Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *перший (бакалаврський)*

Безпека інформації в телемедичних мережах

(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІз-21-1*
Аліна Прокопченко
(власне ім'я, прізвище)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-професійна*

Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. к.т.н. Дарія Чеботарьова*
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ІМІ _____ *Валерій Безрук*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Аліна Прокопченко*
(підпис) (власне ім'я, прізвище)

Керівник _____ *Дарія Чеботарьова*
(підпис) (власне ім'я, прізвище)

Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *перший (бакалаврський)*

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *освітньо-професійна*

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ_____
(підпис)

"*21*" *червня* 2025р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Прокопченко Аліні Володимирівні*
(прізвище, ім'я, по батькові)

1. Тема роботи *Безпека інформації в телемедичних мережах*

затверджена наказом університету від "*02*" *травня* 2025 р. № *63 Стз*

2. Термін подання здобувачем роботи до екзаменаційної комісії *20 червня 2025 р.*

3. Вихідні дані до роботи *проаналізувати сучасний стан та перспективи розвитку телемедицини в Україні та світі; дослідити інфокомунікаційні технології в телемедицині, архітектуру телемедичних мереж та основні інфокомунікаційні засоби необхідні для організації телемедичних мереж; виконати аналіз проблем безпеки в телемедицині, визначити вразливості та ризики в телемедичних мережах; запропонувати способи захисту інформації та підвищення безпеки даних в телемедичних мережах.*

4. Перелік питань, що потрібно опрацювати в роботі

1. Сучасний стан телемедицини в світі

2. Інфокомунікаційні технології в телемедицинію

3. Проблеми безпеки в телемедичних мережах

4. Підвищення безпеки та захист інформації в телемедичних мережах

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____

Слайди у форматі Power Point (назва, мета та задачі роботи, телемедицина в Україні, переваги та недоліки сучасної телемедицини, перспективні тенденції розвитку телемедицини, архітектура телемедичних мереж, компоненти телемедичної мережі, інструменти комунікації для медичних працівників, проблеми безпеки в телемедицині, потенційні вразливості в телемедицині, типи загроз безпеці даних в телемедичних мережах, способи захисту даних пацієнтів в ТММ, модель захищеної телемедичної мережі, система захисту ТММ, система оцінювання заходів безпеки в ТММ, основні напрями контролю безпеки для ТММ, пропозиції щодо підвищення безпеки в ТММ, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*05.05.25*	*Виконано*
2	*Підбір літератури за темою роботи.*	*05.05 - 10.05.25*	*Виконано*
3	*Виконання розділу 1*	*11.05 - 17.05.25*	*Виконано*
4	*Виконання розділу 2*	*18.05 – 24.05.25*	*Виконано*
5	*Виконання розділу 3*	*25.05 – 31.05.25*	*Виконано*
6	*Виконання розділу 4*	*01.06 - 14.06.25*	*Виконано*
7	*Оформлення пояснювальної записки,*		
	презентаційного матеріалу та підготовка		
	до захисту у ЕК	*15.06 - 20.06.25*	*Виконано*

Дата видачі завдання *05 травня 2025 р.*

Здобувач _____
(підпис)

Керівник роботи _____ *доц. Чеботарьова Д.В.*
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 71 с., 21 рис., 1 табл.,19 джерел, 1 додаток

Об'єкт дослідження – телемедичні мережі.

Мета роботи – дослідження проблем безпеки та засобів захисту інформації в телемедичних мережах.

Результати – в роботі проаналізовано сучасний стан та перспективи розвитку телемедицини в Україні та світі; досліджено інфокомунікаційні технології в телемедицині, архітектуру телемедичних мереж та основні інфокомунікаційні засоби, необхідні для організації телемедичних мереж; виконано аналіз проблем безпеки в телемедицині, визначено вразливості та ризики в телемедичних мережах; запропонувано способи захисту інформації та підвищення безпеки даних в телемедичних мережах.

ТЕЛЕМЕДИЦИНА, МЕРЕЖА, БЕЗПЕКА, ЗАХИСТ, ЗАГРОЗА, РИЗИК, КОНФЕДЕНЦІЙНІСТЬ, ВРАЗЛИВІСТЬ, СИСМЕМА, ПАЦІЄНТ, ЛІКАР, ІНФОКОМУНІКАЦІЇ.

THE ABSTRACT

Explanatory note: 71 p., 21 fig., 1 tabl., 19 sources, 1 app.

Object of research - telemedical networks.

The purpose of the work is o study security problems and means of protecting information in telemedical networks.

Results - the work analyzes the current state and prospects for the development of telemedicine in Ukraine and the world; investigates infocommunication technologies in telemedicine, the architecture of telemedical networks and the main infocommunication tools necessary for the organization of telemedical networks; analyzes security problems in telemedicine, identifies vulnerabilities and risks in telemedical networks; proposes ways to protect information and increase data security in telemedical networks..

TELEMEDICINE, NETWORK, SECURITY, PROTECTION, THREAT, RISK, CONFIDENTIALITY, VULNERABILITY, SYSTEM, PATIENT, DOCTOR, INFOCOMMUNICATIONS.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ДМП – дистанційний медичний працівник;

ІК – інфокомунікацій;

ІТ – інформаційні технології;

ПЗ – програмне забезпечення;

СОЗ – система охорони здоров’я;

ТМ – телемедицина;

ТММ – телемедична мережа;

ШІ – штучний інтелект;

APT (Advanced Persistent Threats) –розширені постійні загрози;

EHR (Electronic Health Record) – це електронний медичний запис;

PII (Personally Identifiable Information) – особиста ідентифікована інформація;

PHI (Personal Health Information) – особиста медична інформація;

WBAN (Wireless Body Area Network) – бездротова натільна мережа.

ВСТУП

Телемедицина (ТМ) – це спосіб надання медичних послуг за допомогою телекомунікаційних технологій. Можна використовувати телемедицину , щоб звернутися до лікаря через відеочат або телефонні дзвінки, замість того, щоб приходити до кабінету лікаря. Головна перевага цього підходу полягає в тому, що він дозволяє пацієнтам отримувати допомогу з будь-якої точки світу, без необхідності подорожувати на великі відстані.

Глобальний перехід до телемедицини, прискорений пандемією COVID-19, революціонізував надання медичної допомоги, дозволивши проводити дистанційні консультації та лікування.

В Україні не тільки пандемія, але і війна стали причиною прискореного розвитку та впровадження телемедицини. З 2023 року Україна вийшла на новий рівень в сфері телемедицини. За останні роки було багато зроблено:

- була ухвалена стратегія розвитку телемедицини,
- оновлено нормативно-правові документи в сфері ТМ,
- зросла і продовжує зростати кількість телемедичних послуг;
- відбувається інтеграція гуманітарних телемедичних рішень у медичні заклади [1].

Під час війни Україна отримала телемедичну гуманітарну допомогу на суму близько 4 млн доларів США [1]. Вже успішно функціонують сучасні телемедичні рішення в медичних закладах України, крім того нові телемедичні рішення готуються до впровадження.

Однак це швидке впровадження також призводить до критичних вразливостей у кібербезпеці, зокрема, у захисті конфіденційних медичних даних та забезпеченні безпечної роботи телемедицинних платформ. Якщо ці вразливості не усунути належним чином, вони можуть поставити під загрозу безпеку пацієнтів та цілісність систем охорони здоров'я (СОЗ). Як наслідок,

впровадження надійних заходів кібербезпеки на телемедицинських платформах є надзвичайно важливим.

Дана кваліфікаційна робота присвячена дослідженню питань безпеки інформації в телемедичних мережах та системах. Аналіз інформаційних джерел за тематикою роботи [1 - 19] підтверджує важливість та актуальність даної теми, саме тому ця кваліфікаційна робота є актуальною.

1 СУЧАСНИЙ СТАН ТЕЛЕМЕДИЦИНИ В СВІТІ

Телемедицина - це використання телекомунікацій та інформаційних технологій (ІТ) для забезпечення доступу до оцінки стану здоров'я, діагностики, втручання, консультацій, нагляду та інформації на відстані [2]. Телемедицина описує медичні технології, що використовуються для лікування пацієнтів, які не перебувають у тому ж фізичному місці, що й їхній постачальник медичних послуг, і включає використання між медичними фахівцями для освітніх або консультативних цілей.

1.1 Розвиток телемедицини в світі

Сучасну медицину складно уявити без телемедичних послуг, які полягають в дистанційних консультаціях пацієнтів медичними фахівцями за допомогою інфокомунікаційних мереж: відеозв'язку, чатів, телефонних дзвінків тощо. Головною метою ТМ є надання якісних медичних послуг на відстані, що дозволяє зробити медицину доступнішою та зменшити навантаження на клініки та лікарні. В наш час ТМ це вадлива частина розвитку СОЗ [3]. Телемедичні послуги надають можливість отримувати швидкі відповіді на запити пацієнтів та оперативну допомогу від лікарів у зручному режимі (місце і час).

Ідея телемедицини існує вже досить давно, але застосування ТМ на практиці стало можливим лише з появою інфокомунікаційних технологій. Фактично першими телемедичними послугами були консультації лікарів за допомогою звичайних стаціонарних телефонів. Але розвиток сучасних інфокомунікацій (ІК) і широкий доступ людей до них (інтернет, мобільний зв'язок, наявність у них сучасних гаджетів) зробили можливою сучасну телемедицину по всьому світі. З кожним роком технології удосконалюються та ТМ пропонує нам найновіші засоби для надання повноцінної медичної допомоги в дистанційному форматі.

Згідно з останньою статистикою щодо тенденцій телемедицини, прогнозується, що світовий ринок телемедицини зросте до понад 175,5 мільярдів доларів США у 2026 році [4]. Це майже вчетверо більше, ніж у 2019 році.

Технологія телемедицини (або телеохорони здоров'я) дозволила постачальникам медичних послуг віртуально оцінювати, діагностувати та лікувати пацієнтів, що дозволяє надавати послуги та медичні консультації без проблем, пов'язаних з доступом. Це призвело до появи галузі, яка є не лише більш ефективною, доступною та орієнтованою на пацієнта, ніж будь-коли раніше, але й викликала величезний ажіотаж та популярність.

Телемедицина – це галузь, яка постійно розвивається і зараз визнана одним із найреволюційніших аспектів сучасної медицини. Ця тенденція, схоже , продовжиться наступного року, трансформуючи не лише догляд за пацієнтами, а й багато інших сфер охорони здоров’я [4].

Основні причини зростання телемедицини наведено на рис. 1.1.

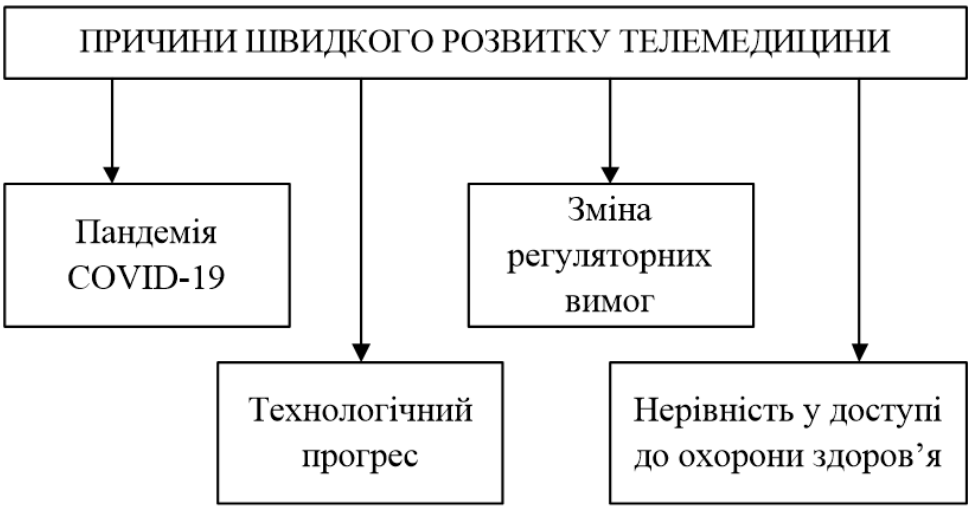

Рисунок 1.1 – Причини швидкого розвитку телемедицини

ТМ стала дуже популярною саме в умовах пандемії COVID-19, коли багато людей не мали можливості вільно переміщуватися та відвідувати лікарів через високі ризики для здоров'я [3]. Пандемія COVID-19 допомогла

прискорити перехід до віртуальної охорони здоров’я та змінити уявлення про її можливості. З початку пандемії і дотепер державні та приватні медичні заклади безпрецедентними темпами переходять на послуги телемедицини.

Технологічний прогрес. Нещодавні технологічні досягнення в охороні здоров'я, включаючи інструменти на базі штучного інтелекту (ШІ), портативні пристрої, заходи кібербезпеки та електронні медичні записи EHR (Electronic Health Record), допомогли підвищити ефективність віртуальної медичної допомоги.

Зміна регуляторних вимог. З початку пандемії COVID-19 дедалі більше регуляторних органів почали визнавати важливість телемедицини та внесли різні зміни до рекомендацій щодо охорони здоров’я, надаючи пацієнтам покращені можливості доступу.

Нерівність у доступі до охорони здоров’я. Телемедицина пропонує віддалений доступ до медичної допомоги для малозабезпечених верств населення, надаючи нужденним спеціалізовану консультацію, незалежно від того, де вони знаходяться у світі.

Щорічна кількість користувачів онлайн-консультацій лікарів у всьому світі різко зростає. За п'ять років з 2017 року до 2022 року кількість користувачів зросла вдвічі з майже 58 мільйонів до 116 мільйонів [4].

Збільшення кількості онлайн-консультацій також призвело до величезної економії часу по всьому світу. В Італії, за оцінками, послуги телемедицини заощаджують пацієнтам із хронічними захворюваннями майже 9,5 годин на рік. Тим часом в Австралії телемедицина пропонує найбільший потенціал для економії часу в охороні здоров'я, де кожен австралійський пацієнт заощаджує в середньому понад шість годин [4].

Норвегія досягла значних успіхів у телемедицині, зокрема, щодо скорочення часу очікування на радіологічне обстеження. Країни Європейського Союзу все частіше використовують певні види технологій телемедицини, причому 77% пропонують послуги телемедицини, 51% пропонують телепсихіатрію та 84% пропонують телерадіологію [4].

Оскільки дедалі більше медичних працівників визнають цінність телемедицини для покращення догляду за пацієнтами, зниження витрат на охорону здоров'я та підвищення операційної ефективності, а такі технології, як штучний інтелект та автоматизація, продовжують розвиватися, телемедицина займатиме дедалі помітніше місце в ландшафті охорони здоров'я.

1.2 Особливості сучасного стану телемедицини в Україні

Значного поширення набула ТМ в Україні за останні роки. Звісно, як і у всьому світі цьому сприяла в свій час пандемія COVID-19, оскільки пацієнти та лікарі потребували альтернативних шляхів надання та отримання медичних послуг. Після цього важливим рушієм розвитку стала війна, оскільки дистанційна медична допомога знову є необхідною великій кількості українців.

В Україні у важких умовах війни телемедицина набула особливого значення, адже вона дозволяє забезпечити доступ до медичних послуг навіть у віддалених або небезпечних регіонах. Це поняття включає не лише консультування пацієнтів телефоном, але й застосування спеціалізованих телемедичних платформ для діагностики, лікування та реабілітації [3].

За даними Національної служби здоров’я України, лише в 2023 році українські лікарі провели понад 9,8 млн дистанційних взаємодій із пацієнтами. Частка телемедичних консультацій наразі складає лише близько 6% від загальної кількості, але кількість віддалених консультацій продовжує зростати, що свідчить про підвищену потребу в таких послугах [3]. На рис. 1.2 показана тенденція зростання телемедицини в Україні після пандемії COVID-19.

Серед пацієнтів, що отримують сьогодні в Україні телемедичну допомогу та дистанційні консультації, основну частину складають маломобільні пацієнти, українці з прифронтових територій або областей, де ведуться бойові дії, а також пацієнти, що мають хронічні захворювання і потребують постійного контакту з лікарями. Саме телемедицина сьогодні дозволяє забезпечити таким пацієнтам безперервний доступ до медичних послуг та

допомогу, що є особливо важливим в сучасних нестабільних умовах та військових реаліях в нашій країні.

Рисунок 1.2 - Тенденція зростання телемедицини в Україні

Сьогодні в Україні ефективно застосовується платформа Helsi, яка пропонує такі можливості:

- послуги онлайн-консультацій,
- запис на прийом або консультацію до лікарів,
- перегляд доступного часу прийому у конкретного лікаря,
- віддалене отримання електронних рецептів,
- збереження медичних історій пацієнтів,
- зручний та швидкий доступ до результатів обстежень та попередніх призначень,
- нагадуваня про прийом ліків,
- нагадування про запис на прийом через повідомлення (SMS або email).

Сьогодні платформа Helsi широко використовується та полегшує процес лікування і моніторингу здоров'я українців [3].

Варто зазначити, що різноманіття телемедичних послуг в Україні вже досить значне (рис. 1.3), крім того постійно з’являються та впроваджуються нові телемедичні послуги.

Рисунок 1.3 – Телемедичні послуги в Україні

Сьогодні телемедицина в Україні за допомогою телемедичних пристроїв і наборів здатна покрити майже весь спектр активностей лікаря:

- прослуховування легень і серця,
- вимірювання температури тіла,

- проведення пульсоксиметрії (перевірка кількості кисню в крові),

- отримання консультації по фото новоутворення на шкірі та багато всього іншого.

До виконання задач телемедицини в Україні вже залучається штучний інтелект (ШІ), який додає можливостей як лікареві мати кращу діагностичну точність, так і пацієнту отримати попередній висновок [4].

Типи реалізації телемедицини в Україні [5] наведені на рис. 1.4.

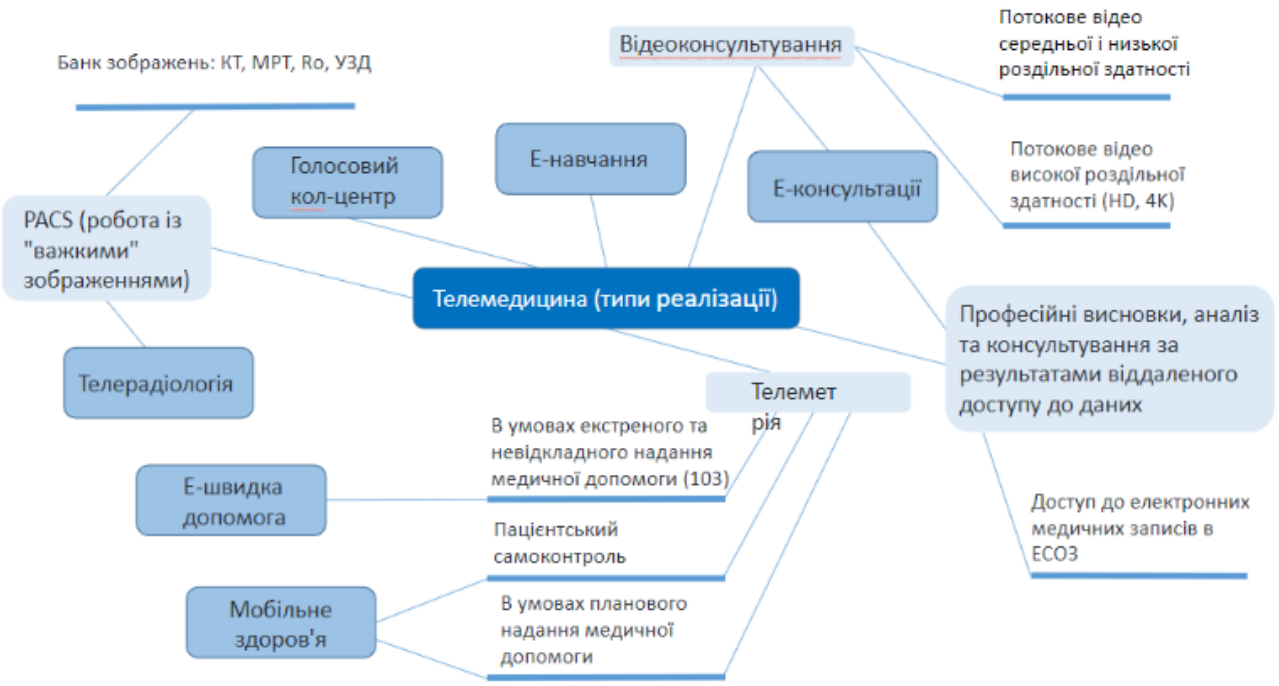

Рисунок 1.4 – Типи реалізації телемедицини в Україні

Зараз в нашій країні ТМ стає все більш доступною та більш зручною, пацієнти та лікарі звикають до ТМ та ефективно її використовують, розвиваються нові послуги та можливості ТМ.

1.3 Переваги та недоліки сучасної телемедицини

Телемедицина має свої переваги та недоліки. Основні переваги ТМ наведено на рис. 1.5, а основін недоліки – на рис. 1.6.

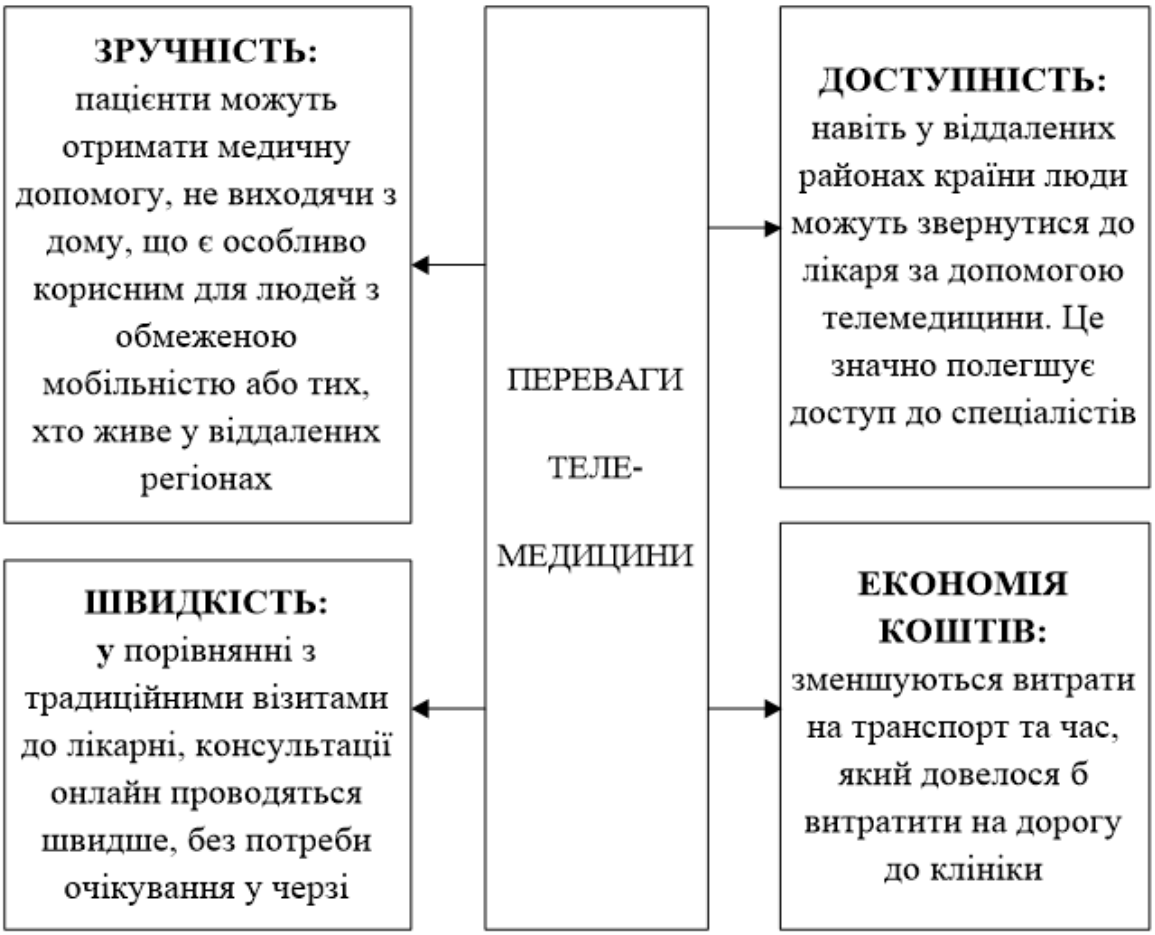

Рисунок 1.5 – Основні переваги ТМ

Телемедицина покращує доступ до медичної допомоги, безперервність та зручність медичного обслуговування, допомогає заощадити кошти (зменшуючи потребу в поїздках для пацієнтів та медичних працівників), пропонує більш гнучкий час та місце прийому.

ТМ допомогає покращувити комунікацію між пацієнтами та медичними працівниками, підвищує задоволеність пацієнтів, забезпечуючи більш зручний та персоналізований досвід догляду, допомогає підвищити ефективність надання медичної допомоги, скоротивши час очікування та кількість прийомів, розширює доступ до спеціалістів, яких немає в місцевості пацієнта, та багато іншого.

Рисунок 1.6 – Основні недоліки ТМ

До найбільш важливих недоліків ТМ відносять можливі технічні проблеми з обладнанням та можливі проблеми безпеки або конфіденційності медичної та персональної інформації.

Телемедицина може бути недоступна для всіх пацієнтів через обмежений доступ до технологій, тому доступ до ТМ може бути нерівним, якщо вона доступна лише пацієнтам, які можуть собі її дозволити.

Між пацієнтом та медичним працівником можуть існувати географічні бар'єри, різниця в часових поясах, мовні бар'єри, що може ускладнити спілкування. Також існує занепокоєння, що телемедицина може призвести до соціальної ізоляції.

1.4 Перспективні тенденції розвитку телемедицини

Згідно інформації з джерелам [2 – 7] можна сформулювати основні тенденції розвитку телемедицини у найближчі роки (рис. 1.7).

Рисунок 1.7 – Основні тенденції розвитку ТМ

ШІ вже використовується в ТМ, але очікується, що в найближчих роках він значно просунеться. Діагностичні інструменти та прогнозна аналітика на базі ШІ стануть більш досконалими, що дозволить постачальникам медичних послуг приймати більш обґрунтовані рішення та надавати пацієнтам ще більш персоналізовану віртуальну допомогу [6].

Оскільки мережі стають більш надійними, а медичне регулювання адаптується до телемедицини, використання телемедицини через міжнародні кордони стає все більш поширеним.

Одним із найперспективніших аспектів телемедицини є її потенціал для подолання розриву в доступі до медичного обслуговування для малозабезпечених та віддалених громад. Оскільки технології телемедицини стають більш просунутими та доступними, це принесе величезні переваги тим, хто зазвичай не має доступу до певних видів медичної допомоги або не має доступу до спеціалістів [7].

Роботодавці та уряди дедалі більше підтримують та заохочують догляд за поведінковим здоров’ям, що лише розширить потребу в легкодоступних та зручних цифрових послугах у сфері психічного здоров’я. Платформи телемедицини продовжуватимуть розвиватися, щоб задовольнити зростаючий попит, пропонуючи інноваційні рішення, такі як віртуальні сеанси терапії, додатки для психічного здоров’я та інструменти дистанційного моніторингу.

Для досягнення довгострокового успіху постачальники послуг телемедицини все частіше шукатимуть та інтегруватимуть сторонні рішення, що підтримують сталий розвиток. Це включає впровадження платформ і технологій, що покращують надання послуг, безпеку даних та залучення пацієнтів. Постачальники співпрацюватимуть з технологічними партнерами для впровадження масштабованих рішень, що відповідають потребам та викликам, що змінюються [7].

2 ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ТЕЛЕМЕДИЦИНІ

Телемедицина охоплює використання електронних та телекомунікаційних технологій для підтримки надання медичної допомоги як для профілактичної, так і для адміністративної діяльності [2].

Оскільки телемедицина можлива тільки завдяки сучасним інфокомунікаціям, стрімкий прогрес інфокомунікаційних технологій сприяє швидкому розвитку телемедицині та телемедичних технологій (рис. 2.1). Процеси глобальної цифрової трансформації, застосування принципово нових технологій обробки даних, можливості збирати та зберігати медичні дані в хмарних сховищах та інші інфокомунікаційні можливості розвитають ТМ та роблять ТМ реальною і доступною для всіх.

Рисунок 2.1 - Тенденції розвитку інфокомунікацій, що сприяють розвитку телемедицини

2.1 Засоби комунікації для телемедицини

Цифрова епоха змінила все спілкування людей, ці зміни також змінюють галузь охорони здоров'я. Оскільки все більше медичних працівників надають дистанційну допомогу через різні цифрові платформи, такі як електронні медичні записи або портали телемедицини, комунікація стала критичним аспектом догляду за пацієнтами.

Інфокомунікаційні засоби та канали зв'язку відіграють важливу роль у підтримці телемедичних послуг, допомагаючи пацієнтам зв'язатися з медичним персоналом. Вибираючи відповідні інструменти, медичні заклади можуть підтримувати якість послуг телемедицини та ефективність комунікації.

Комунікаційні інструменти для телемедицини поділяються на два основні типи. Це синхронні інструменти та асинхронні інструменти. Кожен тип інструменту може використовуватися в різних ситуаціях з різними функціями. [8].

Дистанційна допомога вимагає двох основних типів комунікації – синхронної та асинхронної. Синхронна комунікація відбувається в режимі реального часу, як-от відеодзвінок у реальному часі або телефонна розмова. Це дає пацієнтам відчуття безпосереднього зв’язку зі своїм медичним працівником.

Асинхронна допомога відбувається не в режимі реального часу, але не менш важлива в умовах дистанційного догляду. Це забезпечує гнучкість як для пацієнта, так і для медичного фахівця, оскільки повідомлення можна надсилати та відповідати на них у зручний для користувачів час [9].

Загалом, вибір правильного засобу комунікації залежить від потреб кожної медичної ситуації. Поєднуючи ці два методи, можна оптимізувати ефективність телемедицини, забезпечуючи пацієнтам своєчасну та точну підтримку.

2.1.1 Синхронний зв’язок

Завдяки синхронним комунікаційним інструментам для телемедицини, лікарі та пацієнти можуть обмінюватися інформацією в режимі реального часу. Ці інструменти сприяють негайним консультаціям та діагностиці. Вони вимагають одночасної участі двох сторін у спілкуванні, створюючи інтерактивний досвід, ніби вони зустрічаються віч-на-віч безпосередньо. На рис. 2.2 наведено деякі приклади використання цього типу комунікаційного інструменту для телемедицини [8].

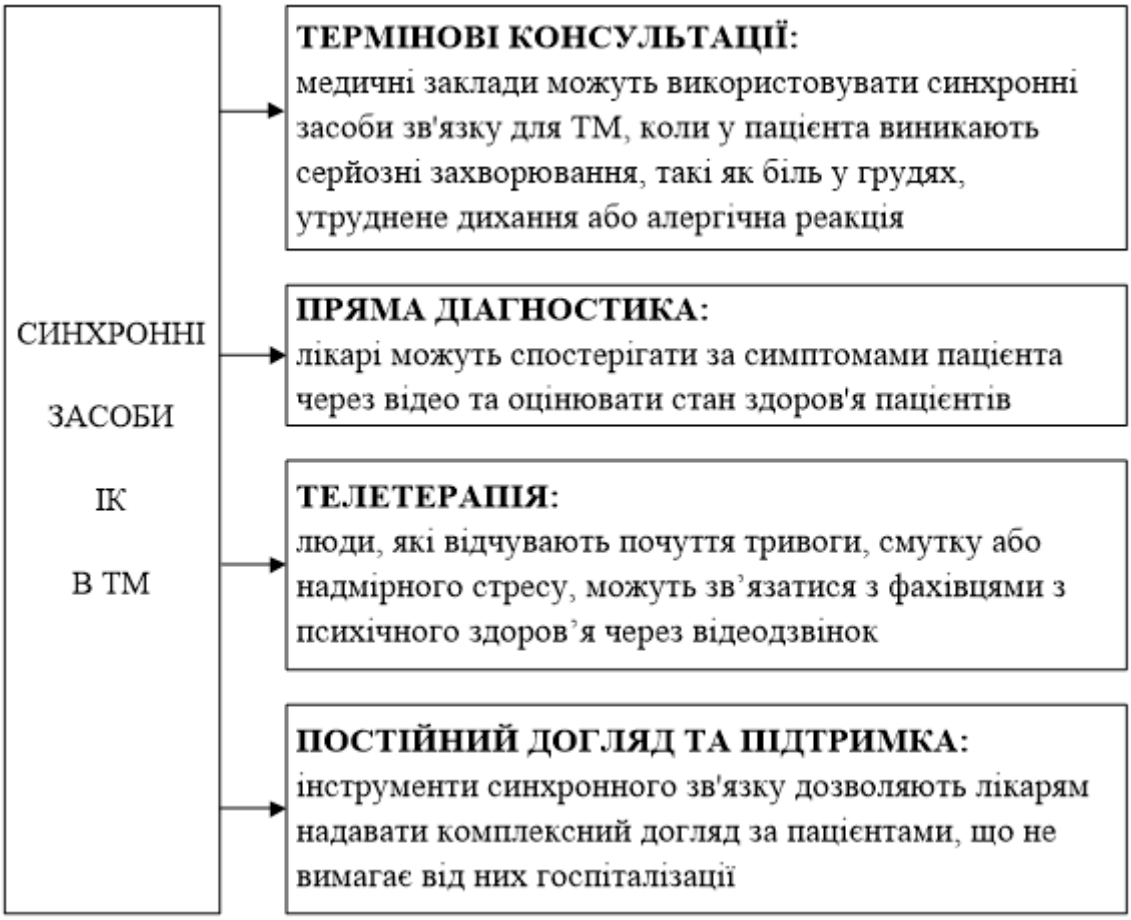

Рисунок 2.2 – Синхронні засоби інфокомунікацій в ТМ

В прикадах, що наведено на рис. 2.2 синхронні засоби інфокомунікації для ТМ допомагають лікарям оцінювати стан пацієнтів та своєчасно приймати

рішення. Завдяки цим інструментам медичні заклади можуть допомогти пацієнтам почуватися безпечніше, тим самим покращуючи їхній досвід. Крім того, безпосереднє спілкування допомагає лікарям надавати точні та своєчасні поради, уникаючи затримок у наданні медичної допомоги. Деякі типові інструменти цього типу включають Zoom for Healthcare, Teladoc Health та Microsoft Teams for Healthcare. Ці засоби комунікації для телемедицини допомагають медичним організаціям в організації онлайн-зустрічей, консультацій та консультування пацієнтів.

2.1.2 Асинхронний зв’язок

На відміну від синхронних засобів зв'язку для ТМ, асинхронний тип не вимагає від лікарів і пацієнтів одночасного безпосереднього спілкування один з одним. Використовуючи цей тип зв'язку, пацієнти можуть надсилати запитання або медичні дані, а лікарі відповідатимуть у потрібний час. Цей тип зв'язку особливо корисний у неекстрених ситуаціях, допомагаючи підвищити ефективність охорони здоров'я без необхідності негайної взаємодії.

Асинхронний тип комунікаційних інструментів для телемедицини може бути використаний для:

- моніторингу пацієнтів із хронічними захворюваннями, такими як діабет, високий кров'яний тиск або хвороби серця;
- надсилання результатів аналізів або призначення ліків, не телефонуючи чи не зустрічаючись з пацієнтами особисто;
- пацієнти можуть ставити запитання щодо незначних симптомів, побічних ефектів ліків або запитувати інструкції щодо догляду без негайного відеодзвінка.

Завдяки асинхронним комунікаційним інструментам для телемедицини, лікарі та пацієнти можуть заощаджувати свій час. Крім того, навантаження на особисті та екстрені служби можна зменшити, вирішуючи менш термінові питання за допомогою текстових повідомлень або електронної пошти. Деякі

яскраві приклади такого типу включають Epic, Cerner, Athenahealth, Medici, OhMD, Spruce Health тощо [8].

2.2 Архітектура телемедичних мереж

Для забезпечення можливості обслуговування зростаючої кількості пацієнтів за допомогою відеоконференцій вкрай важливо використовувати масштабовану архітектуру та актуальний технологічний стек, який забезпечуватиме високоякісну передачу відео/аудіо, безпечне зберігання, керування дзвінками тощо.

Приклад архітектури TMM наведено на рис. 2.3.

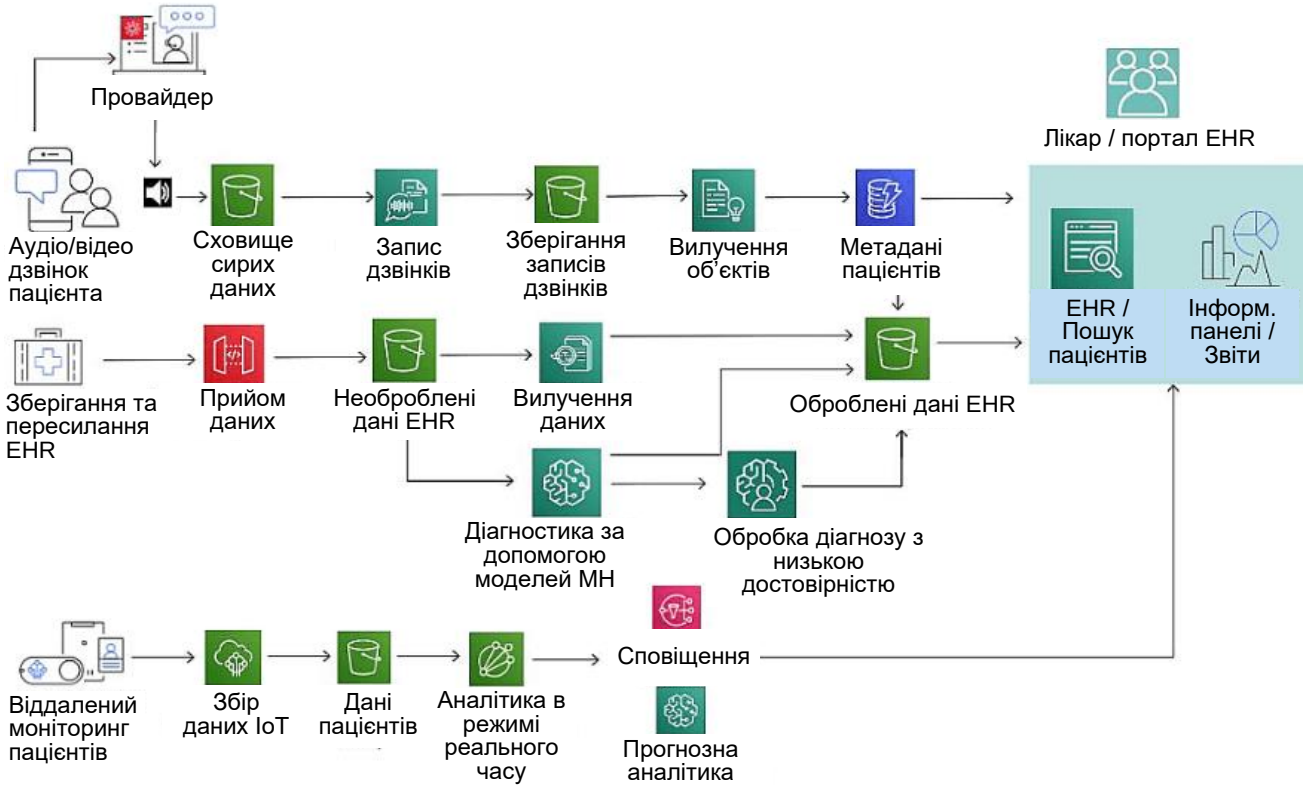

Рисунок 2.3 – Архітектура TMM від Amazon

У випадку побудови архітектури TMM на базі стеку AWS (рис. 2.3), такі постачальники, як Amazon, пропонують численні опції, адаптовані до проектів

у сфері охорони здоров'я та наук про життя. Різні модулі можуть включати функціональність для віддаленого відстеження здоров'я в режимі реального часу, безпечного зберігання даних пацієнтів, управління подіями, транскрипції аудіо/відео, панелей інструментів, дзвінків тощо [10].

В такій архітектурі (рис. 2.3) необроблені аудіо/відео файли можна зберігати в корзині, а дані пацієнтів зберігаються в БД (метадані пацієнтів). Файли можна конвертувати в текстові транскрипції, щоб лікарям не довелося прослуховувати весь відеодзвінок. Для подальшого спрощення діагностики установа, яка впроваджує систему, може аналізувати текстові записи дзвінків за допомогою Amazon Comprehend Medical та автоматично витягувати дані про стан пацієнтів, ліки, методи лікування тощо. Панелі інструментів допоможуть лікарям шукати та отримувати необхідні дані, а також створювати звіти [10].

Подібні архітектури пропонують майже всі основні постачальники, такі як Microsoft, Google та інші. Платформа для відеоконференцій займе ключове місце в будь-якому із запропонованих архітектурних рішень як основний засіб зв'язку між лікарем і пацієнтом. Численні платформи доступні для інтеграції через API (такі як Zoom, Skype, Microsoft Teams, Google Meet тощо) або навіть як індивідуальні рішення, адаптовані до потреб охорони здоров'я (наприклад,Teams або Zoom for Healthcare тощо).

2.3 Інфокомунікаційні засоби в телемедицині

Вибір відповідних архітектурних підходів та оптимального технологічного стеку – це половина шляху до забезпечення високої доступності системи. Можна розглянути архітектуру на основі мікросервісів, яка дозволяє створювати та підтримувати систему як набір незалежних компонентів. Хоча ці компоненти можуть бути написані різними мовами програмування за потреби, модель мікросервісів запобігає виникненню єдиної точки відмови, допомагаючи досягти майже нульового простою під час оновлень, розгортань тощо.

В ТММ використовуються такі інфокомунікаційні засоби: інтернет, бездротові технології для цифрової передачі даних, мобільна телемедицина, бездротове проектування, бездротова натільна мережа WBAN (Wireless Body Area Network), супутниковий зв'язок та стільникові технології, включаючи використання інфрачервоних каналів. Для телемедичних застосувань зв'язок можна класифікувати наступним чином:

- зв'язок на рівні тіла (зв'язок між пацієнтами та телемедичними пристроями, такими як носимі датчики);

- дистанційний зв'язок (зв'язок між телемедичними пристроями та віддаленими серверами, включаючи супутниковий зв'язок, інтернет, GSM/3/4/5G та WAN);

- зв'язок на основі області застосування, включаючи зв'язок для екстреної телемедицини, відеоконференцій та передачі медичних зображень [11].

Для організації ТММ необхідні такі протоколи/стандарти підключення:

- ZigBee/IEEE 802.15.4,

- Bluetooth/IEEE 802.15.1,

- WiMAX/IEEE (широкосмуговий бездротовий доступ) 802.16,

- Wi-Fi/WLAN/IEEE 802.11,

- протокол користувацьких дейтаграм (UDP),

- протокол реального часу (RTP),

- протокол керування транспортуванням у реальному часі (RTCP),

- стек протоколів TCP/IP [11].

На рис. 2.4 зображено основні частини, що складають систему телемедицини, її діяльність та процеси, включаючи пацієнта, дані якого збираються за допомогою датчиків або будь-якими іншими засобами, зберігаються в електронній медичній картці (EHR) або на локальному сервері та передаються через телекомунікаційну мережу до місця призначення.

Серед бездротових технологій, що використовуються для зв'язку на короткій відстані між бездротовими датчиками, використовують Bluetooth, ZigBee та Wi-Fi.

Рисунок 2.4 – Компоненти ТММ

Передача даних пацієнта віддаленому доглядачеві здійснюється за допомогою технологій зв'язку на великій відстані, таких як LoRaWAN, інтернет, GSM, 3G, 4G, LTE та 5G [11].

Зв'язок між компонентами встановлюється за допомогою протоколів зв'язку під час медичної процедури, таких як передача результатів тесту від пацієнта до інтерфейсу користувача для відображення на комп'ютері або іншому відповідному пристрої відображення.

Системи телемедицини складаються з чотирьох основних блоків, які включають блок пацієнта, блок комунікаційних технологій, що керується однією або кількома технологіями бездротового зв'язку, блок віртуального або віддаленого сервера та блок медичного працівника. Разом такі системи можуть покращити доступ до спеціалізованої медичної допомоги [11].

Блок WBAN пацієнта включає віддаленого пацієнта разом з будь-якими біосенсорами, фізіологічними датчиками або зовнішніми датчиками навколо пацієнта. Ці датчики є фізичними пристроями, що використовуються для збору життєво важливих показників пацієнта, і обробляються для передачі через комунікаційний блок. Ці пристрої мають здатність зберігати та отримувати збережені дані, а також взаємодіяти з прикладними програмами для обміну отриманими даними.

Комунікаційний блок відповідає за забезпечення інтерфейсу до всієї системи, від передачі інформаційних бітів на фізичному та канальному рівнях до прикладного рівня для запитів на підключення, до віддалених пристроїв і, нарешті, запиту на канали або протокол, що використовуються в комунікації. Цей блок є центральним у телемедицині, представляючи собою міст, без якого особи, які шукають медичної допомоги, та особи, що здійснюють догляд, не можуть взаємодіяти. Особливо важливими для комунікації є системи ближнього та далекого зв'язку та комунікаційні протоколи.

Віддалений медичний центр - це блок, у якому лікар або доглядач отримує віддалений доступ до потрібних послуг для пацієнта. Інформація про пацієнта з WBAN передана через комунікаційний блок і доступна до неї доглядачеві. Усі передані дані або інформація повинні бути отримані з використанням одного й того ж протоколу передачі. Інформація отримується та зберігається в базі даних, і за допомогою правильної автентифікації лікар може отримати доступ до інформації для діагностики. Для онлайн-консультацій широко використовуються відеоконференції. Для оцінки електронних медичних карток пацієнтів використовуються сумісні камери, мікрофони та інші електронні пристрої та комп'ютери [11].

Блок Медичні працівники стосується персоналу, який надає медичні або доглядові послуги дистанційно, до якого можуть входити лікарі, персонал лікарень, який виконує інтерпретацію даних, персонал швидкої допомоги, медсестри та інші медичні працівники, що беруть участь в процесі надання телемедичних послуг.

2.4 Основні інструменти комунікації для медичних працівників

Завдяки технологічному прогресу медичний персонал може використовувати різні засоби комунікації для ТМ, щоб швидко та безпечно обмінюватися інформацією. Найефективніші інструменти комунікації для медичних працівників наведено на рис. 2.5.

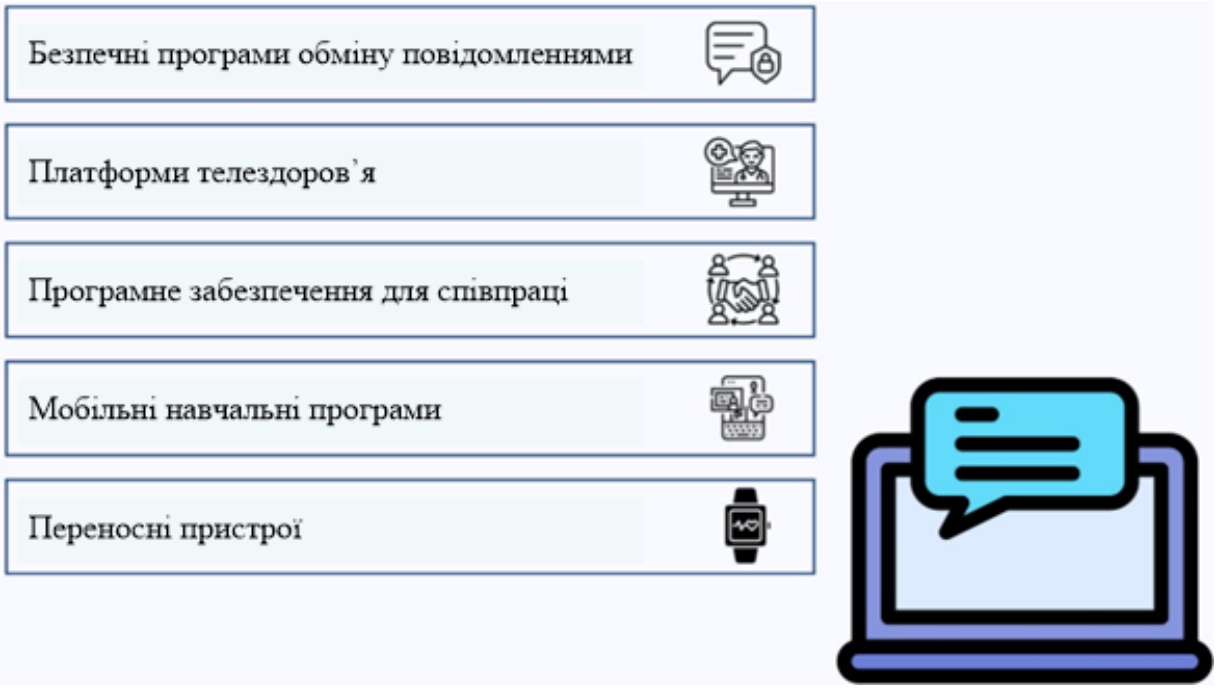

Рисунок 2.5 - Інструменти комунікації для медичних працівників

Програми безпечного обміну повідомленнями є одними з інструментів комунікації, популярних у секторі охорони здоров'я. Ці програми дозволяють медичному персоналу швидко обмінюватися інформацією, забезпечуючи дотримання правил безпеки, таких як HIPAA. Програми безпечного обміну повідомленнями пропонують зашифровані повідомлення, безпечний обмін файлами та платформи зв'язку в режимі реального часу. До таких програм відносяться: Klara, TigerConnect, Spok та інші [8].

Платформи телемедицини також є ефективними інструментами комунікації для ТМ. Деякі популярні платформи включають Doxy.me, Teladoc

Health та Amwell, які інтегровані з електронними медичними картками. Вони дозволяють пацієнтам дистанційно зв’язуватися з лікарями та медичним персоналом за допомогою відеодзвінків, голосових дзвінків та текстових повідомлень. Платформи телемедицини можуть значно покращити надання медичної допомоги, розширюючи охоплення, розширюючи доступ, зменшуючи витрати та підвищуючи задоволеність пацієнтів. Вони також можуть допомогти в лікуванні хронічних захворювань, моніторингу життєво важливих показників та наданні медичної освіти.

Програмне забезпечення для співпраці є дуже важливим. Лікар не працює самостійно, щоб обстежувати та лікувати пацієнтів. Натомість він має співпрацювати з іншими лікарями та медичними працівниками, щоб ставити діагноз та складати плани лікування. Таким чином, програмне забезпечення для співпраці стало одним із найважливіших інструментів комунікації в телемедицині. Деякі програми, такі як Microsoft Teams, Slack та Asana, допомагають медичним командам працювати ефективніше, надаючи інструменти для управління завданнями, обміну документами та внутрішньої комунікації [8]. Використовуючи це програмне забезпечення, медичні працівники можуть легко координувати дії між відділами, відстежувати прогрес лікування та оптимізувати адміністративні процеси. Зосереджуючись на комунікації та зберіганні документів, ці інструменти допомагають зменшити кількість помилок, підвищити ефективність роботи та покращити якість медичних послуг.

Мобільні навчальні додатки є незамінними інструментами комунікації для ТМ. Вони надають медичним працівникам медичні документи, навчальні курси та професійні сертифікати. Ці додатки допомагають покращити прийняття клінічних рішень, підвищити рівень знань та підтримувати кращий догляд за пацієнтами. До таких додатків відносяться: Medscape, UpToDate тощо [8].

Носимі пристрої також є комунікаційними інструментами для телемедицини, які приносять користь як медичним працівникам, так і

пацієнтам. Носимі пристрої, такі як смарт-годинники, біосенсори та персональні монітори здоров'я, відіграють ключову роль у дистанційному моніторингу здоров'я та відстеженні медичних даних у режимі реального часу. Вони допомагають медичним працівникам контролювати частоту серцевих скорочень, рівень кисню в крові, рівень глюкози в крові та інші життєво важливі показники, не вимагаючи госпіталізації пацієнтів. Серед популярних портативних пристроїв для здоров'я – Apple Watch (з функцією ЕКГ), Fitbit та BioIntelliSense BioSticker. Ці пристрої допомагають вчасно виявляти відхилення та покращують лікування хронічних захворювань [8].

3 ПРОБЛЕМИ БЕЗПЕКИ В ТЕЛЕМЕДИЧНИХ МЕРЕЖАХ

3.1 Загальні проблеми в телемедицині

Телемедицина користується великим попитом. Більшість розвинених країн впроваджують телемедицинні послуги, щоб дозволити пацієнтам і лікарям швидко та ефективно отримувати доступ до медичних даних та медичних послуг. Однак, оскільки дані та послуги стають доступними онлайн, безпека даних стає проблемою. Без належного механізму безпеки можуть бути використані вразливості систем телемедицини, що матиме негативний вплив на пацієнтів та медичні послуги в цілому, такі як неправильне лікування та витік конфіденційних даних.

Розширення використання дистанційних технологій в телемедицині, супроводжується суттєвим збільшенням можливостей підключення та вразливостей. Шидке впровадження та адаптація постачальників послуг телемедицини призвели до значного збільшення цифрового сліду та поверхні атак, що наражає на небезпеку як дані постачальників, так і дані пацієнтів. Як наслідок, хакери та злочинні групи можуть використовувати ці вразливості та легко проникати в мережу для отримання фінансової вигоди або збою в роботі. Згідно [2] вже у 2020 році постачальники послуг телемедицини зазнали майже експоненціального зростання цілеспрямованих атак, оскільки їхня популярність різко зросла.

Варто зазначити, що більшість проблем безпеки в ТМ пов’язані саме з проблемами безпеки інфокомунікацій, які лежать в основі ТММ. Але телемедицина, окрім традиційних проблем безпеки, вносить також унікальні нюанси в існуючі вразливості та проблеми. До них належать проблеми, пов'язані з автентифікацією, перевіркою особи, згодою, спільним використанням та записом екрана, а також дотриманням нормативних вимог.

Вони можуть виникати через спеціалізоване обладнання та програмне забезпечення, необхідні для відеозв'язку або збору даних з віддалених медичних пристроїв пацієнтів.

Основні проблеми безпеки наведені на рис. 3.1.

Рисунок 3.1 – Основні проблеми в ТММ

Телемедицина зараз стикається з великими проблемами, пов'язаними з вимогами до авторизації, автентифікації та підзвітності користувачів, що також є поширеними проблемами для інших галузей.

Оскільки телемедицина передбачає збір та передачу особистої медичної інформації (PHI) та особистої ідентифікованої інформації (PII), вона ненавмисно створює надзвичайно цінні цілі для хакерів.

Телемедицина є легкою мішенню з таких причин:

- дані, що передаються через мережу і доступ до інтернету (типові вразливості, пов'язані з даними в процесі передачі);

- інтеграція багатьох мереж і технологій означає відсутність єдиної політики і реалізації безпеки та відсутність централізованого управління, що робить безпеку системи залежною від найслабшої ланки.

Також ТМ є цінною мішенню, оскільки PII та PHI можуть мати високу ціну на чорному ринку [2].

3.2 Потенційні вразливості в телемедицині

Постачальники послуг телемедицини стикаються з тими ж загальними вразливостями, що й усі компанії, на додаток до ризиків, пов'язаних із захищеною медичною інформацією, унікальних для медичної галузі. І хоча не всі вразливості кібербезпеки телемедичних компаній пов'язані із захищеною медичною інформацією, ці ризики є найсерйознішими.

Кіберзлочинці використовують широкий спектр вразливостей та мобілізують складні методи для вилучення захищеної медичної інформації (PHI) у постачальників послуг телемедицини [12].

Основні вразливості в ТМ (рис. 3.2) пов’язані з недосконалою архітектурою кібербезпеки в ТММ, помилками та маніпуляціями користувачів та проблемами в мережах.

Недосконала архітектура кібербезпеки – це прогалини в кіберзахисті будь-якої компанії, що надають хакерам можливості захопити контроль над активами та сіяти хаос. До таких вразливостей відносять:

- слабкі або відсутні брандмауери для запобігання входу вірусів та інших шкідливих програм;

- незахищені мережі, які хакери використовують як точку входу до інших систем;

- слабкі протоколи автентифікації, що дозволяють хакерам обходити захист паролем;

- незашифрована інформація, яку легше вкрасти та використовувати після крадіжки [12].

Рисунок 3.2 – Вразливості в ТММ

Помилки та маніпуляції користувача – це велика вразливість. Навіть найретельніше захищена система кіберзахисту повинна враховувати людські помилки, пов’язані з різними обліковими записами персоналу та клієнтів:

- користувачі, які не пройшли належного навчання, можуть створювати слабкі паролі;

- соціальна інженерія обманом змушує користувачів скомпрометувати власні облікові записи;

- хакери можуть проникати у фізичні простори та використовувати неконтрольовані кінцеві точки.

Проблеми в мережі – ще один вид вразливостей. Збої в роботі мережі, некоректно налаштовані пристрої, відсутність оновлень ПЗ або застаріла інфраструктура можуть бути причинами атак на сервери за допомогою розподіленої відмови в обслуговуванні (DDoS). При цьому:

- хакери можуть завалити сервер нескінченними запитами;
- трафік уповільнює або навіть зупиняє функціональність мережі;
- звідти хакери можуть скористатися будь-якими вразливостями та вимагати викуп, перш ніж дозволити відновити нормальне обслуговування.

Найпрофесійніші хакери застосовують не одну, а різні комбінації атак, використовуючи одночасно кілька вразливостей [12].

3.3 Типи загроз безпеці даних в телемедичних мережах

Безпека даних є серйозною проблемою як для фахівців з телемедицини, так і для пацієнтів. У системах, де медична інформація зберігається на комп’ютері з доступом до інтернету або передається з нього, можливість зовнішнього вторгнення в приватні медичні записи є ризиком, який не можна ігнорувати. Хоча існують способи зменшення цього ризику, він все одно залишається проблемою [13].

Зі зростанням використання телемедицини зростає занепокоєння щодо питань безпеки та конфіденційності даних. Найбільш поширені типи загроз безпеці даних у ТМ представлено на рис. 3.3.

Найбільш проблемною загрозою є витік даних. Це трапляється, коли хакер або інший неавторизований користувач отримує несанкціонований доступ до збережених даних. Витоки даних можуть бути результатом шкідливого ПЗ, соціальної інженерії, фітингу, атак програм-вимагачів, погроз хакерів розкрити конфіденційну інформацію тощо. Чим більше інформації про пацієнтів доступно в інтернеті через ТМ, тим більша ймовірність її витоку.

Рисунок 3.3 – Типи загроз безпеці даних у ТМ

Внутрішні загрози – інсайдери, що є ще однією серйозною загрозою для безпеки даних, оскільки вони мають законний доступ до інформації про пацієнтів та інших конфіденційних даних, яких немає у хакерів. Збої в ПЗ, людські помилки, недбалість або недобросовісні співробітники можуть призвести до витоку даних або розкриття інформації про пацієнтів неавторизованим користувачам. Через цю загрозу організації повинні мати надійні процеси для моніторингу, аудиту та звітності про дії інсайдерів.

Атаки типу «відмова в обслуговуванні» - розроблені для того, щоб вивести комп'ютерні мережі організації з ладу, перевантаживши їх фальшивим трафіком. Хакери можуть використовувати атаки типу «відмова в обслуговуванні» як відволікаючий маневр для крадіжки інформації про пацієнтів, тому важливо мати стратегії пом'якшення наслідків кібератак [13].

Фішингові шахрайства сьогодні дуже розповсюджені. Спуфінг або імітація відомого веб-сайту – це одна з тактик фішингових атак, які намагаються обманом змусити користувачів надати особисту інформацію під виглядом звернення до свого постачальника послуг безпеки для вирішення неіснуючих проблем.

Різні типи кіберзагроз, такі як шкідливі програми, програми-вимагачі та шпигунські програми, привертають більше уваги, оскільки вони новіші, але одна старіша загроза, яка продовжує створювати проблеми, – це шкідливе ПЗ, що додається до завантажень і може приймати різні форми.

У той час як фішингові шахрайства спираються на соціальну інженерію, антиатактичні атаки (розширені постійні загрози APT – Advanced Persistent Threats) пов'язані з крадіжкою даних за допомогою шкідливого ПЗ, розміщеного в комп'ютерних мережах. APT зазвичай є роботою організованої злочинності, висококваліфікованих хакерів або держав. Кіберзлочинці часто використовують проксі-сервери та інші методи для запуску багатофазних атак та підтримки постійного доступу до мережі якомога довше [13].

Інсайдери не завжди є зловмисниками, але люди, які навмисно порушують політику безпеки даних своєї організації, становлять серйозну загрозу. Незалежно від того, чи продають вони інформацію хакерам, чи самі викладають її в інтернет, їхні дії можуть мати серйозні наслідки для конфіденційності пацієнтів.

Актуальними також є мобільні загрози. Мобільні пристрої спрощують доступ до медичної інформації, але вони також створюють нові проблеми. Телефони та інші портативні пристрої є легкою мішенню для хакерів, які шукають легкий доступ до захищеної медичної інформації. Профілактичні заходи включають шифрування, безпечний перегляд веб-сторінок та інші функції безпеки, які виходять за рамки захисту паролем для захисту мобільних пристроїв.

Незахищені медичні вироби також є причиною проблем безпеки. Популярність телемедицини може наражати більше медичного обладнання на

ризик хакерських атак, якщо воно не буде належним чином захищене. Рішення можуть варіюватися від брандмауерів до фізичної ізоляції між системами та інших заходів, які можуть потребувати більше часу та коштів, ніж медичні заклади готові витратити.

Загрози Інтернету речей (IoT) – зростання кількості пристроїв, підключених до Інтернету, призвело до нових викликів кібербезпеці, таких як атаки програм-вимагачів на смарт-телевізори та лікарняне обладнання. Хоча медичний Інтернет речей може не бути основною ціллю для хакерів, сама кількість підключених пристроїв може розкрити інформацію про пацієнтів або інші конфіденційні дані, якщо вони не будуть належним чином захищені.

4 ПІДВИЩЕННЯ БЕЗПЕКИ ТА ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕМЕДИЧНИХ МЕРЕЖАХ

4.1 Способи захисту даних пацієнтів в ТММ

Існує не мало способів захисту даних пацієнтів у телемедицині. На рис. 4.1 наведено деякі найважливіші заходи, які можуть вжити медичні працівники.

Рисунок 4.1 – Способи захисту даних пацієнтів в ТМ

Використання безпечних протоколів зв’язку – медичні працівники повинні використовувати безпечні протоколи зв’язку, такі як TLS або SSL, для шифрування інформації та запобігання її перехопленню.

Використання надійних паролів – паролі слід зберігати конфіденційно та регулярно оновлювати, щоб гарантувати їх відсутність у кіберзлочинності. Медичним працівникам варто використовувати двофакторну автентифікацію для додаткових рівнів захисту від спроб несанкціонованого доступу з боку зловмисників, які вкрали або вгадали пароль користувача.

Шифрування даних в стані спокою на всіх пристроях – усі дані пацієнтів мають бути зашифровані в стані спокою, тобто має бути надійне зберігання на пристрої або в хмарі. Це гарантує, що навіть у разі втрати або крадіжки пристрою зловмисники не зможуть отримати доступ до інформації.

Шифрування даних під час передачі – дані також слід шифрувати під час передачі через такі мережі, як Wi-Fi та LTE. Це запобігає перехопленню трафіку та зчитування зловмисниками до того, як вони досягнуть цільового одержувача.

Обмеження доступу до даних пацієнтів – інформація про пацієнтів повинна бути доступною лише тим, кому вона потрібна для виконання своїх обов’язків. Наприклад, лікарю може знадобитися доступ до всіх записів своїх пацієнтів, але адміністратор не матиме такого ж рівня доступу.

Впроваджденння заходів щодо запобігання втраті даних – медичні працівники можуть використовувати інструменти запобігання втраті даних (DLP), щоб допомогти виявити та захистити конфіденційну інформацію від витоку або компрометації. Ці інструменти можна використовувати для моніторингу всієї активності на пристроях і в мережах, включаючи електронну пошту, обмін файлами та обмін миттєвими повідомленнями.

Регулярна перевірка системи на наявність вразливостей – системи слід регулярно перевіряти, щоб виявляти та усувати будь-які потенційні вразливості безпеки, перш ніж вони спричинять проблеми з доглядом за пацієнтами або захистом даних.

Оновлення ПЗ – програмне забезпечення слід завжди оновлювати останніми оновленнями безпеки, щоб запобігти використанню зловмисниками відомих вразливостей, які вже були виявлені розробниками, але ще не виправлені.

Використання віртуальної приватної мережі (VPN) – це зашифроване з'єднання через Інтернет, яке дозволяє користувачам отримувати доступ до захищеної мережі без фізичної присутності в ній або в межах її периметра. Це може бути корисним для медичних працівників, яким потрібен доступ до інформації про пацієнтів під час подорожей, роботи віддалено з дому тощо.

Безпечні телеконференції – телеконференції слід проводити з використанням захищених відео та аудіо кодерів для захисту інформації про пацієнтів від перехоплення неавторизованими третіми особами.

Використоання найновіших технологій – медичні працівники повинні переконатися, що вони використовують найновіші технології безпеки, такі як брандмауери, антивірусне ПЗ та шифрування.

Впровадження найкращих практик, яких можуть дотримуватися медичні працівники для покращення безпеки даних, включаючи керування паролями, методи безпечного кодування та політики BYOD (привласнення власних пристроїв).

Важливим також є навчання співробітників. Співробітники повинні знати про ризики, пов'язані з ТМ, про те, як захищати дані пацієнтів та вміти виявляти атаки соціальної інженерії.

План дій у надзвичайних ситуаціях – якщо інцидент безпеки все ж таки станеться, медичні працівники повинні мати план реагування та пом'якшення збитків.

Медичні працівники повинні знати про ризики, пов'язані з телемедициною, такі як спроби несанкціонованого доступу до даних пацієнтів з боку хакерів та інших зловмисників, щоб вони могли вжити заходів для зменшення цих загроз, перш ніж ситуація вийде з-під контролю.

Досягти успіху в захисті інформації можна лише при застосуванні комплексного підходу та сукупності всіх можливих способів.

4.2 Модель захищеної телемедичної мережі

В роботі пропонується недорога, портативна та захищена система телемедицини на основі джерела [14]. Для більшої зручності та гнучкості, дана система телемедицини розділена на чотири основні модулі: місцеві лікарі, дистанційний медичний персонал, лікарі-експерти та адміністратор системи охорони здоров'я. Діаграма бізнес-процесів описує робочий процес чотирьох основних модулів запропонованої ТММ (рис. 4.2).

В даній ТММ кожен користувач має бути зареєстрований. Адміністратор СОЗ реєструє лікарів-експертів, дистанційний медичний персонал (це може бути особа, яка працює в місцевій аптеці та відповідає за всю місцеву адміністративну роботу), а також місцевих лікарів.

Дистанційний медичний працівник (ДМП) відповідає за реєстрацію віддалених пацієнтів, а також призначає лікаря для пацієнта під час реєстрації. Коли віддалені пацієнти реєструються, вони отримують ідентифікатор пацієнта, який використовується для подальшого листування [14].

Коли пацієнту потрібні послуги ТММ, він має описати свої проблеми дистанційному медичному пацівнику. ДМП вводить усі дані пацієнта в систему за допомогою клієнтського модуля входу з відповідним ідентифікатором пацієнта. Лікар-експерт перевіряє всю історію хвороби пацієнта. За потреби, лікар-експерт просить ДМП провести певний медичний огляд для пацієнта. Після отримання запиту від лікарів на проведення медичного огляду пацієнтів, ДМП доручає місцевим лікарям виконати призначене завдання.

Місцеві лікарі виконують призначене завдання за допомогою спеціального портативного інструментарію телемедицини. Інструментарій включає різні типів датчиків (наприклад, глюкометр, датчики артеріального тиску, температури, ваги, ЕКГ, положення тіла, тощо.

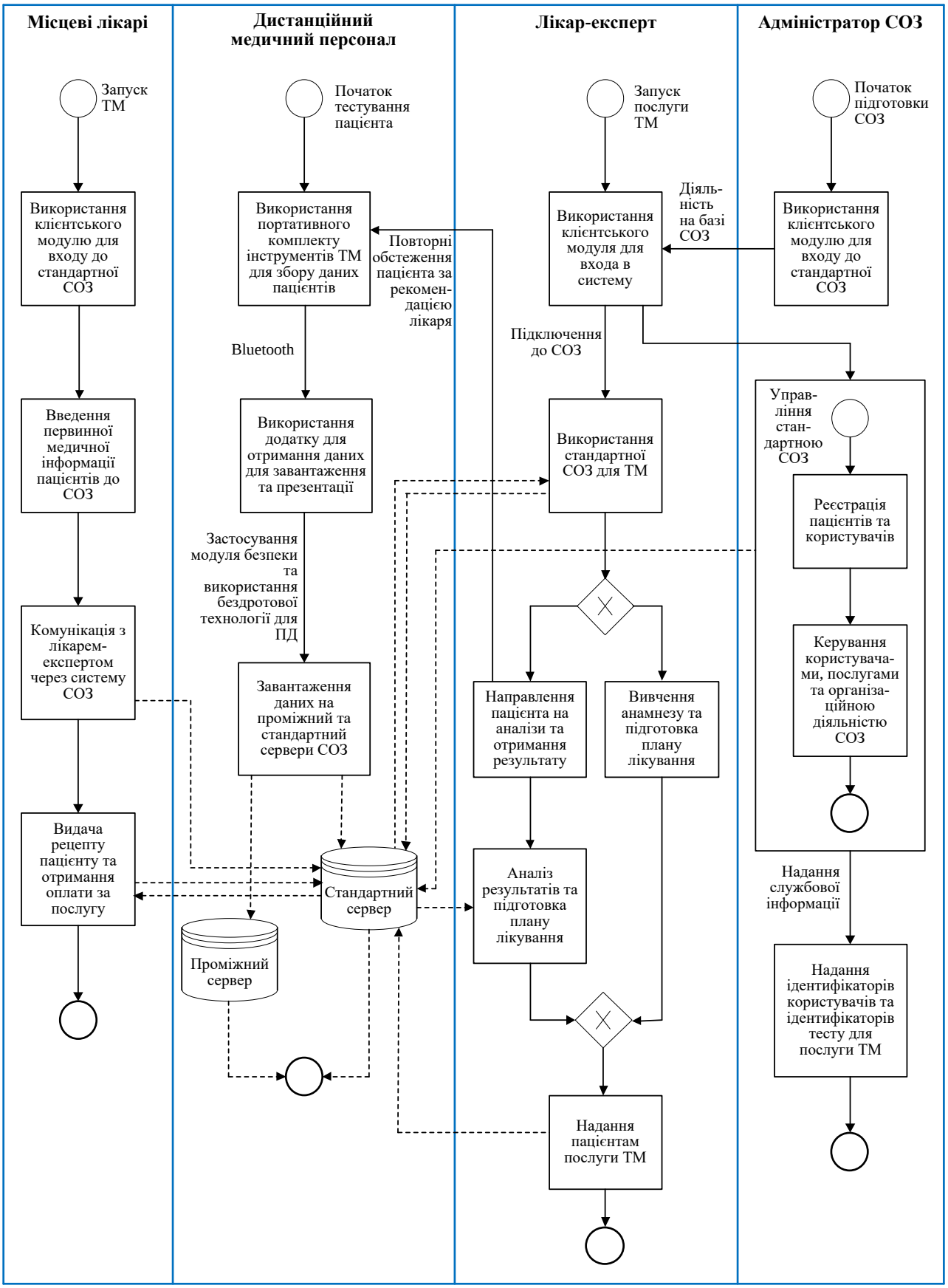

Рисунок 4.2 – Діаграма бізнес-процесу захищеної ТММ

Місцеві лікарі проводять огляд за допомогою мобільного додатку, який підключений до розробленого інструментарію через захищене з'єднання (наприклад, Bluetooth). Місцевим лікарям потрібно увійти в мобільний додаток Android, щоб отримати дані датчиків. Коли дані датчиків отримані застосунком Android, вони відображаються в інтерфейсі застосунку.

Місцеві лікарі бачать дані та завантажують їх на віддалений сервер з відповідним ідентифікатором пацієнта разом з ідентифікатором тесту. Для надсилання даних потрібно відкрити мобільне інтернет-з'єднання. У мобільному додатку мають бути алгоритм шифрування для шифрування даних датчиків. Дані, що надсилаються на сервер стадії, спочатку мають бути зашифрованими. На сайті сервера має бути алгоритм дешифрування для розшифрування та зберігання оригінальних даних. Лікарі-експерти входять до відкритої системи охорони здоров'я та виписують рецепти пацієнту, спостерігаючи за результатами медичних аналізів пацієнта [14].

ДМП входить до системи та отримує рецепт пацієнта. Після цього пацієнти отримують ліки або консультації, призначені лікарями-експертами, від ДМП. Рецепт зберігається в системі і, за потреби, пацієнти можуть отримати рецепт у будь-який час. ДМП також генерує звіт про рахунок-фактуру, звіт про обслуговування, а також призначає прийом для пацієнтів.

Враховуючи різні моделі безпеки, а також правила безпеки та конфіденційності різних організацій, пропонується система захисту для ТММ, що містить 5 модулів безпеки: автентифікація користувачів та безпека додатків, безпека клієнтського рівня, безпека даних пацієнтів, безпека проміжного сервера та безпека бази даних. Блок-схема системи безпеки наведена на рис.4.3.

Рівень автентифікації та безпеки додатків має бути розроблений для автентифікації кожного користувача, а також для забезпечення безпеки додатку. В даній ТММ є три типи користувачів: віддалені лікарі і навчений персонал, лікарі-експерти та ДМП. Для використання такої системи телемедицини необхідно три типи автентифікації.

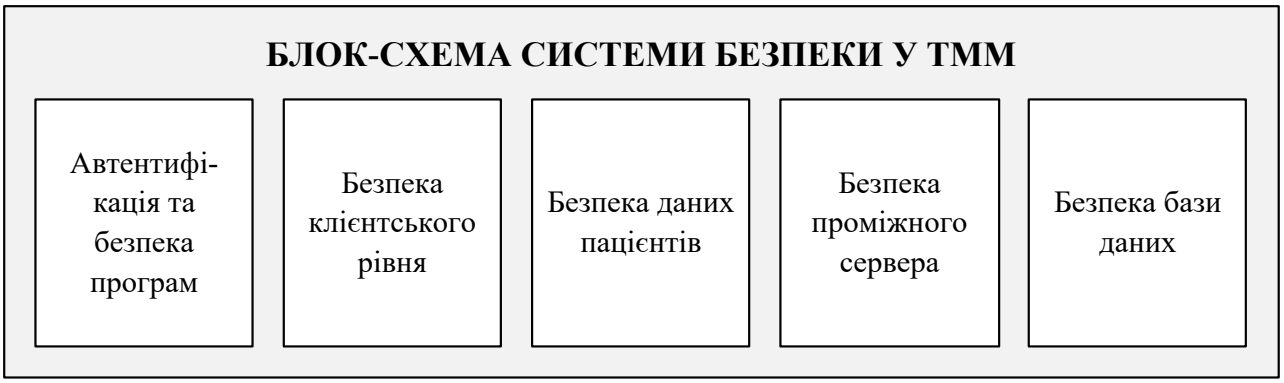

Рисунок 4.3 – Блок-схема системи захисту ТММ

Клієнтський рівень допомагає користувачам взаємодіяти із системою. Він складається з інтерфейсу мобільного додатку і з вебінтерфейсу додатку. Рівень мобільного додатку допомагає віддаленому медичному персоналу отримувати дані датчиків, вебінтерфейс допомагає лікарям виписувати рецепти пацієнтам, а віддаленим лікарям отримувати рецепти від експертів. Мобільний додаток отримує дані з датчика. Необхідно впроваджувати різні заходи безпеки, зокрема алгоритми хешування, щоб отримати дані без будь-якого спотворення даних.

Існують різні типи алгоритмів шифрування: симетричні, асиметричні, спільні або криптографічні хеш-функції для шифрування даних. Для рівня безпеки даних пропонується використовувати розширений алгоритм шифрування. Шифрування має відбуватися у мобільних додатках, а потім зашифровані дані мають надсилатися на віддалений вебсервер. На сервері дані розшифровуються за допомогою того ж алгоритму та зберігаються у базі даних.

Рівні безпеки промужного сервера та баз даних відповідають за веббазу даних, де зберігаються дані пацієнта. Віддалений медичний персонал надсилає дані на вебсервер з дійсним ідентифікатором пацієнта. Дані пацієнта зберігаються в базі даних з дійсним та унікальним ідентифікатором пацієнта та ідентифікатором обстеження. Існує кілька процедур автентифікації для отримання даних з датчиків та їх надсилання на сервер. Крім того, є кроки автентифікації для отримання рецепта від лікарів та його надання пацієнтам.

Загальні кроки безпеки з робочим процесом від з'єднання між мобільним додатком та інструментарієм до сховища даних на вебсервері представлені на рис. 4.4.

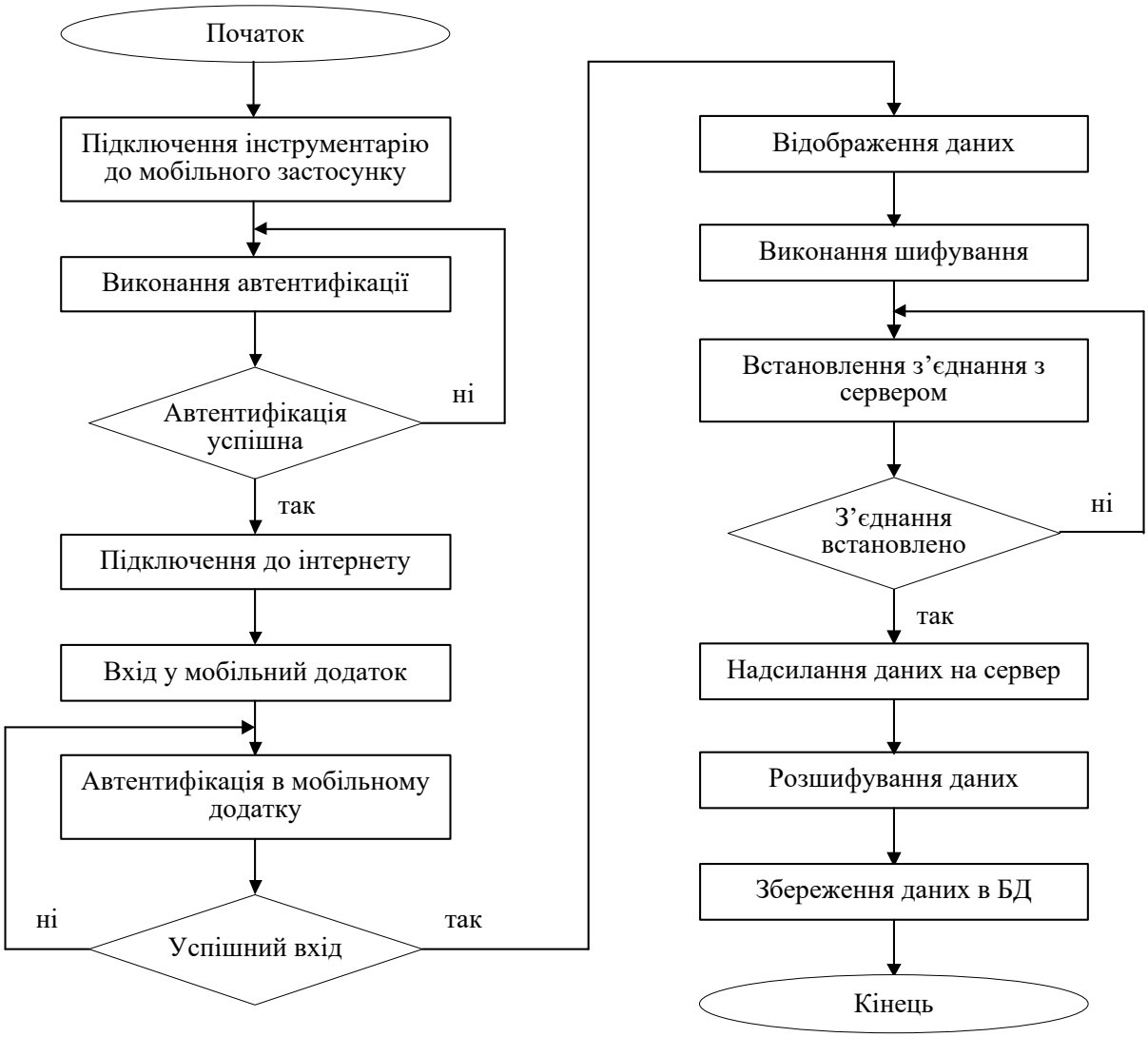

Рисунок 4.4 – Алгоритм безпечного з’єднання між мобільним додатком, інструментарієм та сховищем даних

Після отримання даних від віддалених лікарів лікарі-експерти переглядають дані. Таким чином, вони виписують рецепт для відповідного пацієнта. Віддалений лікар входить у систему та знаходить рецепт, а також видає ліки пацієнтам. Таким чином забезпечується комплексний захист даних пацієнтів при їх передачі.

4.3 Система оцінювання заходів безпеки в ТММ

Також крім системи безпеки доцільно впровадити систему оцінювання засобів безпеки в ТММ. Для цього необхідно визначити конкретні вимоги до ТММ, яких потрібно дотримуватися для забезпечення кібербезпеки. Схема моделі системи показана на рис. 4.5.

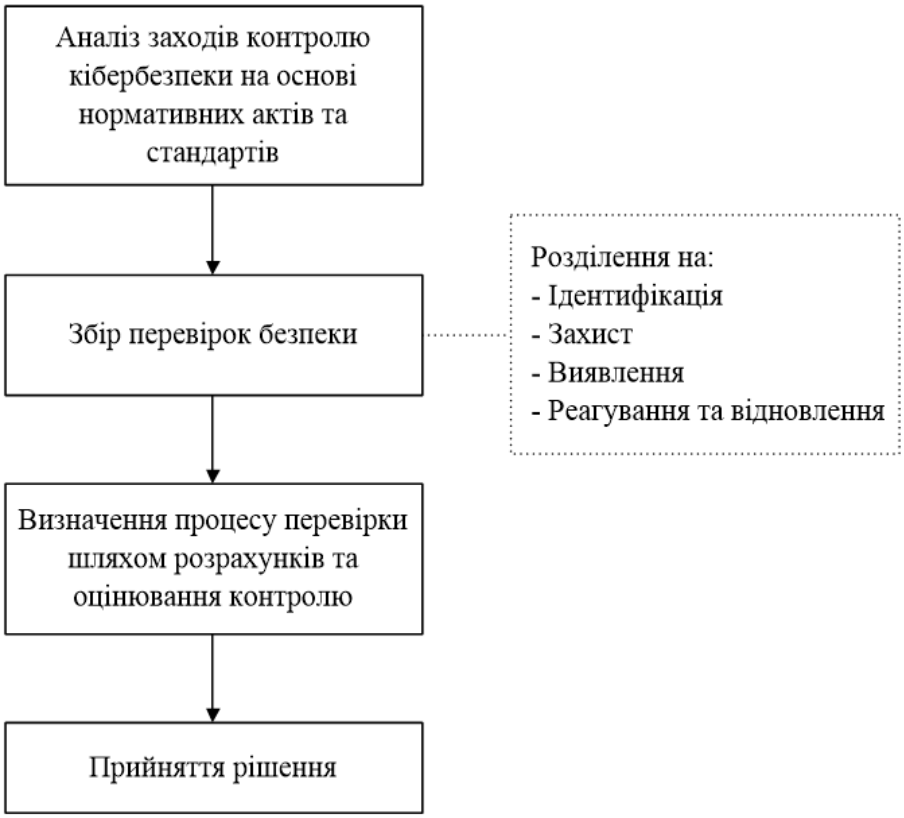

Рисунок 4.5 – Модель системи оцінювання заходів безпеки в ТММ

Для досягнення цієї мети також необхідно дотримуватися аспектів, на яких наголошується в різних стандартах безпеки (наприклад ISO 13485 – спеціалізований стандарт системи управління якістю для компаній-виробників медичних виробів, ISO 14971 – стандарт щодо застосування управління ризиками до медичних виробів, IEC 62304 – програмне забезпечення медичних виробів, ISO 27100 – стандарт щодо системи управління інформаційною безпекою та інші [15]).

Модель реалізується з урахуванням наступних кроків:

- аналіз засобів контролю кібербезпеки, передбачених відповідними нормативними актами та стандартами, включаючи ті, що стосуються медичних виробів, та ті, що стосуються кібербезпеки та захисту даних;

- збір засобів контролю безпеки, що вважаються необхідними для цієї мети, в рамках єдиної структури;

- визначення процесу перевірки безпеки ТММ з використанням отриманої структури як орієнтира, шляхом оцінювання окремих заходів безпеки.

Було визначено основні елементи контролю безпеки для ТММ (табл. 4.1). Різні елементи контролю були визначені на основі елементів кібербезпеки, що розглядаються в різних стандартах [15].

Таблиця 4.1 – Основні напрями контролю безпеки для ТММ

Напрям	Суть	Дії	Зміст
Ідентич-ність	Аналіз корпоратив-ного операційного контексту. Розглядаються ресурси та інвестиції відповідно до стратегічних цілей та цілей управління ризиками	Підхід, що ґрунтується на ризиках	Виявлення, оцінка та усунення ризиків кібербезпеки, пов'язаних з функціонуванням організації
		Відповідність нормативним вимогам	Програмне забезпечення відповідає відповідним нормам та стандартам
		Управління активами	Дані, персонал, пристрої, системи та обладнання визначаються та управляються відповідно до цілей та стратегії управління ризиками
		Безпека третіх сторін	При закупівлі компонентів застосовується суворий контроль для забезпечення безпеки та надійності

Продовження табл. 4.1

Напрям	Суть	Дії	Зміст
Захист	Впровадження заходів для захисту бізнес-процесів та активів	Контроль доступу	Впровадження надійних заходів автентифікації
		Захист даних	Персональні дані обробляються відповідно до процедур, визначених відповідно до чинних нормативних актів
		Керування оновленнями та виправленнями	ПЗ оновлюється за допомогою виправлень безпеки та виправлень помилок для зменшення відомих вразливостей
		Освіта та обізнаність	Користувачів інформують про кібербезпеку та навчають виконувати свої завдання та ролі
		Виведення з експлуатації	Забезпечується безпечне виведення з експлуатації, включаючи безпечне видалення конфіденційних даних
		Сегментація мережі	Мережа поділяється на окремі логічні або фізичні сегменти, щоб обмежити можливе поширення кібератаки
Вияв-лення	Впровадження цілеспрямо-ваних дій для виявлення інцидентів кібербезпеки	Моніторинг та запис діяльності	Реєстрація та моніторинг діяльності користувачів
		Тестування та валідація	Тестування та валідація програмного забезпечення

Продовження табл. 4.1

Напрям	Суть	Дії	Зміст
		Безпека застосунків	Застосунки відповідають вимогам управління
		Тестування обладнання	Оцінювання безпеки апаратного пристрою
Реагу-вання та віднов-лення	Управління інцидентами кібербезпеки. Втручання спрямоване на стримування впливу та своєчасне відновлення уражених процесів і послуг	Моніторинг та запис подій безпеки	Виявляються будь-які аномальні дії та аналізується їх потенційний вплив
		Керування аномаліями та подіями безпеки	Програмним забезпеченням можна керувати, контролювати його та оновлювати з часом
		Підтримка	Дії виконуються для запобігання поширенню події безпеки, пом'якшення її наслідків, вирішення інциденту та забезпечення відновлення уражених систем або активів

Після оцінювання всіх елементів безпеки для прийняття рішень доцільно використовувати методи багатокритеріальної оптимізації з урахуванням сукупності показників якості.

4.4 Пропозиції щодо посилення безпеки та конфіденційності в ТММ

На основі джерел [16 – 19] в роботі сформульовано та запропоновано деякі рекомендації щодо покращення конфіденційності та безпеки телемедицини (рис.4.6).

Безперервне навчання та підвищення обізнаності постачальників послуг

та користувачів. Безпека потребує впровадження програм підвищення обізнаності та навчання з безпеки для всіх членів персоналу, навчання має бути необхідним та доречним для того, щоб члени персоналу могли виконувати свої функції. Постачальники послуг телемедицини та персонал потребують більш постійного навчання експертам щодо найкращих практик конфіденційності та безпеки, щоб переконатися, що вони усвідомлюють свої обов'язки та здатні захищати захищену медичну інформацію.

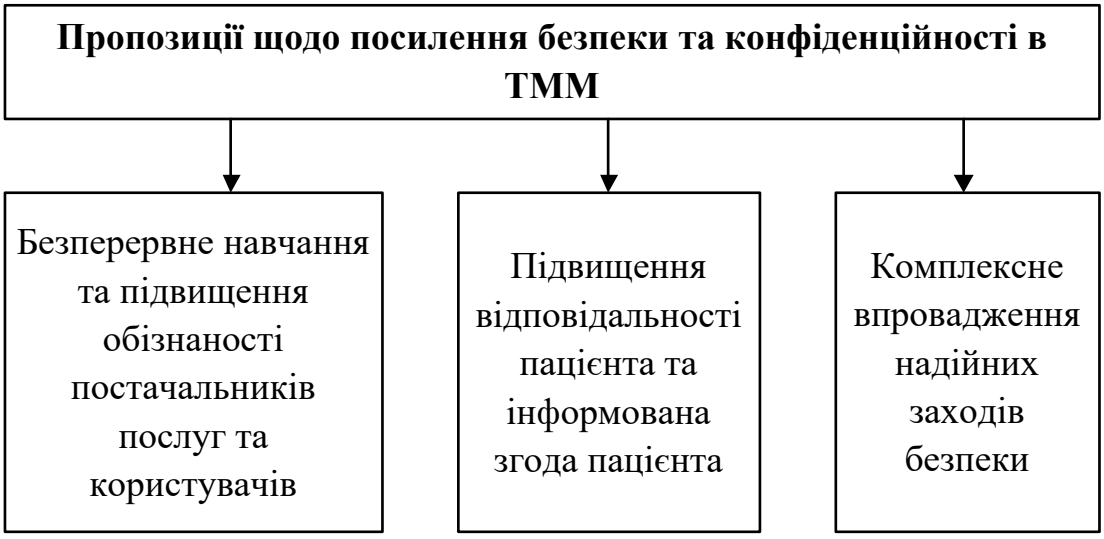

Рисунок 4.6 – Пропозиції щодо підвищення безпеки в ТММ

Важливою є відповідальність пацієнта та інформована згода пацієнта. Пацієнтам потрібна допомога у прийнятті рішень, обґрунтованих безпекою. Сьогодні їм потрібне більше розуміння практики дотримання норм безпеки їхніми постачальниками медичних послуг. Пацієнтам потрібен більший вибір щодо платформ телемедицини та інструкції щодо їх безпечного використання. Пацієнтів можуть попросити про згоду перед прийомом у сфері телемедицини, у них мало варіантів чи альтернатив, навіть якщо вони стурбовані безпекою та конфіденційністю. Перш ніж використовувати або розголошувати захищену медичну інформацію для лікування, оплати чи медичних операцій, постачальники послуг телемедицини повинні отримати згоду пацієнта.

Найголовнішою рекомендацією є комплексне впровадження надійних заходів безпеки. Постачальники послуг телемедицини повинні впроваджувати надійні заходи безпеки для захисту від витоків даних та інших онлайн-небезпек. Це має включати безпечні протоколи входу, шифрування даних та постійне оновлення заходів безпеки. Одним із заходів безпеки, який можна використовувати для покращення безпеки записів телемедицини, є впровадження багатофакторної автентифікації.

ВИСНОВКИ

Галузь охорони здоров'я дедалі більше переходить до телемедицини як способу забезпечення більш зручного та економічно ефективного догляду за пацієнтами. Однак цей крок пов'язаний з викликами безпеки, які медичним працівникам доведеться вирішувати, щоб забезпечити захист конфіденційності пацієнтів.

Безпека даних є критично важливим питанням для всіх галузей, але вона особливо важлива для телемедицини. Дані пацієнтів повинні завжди зберігатися конфіденційними та захищеними, щоб захистити як пацієнтів, так і лікарів. Існує багато способів захисту інформації, і медичні працівники обов’язково повинні їх застосовувати. Використовуючи найновіші технології та дотримуючись найкращих практик, медичні працівники зможуть гарантувати, що дані їхніх пацієнтів завжди в безпеці.

В роботі було розглянуто та проаналізовано ряд питань, що стосуються проблем безпеки та засобів захисту інформації в телемедичних мережах.

В першому розділі розглянуто сучасний стан та перспективи розвитку телемедицини в Україні та світі.

В другому розділі детально розглянуто інфокомунікаційні технології, на основі яких функціонує телемедицина. Проаналізовано синхронні та асинхронні засоби комунікації для телемедицини, досліджено архітектуру телемедичних мереж, інфокомунікаційні засоби та основні інструменти комунікації для медичних працівників.

В третьому розділі досліджені проблеми безпеки в ТММ, особливу увагу приділено потенційним ризикам та аналізу типів загроз в ТММ.

Четвертий розділ присвячено підвищенню безпеки та захисту інформації в ТММ, виконано аналіз способів захисту даних пацієнтів в ТММ, запропонована модель захищеної ТММ та використання системи оцінювання заходів безпеки в ТММ.

Описано структуру запропонованої моделі захищеної ТММ, діаграму бізнес-процесу захищеної ТММ та блок-схему системи захисту ТММ, що містить 5 модулів безпеки: автентифікація користувачів та безпека додатків, безпека клієнтського рівня, безпека даних пацієнтів, безпека проміжного сервера та безпека бази даних. Запропоновано алгоритм безпечного з'єднання між мобільним додатком, інструментарієм та сховищем даних.

Запропоновано модель системи оцінювання заходів безпеки в ТММ та описані основні напрями контролю безпеки для ТММ. Система оцінювання заходів безпеки в ТММ може слугувати цінним інструментом для моніторингу, контролю, виявлення вразливостей і областей для вдосконалення в ТММ. Така система дозволить компаніям ефективно зміцнювати свої стратегії кібербезпеки.

Також в результаті аналізу сучасних джерел запропоновані пропозиції щодо посилення безпеки та конфіденційності в ТММ.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Як розвивається телемедицина в Україні: підсумки й плани на 2024 рік. *Міністерство охорони здоров'я України. Офіційний вебсайт.* 08.01.2024. URL: https://moz.gov.ua/uk/jak-rozvivaetsja-telemedicina-v-ukraini-pidsumki-j-plani-na-2024-rik.

2. Health Industry Cybersecurity - Securing Telehealth and Telemedicine. *HIC-STAT_2023.* 01.10.2023. URL: https://healthsectorcouncil.org/wp-content/uploads/2023/10/HIC-STAT_2023.pdf.

3. Що таке телемедицина: інноваційний підхід до лікування. *Helsi.me.* 13.01.2025. URL: https://helsi.me/blog/shcho-take-telemedytsyna-innovatsiinyi-pidkhid-do-likuvannia.

4. Лобортас О., Кутчак І. «Телемедицина наближає пацієнтів до лікаря, дає можливість бути почутими і здоровішими», – експерти з провадження телемедичних послуг. *Caritas Ukraine ICF.* 06.11.2024. URL: https://caritas.ua/news-en/telemedyczyna-nablyzhaye-pacziyentiv-do-likarya-daye-mozhlyvist-buty-pochutymy-i-zdorovishymy-eksperty-z-provadzhennya-telemedychnyh-poslug/.

5. Сучасний стан розвитку телездоров'я та телемедицини в світі. *Міністерство охорони здоров'я України. Офіційний вебсайт.* 11.04.2024. URL: https://moz.gov.ua/uk/suchasnij-stan-rozvitku-telezdorov-ya-ta-telemedicini-v-sviti.

6. Marley R. Top telehealth trends for 2025. *Healthcare Transformers.* 12.02.2025. URL: https://healthcaretransformers.com/digital-health/current-trends/top-telehealth-trends-2025/.

7. 5 Telehealth Predictions for 2025. *Whereby.* 19.11.2024. URL: https://whereby.com/blog/5-predictions-for-the-future-of-telehealth/.

8. Communication tools for telehealth: An ultimate overview. *Adamo Software.* 05.02.2025. URL: https://adamosoft.com/blog/healthcare-software-development/communication-tools-for-telehealth/.

9. Salazar R. Communication Tools for Telehealth & Remote Healthcare. *Rehab U Practice Solutions.* 25.09.2023. URL: https://rehabupracticesolutions.com/communication-tools/.

10. Turol S., Khizhniak A., Capistrano J. The Technical Side of Embedding Video Calls into Telehealth Apps. *Altoros.* 01.05.2021. URL: https://www.altoros.com/blog/the-technical-side-of-embedding-video-calls-into-telehealth-apps/.

11. Telemedicine: A Survey of Telecommunication Technologies, Developments, and Challenges / C. Alenoghena et al. Journal of Sensor and Actuator Networks (JSAN). 2023. 12(2). P. 2 –38.

12. Top Cybersecurity Vulnerabilities of Telemedicine. RSI Security. Telemedicine and Cybersecurity. 22.10.2020. URL: https://blog.rsisecurity.com/top-cybersecurity-vulnerabilities-of-telemedicine-rsi-security/.

13. Rosemol. Data Security in Telemedicine: What You Need to Know. *Cabot Technology Solutions*. 21.02.2022. URL: https://www.cabotsolutions.com/blog/data-security-in-telemedicine-what-you-need-to-know.

14. Emon T. A., Prodhan U. K., Rahman M. Z. Improving Security of the Telemedicine System for the Rural People of Bangladesh. *International Journal of Advanced Computer Science and Applications (IJACSA).* 2018. T. Vol. 9, № 1. P. 381 – 390.

15. Nobili M., Raguseo D., Setola R. Cybersecuity Analysis of a Telemedicine Platform. *Healthcare.* 2025. 13(2). P. 184. URL: https://doi.org/10.3390/healthcare13020184.

16. Improving Privacy and Security of Telehealth / F. Tazi et al. *Communications of the ACM. Security and Privacy.* 06.08.2024. URL: https://cacm.acm.org/ opinion/improving-privacy-and-security-of-telehealth/.

17. Develop a privacy and security telehealth strategy. *Telehealth.HHS.gov. Privacy and security for telehealth*. 29.07.2024. URL: https://telehealth.hhs.gov/providers/best-practice-guides/privacy-and-security-telehealth/develop-privacy-and-security.

18. Navigating Privacy and Security in Telemedicine for Primary Care / K. Andreadis et al. *The American Journal of Managed Care*. 2024. Vol.30 Is.SP 6. P. SP459–SP463.

19. Telehealth Privacy and Security Tips for Patients. *United States Department of Health and Human Services. HIPAA Home.* 17.10.2023. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/telehealth-privacy-security/index.html.