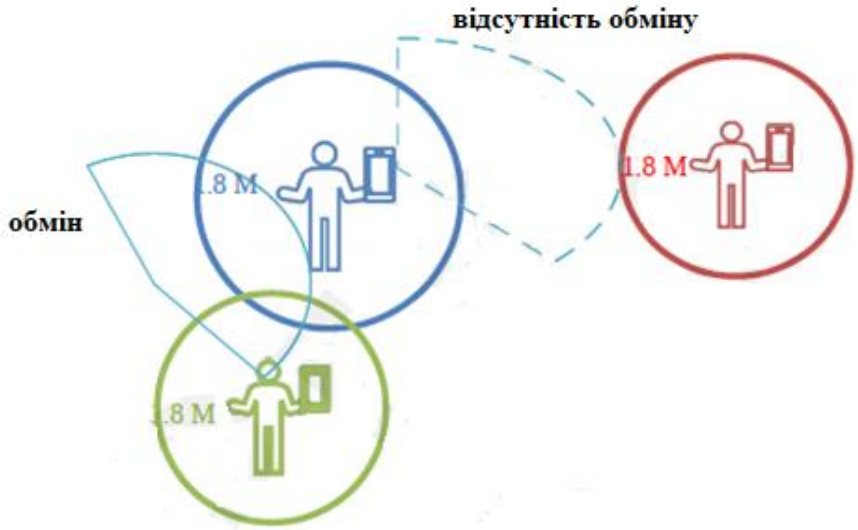

Рисунок 2.16 – Спрощений вигляд взаємодії SDA-COVID-19

5) SDA-COVID-19 також отримує розшарені номери та зберігає їх у реєстрі. Реєстр складається з номера телефону та серійного номера телефону та близькості (відстані), як показано в розділі структури даних.

6) У випадку, якщо людина натискає спеціальну кнопку на смартфоні, він надішле попереджувальне повідомлення на всі записи реєстру.

7) Після отримання попереджувального повідомлення стан телефону зміниться на статус “Ризик”, отже, власник телефону повинен перебувати на карантині протягом 14 днів і зв’язатися з найближчим закладом охорони здоров’я. Власник телефону повинен застосовувати запобіжні заходи, щоб не заразити інших. Телефон також надсилатиме повідомлення про забруднення іншим у своєму реєстрі у вигляді ланцюгового повідомлення.

8) Як тільки власник телефону вилікується, його / її статус буде змінено лікарем із акредитованого медичного закладу. Лікар підпише власника телефону з його / її даними, використовуючи метод двосторонньої факторної автентифікації.

2.3.4 Структура даних

Основа запропонованого SDA-COVID-19 складається з двох основних таблиць бази даних: таблиці бази даних власника телефону, яка знаходиться на

смартфоні власника. Друга таблиця бази даних називається реєстром, яка також знаходиться на смартфоні власника. Таблиця бази даних власника телефону складається з 12 атрибутів і відображена на таблиці 2.3

Таблиця 2.3 – бази даних з іменем власник телефону.

Власник телефону	
роль	користувач-лікар (зарезервовано для встановлення установою)
QRID	серійний номер телефону + номер телефону (13 цифр)
Ім’я	Varchar 30
Національний ID номер	Varchar (24) може бути перевірено
Стать	Чоловік/жінка
Дата народження	Дата
Адреса – будинок, вулиця, місто, країна	Локація по гугл картах
діабет	Так/ні
серцево-судинне захворювання	Так/ні
хронічні респіраторні захворювання	Так/ні
гіпертонія	Так/ні
рак	Так/ні

Таблиця власника телефону буде заповнена власником телефону, використовуючи дані для завантаження. Користувач може отримати доступ до двох застосунків QRID для побудови QRID, для цілей ідентифікації та Google Maps, для визначення місцезнаходження. Дані, що відносяться до таблиці бази даних, заповнюються лише один раз. Та сама таблиця використовується, коли її заповнює медичний заклад, який має облікові дані та використовує схему двосторонньої факторної автентифікації. Роль лікаря має більше привілеїв, ніж роль користувача, наприклад змінити атрибут стану в таблиці бази даних реєстру з Ризикований / Хворий на Здоровий.

Друга таблиця бази даних – це Реєстр, який складається з 6 атрибутів і відображена в таблиці 2.4.

Таблиця 2.4 – бази даних реєстру та атрибути

Регістр	
Порядковий номер	Цілий номер
QRID	від інших власників телефонів
Близькість	0 – 1.8 м
Timestamp (мітка часу)	Час + дата
Статус	Здоровий/ризикований/хворий (змінити статус може лише роль лікаря)
Місцезнаходження	Базується на Google

Атрибути заповнюються автоматично SDA-COVID-19. Реєстр оновлюється автоматично, коли два смартфони знаходяться на відстані 1,8 м. Атрибут «Статус» відображає спочатку "Здоровий", як тільки людина знаходиться в радіусі 1,8 м від людини зі смартфоном "Ризик" або "Хворий", статус зміниться на ризикований. Тільки особа з роллю лікаря може змінити атрибут «Статус» назад на «Здоровий». Зміна статусу атрибута захищена двостороннім коефіцієнтом безпеки. Крім того, реєстр таблиці бази даних буде автоматично оновлюватися щодня, стираючи всі записи, яким 24 дні, це атрибут «Timestamp».

2.3.5 Екрани вводу та виводу SDA-COVID-19

У SDA-COVID-19 є два типи екранів: спочатку екран початкової реєстрації. Цей екран введення, (рис 2.17), дозволяє реєструватись у SDA-COVID-19 і базується на таблиці бази даних власника телефону.

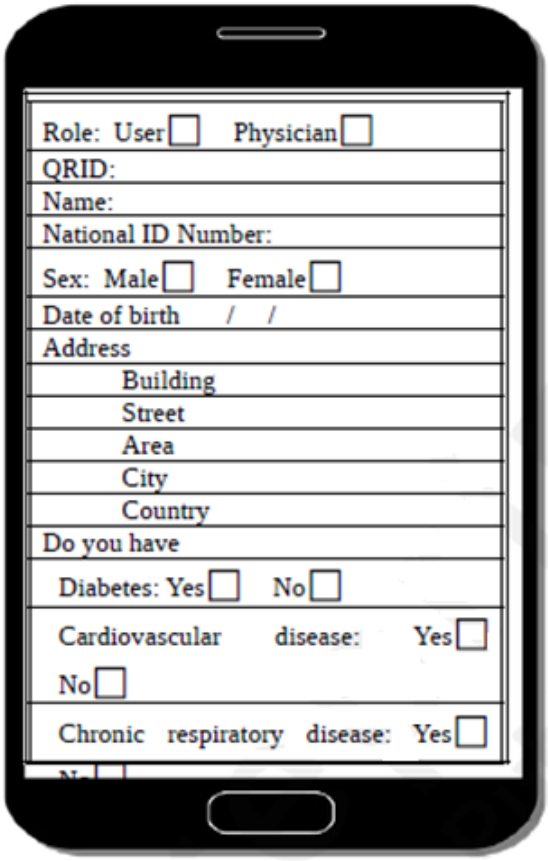

Рисунок 2.17 – Екран первинної реєстрації

Другий інтерфейс – це вихідний екран, показаний на рисунку 2.18, який відображає: QRID та статус власника телефону. Статус власника телефону має три типи: здоровий, ризикований, хворий. Статус здорового кольору пофарбований зеленим кольором, статус ризикованого – синім кольором, а статус хворого – червоним.

Рисунок 2.18 – Статус власника телефону хворий, ризикований, здоровий

SDA-COVID-19 дозволить користувачеві отримувати повідомлення та попередження про заражених COVID-19 людей, які можуть перетнути її / його шлях. SDA-COVID-19 буде відстежувати всіх людей, які могли знаходитись поблизу власника телефону за минулий період. Після виявлення інфікованої людини всі люди, які її зустрічали, будуть попереджені.

2.4 Висновок до розділу 2

В цьому розділі розглянуто автоматизоване відстеження контактів які хворі на Covid-19 за допомогою геолокації з використанням застосунків. Багато країн вже розробили застосунки відстеження контактів, які дають багатообіцяючі результати, але мають значні проблеми щодо конфіденційності. В розділі вирішено проблему конфіденційності, уникаючи будь-яких застосунків на основі смартфонів для відстеження контактів через бездротове підключення (наприклад, Bluetooth, Wi-Fi, NFC тощо). Запропонована модель використовує дані геолокації користувачів мобільних пристроїв безпосередньо від мобільних операторів. Таким чином загальна ефективність відстеження контактів значно покращується, зберігаючи конфіденційність користувачів.

Також одним із основних елементів розділу є застосунок SDA-COVID 19. SDA-COVID-19 дозволить користувачеві отримувати повідомлення та попередження про заражених COVID-19 людей, які можуть перетнути її / його шлях. SDA-COVID-19 буде відстежувати всіх людей, які могли знаходитись поблизу власника телефону за певний період. Після виявлення інфікованої людини всі люди, які її зустрічали, будуть попереджені. SDA-COVID-19 пропонується у двох версіях: на основі GSM та на основі Bluetooth. Версія SDA-COVID-19 на основі GSM повинна використовуватися з даними, якими обмінюється постачальник послуг зв'язку. Версія Bluetooth SDA-COVID-19 – це повністю розподілена система, яка не потребує проміжних засобів для зв'язку, окрім Bluetooth. Ця версія буде більш популярним варіантом, оскільки проблема

конфіденційності вирішена, але споживання батареї слід винести як окрему проблему.

3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

3.1 Охорона праці

Охорона праці – це система законодавчих, організаційно-технічних, соціально-економічних, санітарно-гігієнічних і лікувально-профілактичних мір і засобів, спрямованих на збереження життя, здоров'я й працездатності людини в процесі праці. Завдання охорони праці полягає в тому, щоб звести до мінімуму ймовірність поразки працюючого під дією небезпечного виробничого фактора або захворювання під дією шкідливого виробничого фактора з одночасним забезпеченням комфортних умов при максимальній продуктивності праці. Закон України "Про охорону праці" визначає основні положення по реалізації конституційного права громадян на охорону їх життя і здоров'я в процесі трудової діяльності; регулює взаємини між адміністрацією і працівником в незалежності від форм власності; встановлює єдиний порядок організації охорони праці в Україні [64].

В даній класифікаційній роботі описується система геолокації інфекційного хворого, в якій використовується різне апаратне забезпечення в тому числі персональний комп’ютер та смартфони. Здебільшого саме смартфони використовуються, бо за допомогою них, можна моніторити стан людини, яка заражена або наближена до зіткнення з COVID – 19. Адже на них можна скачувати та встановлювати різні застосунки відстеження контактів. Тому необхідним є дотримання гігієни з смартфоном, тому що він теж несе певну небезпеку людині яка використовує його.

Мобільний телефон (смартфон) – це дуже зручний та корисний засіб, однак, його використання потребує певних гігієнічних навичок. Окрім наявних переваг, цей гаджет має деякі небезпечні для здоров’я людини аспекти, одним з яких є електромагнітне випромінювання [65].

Щоб захистити себе від дії електромагнітного випромінювання, кожен власник мобільного телефону (смартфону) повинен вживати заходів безпеки і дбати про своє здоров'я:

- показник шкідливого впливу телефонів на здоров'я людини вказується у супровідних документах до пристрою. Максимально допустимий рівень SAR дорівнює 1,6 Вт / кг. Вибираючи новий апарат, необхідно звертати увагу на цей показник і не купувати телефони з рівнем SAR вище 1,2;
- довгі й часті розмови, на думку деяких лікарів, можуть спровокувати розвиток і ріст пухлин мозку. Для зниження ризику рекомендується користуватися провідною гарнітурою або використовувати гучний зв'язок;
- максимальний пік електромагнітного випромінювання помічений в моменти пошуку мережі, дозвону і з'єднання. Наполегливо рекомендуємо підносити телефон до вуха лише після того, як абонент відповість на дзвінок, тримаючи весь цей час трубку в руці і спостерігаючи за індикацією на дисплеї (або вібрацією);
- під час очікування телефон постійно тримає зв'язок з базовою станцією, тому ні в якому разі не можна розташовувати його поруч із собою в періоди сну або відпочинку. З цієї ж причини мобільному апарату не місце в нагрудній або брючній кишені;
- передача даних по каналам (GPRS, EDGE, 3G та 4G) посилює випромінювання у той час, коли на апарат закачуються безкоштовні ігри та нові додатки. Не обов'язково тримати пристрій у руках – краще поставити на закачування кілька файлів і відкласти трубку в сторону;
- металеві предмети беруть на себе роль екрану і збільшують інтенсивність електромагнітного поля. З цієї причини слід утримуватися від телефонних бесід в транспорті і знімати під час довгих розмов окуляри з металевою оправою і великі сережки з металу;
- не бажано спілкування по мобільному телефону (смартфону) під час руху в автомобілі чи іншому транспорті, і не тільки через відволікання уваги від

дороги, а й через те, що під час руху телефон переходить на максимальну потужність, щоб з'єднатися з базовими станціями зв'язку;

- чим нижче сигнал прийому мережі, тим вище електромагнітне випромінювання. Боротися з цим можна, вибираючи оператора зв'язку з хорошою зоною покриття і утримуючись від бесід у місцях з низьким сигналом;
- під час зарядки мобільний телефон (смартфон) стає ще небезпечніше для здоров'я. Тому, якщо телефон розрядився, краще спочатку зарядити його, і тільки потім, відключивши від мережі, продовжити спілкування;
- зарядний пристрій, який виконав своє завдання, продовжує споживати електроенергію і виробляти шкідливе випромінювання. Відразу ж після підзарядки телефону (смартфону) зарядний пристрій необхідно витягнути з розетки;
- особливо обережними при користуванні мобільними телефонами повинні бути вагітні жінки;
- мобільний телефон (смартфон) – джерело бактерій, адже мало кому прийде в голову мити руки перед тим, як відповісти на дзвінок або зателефонувати. Для захисту від інфекцій трубку потрібно іноді протирати спеціальними вологими серветками, а перед їжею не забувати про правила гігієни.

Тому, в результаті роботи над даною темою було проведено аналіз шкідливого впливу смартфона на користувача , з яким стикається розробник різного програмного забезпечення для смартфона по відстеженню контактів та описано норми при яких зменшується вплив смартфона на людину.

3.2 Безпека в надзвичайних ситуаціях

3.2.1 Створення метеорологічних умов виробничого середовища користувачів ВДТ ЕОМ, ПЕОМ

Згідно з Гігієнічною класифікацією праці за показниками шкідливості та небезпечності чинників виробничого середовища, тяжкості та напруженості трудового процесу умови праці користувачів ЕОМ мають відповідати І класу (оптимальним) або ІІ класу (допустимим) умовам праці[66].

Для створення оптимальних умов зорової роботи, виключення швидкої втоми очей і сприяння високій продуктивності праці освітлення має бути достатнім, рівномірним і стабільним, відповідати встановленим нормам і характеру здорової роботи.

Приміщення з ВДТ, ЕОМ мають бути забезпечені природним і штучним освітленням. Коефіцієнт природного освітлення (КПО) має бути не нижчим 1,5%. Розраховують площу світлових прорізів, яка забезпечує нормоване значення КПО в робочій зоні користувачів комп'ютерів, відповідно до ДБН В.2.5-28-2006.

За виробничої потреби дозволено експлуатувати ЕОМ у приміщеннях без природного освітлення, але після узгодження з органами держгірпромнагляду та органами і установами санітарно-епідеміологічної служби.

Штучне освітлення має бути загальним, робочим і рівномірним. У випадку, коли робота переважно з документами, допускається додатково використовувати місцеве освітлення. Але світильники місцевого освітлення мають бути з напівпрозорим відбивачем світла із захисним кутом не меншим 40°, не створювати відблисків на поверхні екрана ВДТ та не підвищувати загальну освітленість екрана більше 300 лк. Рівень освітленості в зоні розташування документів має бути в границях 300...500 лк.

Як джерела штучного світла застосовують переважно люмінесцентні лампи типу ЛБ. У разі влаштування відбитого освітлення допускають

застосовувати металогалогенні лампи потужністю 250 Вт, а у світильниках місцевого освітлення – лампи розжарювання.

Систему загального освітлення має бути виконано у вигляді суцільних або переривчатих ліній світильників, що розмішують збоку від виробничих місць (переважно зліва), паралельно лінії зору працівників. Допускається застосовувати світильники таких класів світлорозподілу: світильники прямого світла – П; переважно прямого світла – Н; переважно відбитого світла – В.

У разі розташування ВДТ і ЕОМ по периметру приміщення лінії світильників мають бути розміщені локально над робочими місцями.

Світильники загального освітлення мають складатися із розсіювача, дзеркальної екранної сітки або віддзеркалювача. Укомплектовані світильники ВЧПРА. Використовувати світильники без розсіювачів та екранних сіток заборонено. Захисний кут світильників має бути не більшим 40°, а яскравість в зоні кутів випромінювання 50°...90° у подовжній та поперечній площинах не більшою 200 кд/м2. Коефіцієнт запасу освітлювальної установки має бути 1.4, коефіцієнт пульсації не перевищувати 5%, яскравість відблисків на крані ВДТ не більше 40 кд/м2; яскравість стелі піл час застосування системи відбивного освітлення не більше 200 кд/м2; нерівномірність розподілу яскравості робочих поверхонь в полі зору користувача ВДТ не має перевищувати 3:1, а робочих поверхонь і навколишніх предметів (стіни, обладнання) – 5:1. Система вимикачів має забезпечувати освітлення тільки потрібних для роботи зон приміщення та регулювати інтенсивність штучного освітлення залежно від інтенсивності природного освітлення.

Для забезпечення нормованих значень освітлення в приміщеннях з ВДТ, ЕОМ і ПЕОМ потрібно очищати скло та світильники не рідше ніж 2 рази на рік і своєчасно проводити заміну перегорілих ламп.

Уміст шкідливих речовин у повітрі робочої зони не має перевищувати ГДК Відповідно до ГОСТ 12.1.005 – 88 уміст озону не більше 0,1 мг/м3, вміст оксидів азоту – не більше 5 мг/м3. уміст пилу – не більше 4 мг/м3.

Параметри мікроклімату мають відповідати вимогам ДСН 3.3.6.042 (табл. 3.1) а іонний склад повітря – вимогам СН 2152 – 80 (табл.3.2).

Таблиця 3.1 – Оптимальні величини температури, відносної вологості та швидкості руху повітря для приміщень з ВДТ, ЕОМ і ПЕОМ

Період року	Категорія робіт	Температура повітря, °С	Відносна вологість повітря, %	Швидкість руху повітря, м/с
Холодний	Легка – 1 а	22-24	40-60	0,1
	Легка – 1б	21-23	40-60	0,1
Теплий	Легка – 1 а	23-25	40-60	0,1
	Легка – 1б	22-24	40-60	0,2

Таблиця 3.2 – Рівні іонізації повітря приміщень під час роботи на ВДТ, ЕОМ та ПЕОМ

Рівні	Кількість іонів у см3 повітря	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально допустимі	50000	50000

Для підтримання оптимальних значень параметрів повітря робочої зони потрібно застосовувати вентиляцію приміщень, кондиціонування повітря, використовувати установки або прилади зволожування та штучної іонізації. У приміщеннях з ЕОМ рівні звукового тиску, рівні звуку та еквівалентні рівні звуку мають відповідати вимогам ДСН 3.3.6.037-99 та ДСанПіН 3.3.2.007 98 (табл 3.3). Устаткування, яке є джерелом шуму (АЦП, принтери тощо), слід розташовувати поза приміщеннями з ЕОМ, ПЕОМ.

Для забезпечення допустимих рівнів шуму на робочих місцях потрібно застосовувати засоби звукопоглинання, вибір яких обґрунтовано спеціальними інженерно-акустичними розрахунками. Як засоби шумопоглинання застосовують негорючі або важкогорючі спеціальні перфоровані плити, панелі, мінеральну вату з максимальним коефіцієнтом звукопоглинання в границях частот 31,5...8000 Гц або інші матеріали аналогічного призначення, які дозволені для оздоблення приміщень органами державного санітарно-епідеміологічного нагляду. Крім того, приміщення потрібно обладнувати підвісними стелями із матеріалів, які мають аналогічні властивості.

Таблиця 3.3 – Допустимі рівні звуку, еквівалентні рівні звуку, рівні звукового тиску в октавних смугах частот

Види трудової діяльності	Рівні звукового тиску, дБ, в октавних смугах із середньо геометричними частотами, Гц									Рівні звуку, еквівалентні рівні звуку, дБА/дБАекв
	31,5	63	125	250	500	1000	2000	40000	80000	
Програмісти ЕОМ	86	71	61	54	49	45	42	40	38	50
Оператори в залах оброблення інформації на ЕОМ	96	83	74	68	63	60	57	55	54	65
Приміщення для розміщення штучних агрегатів ЕОМ	103	91	83	77	73	70	68	66	64	75

Рівні вібрації під час виконання робіт на ЕОМ у виробничих приміщеннях не мають перевищувати допустимих значень, які визначені ДСанПіН 3.3.2.007-98.

Рівень інфрачервоного випромінювання має відповідати вимогам ДСН 3.3.6.042-99 і не перевищувати 35 ... 100 Вт/м2 залежно від опромінюваної площі тіла.

Допустима інтенсивність ультрафіолетового випромінювання не має перевищувати величини, які визначені СН 4557-88 та ДСанПіН 3.3.2.007-98:

- випромінювання в області С (220...280 нм) – 0.001 Вт/м2;
- в області В (280...320 нм) – не перевищувати 0,01 Вт/ м2;
- в області А (320...400 нм) – 10,0 Вт/м2.

Значення напруженості електромагнітних полів на робочих місцях із ВДТ мають відповідати нормативним значенням ГОСТ 12.1.006-84 і ДСанПіН 3.3.2.007-98 (табл 3.4)

Таблиця 3.4 – Допустимі рівні електромагнітних випромінювань радіочастотного діапазону

Діапазон частот, МГц	Допустимі рівні ЕМП	
	Електрична складова Е, В/м	Магнітні складова Н, А/м
0.06…3.0	50	5
3.0….30.0	20	–
30.0….50.0	10	0.3
50.0…300.0	5	–

Гранично допустима напруженість електростатичного поля на робочих місцях не має перевищувати 20 кВ/м (ГОСТ 12.1.045 84, ДСанПіН 3.3.2.007-98). Поверхневий електростатичний потенціал ВДТ не має перевищувати 500 В.

Потужність експозиційної дози рентгенівською випромінювання на відстані 0,05м від екрана та корпуса ВДТ за будь-яких положень регульованих пристроїв не має перевищувати 7.74·10-12 А/кг, що відповідає еквівалентній дозі 0,1 мбер/год (100 мкР/гол) (НПАОГІ 0.00-1.28-10).

3.3 Висновок до розділу 3

В даному розділі дано визначення, що таке охорона праці та розглянуто основні норми по використанню смартфона людиною. Його вплив на користувача, адже до теми класифікаційцної роботи стосується такий пристрій як мобільний телефон, тому що застосунки для відстеженння контактів, найчастіше використовуються саме смартфонами.

Також було проаналізовано питання безпеки в надзвичайних ситуаціях, а саме створення метеорологічних умов виробничого середовища користувачів ВДТ ЕОМ, ПЕОМ.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи магістра було досягнуто поставленої мети дослідження а саме, описано усі методи визначення місця розташування які необхідні для знаходження тої чи іншої людини. Наведено приклади застосунків для відстеження контактів які хворіють або можуть бути в стані ризику на Covid-19. Застосунки в свою чергу розділяються до трьох архітектур: централізованої, децентралізованої та гібридної. У ході виконання даного дослідження отримано наступні результати:

- Забезпечено актуальний огляд сучасних проблем застосунків відстеження контактів у боротьбі проти COVID-19 в сучасному світі.
- Обговорено рекомендації щодо вирішення цих проблем.
- Досліджено сучасні наслідки використання цифрового відстеження контактів та майбутніх спалахів інфекційних хвороб.
- Досліджено методи визначення місця розташування.
- Розглянуто роль телемедицини в час пандемії.

Тому, вплив пандемії COVID-19 представляє безпрецедентний виклик органам охорони здоров'я та відповідним урядам у всьому світі. Це призвело до сильного тиску на медичні служби та внесло докорінні зміни у спосіб життя як окремих людей, так і організацій. Щоб зупинити зараження вірусом органи охорони здоров’я розглянули та запровадили надійні системи відстеження контактів, які включають використання програм цифрового відстеження контактів.

Якщо програми для відстеження контактів будуть мати успіх, тоді важливо, щоб уряди та політики формували довіру своїх громадян та демонстрували достатню прозорість щодо того, як збираються та використовуються дані користувачів. Їх ефективність та спосіб вирішення цих проблем в даний час у боротьбі з цією новою хворобою визначатимуть роль

цифрових технологій відстеження контактів у майбутніх спалахах пандемії та які уроки можна витягнути з виявлених недоліків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. World Health Organization. "Telemedicine: opportunities and developments in member states. 2010." (2018).

2. Gadzinski, Adam J., et al. "Telemedicine and eConsults for hospitalized patients during COVID-19." *Urology* (2020).

3. Ibrahim, J. F. M., E. Kurovics, and L. A. Gömze. "MultiScience-XXXIII. microCAD International Multidisciplinary Scientific Conference." (2019).

4. Bay, Jason, et al. "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders." *Government Technology Agency-Singapore, Tech. Rep* (2020).

5. Castelluccia, Claude, et al. "ROBERT: ROBust and privacy-presERving proximity Tracing." (2020).

6. Small, Logan, et al. "Summary of Bluetooth Contact Tracing Options." (2020)..

7. COVIDSafe, "CocidSafe" [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/AU-COVIDSafe.

8. Ahmed, Nadeem, et al. "A survey of covid-19 contact tracing apps." *IEEE Access* 8 (2020): 134577-134601.

9. DTA. "CovidSafe" [Електронний ресурс] / DTA – Режим доступу до ресурсу: https://github.com/AU-COVIDSafe, 2020.

10. Ministry of Electronics and Information Technology. “Aarogya setu,” [Електронний ресурс] / Ministry of Electronics and Information Technology – Режим доступу до ресурсу: https://github.com/nic-delhi/AarogyaSetu_Android, 2020..

11 Sharma, Upasana. "Understanding aarogya setu: navigating privacy during a pandemic proves to be tricky." *LSE Covid 19 Blog* (2020).

12 Apple. “Privacy preserving contact tracing” [Електронний ресурс] / Apple. – 2020. – Режим доступу до ресурсу: https://www.apple.com/covid19/contacttracing,

13 Leith, D., and Stephen Farrell. "GAEN Due Diligence: Verifying The Google/Apple Covid Exposure Notification API." CoronaDef21, Proceedings of NDSS ‘21 2021 (2020).

14. C. Troncoso and et.al.,. “DP-3T,” [Електронний ресурс] / C. Troncoso and et.al., – Режим доступу до ресурсу: https://github.com/DP-3T..

15. Reelfs, Jens Helge, Oliver Hohlfeld, and Ingmar Poese. "Corona-Warn-App: Tracing the Start of the Official COVID-19 Exposure Notification App for Germany." *arXiv preprint arXiv:2008.07370* (2020).

16. Ahmed, Nadeem, et al. "A survey of covid-19 contact tracing apps." IEEE Access 8 (2020): 134577-134601.

17. Rivest, Ronald L., et al. "The PACT protocol specification." Private Automated Contact Tracing Team, MIT, Cambridge, MA, USA, Tech. Rep. 0.1 (2020).

18. Chan, Justin, et al. "Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing." *arXiv preprint arXiv:2004.03544* (2020).

19. University of Washington and Microsoft. “Covidsafe,” [Електронний ресурс] / University of Washington and Microsoft – Режим доступу до ресурсу: https://covidsafe.cs.washington.edu/t, 2020..

20. . C. Troncoso and et.al.,. “DP-3T,” [Електронний ресурс] / C. Troncoso and et.al., – Режим доступу до ресурсу: https://github.com/DP-3T..

21. Fan, Bin, et al. "Cuckoo filter: Practically better than bloom." *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. 2014.

22. Stanford. Covid watch [Електронний ресурс] / Stanford. – 2020. – Режим доступу до ресурсу: https://www.covid-watch.org.

23. Ahmed, Nadeem, et al. "A Survey of COVID-19 Contact Tracing Apps." arXiv e-prints (2020): arXiv-2006.

24. Niyogi, Sourabh, et al. "Tcncoalition/tcn: Specification and reference implementation of the tcn protocol for decentralized, privacy-preserving contact tracing." (2020).

25. Diffie, W., and M. E. Hellman. "" New Directions in Cryptography" IEEE Transactions on Information Theory, v. IT-22, n. 6." (1976).

26. Chaum, David. "Blind signatures for untraceable payments." *Advances in cryptology*. Springer, Boston, MA, 1983.

27. HaMagen: contact tracing app. https://govextra.gov.il/ministry-of-health/hamagen-app/ download-en/, 2020. Israel's Ministry of Health.

28. Path Check Foundation. "Covid safe paths," [Електронний ресурс] / Path Check Foundation – Режим доступу до ресурсу: https://covidsafepaths.org/, 2020.

29. Raskar, Ramesh, et al. "COVID-19 Contact-Tracing Mobile Apps: Evaluation and Assessment for Decision Makers." arXiv preprint arXiv:2006.05812 (2020).

30. Castelluccia, Claude, et al. "DESIRE: A Third Way for a European Exposure Notification System Leveraging the best of centralized and decentralized systems." (2020).

31. Beskorovajnov, Wasilij, et al. "ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized-Decentralized Divide for Stronger Privacy." *IACR Cryptol. ePrint Arch.* 2020 (2020): 505.

32. Trieu, Ni, et al. "Epione: Lightweight contact tracing with strong privacy." *arXiv preprint arXiv:2004.13293* (2020).

33. De Cristofaro, Emiliano, and Gene Tsudik. "Practical private set intersection protocols with linear complexity." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2010.

34. Chen, Hao, Kim Laine, and Peter Rindal. "Fast private set intersection from homomorphic encryption." *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017.

35. Yin, Hongying. "Location based service." *T-109.551 Research Seminar on Location Business II*. 2002.

36. Track, Snap. "Location Technologies for GSM, GPRS and WCDMA Networks." *HTTP:(Accessed on 25 Jan 2008)* (2002).

37. Brída, Peter. "Location Technologies for GSM." *Transcom, June* (2003): 119-122.

38. Самойленко Ю. П. Закон України "Про телемедицину" [Електронний ресурс] / Самойленко Ю. П.. – 2012. – Режим доступу до ресурсу: http://search.ligazakon.ua/l_doc2.nsf/link1/JF7V800A.html.

39. Mannan, Dr Kazi Abdul, and Kazi Abdul Mannan. "Knowledge and perception towards Novel Coronavirus (COVID 19) in Bangladesh." International Research Journal of Business and Social Science 6.2 (2020).

40. Eurosurveillance Editorial Team. "Note from the editors: World Health Organization declares novel coronavirus (2019-nCoV) sixth public health emergency of international concern." Eurosurveillance 25.5 (2020): 200131e.

41. Green, Manfred S. "Did the hesitancy in declaring COVID-19 a pandemic reflect a need to redefine the term?." The Lancet 395.10229 (2020): 1034-1035.

42. Hua, Jinling, and Rajib Shaw. "Corona virus (Covid-19)“infodemic” and emerging issues through a data lens: The case of china." International journal of environmental research and public health 17.7 (2020): 2309.

43. Bay, Jason, et al. "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders." Government Technology Agency-Singapore, Tech. Rep (2020).

44. Cho, Hyunghoon, Daphne Ippolito, and Yun William Yu. "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs." arXiv preprint arXiv:2003.11511 (2020).

45. Ollikainen, Ville, and Kimmo Halunen. "Rendezvous based pandemic tracing by sharing Diffie-Hellman generated common secrets." (2020).

46. Mishra, Praveen Kumar. "Bluetooth Security Threats." International Journal of Computer Science & Engineering Technology (IJCSET) Vol 4 (2013).

47. Naveed, Muhammad, et al. "Inside Job: Understanding and Mitigating the Threat of External Device Mis-Binding on Android." NDSS. 2014.

48. Spill, Dominic, and Andrea Bittau. "BlueSniff: Eve Meets Alice and Bluetooth." WOOT 7 (2007): 1-10.

49. Bai, Xiaolong, et al. "Staying secure and unprepared: Understanding and mitigating the security risks of apple zeroconf." 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016.

50. Raskar, Ramesh. "Private kit: Safe paths-can we slow the spread without giving up individual privacy?." (2020).

51. Hekmati, Arvin, Gowri Ramachandran, and Bhaskar Krishnamachari. "CONTAIN: privacy-oriented contact tracing protocols for epidemics." arXiv preprint arXiv:2004.05251 (2020).

52. Rahman, Md, et al. "An automated contact tracing approach for controlling covid-19 spread based on geolocation data from mobile cellular networks." *arXiv preprint arXiv:2007.02661* (2020).

53. Bell, James, et al. "Tracesecure: Towards privacy preserving contact tracing." arXiv preprint arXiv:2004.04059 (2020).

54. Trogh, Jens, et al. "Outdoor location tracking of mobile devices in cellular networks." EURASIP Journal on Wireless Communications and Networking 2019.1 (2019): 115.

55. Pahlavan, Kaveh, Xinrong Li, and Juha-Pekka Makela. "Indoor geolocation science and technology." IEEE Communications Magazine 40.2 (2002): 112-118.

56. Ather, Amber, et al. "Coronavirus disease 19 (COVID-19): implications for clinical dental care." Journal of endodontics (2020).

57. Rahman, Md Tanvir, and Risala Tasin Khan. "An Automated Contact Tracing Approach for Predicting and Warning Probable Covid-19 Patients using Cell Phone Network."

58. “COVID-19 Screening Questnnaire—Tanner Health System”, https://www.surveymonkey.com/r/TannerCOVIDQuestionnaire (Retrieved on May 30, 2020)

59. Raskar, Ramesh, et al. "Apps gone rogue: Maintaining personal privacy in an epidemic." arXiv preprint arXiv:2003.08567 (2020).

60. Ahmed, Nadeem, et al. "A survey of covid-19 contact tracing apps." IEEE Access 8 (2020): 134577-134601.

61. Statista. "Number of smartphone users worldwide from 2016 to 2021 (in billions)." (2019).

62. Silver, L. "Smartphone ownership is growing rapidly around the world, but not always equally. Pew Research Center. 2019."

63. Cacovean, Dan, Irina Ioana, and Gabriela Nitulescu. "IoT System in Diagnosis of Covid-19 Patients." Informatica Economica 24.2 (2020): 75-89.

64. Законодавство України. Закон "Про охорону праці" [Електронний ресурс] / Законодавство України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2694-12#Text.

65. Гігієна користування мобільним телефоном [Електронний ресурс] – Режим доступу до ресурсу: https://dpss-ks.gov.ua/novini/gigiyena-koristuvannya-mobilnim-telefonom.

66. Вимоги до приміщень, розміщення в них ВДТ, ЕОМ, ПЕОМ [Електронний ресурс] – Режим доступу до ресурсу: http://webcache.googleusercontent.com/search?q=cache:yH4FdbCxc0MJ:opcb.kpi.ua/wp-content/uploads/2011/11/8. .

ДОДАТКИ

Додаток А

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

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

9–10 грудня 2020 року

ТЕРНОПІЛЬ
2020

УДК 004.326
[1]Головко О.–ст.гр.СА-61, [1]Мацюк А.–ст.гр.КА-31, [2]Яскілка О.–ст.гр.КН-321
([1]Тернопільський національний технічний університет імені Івана Пулюя)
([2]Технічний коледж ТНТУ імені Івана Пулюя)

ВИКОРИСТАННЯ СМАРТФОНІВ ТА НОСИМИХ ПРИСТРОЇВ ДЛЯ МОНІТОРИНГУ ЗМІН ПОВЕДІНКИ ПІД ЧАС COVID-19

UDC 004.326
Holovko O., Matsiuk A., Yaskilka O.

USING SMARTPHONES AND WEARABLE DEVICES TO MONITOR BEHAVIORAL CHANGES DURING COVID-19

Ключові слова: МОБІЛЬНЕ ЗДОРОВ'Я; COVID-19; ПОВЕДІНКОВИЙ МОНІТОРИНГ; СМАРТФОНИ; НОСИМІ ПРИСТРОЇ; МОБІЛЬНІСТЬ; ПЛАТФОРМА МОНІТОРИНГУ ЗДОРОВ'Я

Key words: MOBILE HEALTH; COVID-19; BEHAVIORAL MONITORING; SMARTPHONES; WEARABLE DEVICES; MOBILITY; HEALTH MONITORING PLATFORM

11 березня 2020 року Всесвітня організація охорони здоров'я оголосила про спалах вірусу SARS-CoV-2, який переріс у пандемію. Цей новий коронавірус викликає гостре респіраторне захворювання (COVID-19), про яке вперше було повідомлено у місті Ухань, провінція Хубей, Китай [1]. Станом на 1 листопада 2020 року кількість випадків зараження зросло до 45 мільйонів людей і поширилося на 213 країн. COVID-19 може бути смертельним із оцінкою 1% випадків летальності, і цей рівень зростає для дорослих та людей з проблемами зі здоров'ям [5]. Спалах COVID-19 є причиною безпрецедентного навантаження на системи охорони здоров'я країн і призводить до значних економічних втрат та можливої глобальної рецесії [6].

Високоефективного лікування поки не існує, а вакцини лише на етапі реєстрації. Широко прийнятою стратегією боротьби з короновірусом є використання нефармацевтичних втручань, таких як соціальне дистанціювання та повна ізоляція, для контролю за розповсюдженням вірусу та послаблення тиску на функціонування системи охорони здоров'я [2]. Нефармацевтичні втручання впроваджені у багатьох країнах, включаючи Китай, Італію, Іспанію, Великобританію та Нідерланди. Такі заходи значно зменшують кількість нових підтверджених випадків захворювання [4].

Виникає необхідність об'єктивного та кількісного способу моніторингу поведінки населення для оцінки впливу та реакції на такі заходи щодо обмеження поширення вірусу. Крім того, потрібно відстежувати потенційні наслідки хвороби, зокрема у зимові місяці, коли заходи соціального дистанціювання пом'якшуються. Розуміння потенційних сезонних стрибків COVID-19 вимагає глибокої обізнаності ефектів різних нефармацевтичних втручань, а в подальшому ефективного використання отриманої інформації.

Доступність широкосмугових мобільних мереж 3G та 4G, смартфонів та носимих давачів дозволяє відбирати набір даних із високою точністю і якістю в режимі реального часу від великої кількості учасників та значно полегшує віддалений контроль поведінки [3]. Використовуючи модулі давачів у смартфонах, такі як мережеве та GPS-відстеження місцерозташування та фітнес-пристрої, які дають змогу визначати кількість кроків та частоту серцевих скорочень, можна отримати доступ до даних про мобільність та здоров'я населення.

Для управління даними, зібраними з різних давачів та мобільних пристроїв, були розроблені такі платформи, як віддалена оцінка захворювань та рецидивів (RADAR) – база [7], мобільна платформа охорони здоров'я. Ця платформа була використана для віддаленого моніторингу в різних випадках використання, включаючи захворювання центральної нервової системи (великий депресивний розлад [MDD], епілепсія та розсіяний склероз [MS]) в рамках

ініціативи інноваційних лікарських засобів (IMI2) RADAR Central Nervous System – програма системи (CNS).

Досліджено корисність базової платформи RADAR як набір інструментів для тестування ефекту та реакції нефармацевтичних препаратів, спрямованих на обмеження розповсюдження інфекційних захворювань, таких як COVID-19, шляхом використання даних учасників, зібраних з листопада 2017 року, як частина поточних досліджень RADAR-CNS. Зокрема, створено засоби вимірювання мобільності (проксі для фізичного дистанціювання), використання телефону (проксі віртуальної соціальності) та фізіологічні вимірювання (частота серцевих скорочень та сну). Особливості змін порівняні з базовою лінією, проведено спільний аналіз цих особливостей, щоб надати цілісне уявлення та інтерпретувати ці зміни поведінки під час COVID-19.

RADAR, платформа збору даних, що вільно розгортається, використовує дані з пристроїв та мобільних технологій, може бути використана для швидкої кількісної оцінки та надання цілісного уявлення про зміни поведінки у відповідь на втручання в галузі охорони здоров'я в результаті інфекційних спалахів, таких як COVID-19. RADAR може бути дієвим підходом до впровадження системи раннього попередження та пасивної оцінки місцевої реакції суспільства на втручання в епідемії та пандемії, і може допомогти країнам вийти з ізоляції.

Література.

1. Bai Y, Yao L, Wei T, Tian F, Jin D, Chen L, et al. Presumed asymptomatic carrier transmission of COVID-19. JAMA 2020 Feb 21:1406-1407
2. Lau H, Khosrawipour V, Kocbach P, Mikolajczyk A, Schubert J, Bania J, et al. The positive impact of lockdown in Wuhan on containing the COVID-19 outbreak in China. J Travel Med 2020 May 18;27(3)
3. Pandian P, Mohanavelu K, Safeer K, Kotresh T, Shakunthala D, Gopal P, et al. Smart Vest: wearable multi-parameter remote physiological monitoring system. Med Eng Phys 2015 May
4. Lau H, Khosrawipour V, Kocbach P, Mikolajczyk A, Schubert J, Bania J, et al. The positive impact of lockdown in Wuhan on containing the COVID-19 outbreak in China. J Travel Med 2020 May 18
5. Huang C, Wang Y, Li X, Ren L, Zhao J, Hu Y, et al. Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China. Lancet 2020 Feb;395(10223):497-506.
6. Wu Z, McGoogan JM. Characteristics of and important lessons from the coronavirus disease 2019 (COVID-19) outbreak in China: summary of a report of 72 314 cases from the Chinese Center for Disease Control and Prevention. JAMA 2020 Feb 24:A.
7. Ranjan Y, Rashid Z, Stewart C, Conde P, Begale M, Verbeeck D, Hyve, RADAR-CNS Consortium. RADAR-Base: open source mobile health platform for collecting, monitoring, and analyzing data using sensors, wearables, and mobile devices. JMIR mHealth uHealth 2019 Aug 01

УДК 004.326
Головко О. – ст. гр.СА-61, Станько А.А. – аспірант
(Тернопільський національний технічний університет імені Івана Пулюя)

ТЕЛЕМЕДИЦИНА В ЕПОХУ COVID-19

UDC 004.326
Holovko O., Stanko A.

TELEMEDICINE IN THE COVID-19 ERA

Ключові слова: ТЕЛЕКОНСУЛЬТАЦІЇ, ОХОРОНА ЗДОРОВ'Я, ІНФОРМАЦІЙНІ ТА КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ, ТЕЛЕМЕДИЦИНА
Key words: TELECONSULTATION, HEALTHCARE, INFORMATION AND COMMUNICATION TECHNOLOGY, TELEMEDICINE

Відомо, що COVID-19 поширюється аерозольними краплями. Щоб уникнути безпосереднього контакту, не перешкоджаючи наданню медичних послуг, телемедицину, яка зараз є частиною цифрових систем охорони здоров'я різних країн, слід застосовувати більш ефективно. За винятком гострих випадків, хронічними захворюваннями та наступними візитами можна керувати за допомогою телемедицини. Таким чином, зменшуються зайві відвідування медичних закладів, забезпечуючи лікування важкохворих. Всесвітня організація охорони здоров'я (ВООЗ) розглядає телемедицину як спосіб надання медичної допомоги, коли відстань є критичним фактором.

Для обміну актуальною інформацією важливо використовувати усі можливості інформаційних та комунікаційних технологій. Під час пандемії COVID-19 велика кількість законів та обмежень було переглянуто, а нові можливості постійно вивчаються. Застосування телемедицини розпочинається у сферах, які колись вважалися потенційно небезпечними для використання в охороні здоров'я; однак відсутність єдиного законодавства щодо інтеграції телемедицини у охорону здоров'я є значним викликом при його тривалому застосуванні в умовах пандемії [1].

Щоб бути ефективними, медичні працівники повинні мати необхідну освіту, ліцензію та професійний потенціал для надання медичних послуг використовуючи телемедицину. З метою розширення сфери правова площина використання телемедицини зазнала змін, правила які стосуються вимог щодо встановлення відносин між пацієнтом та постачальником стають менш суворими. Закони про тестування прямого доступу дозволили лабораторіям робити діагностичні тести після телеконсультації з лікарем . Адміністрація США з питань боротьби з наркотиками дозволила призначати контрольовані речовини за допомогою телеконсультацій в аудіовізуальному режимі двостороннього зв'язку в режимі реального часу [2]. Проте за таких обставин важко вести записи, забезпечувати конфіденційність. Такі платформи, як Messenger, Video Chat, Google Video та Skype, використовувались відповідно до нових регуляторних можливостей в телемедицині [3].

Телемедицина може використовуватись для попереднього відбору пацієнтів які мають потрапити до лікарні. Цей процес проводяться у два етапи, спочатку телефонне опитування потенційних випадків захворювання на COVID-19 або можливих контактів з хворими, після чого проводиться відбір в офісі, який визначає випадки, що були в інкубаційному періоді під час телефонного відбору та мали симптоми до візиту в офіс .

Хронічні захворювання, такі як цукровий діабет, гіпертонія та імунодефіцитні захворювання, можуть бути під контролем телемедицини без збільшення ризику ускладнень. Телемедицина зменшує вартість наступних візитів, і не впливає на лікування хронічних захворювань у порівнянні з відвідуваннями медичних закладів.

Викладання медицини переважно було перенесено на онлайн-формати за допомогою інтерактивних семінарів, групових дискусій та практикування клінічних навичок [4]. Студенти

можуть виконувати клінічні завдання за допомогою навчених медичних працівників, тим самим повільно замінюючи роль викладача як наставника у віртуальному середовищі. Онлайн-курс хірургічного втручання може проводитись там, де студентам можна надати телемода. Незважаючи на те, що операції можна демонструвати в прямому ефірі та можливі дискусії між учасниками в різних місцях, безпосередня взаємодія пацієнта, клінічне обстеження та виявлення фізичних ознак неможливі на віртуальній платформі. Крім того, при проведенні онлайн-практичного іспиту відсутня повна оцінка компетентності.

Емпатію під час спілкування з постачальником та пацієнтом, що підвищує відповідність пацієнта та довіру до нього, важко довести до телемедицини в епоху COVID-19. Основною причиною є ефект дезінгібування через Інтернет [5]. Це стан, коли людина психологічно відключається від свого фактичного буття, коли вона не стикається одна з одною. Існує три можливі способи посилити емпатію під час телеконсультацій. По-перше, це активне прослуховування та надання пацієнту можливості вести розмову. Другий – це подальше спостереження після призначення через текстові повідомлення та електронні листи, щоб пацієнт не почувався забутим. Третій – персоналізувати спілкування за допомогою психографічної сегментації. З точки зору психології, пацієнти самостійно вдосконалюють спілкування та лікування під час використання телемедицини.

Однак телемедицина у галузі охорони здоров'я не позбавлена обмежень. Недобросовнісні особи можуть представляти справжніх пацієнтів. Під час відеоконсультацій існує можливість зловживання приватним життям пацієнтів. При асинхронному спілкуванні, такому як електронна пошта, відповідь затримується. Виписування ліків у телекомунікаціях може спричинити помилки. В одному з опитувань охорони здоров'я було зазначено, що вимоги щодо відшкодування та ліцензування є серйозними проблемами [6]. Також будь-яке порушення технології може призвести до втрати конфіденційності пацієнта.

При стратегічному використанні ТМ може бути потужним інструментом для навчання та надання медичної допомоги в умовах пандемії. Для того, щоб використовувати його в повному обсязі, потрібно вирішити юридичні питання. Для кращого результату необхідна подальша підготовка медичних працівників.

Література.

1. Smith, Anthony C., et al. "Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19)." Journal of telemedicine and telecare (2020): 1357633X20916567.
3. American Society of Plastic Surgeons. Informed consent:telemedicine[Internet]. 2020. https://www.plasticsurgery.org/documents/medical-professionals/Telemedicine-Informed Consent.pdf.
4. Pool MM, Saul HC. HIPAA waivers and compliance in COVID-19 pandemic [Internet]. 2020 March 17. Available from: https://www.agg.com/news-insights/publications/ hipaa-waivers-and-compliance-in-covid-19-pandemic/.
5. Mukundan Jr, Srinivasan, et al. "Trial telemedicine system for supporting medical students on elective in the developing world." Academic radiology 10.7 (2003): 794-797.
6. Terry, Christopher, and Jeff Cain. "The emerging issue of digital empathy." American journal of pharmaceutical education 80.4 (2016).
7. Kumar, Praveen, Farhanul Huda, and Somprakas Basu. "Telemedicine in the COVID-19 era: the new normal." European Surgery (2020): 1-2.
8. Lacktman NM, Rosen DL, Chmielewski MR, Beaver NA. 2017 Telemedicine & Digital Health Survey [Internet]. 2017 Nov 15.