

БАКАЛАВРСЬКА РОБОТА

БР. ІІ - 12.00.00.000 ІІЗ

Група ІІ-22-1

Красовський Євген

2026

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Красовський Євген Олександрович

(прізвище, ім'я, по батькові)

УДК 004.4
(індекс)

БАКАЛАВРСЬКА РОБОТА

Розробка та тестування безпеки застосувань електронних медичних

сервісів

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач освітнього рівня Є.О. Красовський
(підпис, ініціали та прізвище здобувача)

Науковий керівник Пасека Надія Мирославівна, к.т.н., доцент
(підпис, прізвище, ім'я, по батькові, науковий ступінь, вчене звання керівника)

Допущено до захисту

Завідувач кафедри

доц. Бандура В.В.
(посада) (підпис) (дата) (ініціали та прізвище)

Івано-Франківськ – 2026

Івано-Франківський національний технічний університет нафти і газу

Інститут, факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Ступінь вищої освіти бакалавр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:

Зав. кафедрою ІІЗ

доц.

В.В. Бандура

“ ” 2026 р.

ЗАВДАННЯ

НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТОВІ

Красовському Євгену Олександровичу

(прізвище, ім'я, по-батькові)

1. Тема проекту (роботи) “ Розробка та тестування безпеки застосувань електронних медичних сервісів”

керівник проекту (роботи) Пасека Надія Мирославівна, к.т.н., доцент

затверджені наказом закладу вищої освіти від “ 21 ” квітня 2026р. № 179 /7

2. Строк подання студентом проекту (роботи) 10 червня 2026 р.

3. Вихідні дані до проекту (роботи) Результати і матеріали отримані під час проходження переддипломної практики

4. Зміст розрахунково - пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз предметної області захисту даних в електронних медичних сервісах

2. Технологічні засади мережевої взаємодії, архітектура протоколів медичних сервісів

3. Архітектура мережевої взаємодії та аналіз вразливостей інформаційних каналів

4. Моделювання загроз безпеки застосувань електронних медичних сервісів

5. Інтеграція факторів кібербезпеки

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

1. Ризики інформаційної безпеки в медичному середовищі (рис. 1.1, ст.14)

2. Схематичний огляд досліджуваної системи (рис. 1.2, ст.17)

3. Атрибути цільового базису кібербезпеки (рис. 1.3, ст.19)

4. Опис елементів методології STRIDE (рис. 1.4, ст. 2.1)

5. OSI та TCP/IP моделі (рис. 2.1, ст. 29)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання _____ 2026 р.

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту	Примітка
1	Аналіз предметної області захисту даних в електронних медичних сервісах	04.02.2026	виконано
2	Технологічні засади мережевої взаємодії, архітектура протоколів медичних сервісів	15.03.2026	виконано
3	Архітектура мережевої взаємодії та аналіз вразливостей інформаційних каналів	21.04.2026	виконано
4	Моделювання загроз безпеки застосувань електронних медичних сервісів	28.04.2026	виконано
5	Інтеграція факторів кібербезпеки	03.05.2026	виконано
6	Оформлення пояснювальної записки дипломної роботи завідувачем кафедри	10.06.2026	виконано

Студент – дипломник _____ Красовський Є.О.
(підпис)

Керівник роботи _____ Пасєка Н.М.
(підпис)

АНОТАЦІЯ

Бакалаврська робота містить 78 сторінок, 19 рисунків, список використаних джерел із 36 найменуваннями.

Метою роботи є розробка та дослідження методів забезпечення і тестування безпеки застосувань електронних медичних сервісів шляхом аналізу мережових комунікацій, використання криптографічних механізмів та моделювання кіберзагроз.

Об'єктом дослідження є процеси функціонування та забезпечення безпеки електронних медичних сервісів.

Предметом дослідження є методи, моделі та засоби забезпечення і тестування кібербезпеки застосувань електронних медичних сервісів.

В першому розділі сформовано теоретичні засади забезпечення безпеки електронних медичних сервісів та визначено основні ризики інформаційної безпеки.

В другому розділі проаналізовано мережеву інфраструктуру, протоколи передачі даних і нормативні вимоги, що визначають безпечне функціонування медичних сервісів.

В третьому розділі проведено експериментальні дослідження, змодельовано загрози та підтверджено ефективність комплексного підходу до забезпечення кібербезпеки.

Висновок: результатом роботи є інтеграція факторів кібербезпеки в модель NHQA, що дозволяє підвищити рівень якості медичних сервісів шляхом врахування безпекових характеристик поряд із функціональними показниками.

КЛЮЧОВІ СЛОВА: ЕЛЕКТРОННІ МЕДИЧНІ СЕРВІСИ, КІБЕРБЕЗПЕКА, ЗАХИСТ ДАНИХ, МЕРЕЖЕВІ ПРОТОКОЛИ, TLS, DNS, КРИПТОГРАФІЯ, STRIDE, АНАЛІЗ ТРАФІКУ, ІНФОРМАЦІЙНА БЕЗПЕКА, МЕДИЧНІ ДАНІ, НОРМАТИВНЕ РЕГУЛЮВАННЯ

ANNOTATION

The bachelor's thesis contains 78 pages, 19 figures, a list of used sources with 36 names.

The purpose of the work is to develop and study methods for ensuring and testing the security of electronic medical services applications by analyzing network communications, using cryptographic mechanisms and modeling cyber threats.

The object of the study is the processes of functioning and ensuring the security of electronic medical services.

The subject of the study is methods, models and means of ensuring and testing the cybersecurity of electronic medical services applications.

The first section forms the theoretical principles of ensuring the security of electronic medical services and identifies the main risks of information security.

The second section analyzes the network infrastructure, data transmission protocols and regulatory requirements that determine the secure functioning of medical services.

In the third section, experimental studies are conducted, threats are simulated and the effectiveness of a comprehensive approach to ensuring cybersecurity is confirmed.

Conclusion: the result of the work is the integration of cybersecurity factors into the HHQA model, which allows to increase the quality of medical services by taking into account security characteristics along with functional indicators.

KEYWORDS: ELECTRONIC HEALTH SERVICES, CYBERSECURITY, DATA PROTECTION, NETWORK PROTOCOLS, TLS, DNS, CRYPTOGRAPHY, STRIDE, TRAFFIC ANALYSIS, INFORMATION SECURITY, MEDICAL DATA, REGULATION

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	8
ВСТУП.....	9
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАХИСТУ ДАНИХ В ЕЛЕКТРОННИХ МЕДИЧНИХ СЕРВІСАХ.....	12
1.1. Концептуальні основи та виклики впровадження гібридних моделей у системі охорони здоров'я.....	12
1.1.2. Методологія оцінки якості гібридних систем	12
1.1.3. Ризики інформаційної безпеки в медичному середовищі.....	13
1.2. Мета та завдання дослідження.....	15
1.3. Технічні параметри та обмеження об'єкта дослідження.....	17
1.4. Теоретичні аспекти кібербезпеки та мережевих комунікацій.....	18
1.5. Криптографічні методи захисту медичної інформації	21
1.5.1. Симетричне шифрування	22
1.5.2. Криптографічне хешування та забезпечення цілісності даних	24
1.5.3. Асиметричне шифрування та механізми обміну ключами.....	25
1.6 Висновки по розділу	27
РОЗДІЛ 2. ТЕХНОЛОГІЧНІ ЗАСАДИ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ, АРХІТЕКТУРА ПРОТОКОЛІВ ТА НОРМАТИВНЕ РЕГУЛЮВАННЯ МЕДИЧНИХ СЕРВІСІВ	28
2.1. Мережеві комунікації та архітектура протоколів медичних сервісів.....	28
2.1.2. Протокол захисту транспортного рівня (TLS)	30
2.1.3. Протокол керування передачею (TCP)	34
2.2. Архітектура мережевої взаємодії та аналіз вразливостей інформаційних каналів	35
2.2.1. Мережевий протокол IP.....	35

					БР.ІП – 12.00.00.000 ПЗ					
Змн.	Арк.	№ докум.	Підпис	Дата	Розробка та тестування безпеки застосувань електронних медичних сервісів Пояснювальна записка			Літ.	Арк.	Акрушіє
Розроб.		Красовський Є.О.								
Перевір.		Пасєка Н.М.							6	
Реценз.		Юрчищин В.М.						ІФНТУНГ ІП-22-1		
Н. Контр.		Піх М.М.								
Затверд.		Бандура В.В.								

2.2.2. Система доменних імен	36
2.2.3. Класифікація загроз мережевій безпеці	36
2.3. Технологія бездротової передачі даних Bluetooth Low Energy для медичних сервісів.....	37
2.4. Загальний регламент захисту даних (GDPR)	40
2.4.1. Регламент медичних виробів (MDR).....	41
2.4.2. Директива з мережевої та інформаційної безпеки (NIS2)	41
2.5. Технологічна парадигма електронного медичного сервісу	43
2.5.1. Опис протоколів передачі даних	45
2.5.2. Структура пакету передачі медичних даних	47
2.6 Висновки по розділу	49

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ ЗАГРОЗ БЕЗПЕКИ ЗАСТОСУВАНЬ

ЕЛЕКТРОННИХ МЕДИЧНИХ СЕРВІСІВ	50
3.1. Аналіз мережових комунікацій.....	50
3.2. Аналіз DNS-трафіку та ідентифікація вузлів	51
3.3. Дослідження комунікації за протоколом Bluetooth Low Energy	60
3.4. Систематизація кіберзагроз медичних даних на основі STRIDE моделі .	62
3.5. Оцінка відповідності системи обробки медичних даних принципам кібербезпеки та нормативним директивам.....	65
3.6. Інтеграція факторів кібербезпеки в модель NHQA	67
3.7 Висновки по розділу	69

ВИСНОВКИ	70
-----------------------	-----------

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	72
--	-----------

БІБЛІОГРАФІЧНА ДОВІДКА.....	76
------------------------------------	-----------

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BLE – Bluetooth Low Energy

GDPR – General Data Protection Regulation

HHQA – Hybrid Healthcare Quality Assessment

MDR – Medical Device Regulation

NIS2 – Network and Information Security Directive 2

STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure,
Denial of Service, Elevation of Privilege

TCP – Transmission Control Protocol

TLS – Transport Layer Security

EHR – Electronic Health Record

PHI – Protected Health Information

MITM – Man-in-the-Middle

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується активною цифровізацією систем охорони здоров'я, що зумовлює широке впровадження електронних медичних сервісів, зокрема електронних медичних записів, телемедицини, мобільних застосувань та інтелектуальних систем моніторингу стану пацієнтів. Такі сервіси забезпечують підвищення доступності медичної допомоги, оптимізацію процесів обробки даних та покращення якості прийняття клінічних рішень. Водночас інтенсивна інтеграція інформаційно-комунікаційних технологій у медичну сферу супроводжується зростанням кіберзагроз, що ставить під сумнів безпеку, конфіденційність і цілісність медичних даних.

Особливістю електронних медичних сервісів є їхня інтеграція у складні гібридні інформаційні середовища, які поєднують хмарні технології, мобільні платформи та IoT-пристрої. Це значно розширює поверхню атаки та ускладнює процеси управління безпекою. Крім того, використання різноманітних мережевих протоколів, зокрема TCP/IP, DNS, TLS та Bluetooth Low Energy, створює додаткові ризики, пов'язані з перехопленням даних, підміною інформації та несанкціонованим доступом.

У цьому контексті особливої актуальності набуває розробка та тестування безпеки застосувань електронних медичних сервісів із урахуванням сучасних підходів до кіберзахисту, криптографічного забезпечення та нормативно-правового регулювання. Важливим аспектом є також моделювання загроз, аналіз мережевого трафіку та оцінка відповідності систем вимогам міжнародних стандартів безпеки.

Актуальність роботи

Актуальність зумовлена стрімким зростанням обсягів медичних даних, які обробляються в електронному вигляді, а також підвищенням вимог до їх захисту. Медична інформація належить до категорії чутливих персональних даних, що робить її привабливою ціллю для кіберзлочинців. Порушення

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

безпеки таких даних може призвести до серйозних наслідків, включаючи фінансові втрати, репутаційні ризики та загрозу життю і здоров'ю пацієнтів.

Додатковим фактором актуальності є необхідність відповідності сучасних медичних сервісів міжнародним нормативним вимогам, таким як GDPR, MDR та NIS2, які регламентують процеси обробки, зберігання та передачі персональних даних. Недотримання цих вимог може призвести до юридичної відповідальності та обмеження функціонування систем.

З огляду на це, особливої ваги набуває розробка ефективних методів тестування безпеки, аналізу мережевих взаємодій та моделювання загроз, що дозволяє підвищити рівень захищеності електронних медичних сервісів і забезпечити їх надійне функціонування.

Метою роботи є розробка та дослідження методів забезпечення і тестування безпеки застосувань електронних медичних сервісів шляхом аналізу мережевих комунікацій, використання криптографічних механізмів та моделювання кіберзагроз.

Завдання дослідження

1. Провести аналіз предметної області захисту даних в електронних медичних сервісах.
2. Дослідити ризики інформаційної безпеки у медичному середовищі.
3. Проаналізувати мережеві протоколи та архітектуру комунікацій медичних сервісів.
4. Дослідити криптографічні методи захисту медичної інформації.
5. Дослідити особливості передачі даних за протоколом Bluetooth Low Energy.
6. Змодельовати загрози безпеки із застосуванням STRIDE-моделі.
7. Оцінити відповідність системи нормативним вимогам кібербезпеки.
8. Інтегрувати фактори кібербезпеки у модель оцінки якості медичних сервісів.

Об'єктом дослідження є процеси функціонування та забезпечення безпеки електронних медичних сервісів.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

Предметом дослідження є методи, моделі та засоби забезпечення і тестування кібербезпеки застосувань електронних медичних сервісів.

Методи дослідження

У роботі використано методи системного аналізу для дослідження предметної області, методи моделювання загроз (STRIDE) для ідентифікації ризиків, методи аналізу мережевого трафіку для виявлення вразливостей, криптографічні методи для забезпечення захисту даних, а також методи порівняльного аналізу для оцінки відповідності нормативним вимогам.

Наукова новизна

Наукова новизна одержаних результатів полягає у комплексному підході до дослідження безпеки електронних медичних сервісів, що поєднує аналіз мережевих протоколів, моделювання загроз та інтеграцію факторів кібербезпеки у модель оцінки якості систем. Удосконалено підхід до оцінювання безпеки шляхом врахування специфіки медичних даних і гібридних середовищ.

Практичне застосування

Практичне значення роботи полягає у можливості використання отриманих результатів для підвищення рівня захищеності електронних медичних сервісів, зокрема при розробці, тестуванні та впровадженні медичних інформаційних систем. Запропоновані підходи можуть бути застосовані для аналізу безпеки мережевих комунікацій, виявлення вразливостей та забезпечення відповідності нормативним вимогам. Результати роботи також можуть бути використані в освітньому процесі та при подальших наукових дослідженнях.

Бакалаврська робота містить 78 сторінок, 19 рисунків, 3 розділи список використаних джерел із 36 найменуваннями.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАХИСТУ ДАНИХ В ЕЛЕКТРОННИХ МЕДИЧНИХ СЕРВІСАХ

1.1. Концептуальні основи та виклики впровадження гібридних моделей у системі охорони здоров'я

1.1.1. Передумови цифровізації медичної галузі

Сучасна парадигма охорони здоров'я характеризується низкою системних викликів, зокрема демографічним старінням населення, зростанням превалентності хронічних нозологій та прогресуючим дефіцитом кваліфікованого медичного персоналу. У відповідь на ці виклики впроваджується концепція е-здоров'я (e-health), що передбачає інтеграцію інформаційно-комунікаційних технологій (ІКТ) у клінічну практику. Це охоплює використання пацієнтських порталів, портативних діагностичних пристроїв та систем електронних медичних карток (EHR). Інтеграція цифрових рішень із традиційними формами медичної допомоги (наприклад, очними консультаціями) формує гібридну модель охорони здоров'я.

Релевантним прикладом такої моделі є проект застосування носимих пристроїв (wearables) для моніторингу вітальних показників у домашніх умовах дозволяє оптимізувати лікувально-діагностичний процес. Такий підхід забезпечує дистанційний контроль за станом пацієнта, знижує госпітальне навантаження та мінімізує вплив стресогенних факторів («ефект білого халата»), що позитивно корелює з точністю діагностичних даних та раннім виявленням післяопераційних ускладнень.

1.1.2. Методологія оцінки якості гібридних систем

Впровадження цифрових сервісів потребує комплексної трансформації організаційної структури та перегляду професійних ролей медичного персоналу. З метою управління якістю переходу до гібридних моделей було

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

розроблено модель оцінки якості (NHQA) та відповідний інструментарій самодіагностики (Tossaint-Schoenmakers et al.).

Застосування методу концептуального картування (concept mapping) дозволило ідентифікувати детермінанти ефективності е-здоров'я, структуровані за вісьмома кластерами:

- Технологічний стек: юзабіліті та функціональність застосунків.
- Стратегічне управління: реінжиніринг бізнес-процесів та цільове планування.
- Клінічна ефективність: вплив цифрових інтервенцій на соматичний стан пацієнта.
- Інституційне навчання: безперервна оцінка та вдосконалення системи на засадах ко-креації (спільної участі стейкхолдерів).

1.1.3. Ризики інформаційної безпеки в медичному середовищі

Інтенсифікація використання цифрових сервісів детермінує зростання вразливості медичної інфраструктури до кіберзагроз. Сектор охорони здоров'я є пріоритетною мішенню для кіберзлочинності через високу цінність персональних даних та конфіденційність медичної інформації.

Критичні фактори вразливості включають:

- Технологічну доступність інструментів атаки: наявність готових експлуатаційних пакетів (malware-as-a-service) та орендованих обчислювальних потужностей знижує поріг входу для зловмисників.
- Низький рівень захищеності ІТ-інфраструктури: значна частина медичних систем характеризується відсутністю адекватних механізмів протидії сучасним векторам атак.

Таким чином, інституціалізація е-здоров'я вимагає імперативного посилення заходів кібербезпеки для забезпечення цілісності, доступності та конфіденційності медичних даних у гібридному середовищі.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		13

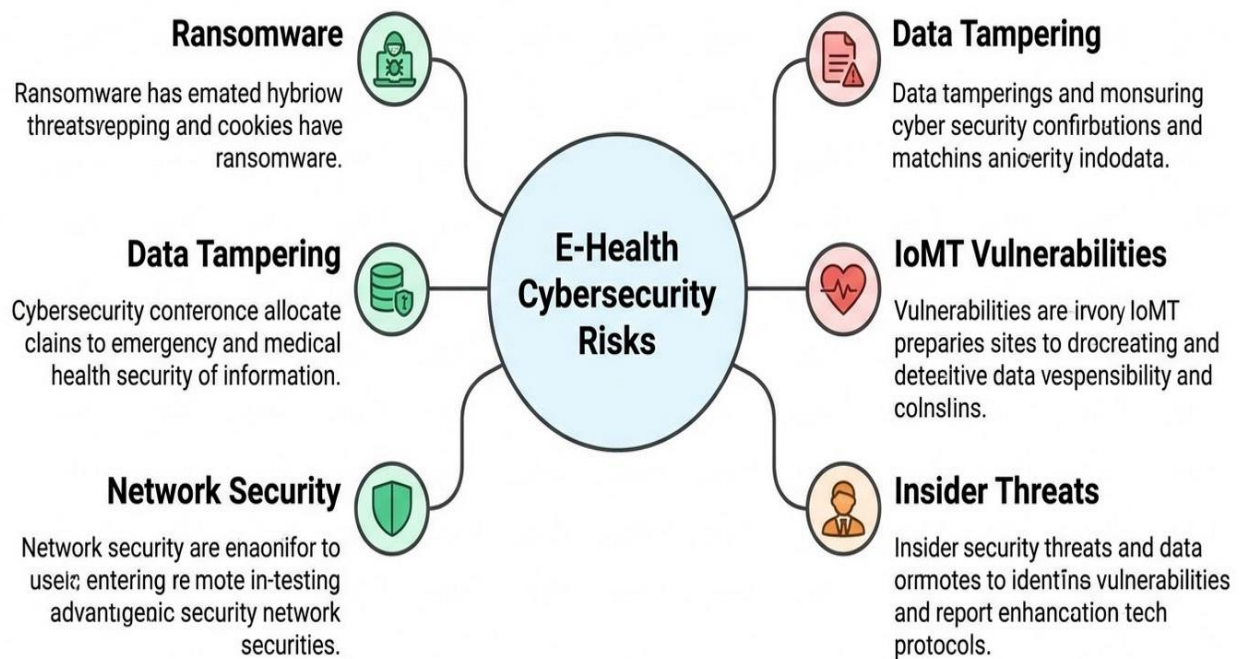


Рисунок 1.1 – Ризики інформаційної безпеки в медичному середовищі

У медицині порушення доступності даних може мати фатальні наслідки, оскільки затримка в отриманні інформації безпосередньо загрожує життю пацієнта. Атаки програм-вимагачів (Ransomware) - блокування доступу до електронних медичних карток (EHR) або систем візуалізації (MPT, KT). Медичні заклади є пріоритетними цілями, оскільки вони схильні швидше сплачувати викуп через критичність часу. Маніпуляція даними (In-transit attacks) - перехоплення та зміна даних під час передачі від носивного пристрою до сервера (наприклад, зміна показників глюкози або артеріального тиску), що може призвести до встановлення хибного діагнозу або призначення невірної лікування.

Медичне середовище часто є гетерогенним — воно поєднує надсучасні хмарні сервіси із застарілим обладнанням. Багато медичних пристроїв (наприклад, рентген-апарати) працюють на базі ОС, які більше не отримують оновлень безпеки, що робить їх відкритими для відомих експлуатацій. Вразливості IoT та медичних пристроїв (IoMT) - інсулінові помпи,

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

кардіостимулятори та монітори часто мають слабкі механізми автентифікації або використовують незашифровані канали зв'язку. Небезпека «тіньового ІТ», тобто використання персоналом несанкціонованих месенджерів або хмарних сховищ для обміну медичними даними через незручність офіційних систем.

Медичні дані (PHI — Protected Health Information) на чорному ринку коштують значно дорожче за фінансові дані, оскільки їх неможливо «анулювати» чи змінити, як номер кредитної картки.

Внутрішні загрози (Insider Threats) - несанкціонований доступ персоналу до карток публічних осіб або злив даних через фінансову вигоду.

Витоки через треті сторони. Оскільки гібридна медицина залучає розробників додатків та хмарних провайдерів, слабка ланка в безпеці одного підрядника ставить під загрозу всю базу даних пацієнтів.

У контексті даної роботи про додатки для е-здоров'я, мережевий аспект є найуразливішим:

- Відсутність наскрізного шифрування (End-to-End Encryption) - Дані можуть бути захищені на сервері, але вразливі під час проходження через публічні Wi-Fi мережі пацієнта.

- Слабкі механізми автентифікації - використання лише паролів без багатофакторної автентифікації (MFA) дозволяє зловмисникам легко отримувати доступ до облікових записів пацієнтів через методи соціальної інженерії або брутфорс.

1.2. Мета та завдання дослідження

Згідно з архітектурою моделі, представленою у додатку, оцінка якості технологічного забезпечення здійснюється в межах двох структурних кластерів: «Якість інфраструктури інформаційних технологій» та «Застосунок е-здоров'я».

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		15

Попри стратегічну важливість забезпечення кібербезпеки інформаційних систем у медичній галузі, на сучасному етапі відповідні індикатори не імплементовані в модель HHQA (Hybrid Healthcare Quality Assessment). У зв'язку з цим, метою даного дослідження є теоретичне обґрунтування та практичне розширення моделі HHQA шляхом інтеграції верифікаційних вимог до кібербезпеки. Результати дослідження представлені у формі розробленого контрольного списку (check-list).

Методологія розробки факторів контрольного списку ґрунтується на комплексному підході, що включає:

- Компаративний аналіз нормативно-правової бази: проведено огляд чинних регламентів з метою детермінації високорівневих криптографічних стандартів, релевантних для медичних цифрових екосистем.

- Емпіричне дослідження (Case Study) - здійснено апробацію методик на прикладі функціонування мобільного медичного застосунку та пов'язаного з ним носимого пристрою (wearable device). Об'єктом технічного аналізу стали процеси моніторингу вітальних показників (термометрія, ЧСС) та подальша дисемінація даних через клієнт-серверну архітектуру.

Особливу увагу в роботі приділено безпеці комунікаційних каналів у системі «пристрій — застосунок — сервер». Дослідження спрямоване на верифікацію протоколів автентифікації, алгоритмів шифрування та методів забезпечення цілісності трансмісії даних. На підставі отриманих емпіричних даних побудовано модель загроз, що дозволяє ідентифікувати потенційні вразливості в архітектурі обміну даними.

Синергія результатів аналізу нормативних вимог та виявлених технічних вразливостей дозволила сформулювати низку факторів, інтегрованих у кластер «Застосунок е-здоров'я». Запропоноване розширення моделі HHQA сприятиме підвищенню надійності систем гібридної медицини та забезпеченню належної якості надання медичних послуг у цифровому середовищі.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3. Технічні параметри та обмеження об'єкта дослідження

У межах даного дослідження аналізується мобільний застосунок для е-здоров'я, що функціонує в екосистемі гібридної медичної допомоги. Програмне забезпечення постачається в комплекті з носимим пристроєм типу «смарт-годинник». Як показано на рисунку 1.1, архітектура системи передбачає з'єднання носимого пристрою зі смартфоном через протокол Bluetooth, тоді як мобільний застосунок здійснює подальшу дисемінацію даних на віддалені сервери через мережу інтернет.



Рисунок 1.2 - Схематичний огляд досліджуваної системи

Носимий пристрій — смарт-годинник підключений до смартфона із застосунком для е-здоров'я. Смартфон, у свою чергу, з'єднаний із серверами через мережу інтернет. Основна увага в цій роботі приділена першому вузлу (hop) на маршруті між смартфоном та серверами. Цей перший етап передачі даних здійснюється через мережу Wi-Fi.

Першочерговим завданням дослідження була комплексна оцінка безпеки обох комунікаційних каналів шляхом декомпозиції та аналізу мережевого трафіку. Для реалізації цього завдання застосовувався спеціалізований інструментарій для мережевого моніторингу у поєднанні з аналізатором протоколу BLE (Bluetooth Low Energy). Проте, через технічні обмеження BLE-аналізатора, захоплення трафіку на сегменті «пристрій —

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		17

смартфон» виявилося неможливим. Відповідно, верифікація безпеки Bluetooth-з'єднання винесена за межі даного етапу дослідження і розглядається як перспективний напрям для подальшої роботи.

Таким чином, фокус роботи зосереджено на аналізі захищеності мережевої комунікації між клієнтським терміналом (смартфоном) та серверною інфраструктурою. З огляду на захист прав інтелектуальної власності розробника, детальна інформація про внутрішню архітектуру ПЗ та специфічні засоби захисту периметра (наприклад, конфігурації міжмережевих екранів) була недоступною. Доказова база висновків ґрунтується виключно на відкритих специфікаціях виробника та результатах об'єктивного аналізу мережевого трафіку.

1.4. Теоретичні аспекти кібербезпеки та мережесих комунікацій

Відповідно до положень, викладених у попередніх пунктах, інтеграція концепції кібербезпеки є критичною детермінантою успішної імплементації систем гібридної медичної допомоги. Об'єктивна оцінка захищеності інформаційної системи базується на фундаментальному розумінні методів та принципів забезпечення кібербезпеки. У даному розділі проведено теоретичний аналіз методів превенції та детекції загроз, а також визначено ключові концепти й принципи функціонування мережесих комунікацій та протоколів передачі даних (зокрема Bluetooth).

Зазначені концептуальні засади є методологічною базою для інтерпретації нормативно-правових вимог, що регламентують мінімальний рівень захищеності застосунків сегмента е-здоров'я. Крім того, вони дозволяють провести верифікацію архітектури комунікацій досліджуваного застосунку на предмет її відповідності критеріям безпеки.

Кібербезпека визначається як сукупність заходів, спрямованих на захист обчислювальних систем від несанкціонованого доступу та нівелювання його негативних наслідків [1]. Стратегічною метою є

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

забезпечення цілісності та конфіденційності даних, апаратних і програмних ресурсів, а також мережевої інфраструктури від навмисної компрометації з боку нелегітимних суб'єктів.

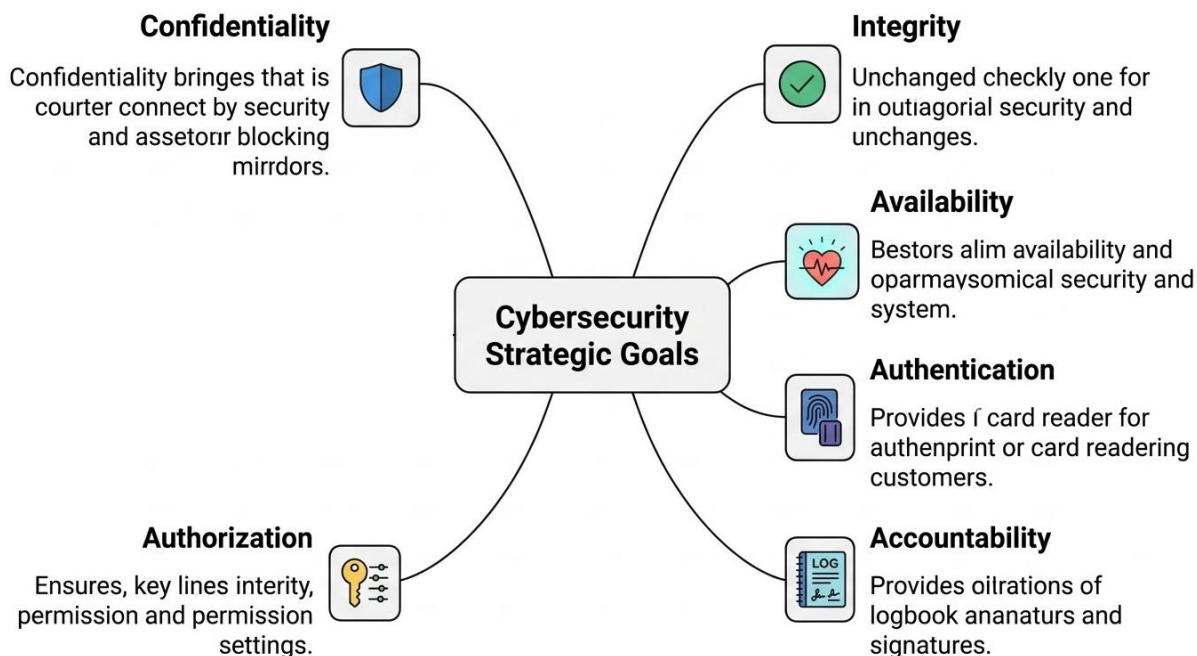


Рисунок 1.3 – Атрибути цільового базису кібербезпеки

В академічній та практичній площині виділяють шість атрибутів, що становлять цільовий базис кібербезпеки (рис. 1.3):

1. Конфіденційність (Confidentiality) - обмеження доступу до персоналізованої інформації виключно колом авторизованих суб'єктів у станах транзиту (in transit) та зберігання (at rest). Реалізується переважно через криптографічне перетворення даних, що унеможлиблює інтерпретацію змісту неавторизованими сторонами. Спорідненим концептом є анонімність, що гарантує відсутність зв'язку між даними та ідентичністю суб'єкта.

2. Цілісність (Integrity) - властивість системи, що гарантує неможливість несанкціонованої модифікації даних, програмних компонентів або апаратних ресурсів.

3. Доступність (Availability) - забезпечення безперешкодного доступу легітимних користувачів до інформаційних та обчислювальних ресурсів у разі потреби.

4. Автентифікація (Authentication) - процедура верифікації справжності об'єкта, суб'єкта або джерела даних, що дозволяє виключити можливість імітації (маскараду) з боку злоумисника.

5. Авторизація (Authorisation) - процес надання певних прав доступу до ресурсів системи, регламентований адміністратором або власником ресурсу.

6. Підзвітність (Accountability) - можливість однозначної ідентифікації суб'єкта, відповідального за певну операцію, на основі доказової бази транзакційних логів. Цей атрибут забезпечує невідомність — неможливість заперечення факту виконання дії її ініціатором.

Для превенції кібератак необхідно здійснювати ідентифікацію та усунення архітектурних вразливостей на етапі проєктування системи. Це реалізується через моделювання загроз, що передбачає аналіз потенційних агентів загроз та можливих векторів атак [2].

У даній роботі застосовується методологія STRIDE, яка класифікує загрози за шістьма категоріями:

1. Spoofing (Підміна) - імітація ідентичності легітимного користувача для отримання несанкціонованого доступу.

2. Tampering (Втручання) - несанкціонована зміна інформаційних активів, що порушує їхню цілісність.

3. Repudiation (Відмова) - уникнення відповідальності за вчинені дії через неможливість їх верифікації.

4. Information Disclosure (Розголошення) - компрометація конфіденційних або непублічних даних.

5. Denial of Service (Відмова в обслуговуванні) - спрямований вплив на доступність системи.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

6. Elevation of Privilege (Підвищення привілеїв) - експлуатація вразливостей для отримання прав доступу, що перевищують установлені регламентом [3].

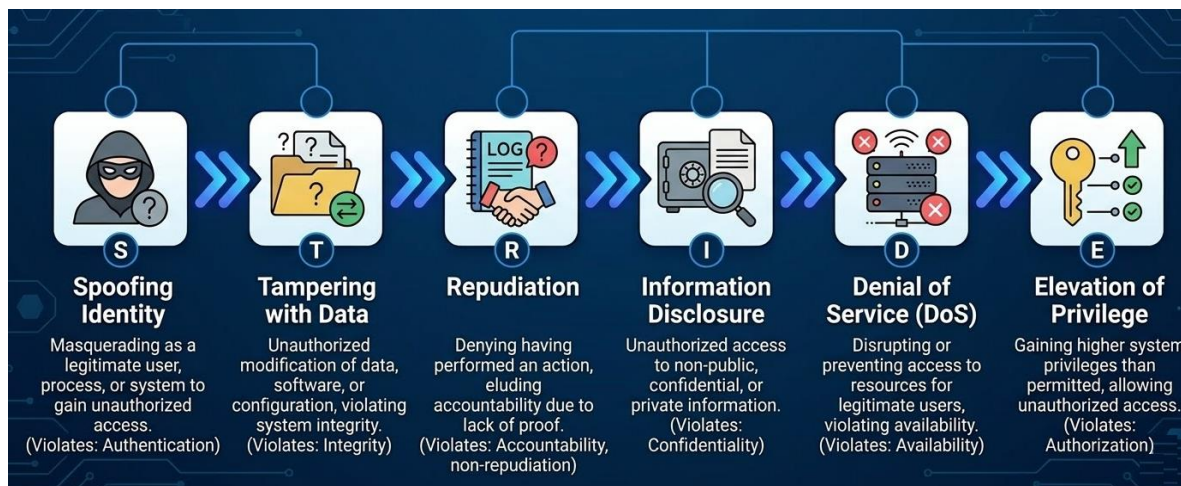


Рисунок 1.4 – Опис елементів методології STRIDE

Комунікаційні канали досліджуваного застосунку підлягали аудиту на предмет вразливостей згідно з класифікацією STRIDE. Враховуючи необхідність мінімізації зазначених ризиків у сегменті е-здоров'я, ці фактори інтегровані до розроблюваного контрольного списку для модернізації моделі ННQA.

Слід зауважити, що аналіз вразливостей категорії Elevation of privilege винесено за межі об'єкта даного дослідження, оскільки їхня ідентифікація потребує повного доступу до вихідного коду застосунку та специфікацій внутрішньої архітектури.

1.5. Криптографічні методи захисту медичної інформації

У межах даної роботи криптографічні методи становлять особливий інтерес, оскільки нормативні вимоги у сфері охорони здоров'я детермінують обов'язкове забезпечення конфіденційності персональних даних пацієнтів. Інформація, що перебуває у станах зберігання (at rest) або транзиту (in transit)

між суб'єктом та об'єктом надання медичних послуг, повинна бути захищена від несанкціонованої інтерпретації сторонніми особами. Зазначений рівень захисту досягається шляхом шифрування — криптографічного перетворення вихідного детермінованого тексту (plaintext) у криптограму (ciphertext). Зворотна процедура — дешифрування — має бути технічно неможливою для суб'єктів, які не володіють відповідними повноваженнями та легітимним ключем.

У даному підрозділі проаналізовано три фундаментальні типи криптографічних алгоритмів: симетричне шифрування, хешування та асиметричне шифрування.

1.5.1. Симетричне шифрування

Методологія симетричного шифрування передбачає використання єдиного спільного криптографічного ключа для процесів інкапсуляції та розкриття даних. Ключ являє собою преінстальовану секретну послідовність символів, якою сторони-кореспонденти обмінюються за захищеним протоколом до ініціації сеансу зв'язку. Процедура трансформації вихідного змісту повідомлення в зашифрований вигляд базується на алгоритмі, що використовує цей ключ. Згідно з принципом Керкгоффза, стійкість криптосистеми визначається не секретністю математичної моделі самого алгоритму, а виключно таємністю ключа [4]. Це дозволяє проводити відкритий аудит і верифікацію надійності алгоритмів міжнародною науковою спільнотою.

До найбільш верифікованих і поширених стандартів симетричного шифрування належить Advanced Encryption Standard (AES). Механізм функціонування AES ґрунтується на ітеративному розширенні ключа на визначену кількість раундів трансформації. Кожен цикл включає операції додавання раундового ключа, перестановки та заміни байтів повідомлення за детермінованими матрицями. Алгоритм AES класифікується як

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

стандартизований та рекомендований для застосування в критичних інформаційних інфраструктурах.

AES — це блочний шифр, який обробляє дані фіксованими блоками по 128 біт (16 байт) за раз.

Процес шифрування AES складається з кількох повторюваних раундів трансформації (кількість раундів — 10, 12 або 14 — залежить від довжини ключа: 128, 192 або 256 біт відповідно). Кожен раунд, крім останнього, включає чотири основні етапи:

- SubBytes (Заміна байтів) - кожен байт поточного стану (матриці стану) замінюється іншим байтом згідно з фіксованою таблицею заміन (S-box). Це забезпечує нелінійність шифрування.

- ShiftRows (Зсув рядків) - Кожен рядок матриці стану зсувається циклічно вліво на певну кількість позицій (0, 1, 2 або 3). Це перемішує дані між стовпцями.

- MixColumns (Перемішування стовпців) - кожен стовпець матриці стану обробляється як поліном і множиться (у полі Галуа) на фіксовану матрицю. Це забезпечує дифузію даних усередині блоку.

- AddRoundKey (Додавання раундового ключа) - кожен байт поточного стану додається (за допомогою операції XOR) до відповідного байта раундового ключа, який отримується з вихідного секретного ключа за спеціальним алгоритмом розширення ключа. Це єдиний етап, де використовується секретний ключ.

Ці чотири етапи повторюються в циклі раундів. В останньому раунді етап MixColumns пропускається. Отримана після всіх раундів матриця стану і є шифротекстом.

Ключовим параметром симетричних криптосистем є режим функціонування (mode of operation), який регламентує обробку повідомлень, обсяг яких перевищує розмір блоку шифрування. Вибір конкретного режиму детермінує рівень захищеності системи. Зокрема, використання режиму Galois Counter Mode (GCM) дозволяє реалізувати автентифіковане

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

шифрування: поряд із забезпеченням конфіденційності, він дозволяє верифікувати автентичність та цілісність даних за допомогою коду автентифікації повідомлення (MAC — Message Authentication Code) [5].

1.5.2. Криптографічне хешування та забезпечення цілісності даних

Механізми хешування відіграють фундаментальну роль у верифікації цілісності та автентичності джерела інформації. Криптографічна хеш-функція визначається як математичний алгоритм, що перетворює вхідний масив даних довільної довжини у фіксований вихідний рядок, відомий як хеш-значення або «цифровий відбиток» повідомлення. Процес трансформації базується на ітеративному виконанні логічних операцій (XOR, бітові зсуви) та нелінійних підстановок.

Для забезпечення криптографічної стійкості хеш-функції повинні відповідати трьом фундаментальним критеріям:

1. Стійкість до знаходження прообразу - властивість односторонності, що робить обчислювально неможливим відновлення вихідних даних на основі наявного хеш-значення.

2. Стійкість до знаходження другого прообразу - складність пошуку альтернативного вхідного значення, яке б генерувало ідентичний хеш для вже заданого входу.

3. Стійкість до колізій - мінімізація ймовірності того, що два довільні різні вхідні масиви призведуть до формування однакових хеш-значень. Ця властивість є критичною для контролю цілісності: будь-яка модифікація вихідного тексту призводить до радикальної зміни результуючого хешу (ефект лавини).

У сучасній криптографії хешування класифікується за ознакою використання додаткових параметрів на дві категорії:

- безключове хешування (MDC — Modification Detection Codes) - алгоритми, що не потребують секретного ключа. До цієї групи належать застарілі стандарти MD5 та SHA-1, які на сучасному етапі розвитку

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

обчислювальних потужностей вважаються вразливими до атак методом «грубої сили» та пошуку колізій. Рекомендованим стандартом для застосування в медицині є сімейство SHA-2 (зокрема SHA-256), що забезпечує належний рівень криптостійкості.

- хешування з використанням ключа (MAC — Message Authentication Code): передбачає залучення секретного ключа для формування значення, що дозволяє одночасно підтвердити як цілісність даних, так і автентичність відправника.

Застосування хеш-функцій є невід'ємною частиною протоколів формування цифрових підписів, безпечного зберігання паролів та автентифікації повідомлень у системах е-здоров'я.

1.5.3. Асиметричне шифрування та механізми обміну ключами

Асиметрична криптографія, або криптографія з відкритим ключем, базується на використанні пари ієрархічно пов'язаних ключів: відкритого (public key) та особистого (private key). Принцип функціонування полягає у вільному розповсюдженні відкритого ключа для ініціації сеансу зв'язку. Сторона-відправник застосовує відкритий ключ реципієнта для шифрування даних, тоді як дешифрування здійснюється виключно власником пари за допомогою конфіденційного особистого ключа.

Безпека асиметричних криптосистем ґрунтується на обчислювальній складності певних математичних задач. Зокрема, алгоритм RSA базується на задачі факторизації: операція множення двох великих простих чисел є тривіальною, проте розкладання отриманого добутку на множники для відновлення ключів є практично нездійсненним при достатній довжині ключа.

Окрему категорію становлять алгоритми обміну ключами, серед яких фундаментальним є протокол Диффі-Геллмана (Diffie-Hellman, DH). Механізм передбачає узгодження спільних параметрів домену — основи α та простого числа p . Кожна зі сторін генерує випадкове число (a та b), що є

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		25

приватним ключем, і обчислює відповідний відкритий ключ шляхом піднесення основи до степеня приватного ключа ($a \bmod p$ та $b \bmod p$). Після обміну відкритими ключами сторони обчислюють спільний секрет, використовуючи властивості модульної арифметики: $(ab)a \equiv (aa)b \pmod{p}$. Отримане значення використовується як сеансовий ключ. Стійкість DH базується на складності розв'язання задачі дискретного логарифмування.

Сучасною ітерацією даного протоколу є алгоритм на еліптичних кривих — ECDHE (Elliptic Curve Diffie-Hellman Ephemeral). ECDHE — це криптографічний протокол, який дозволяє двом сторонам (наприклад, вашому браузеру та серверу) узгодити спільний секретний ключ через незахищений канал зв'язку. Цей спільний секрет потім використовується як сеансовий ключ для швидкого симетричного шифрування (наприклад, AES) основного обміну даними. Його безпека детермінована складністю задачі дискретного логарифму еліптичної кривої (ECDLP). У цій моделі відкриті ключі обчислюються як результат множення приватного ключа на базову точку кривої P (наприклад, kP та lP). Спільний секрет S визначається як точка на кривій, отримана в результаті множення приватного ключа однієї сторони на відкритий ключ іншої ($k \cdot lP = l \cdot kP$).

Ефективність асиметричних методів залежить від автентичності використаного відкритого ключа. Для запобігання атакам типу «людина посередині» (MITM) застосовуються цифрові сертифікати, видані довіреним центром сертифікації (Certificate Authority, CA). Сертифікат підтверджує належність відкритого ключа конкретному суб'єкту. Важливою умовою експлуатації є розмежування функцій ключів: ключі, що використовуються для формування цифрових підписів у сертифікатах, не повинні застосовуватися для шифрування даних, оскільки це підвищує ризики компрометації криптосистеми.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						26
Змн.	Арк.	№ докум.	Підпис	Дата		

1.6 Висновки по розділу

У першому розділі здійснено комплексний аналіз предметної області захисту даних в електронних медичних сервісах, що дозволило визначити ключові особливості функціонування таких систем в умовах цифрової трансформації охорони здоров'я. Обґрунтовано доцільність використання гібридних моделей, які забезпечують поєднання централізованих і розподілених підходів, водночас створюючи нові виклики у сфері безпеки та управління даними. Встановлено основні ризики інформаційної безпеки, зокрема загрози несанкціонованого доступу, витоку конфіденційної інформації та порушення цілісності медичних даних. Розглянуто теоретичні засади кібербезпеки та доведено ефективність застосування криптографічних методів, включаючи симетричне й асиметричне шифрування та хешування. У результаті сформовано теоретичну базу дослідження, яка визначає підходи до забезпечення захисту медичних інформаційних систем.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 2. ТЕХНОЛОГІЧНІ ЗАСАДИ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ, АРХІТЕКТУРА ПРОТОКОЛІВ ТА НОРМАТИВНЕ РЕГУЛЮВАННЯ МЕДИЧНИХ СЕРВІСІВ

2.1. Мережеві комунікації та архітектура протоколів медичних сервісів

У контексті функціонування мобільних застосунків сегмента е-здоров'я критично важливим є забезпечення безпечного обміну даними між клієнтською частиною (додатком на пристрої користувача) та серверною інфраструктурою власника застосунку. Дана взаємодія здійснюється через публічну мережу Інтернет, що детермінує необхідність суворого дотримання протоколів безпеки. Опис та аналіз мережевих комунікацій базується на шаруватих моделях, де кожен рівень (шар) виконує чітко визначені функції та оперує власним набором протоколів. У даному розділі розглянуто концептуальну модель стека протоколів та механізми забезпечення безпеки на різних рівнях.

2.1.1. Архітектура мережевих рівнів

Найбільш релевантною моделлю для опису сучасних комп'ютерних мереж та інтернету є модель TCP/IP. Ця модель ієрархічно структурує процес мережевої комунікації, виділяючи п'ять функціональних рівнів:

- Фізичний рівень (Physical layer)
- Канальний рівень (Data Link layer)
- Мережевий рівень (Network layer)
- Транспортний рівень (Transport layer)
- Прикладний рівень (Application layer)

Кожен рівень імплементує певні протоколи — сукупність стандартизованих правил, що регламентують взаємодію між кореспондентами, забезпечуючи сумісність та взаєморозуміння систем.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		

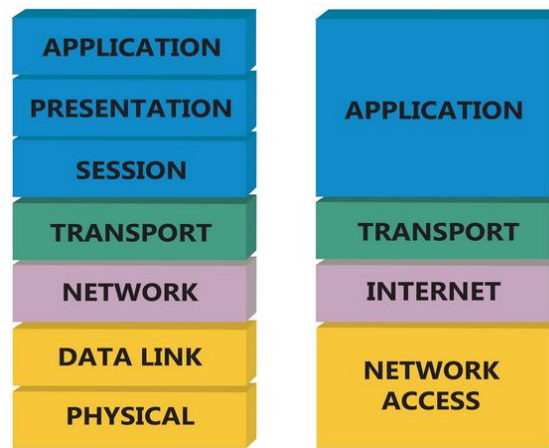


Рисунок 2.1 – OSI та TCP/IP моделі

У межах даної роботи аналізу підлягають рівні, починаючи з мережевого.

Мережевий рівень відповідає за організацію даних у пакети та забезпечення їхньої доставки через транзитні системи та гетерогенні мережі до кінцевого одержувача. Функціонал цього рівня включає маршрутизацію та логічну адресацію. Базовим протоколом даного рівня є Інтернет-протокол (IP — Internet Protocol).

Транспортний рівень гарантує доставку цілісного повідомлення відповідному процесу (порту) на кінцевому вузлі. У зв'язку з обмеженням максимального розміру блоку даних (MTU), що може бути переданий фізичною мережею, на цьому рівні здійснюється сегментація вихідного повідомлення на менші пакети та їхня подальша реасемблюваність на стороні отримувача. Основними протоколами транспортного рівня є Протокол керування передачею (TCP — Transmission Control Protocol), що забезпечує надійну доставку з встановленням з'єднання, та Протокол користувацьких дейтаграм (UDP — User Datagram Protocol), орієнтований на швидкість без гарантії доставки.

Критично важливим для безпеки є те, що поверх протоколу TCP може бути імплементований протокол Transport Layer Security (TLS), який забезпечує механізми криптографічного захисту, включаючи шифрування

даних, контроль цілісності та автентифікацію сторін.

Прикладний рівень є верхнім рівнем моделі TCP/IP і слугує інтерфейсом між мережевою інфраструктурою та кінцевим програмним забезпеченням (застосунком). Він регламентує формати представлення даних (бітів) системами, забезпечуючи їхню коректну інтерпретацію різнорідними обчислювальними архітектурами. Протоколи цього рівня (наприклад, HTTP/HTTPS) безпосередньо взаємодіють з логікою застосунку е-здоров'я.

2.1.2. Протокол захисту транспортного рівня (TLS)

Протокол Transport Layer Security (TLS) є клієнт-серверним протоколом безпеки, що функціонує між транспортним та прикладним рівнями моделі TCP/IP. Основним цільовим призначенням TLS є забезпечення автентифікації кореспондентів, конфіденційності та цілісності передаваних даних. Архітектурно TLS являє собою ієрархічну структуру, що складається з двох основних рівнів.



Рисунок 2.2 – Рівні протоколів та підпротоколів

Нижній рівень представлений протоколом запису TLS (TLS Record)

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		30

Protocol). Він відповідає за фрагментацію даних, їх стиснення та криптографічне перетворення (шифрування) інформації, що надходить від протоколів вищого рівня. TLS Record Protocol функціонує безпосередньо над надійним транспортним протоколом, як-от TCP.

Верхній рівень складається з чотирьох спеціалізованих підпротоколів:

- Протокол встановлення зв'язку (TLS Handshake Protocol): забезпечує процедуру початкового узгодження параметрів безпеки та автентифікацію сторін.

- Протокол зміни специфікації шифру (TLS Change Cipher Spec Protocol): сигналізує про перехід на використання узгоджених криптографічних параметрів та стратегій шифрування.

- Протокол попередження (TLS Alert Protocol): призначений для передачі повідомлень про помилки або критичні стани з'єднання.

- Протокол даних прикладного рівня (TLS Application Data Protocol): здійснює безпечне транспортування корисної інформації застосунку.

Процес ініціації сесії розпочинається з повідомлення `client_hello`, що містить версію протоколу, випадкове число (`client random`), ідентифікатор сесії та перелік підтримуваних наборів шифрів (`cipher suites`). Набори шифрів детермінують алгоритми асиметричного та симетричного шифрування, а також хеш-функції, сумісні з клієнтською стороною.

Серверна сторона відповідає повідомленням `server_hello`, обираючи найвищу спільну версію протоколу та оптимальний набір шифрів. Прикладом структури набору шифрів є `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`, де:

- ECDHE — алгоритм обміну ключами;
- RSA — метод верифікації цифрових сертифікатів;
- AES_256_GCM — алгоритм симетричного шифрування з автентифікацією;
- SHA384 — функція контролю цілісності.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		

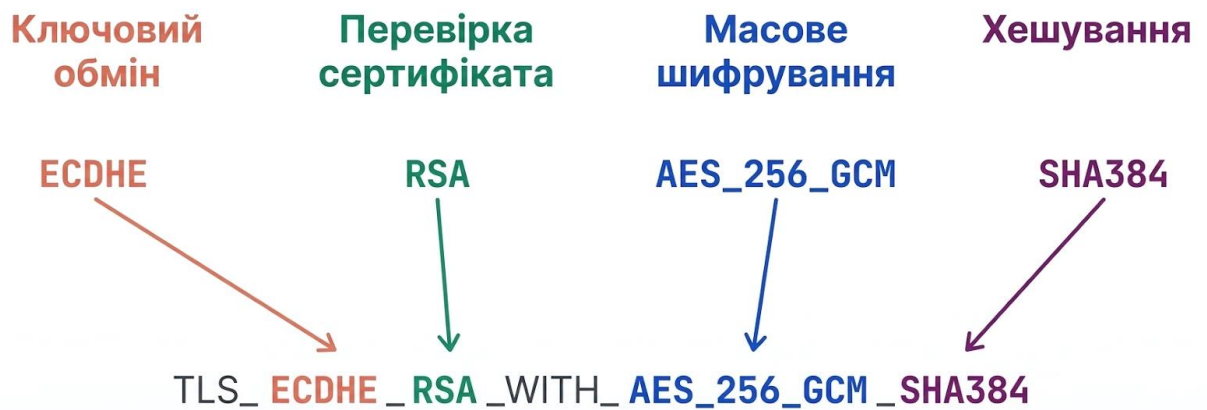


Рисунок 2.3 - Набори шифрів визначають криптографічні алгоритми, що застосовуються для обміну ключами, верифікації, шифрування та хешування

Після обміну відкритими ключами та верифікації серверного сертифіката сторони генерують спільний «головний секрет» (master prime secret). Процедура завершується обміном повідомленнями `change_cipher_spec` та `finished`, що підтверджує коректність обчислених ключів.

Після завершення фази встановлення зв'язку керування передається протоколу запису. У класичній схемі до кожного блоку даних додається код автентифікації повідомлення (MAC — Message Authentication Code), що генерується на основі секретного ключа, порядкового номера та змісту пакета. Це унеможливорює непомітну модифікацію даних під час транзиту.

У сучасних ітераціях протоколу (TLS 1.2 та 1.3) перевага надається алгоритмам Authenticated Encryption with Associated Data (AEAD), зокрема AES-GCM. Дані алгоритми інтегрують функції конфіденційності та автентифікації в єдиний криптографічний процес, формуючи спеціальний тег автентифікації. Це забезпечує високу стійкість до випадкових викривлень та цілеспрямованих атак на цілісність інформаційного потоку.

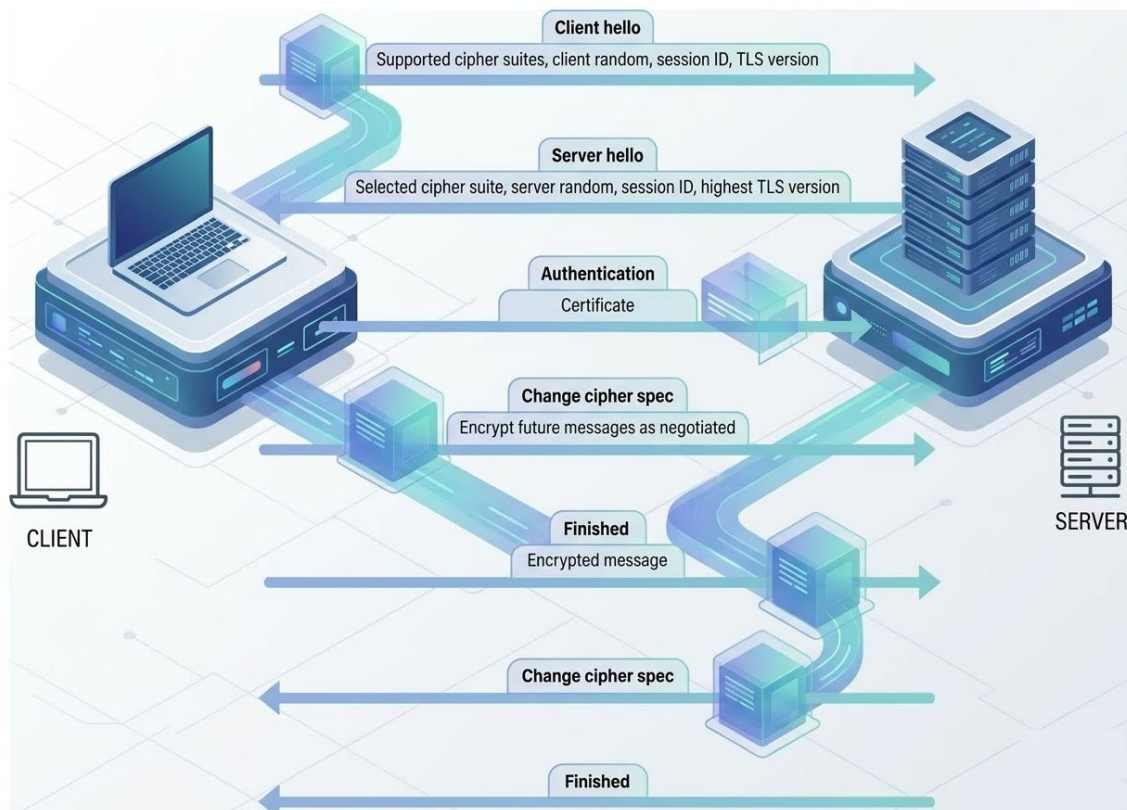


Рисунок 2.4 –Процес встановлення захищеного сеансу зв’язку між клієнтом та сервером за протоколом TLS

На представленому рисунку 2.4 візуалізовано поетапний процес встановлення захищеного сеансу зв’язку між клієнтом та сервером за протоколом TLS (Transport Layer Security). Алгоритм взаємодії базується на послідовному обміні службовими повідомленнями для узгодження параметрів безпеки.

Процедура ініціалізується клієнтською стороною через повідомлення Client hello, у якому передаються доступні набори шифрів (cipher suites), випадкове число (client random), ідентифікатор сесії та підтримувана версія протоколу. У відповідь сервер надсилає Server hello, обираючи оптимальний набір шифрів та версію TLS, а також генерує власне випадкове число (server random).

Наступним критичним етапом є фаза автентифікації (Authentication), під час якої сервер надає свій цифровий сертифікат для підтвердження легітимності вузла. Після верифікації та обміну ключами відбувається

перехід до фіналізації з'єднання. Повідомлення Change cipher spec сигналізує про те, що всі наступні інформаційні пакети будуть зашифровані згідно з узгодженими раніше параметрами.

Завершення фази підтверджується повідомленням Finished, яке містить зашифровані дані для перевірки цілісності та коректності встановлених ключів обома сторонами. Після успішного обміну цими повідомленнями канал вважається захищеним і готовим до передачі даних прикладного рівня.

2.1.3. Протокол керування передачею (TCP)

Transmission Control Protocol (TCP) є фундаментальним протоколом транспортного рівня, що забезпечує надійну, орієнтовану на з'єднання передачу даних. Основними функціями TCP є гарантована доставка сегментів повідомлення у вихідній послідовності та верифікація цілісності інформаційного потоку. Функціонування протоколу базується на клієнт-серверній моделі, де ініціатором з'єднання виступає клієнтський процес.

Встановлення логічного зв'язку між кореспондентами здійснюється за допомогою процедури three-way handshake, під час якої узгоджуються ключові параметри сесії.

Етапи встановлення з'єднання:

1. SYN (Synchronize).

Клієнт надсилає запит на встановлення з'єднання, встановлюючи прапор SYN у заголовку сегмента. Повідомлення містить початковий порядковий номер (ISN — Initial Sequence Number), згенерований випадковим чином. Цей номер є точкою відліку для подальшої нумерації сегментів, що дозволяє реконструювати цілісне повідомлення на стороні отримувача.

2. SYN-ACK (Synchronize-Acknowledgment).

У разі наявності вільних ресурсів сервер підтверджує запит, надсилаючи сегмент із встановленими прапорами SYN та ACK. На цьому етапі сервер транслює власний ISN, що детермінує можливість

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

двостороннього обміну даними.

3. ACK (Acknowledgment): Після отримання відповіді від сервера клієнт надсилає фінальне підтвердження. Завершення цього етапу сигналізує про успішне встановлення повнодуплексного надійного каналу зв'язку.

TCP забезпечує високу стійкість до втрат даних, проте імплементація механізмів контролю потоку та повторної передачі сегментів вимагає додаткових обчислювальних ресурсів та створює часові затримки.

У системах, де пріоритетною є мінімізація затримок (наприклад, потокова передача даних у реальному часі), альтернативою виступає протокол користувацьких дейтаграм (UDP — User Datagram Protocol). На відміну від TCP, UDP не передбачає встановлення з'єднання та не гарантує доставку сегментів. Хоча протокол імплементує механізм контрольної суми для базової перевірки помилок, він позбавлений засобів автоматичного відновлення втрачених даних, що робить його менш надійним, але більш продуктивним у специфічних сценаріях використання.

2.2. Архітектура мережевої взаємодії та аналіз вразливостей інформаційних каналів

2.2.1. Мережевий протокол IP

На мережевому рівні функціонування стека TCP/IP ключову роль відіграє Інтернет-протокол (IP), відповідальний за міжмережеву трансляцію даних. Актуальними є дві версії протоколу: IPv4 та IPv6. Ідентифікація вузлів та мережевих інтерфейсів здійснюється за допомогою унікальних IP-адрес.

Перехід до стандарту IPv6 зумовлений вичерпанням адресного простору IPv4 та необхідністю імплементації розширених механізмів безпеки (наприклад, вбудована підтримка IPsec). Формат адресації IPv4 базується на 32-бітній схемі, що традиційно представляється у вигляді чотирьох десяткових октетів (наприклад, 255.255.255.255). Натомість IPv6 оперує 128-бітною адресою, для запису якої використовується шістнадцяткова система

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

числення (наприклад, 345f:244f:576a:1456:1345:234b:865c:765c).

Процес інкапсуляції даних на мережевому рівні передбачає додавання IP-заголовка, що містить адреси джерела та призначення. Подальша маршрутизація пакетів здійснюється спеціалізованими вузлами — маршрутизаторами, які визначають оптимальний шлях через гетерогенні мережі на основі таблиць маршрутизації.

2.2.2. Система доменних імен

Попри те, що мережева ідентифікація базується на числових IP-адресах, для кінцевого користувача така система є непрактичною. Система доменних імен (DNS — Domain Name System) — це глобально розподілена ієрархічна база даних, що забезпечує відображення символьних доменних імен на відповідні їм IP-адреси. DNS функціонує як протокол прикладного рівня.

Процес перетворення імені в адресу називається резолуцією (resolution) і виконується системним компонентом — резолвером. Алгоритм пошуку передбачає першочергову перевірку локального кешу; у разі відсутності запису резолвер ініціює рекурсивні або ітеративні запити до ієрархічної структури DNS-серверів (кореневих, TLD та авторитетних серверів імен).

2.2.3. Класифікація загроз мережевій безпеці

Стабільність та конфіденційність систем мережевої комунікації піддаються впливу різноманітних векторів атак. У таблиці 2.1 наведено систематизацію основних типів кіберзагроз та їхніх характеристик.

Класифікація та опис мережевих атак

Тип атаки	Опис та механізм реалізації
Атака через побічні канали	Деструктивний аналіз фізичних параметрів функціонування вузла (споживання енергії, часові затримки, ЕМ-випромінювання) з метою компрометації криптографічних ключів.
Фізична атака	Прямий фізичний вплив на апаратне забезпечення, що призводить до відмови в обслуговуванні (DoS).
Атака зниження рівня (Downgrade)	Примусове переведення протоколу на використання застарілих або слабких криптографічних алгоритмів.
Атака методом «грубої сили» (Brute-force)	Вичерпний перебір усіх можливих комбінацій значень для зламу автентифікації або дешифрування.
Перехоплення (Eavesdropping)	Несанкціонований моніторинг трафіку для аналізу патернів комунікації та збору конфіденційної інформації.
«Людина посередині» (MITM)	Перехоплення та потенційна модифікація даних зломисником, який непомітно для сторін вбудовується в канал зв'язку.
Створення перешкод (Jamming)	Генерація шумів у бездротових діапазонах для блокування передачі сигналів (різновид DoS-атаки).
Атака повторного відтворення	Несанкціоноване захоплення легітимного повідомлення та його повторна трансляція для імітації автентичного відправника.
Маршрутні атаки	Маніпуляція таблицями маршрутизації для створення петель, хибних маршрутів або втрати пакетів.
Шкідливе ПЗ (Віруси, хробаки)	Програмні засоби, здатні до самореплікації та деструктивного впливу на цілісність і доступність мережевих ресурсів.
Тип атаки	Опис та механізм реалізації

2.3. Технологія бездротової передачі даних Bluetooth Low Energy для медичних сервісів

У межах даної роботи взаємодія між смарт-годинником та мобільним застосунком реалізується за допомогою протоколу Bluetooth Low Energy (BLE). Технологія Bluetooth є стандартом бездротового зв'язку, призначеним для організації енергоефективної комунікації малого радіуса дії між гетерогенними пристроями. Передача даних здійснюється за допомогою радіосигналів у неліцензованому діапазоні ISM (Industrial, Scientific, and Medical) на частоті 2,4 ГГц.

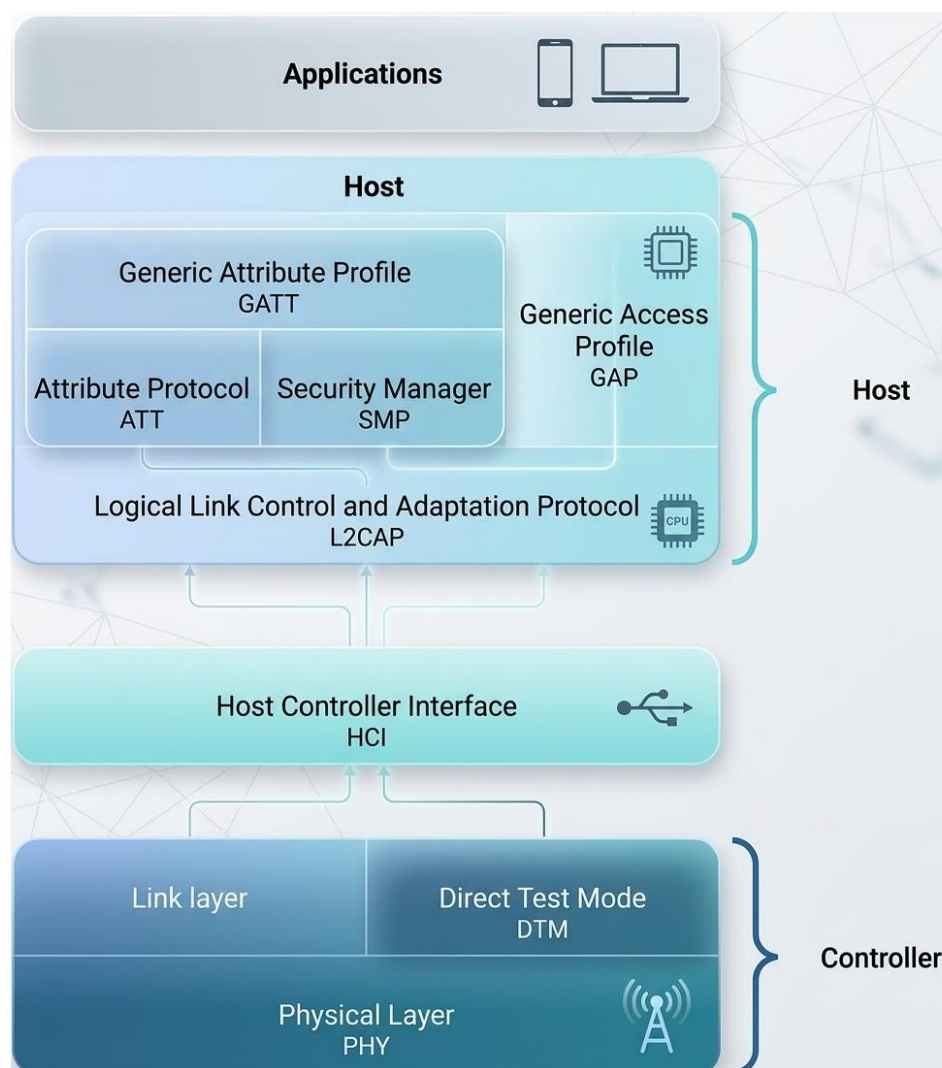


Рисунок 2.5 – Архітектура Bluetooth стеку

Специфікація Bluetooth Low Energy (BLE) оптимізована для систем, що потребують мінімального енергоспоживання при збереженні стабільності з'єднання. Дана характеристика є критично важливою для сегмента носійної електроніки (wearable devices), оскільки дозволяє суттєво продовжити термін автономної роботи сенсорів та медичних моніторів.

Архітектура BLE базується на багаторівневому стеку протоколів, структуру якого наведено на рисунку 2.5. З огляду на об'єкт дослідження, детальному аналізу підлягає лише рівень Менеджера безпеки (Security Manager — SM), оскільки він відповідає за криптографічні механізми, автентифікацію та захист даних від несанкціонованого доступу.

Функціональний опис інших рівнів стека (Physical Layer, Link Layer, L2CAP тощо) не є об'єктом даної роботи.

Рівень менеджера безпеки (Security Manager — SM) у стеку протоколів BLE детермінує логіку встановлення довіри між пристроями, забезпечуючи механізми спарювання (pairing), автентифікації та шифрування каналу зв'язку. Процес спарювання є фундаментальним для створення захищеного з'єднання і реалізується за допомогою одного з чотирьох методів, вибір якого залежить від апаратних можливостей вводу-виводу (IO Capabilities) обох вузлів.

Методологія спарювання пристроїв:

- Just Works застосовується у випадках, коли пристрої позбавлені засобів відображення або введення даних. Даний метод є найменш захищеним, оскільки не передбачає обміну паролями та не забезпечує резистентності до атак типу «людина посередині» (MITM).

- Numeric Comparison - передбачає генерацію обома пристроями ідентичних шестизначних значень підтвердження. Верифікація здійснюється користувачем; у разі невідповідності значень протокол негайно переривається.

- Passkey Entry - один із пристроїв генерує та відображає числовий код, який необхідно ввести на іншому вузлі для підтвердження легітимності сесії.

- Out of Band - використовує альтернативні інтерфейси зв'язку (наприклад, NFC) для передачі криптографічних параметрів, що значно підвищує рівень безпеки за рахунок обмеженого радіуса дії допоміжного каналу.

Процедура спарювання реалізується у три послідовні етапи:

Етап I. Узгодження параметрів (Pairing Feature Exchange). Кореспонденти обмінюються інформацією про свої ІО-можливості, вимоги до рівня автентифікації та специфікації ключів, які підлягають розповсюдженню.

Етап II. Автентифікація та генерація ключів (Short Term Key

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						39
Змн.	Арк.	№ докум.	Підпис	Дата		

Generation). На основі отриманих даних обирається відповідний метод спарювання. Сторони генерують ефемерні пари ключів (на основі алгоритму ECDH у версіях BLE 4.2+), здійснюють обмін відкритими ключами та проводять взаємну автентифікацію за допомогою криптографічних функцій підтвердження.

Етап III. Розповсюдження ключів (Transport Specific Key Distribution). На заключному, опціональному етапі, виконується обмін додатковими ключами, такими як ідентифікаційний ключ (IRK) для забезпечення приватності та ключ підпису (CSRK) для автентифікації даних на рівні АТТ.

Розглянемо нормативно-правове регулювання та стандарти кібербезпеки.

Експоненціальне зростання ролі цифрових технологій у різних сферах суспільних послуг зумовило розробку та впровадження комплексних регуляторних механізмів на національному та загальноєвропейському рівнях. У даному розділі проаналізовано ключові нормативні акти, що визначають мінімальні вимоги до забезпечення кібербезпеки медичних застосунків та програмного забезпечення (ПЗ). Визначені критерії слугуватимуть базисом для оцінки захищеності екосистеми та формування рекомендацій для моделі HHQA (Health Hardware Quality Assessment).

2.4. Загальний регламент захисту даних (GDPR)

Загальний регламент захисту даних (General Data Protection Regulation — GDPR) встановлює уніфіковані правила обробки та захисту персональних даних суб'єктів у межах ЄС. Згідно з положеннями регламенту, організації зобов'язані впроваджувати технології шифрування, псевдонімізації або анонімізації конфіденційної інформації. Ключовою вимогою є реалізація «належних технічних та організаційних заходів» для запобігання несанкціонованому доступу та інтерпретації персональних даних третіми сторонами.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4.1. Регламент медичних виробів (MDR)

Відповідно до регламенту медичних виробів (Medical Device Regulation — MDR), пристрої медичного призначення та їхні аксесуари, включно зі спеціалізованим програмним забезпеченням (SaMD — Software as a Medical Device), класифікуються як медичні вироби. MDR покладає на виробників обов'язок щодо створення системи постмаркетингового нагляду (Post-Market Surveillance — PMS), яка передбачає безперервний моніторинг безпеки та експлуатаційних характеристик продукту після його виходу на ринок.

Виробники мають забезпечити регулярне оновлення ПЗ та ідентифікацію потенційних ризиків, дотримуючись принципу «сучасного рівня техніки» (state-of-the-art). Архітектура пристроїв повинна бути спроектована таким чином, щоб мінімізувати кіберзагрози та унеможливити несанкціоноване втручання. Обов'язковою є документальна фіксація заходів із забезпечення цілісності, доступності та конфіденційності даних на всіх рівнях взаємодії компонентів системи.

2.4.2. Директива з мережевої та інформаційної безпеки (NIS2)

Директива NIS2 є засадничим європейським актом, що регламентує високий рівень кібербезпеки мереж та інформаційних систем. Норматив зобов'язує держави-члени ЄС забезпечити впровадження організаціями технічних заходів для нівелювання ризиків безпекових інцидентів та мінімізації їхніх наслідків.

У разі виникнення інциденту (порушення функціонування сервісів) організації повинні негайно інформувати відповідну Команду реагування на комп'ютерні інциденти (CSIRT). Кожна країна ЄС має забезпечити функціонування принаймні однієї CSIRT, яка виступає контактним центром для міжнародної співпраці та обміну інформацією про загрози.

Директива NIS2 акцентує на проактивному підході до безпеки, висуваючи наступні вимоги:

- розробка та дотримання політик використання криптографічних засобів і шифрування.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						41
Змн.	Арк.	№ докум.	Підпис	Дата		

- впровадження механізмів багатофакторної автентифікації (MFA), що передбачає використання кількох незалежних чинників підтвердження особи (наприклад, комбінації пароля та біометричних даних або динамічного PIN-коду).
- проведення регулярних оцінок ризиків та навчання персоналу з питань кібергігієни.
- наявність планів безперервності бізнес-процесів та управління операціями під час і після безпекових криз.

Аналіз таблиці 2.2 показує, що описувана екосистема імплементує концепцію Data Protection by Design (захист даних на етапі проектування). Використання стійких криптографічних протоколів на транспортному рівні (TLS) та рівні персональних мереж (BLE SM) безпосередньо задовольняє вимоги Статті 32 GDPR щодо технічних заходів безпеки та MDR щодо стійкості програмного забезпечення до кіберзагроз.

Таблиця 2.2

Відповідність функціоналу системи e-health вимогам GDPR та MDR

Категорія	Функціонал додатка/пристрою	Релевантна стаття GDPR	Релевантна стаття MDR (2017/745)
Захист даних при передачі	Використання протоколів TLS 1.3 для зв'язку з хмарою та BLE Secure Connections для синхронізації з годинником.	Ст. 32: Безпека обробки (вимога шифрування персональних даних).	Додаток I, розд. 17.2: Проектування пристроїв для забезпечення цілісності та конфіденційності.
Автентифікація користувача	Підтримка двофакторної автентифікації (2FA) та біометричного розблокування застосунку.	Ст. 5(1)(f): Цілісність та конфіденційність (захист від несанкціонованої обробки).	Додаток I, розд. 17.4: Захист від несанкціонованого доступу, що може загрожувати безпеці пристрою.
Керування доступом та правами	Можливість експорту медичних звітів у PDF та керування дозволами на поширення даних із лікарем.	Ст. 15: Право на доступ; Ст. 20: Право на мобільність даних.	Додаток I, розд. 23.4: Вимоги до інформації, що надається користувачеві (доступ до результатів вимірювання).

Життєвий цикл ПЗ	Регулярні оновлення прошивки (OTA) та патчі безпеки для мобільного застосунку.	Ст. 25: Захист даних на етапі проєктування та за замовчуванням.	Ст. 83-86: Постмаркетинговий нагляд (PMS); впровадження оновлень для мінімізації ризиків.
Зберігання даних	Хмарне зберігання на серверах у межах ЄС (відповідність суверенітету даних).	Ст. 44-46: Передача персональних даних до третіх країн або міжнародних організацій.	Додаток I, розд. 17.1: Надійність та продуктивність ПЗ у межах визначеного життєвого циклу.
Мінімізація даних	Збір лише тих показників, що необхідні для моніторингу стану здоров'я (ROP, сон, активність).	Ст. 5(1)(с): Мінімізація даних (обмеження збору необхідним обсягом).	Додаток I, розд. 1: Загальні принципи безпеки та продуктивності (мінімізація побічних ризиків).
Категорія	Функціонал додатка/пристрою	Релевантна стаття GDPR	Релевантна стаття MDR (2017/745)
Захист даних при передачі	Використання протоколів TLS 1.3 для зв'язку з хмарою та BLE Secure Connections для синхронізації з годинником.	Ст. 32: Безпека обробки (вимога шифрування персональних даних).	Додаток I, розд. 17.2: Проєктування пристроїв для забезпечення цілісності та конфіденційності.

2.5. Технологічна парадигма електронного медичного сервісу

Програмний комплекс «електронного здоров'я» являє собою платформу, розроблену для проактивного моніторингу соматичних показників та інтегрованого аналізу фізичної активності користувача. Архітектура застосунку базується на принципах превентивної медицини та біометричної аналітики, забезпечуючи безперервний цикл збору, обробки та візуалізації даних.

Центральним компонентом інтерфейсу є модуль «Сьогодні» (Today), який виконує роль агрегатора поточної інформації. Система здійснює кількісну оцінку локомоторної активності (кількість кроків) та енергетичних витрат організму (метаболічний еквівалент у калоріях). Окрему увагу приділено параметрам серцево-судинної системи та архітектурі сну, що

дозволяє проводити комплексну оцінку відновлювальних ресурсів організму.



Рисунок 2.6 – Вигляд додатку електронного медичного сервісу

Важливою складовою системи є блок візуалізації трендів. Використання методів графічної інтерпретації тижневих циклів активності дозволяє користувачеві відстежувати динаміку змін у довгостроковій перспективі. Така візуалізація не лише фіксує прогрес, а й слугує базисом для формування адаптивних алгоритмів досягнення цільових фізичних показників, що підвищує комплаєнс користувача щодо здорового способу життя.

Застосунок функціонує як ядро екосистеми підключених пристроїв. Модуль інтеграції з периферійним обладнанням забезпечує стабільну синхронізацію зі смарт-годинниками та іншими трекерами через захищені протоколи передачі даних. Система здійснює верифікацію статусу підключення та моніторинг енергоефективності термінальних пристроїв, що гарантує безперервність надходження первинних біометричних даних для подальшого аналізу.

Навігаційна модель застосунку структурована за ієрархічним

принципом, що забезпечує швидкий доступ до трьох фундаментальних рівнів даних:

- Timeline (Стрічка подій) - хронологічна фіксація активності та медичних подій.
- Dashboard (Панель показників): аналітика та синтез метрик здоров'я.
- Profile (Профіль): Персоналізація налаштувань та зберігання антропометричних параметрів.

Таким чином, застосунок «e-health» виступає як ефективний інструмент самоконтролю, що поєднує інтуїтивну доступність інтерфейсу з глибиною науково обґрунтованого аналізу даних, сприяючи формуванню усвідомленого підходу до управління персональним здоров'ям.

2.5.1. Опис протоколів передачі даних

Для забезпечення цілісності, конфіденційності та безперервності потоку біометричних даних у системі «e-health» використовується багаторівневий стек комунікаційних протоколів. Архітектура передачі даних розділена на два основні сегменти: локальний (PAN — Personal Area Network) та мережевий (WAN — Wide Area Network).

1. Локальний рівень: Bluetooth Low Energy (BLE)

Зв'язок між термінальним пристроєм (смарт-годинником) та мобільним шлюзом (смартфоном) базується на стандарті Bluetooth 4.0+ (Low Energy), що мінімізує енергоспоживання при збереженні високої надійності.

GAP (Generic Access Profile) - визначає ролі пристроїв. Смарт-годинник виступає як периферійний пристрій, що транслює рекламні пакети, а смартфон — як центральний пристрій, що ініціює з'єднання.

GATT (Generic Attribute Profile) - використовується для ієрархічної структуризації даних. Показники серцевого ритму, сатурації та кроків групуються у відповідні сервіси (Services) та характеристики (Characteristics).

- Security Manager (SM) - забезпечує автентифікацію та шифрування на рівні каналу зв'язку, запобігаючи перехопленню даних (MITM-атаки) під час

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

первинного сполучення (Pairing).

2. Мережевий рівень: Стек TCP/IP та DNS

Після агрегації даних смартфоном вони інкапсулюються для передачі на віддалені сервери аналітики.

DNS (Domain Name System) здійснює розрішення доменних імен (наприклад, api.e-health.net) в IP-адреси цільових серверів.

TCP (Transmission Control Protocol) забезпечує гарантовану доставку пакетів даних. У контексті медичної інформації це критично важливо, оскільки втрата навіть невеликого сегмента часового ряду може призвести до некоректної діагностичної інтерпретації.

3. Рівень безпеки: TLS (Transport Layer Security)

Для захисту персональних та медичних даних при передачі через відкриті мережі використовується протокол TLS.

Handshake Protocol здійснює обмін ключами за алгоритмом ECDHE (Elliptic Curve Diffie-Hellman) та автентифікацію сервера за допомогою сертифікатів RSA/ECDSA. Це гарантує, що дані надсилаються саме на легітимний сервер «e-health».

Record Protocol виконує масове шифрування даних за допомогою симетричних алгоритмів (наприклад, AES-256-GCM), забезпечуючи цілісність кожного пакета через механізми хешування (SHA-384).

4. Прикладний рівень: REST API та JSON

На верхньому рівні взаємодія відбувається через архітектурний стиль REST (Representational State Transfer). HTTPS використовує методи POST для передачі нових біометричних записів та GET для синхронізації історичних даних із хмарного сховища. JSON слугує форматом серіалізації даних. Завдяки своїй легкості та структурованості, JSON дозволяє ефективно описувати складні об'єкти, такі як графіки активності або параметри фаз сну, забезпечуючи швидку парсинг-обробку як на стороні клієнта, так і на сервері.

Ця багаторівнева модель забезпечує високу відмовостійкість системи та відповідність сучасним стандартам безпеки медичних даних (таких як

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						46
Змн.	Арк.	№ докум.	Підпис	Дата		

GDPR або HIPAA).

2.5.2. Структура пакету передачі медичних даних

Наведемо приклад структури JSON-пакета, який використовується для серіалізації даних про серцевий ритм. У системі такий пакет формується мобільним додатком після отримання сирих даних від смарт-годинника через BLE і готується до відправки на сервер через захищений TLS-канал.

Приклад структури JSON-пакета подано на рисунку 2.7.

```
{
  "header": {
    "version": "1.0",
    "message_id": "550e8400-e29b-41d4-a716-446655440000",
    "timestamp": "2026-03-17T11:53:30Z",
    "user_uuid": "auth0|6123abcd4567efgh"
  },
  "device_metadata": {
    "device_model": "e-health Watch S2",
    "firmware_version": "v2.4.1",
    "battery_level": 78,
    "connection_type": "BLE_5.0"
  },
  "payload": {
    "metric_type": "heart_rate",
    "unit": "bpm",
    "data_points": [
      {
        "time": "2026-03-17T11:50:00Z",
        "value": 72,
        "quality_index": 0.98
      },
      {
        "time": "2026-03-17T11:51:00Z",
        "value": 75,
        "quality_index": 0.95
      }
    ]
  }
}
```

Рисунок 2.7 - Структура JSON-пакета передачі медичних даних

```
],
  "statistics": {
    "min": 70,
    "max": 82,
    "avg": 74.5
  },
  "security_tag": "sha256-hash-value"
}
```

Рисунок 2.8 - Структура JSON-пакета передачі медичних даних (закінчення)

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

Виконаємо семантичний опис полів.

Блок header:

- message_id - унікальний ідентифікатор транзакції (UUID), що дозволяє уникнути дублювання записів у базі даних (ідемпотентність).
- timestamp - час формування пакета у форматі ISO 8601.
- user_uuid - знеособлений ідентифікатор користувача, отриманий після успішної автентифікації.

Блок device_metadata містить технічну інформацію про джерело даних. Це важливо для корекції алгоритмів аналізу, оскільки різні сенсори мають різну похибку.

Блок payload:

- metric_type та unit - визначають контекст даних (частота серцевих скорочень у ударах за хвилину).
- data_points - масив об'єктів, де кожне значення має свій часовий штамп.
- quality_index - показник достовірності сигналу (від 0 до 1). Якщо під час заміру користувач рухався, індекс буде низьким, і система може ігнорувати цей замір як артефакт.

Блок security_tag містить контрольну суму або цифровий підпис пакета, що перевіряється сервером для підтвердження того, що дані не були модифіковані після формування в додатку.

Процес обробки та передачі наступний. При натисканні кнопки синхронізації або у фоновому режимі відбуваються такі етапи:

1. Серіалізація: Об'єкт даних у пам'яті смартфона перетворюється на цей текстовий рядок JSON.
2. Стиснення (опціонально): Для економії трафіку пакет може бути стиснений алгоритмом GZIP.
3. Інкапсуляція в HTTPS: JSON-текст стає "тілом" (Body) HTTP-запиту: POST /api/v1/sync/metrics.
4. Шифрування TLS: Весь HTTP-пакет шифрується на транспортному

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						48
Змн.	Арк.	№ докум.	Підпис	Дата		

рівні (алгоритмом AES-256), про який ми говорили раніше.

Цей підхід дозволяє системі бути гнучкою: якщо в майбутньому годинник почне вимірювати, наприклад, рівень кисню в крові (SpO2), структура JSON залишиться майже незмінною, додасться лише новий `metric_type`.

2.6 Висновки по розділу

У другому розділі досліджено технологічні засади мережевої взаємодії та архітектуру протоколів, що використовуються в електронних медичних сервісах. Встановлено, що базові мережеві протоколи, зокрема TCP/IP, DNS і TLS, є критично важливими для забезпечення надійної передачі даних, але водночас містять потенційні вразливості. Проаналізовано ключові загрози мережевій безпеці, включаючи атаки на транспортному рівні, підміну DNS-запитів та перехоплення трафіку. Окремо досліджено специфіку застосування технології Bluetooth Low Energy, яка, попри свою ефективність, потребує додаткових заходів захисту. Також узагальнено вимоги нормативно-правових актів, що регламентують обробку медичних даних, що дозволило визначити основні принципи побудови безпечних медичних сервісів.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		49

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ ЗАГРОЗ БЕЗПЕКИ ЗАСТОСУВАНЬ ЕЛЕКТРОННИХ МЕДИЧНИХ СЕРВІСІВ

3.1. Аналіз мережевих комунікацій

Для оцінки рівня захищеності сучасних систем мобільного моніторингу показників здоров'я було проведено комплексне дослідження екосистеми, що включає мобільний застосунок та смарт-годинник (див. рис. 1.1). Основний фокус експерименту спрямований на аналіз протоколів комунікації між апаратним забезпеченням (годинником), клієнтським застосником (смартфоном) та серверною інфраструктурою виробника. У даному розділі наведено опис методології проведення тестування, технічні умови експерименту та отримані результати.

Для детермінованого аналізу взаємодії між мобільним застосунком та хмарними серверами було застосовано спеціалізоване програмне забезпечення для аналізу мережевих протоколів — Wireshark. Даний інструментарій дозволяє здійснювати перехоплення та детальну інспекцію мережевого трафіку в режимі реального часу. В межах експерименту було зафіксовано чотири окремі сесії передачі даних, під час яких здійснювався активний моніторинг температури тіла та частоти серцевих скорочень (ЧСС) за допомогою сенсорів годинника.

Технічна конфігурація середовища для перехоплення пакетів між застосунком та сервером була реалізована з урахуванням архітектурних особливостей інструменту Wireshark. Оскільки мережевий аналізатор фіксує трафік лише через інтерфейси хоста, на якому він інстальований, було застосовано метод транзитної точки доступу.

Для реалізації даної схеми на ноутбучі, що виконував роль аналізатора, була сконфігурована віртуальна Wi-Fi точка доступу, до якої підключався

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

смартфон із цільовим програмним забезпеченням. Така архітектура дозволила перенаправити весь вхідний та вихідний трафік смартфона через мережевий стек ноутбука, забезпечуючи можливість повного захоплення пакетів без необхідності модифікації апаратного забезпечення або встановлення додаткових прав доступу (root) на смартфоні.

У наступних підрозділах наведено результати аналізу отриманих дамтів трафіку, зокрема перевірку параметрів шифрування, цілісності пакетів та автентифікації сесій.

3.2. Аналіз DNS-трафіку та ідентифікація вузлів

Відповідно до теоретичних засад, викладених у другому розділі, мережева ідентифікація вузлів у стеку протоколів TCP/IP базується на використанні унікальних IP-адрес. Процес встановлення з'єднання між мобільним застосунком та серверною інфраструктурою потребує попередньої резолуції доменних імен у відповідні числові ідентифікатори. Використання протоколу DNS (Domain Name System) дозволяє трансформувати людиночитане доменне ім'я (наприклад, e-health.com) у легітимну IP-адресу, що є необхідною умовою для подальшого аналізу та фільтрації мережевого трафіку.

З метою сегрегації цільового трафіку у середовищі Wireshark було застосовано фільтрацію DNS-запитів (Queries) та відповідей (Responses), що містять субрядок «e-health». Результати цієї операції, представлені на рисунку 3.1, демонструють активність резолвера під час ініціації сесій.

В ході аналізу було ідентифіковано три унікальні IPv4-адреси, асоційовані з сервісами додатку моніторингу здоров'я: 89.30.121.150, 89.30.121.170, 89.30.121.180.

Виявлення цих адрес дозволяє надалі сфокусувати увагу на інспектуванні виключно тих TCP-потоків, які спрямовані до зазначених вузлів, що значно спрощує аналіз криптографічних параметрів TLS-з'єднань.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

No.	Info
37	Standard query 0xdc43 A scalews.e-health.net
38	Standard query response 0xdc43 A scalews.e-health.net A 89.30.121.170
55	Standard query 0x98db A prod.rudderstack.e-health.net
56	Standard query response 0x98db A prod.rudderstack.e-health.net CNAME front.e-health.com A 89.30.121.150
97	Standard query 0x2e04 A static.e-health.com
101	Standard query response 0x2e04 A static.e-health.com CNAME cdn-eu.e-health.net A 89.30.121.180
3866	Standard query 0x4327 A prod.rudderstack.e-health.net
3870	Standard query response 0x4327 A prod.rudderstack.e-health.net CNAME front.e-health.com A 89.30.121.150
6709	Standard query 0x3b56 A prod.rudderstack.e-health.net
6710	Standard query 0x3b56 A prod.rudderstack.e-health.net
6711	Standard query response 0x3b56 A prod.rudderstack.e-health.net CNAME front.e-health.com A 89.30.121.150
6713	Standard query response 0x3b56 A prod.rudderstack.e-health.net CNAME front.e-health.com A 89.30.121.150

Рисунок 3.1 - Пакети, передані за протоколом DNS

Одне із захоплених (handshakes) представлено на рисунку 3.2. Детальна інформація щодо перших двох пакетів наведена на рисунках 3.3 та 3.4.

No.	Protocol	Info
39	TCP	61977 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=2520752998 TSecr=0 WS=1024
40	TCP	443 → 61977 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
41	TCP	61977 → 443 [ACK] Seq=1 Ack=1 Win=88064 Len=0

Рисунок 3.2. - Three-way handshake протоколу TCP між мобільним застосунком та одним із серверів

Transmission Control Protocol, Src Port: 61977, Dst Port: 443, Seq: 0, Len: 0
Source Port: 61977
Destination Port: 443
[Stream index: 1]
▶ [Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2667688043
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 = Header Length: 40 bytes (10)
▶ Flags: 0x002 (SYN)
Window: 65535
[Calculated window size: 65535]
Checksum: 0x8589 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
▼ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
▶ TCP Option - Maximum segment size: 1460 bytes
▶ TCP Option - SACK permitted
▶ TCP Option - Timestamps: TSval 2520752998, TSecr 0
▶ TCP Option - No-Operation (NOP)
▶ TCP Option - Window scale: 10 (multiply by 1024)
▼ [Timestamps]
[Time since first frame in this TCP stream: 0.00000000 seconds]
[Time since previous frame in this TCP stream: 0.00000000 seconds]

Рисунок 3.3 - Запит на синхронізацію (SYN) від клієнтської сторони

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		52

```

Transmission Control Protocol, Src Port: 443, Dst Port: 61977, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 61977
  [Stream index: 1]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2640538704
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2667688044
  1000 .... = Header Length: 32 bytes (8)
  [Flags: 0x012 (SYN, ACK)]
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0xe18d [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    TCP Option - Maximum segment size: 1460 bytes
    TCP Option - No-Operation (NOP)
    TCP Option - No-Operation (NOP)
    TCP Option - SACK permitted
    TCP Option - No-Operation (NOP)
    TCP Option - Window scale: 7 (multiply by 128)
  [Timestamps]
    [Time since first frame in this TCP stream: 0.028385000 seconds]
    [Time since previous frame in this TCP stream: 0.028385000 seconds]
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 39]
    [The RTT to ACK the segment was: 0.028385000 seconds]
    [IRTT: 0.034413000 seconds]

```

Рисунок 3.4 - Відповідь сервера з підтвердженням синхронізації (SYN-ACK)

Поверх протоколу TCP протокол TLS забезпечує захищене з'єднання та шифрування даних. Це продемонстровано на рисунку 3.5.

```

  Internet Protocol Version 4, Src: 89.30.121.170, Dst:
  Transmission Control Protocol, Src Port: 443, Dst Port: 61977, Seq: 3783, Ack: 598, Len: 79
  Transport Layer Security

```

Рисунок 3.5 - Протокол IP здійснює доставку пакетів між IP-адресами, тоді як TCP забезпечує транспортування сегментів між процесами.

На рисунку 3.5 поверх протоколу TCP функціонує протокол TLS, що гарантує безпеку передачі.

Перед тим як сервер та застосунок зможуть розпочати обмін даними, необхідно виконати процедуру встановлення зв'язку TLS (TLS handshake). На цьому етапі сервер і застосунок узгоджують параметри безпеки з'єднання, як було детально описано у другому розділі. На рисунку 3.6 представлено загальний огляд процесу квітування між сервером та клієнтом. Останні два пакети демонструють перехід до протоколу даних прикладного рівня (Application Data Protocol), за допомогою якого здійснюється безпосередня передача корисної інформації застосунку.

No.	Info
820	Client Hello (SNI=scalews.e-health.net)
821	Server Hello
822	Certificate
823	Certificate Status, Server Key Exchange, Server Hello Done
827	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
828	Change Cipher Spec, Encrypted Handshake Message
829	Application Data
831	Application Data

Рисунок 3.6 - Пакети, виділені синім кольором, відображають процес TLS між сервером та клієнтом

Одним із параметрів, що узгоджуються під час встановлення з'єднання, є версія протоколу TLS, яку використовуватимуть обидві сторони. У повідомленні Client Hello клієнт пропонує найвищу версію TLS, яку він здатний підтримувати. У захопленому трафіку клієнт використовував як TLSv1.2, так і TLSv1.3, що продемонстровано на рисунку 3.7.

No.	Protocol	Info
2862	TLSv1.2	Application Data
50	TLSv1.3	Application Data

Рисунок 3.7 - Процес комунікації де використовувалися протоколи TLSv1.2 та TLSv1.3

Пошук пакетів, надісланих з іншими номерами версій, підтвердив, що в системі застосовуються лише ці дві ітерації протоколу. Ці версії є найбільш актуальними стандартами TLS на сьогодні. У той час як TLSv1.2 завжди передбачає повну процедуру full handshake, TLSv1.3 дозволяє застосовувати скорочене квітування для відновлення сесії за допомогою існуючого попередньо узгодженого ключа (pre-shared key). Саме такий механізм спостерігається для перших двох наборів шифрів (ciphersuites), наведених на рисунку 3.8. Протокол TLSv1.3 володіє розширеними функціями безпеки порівняно з попередніми версіями, проте TLSv1.2 все ще широко використовується і вважається безпечним згідно зі стандартами NCSC [22].

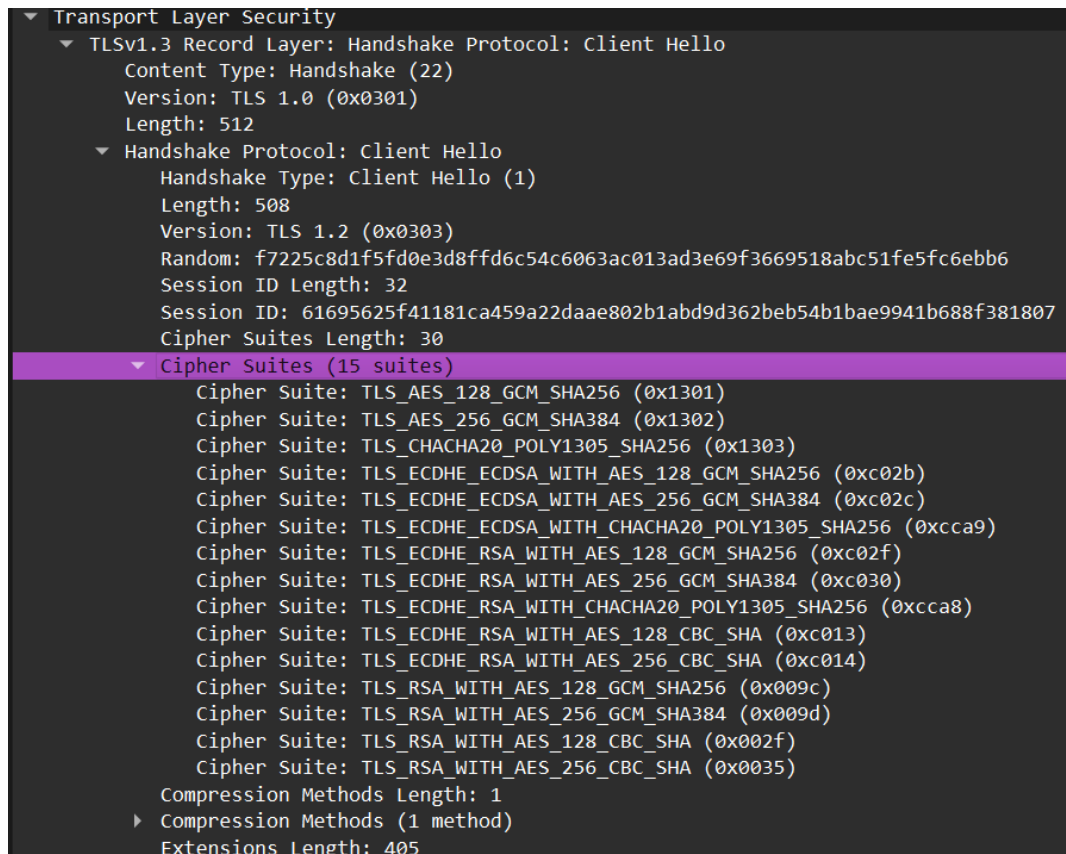


Рисунок 3.8 - Повідомлення Client Hello для протоколу TLSv1.3. Клієнт пропонує 15 наборів шифрів (cipher suites)

Нижче наведено детальний технічний аналіз структури повідомлення Client Hello, яке є першим кроком у встановленні захищеного з'єднання TLS (Handshake Protocol). Це повідомлення ініціюється клієнтом (смартфоном із додатком) і містить набір параметрів, необхідних для узгодження алгоритмів шифрування з сервером.

Повідомлення Client Hello є ключовим етапом фази узгодження (negotiation). Його основна мета — повідомити серверу про криптографічні можливості клієнта.

1. Поле Random

Це 32-байтове значення, яке генерується клієнтом. Зазвичай складається з 4 байтів поточного часу та 28 байтів, згенерованих криптографічно стійким генератором випадкових чисел (хоча в сучасних реалізаціях часто всі 32 байти є випадковими).

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

Це значення використовується пізніше обома сторонами для обчислення Master Secret — головного ключа, на основі якого створюються сеансові ключі для шифрування даних. Наявність поля Random запобігає «атакам повторного відтворення» (replay attacks), оскільки кожна сесія матиме унікальний ключ.

2. Поле Session ID

Це унікальний номер, який присвоюється конкретній сесії зв'язку. Якщо клієнт раніше вже встановлював з'єднання з цим сервером, він може відправити попередній Session ID, щоб пришвидшити процес Session Resumption. У новій версії протоколу це поле часто використовується для забезпечення зворотної сумісності з проміжними пристроями (middleboxes), які можуть не підтримувати TLS 1.3, або заповнюється випадковими даними, якщо сесія нова.

3. Поле Cipher Suites

Клієнт передає список підтримуваних комбінацій алгоритмів (наприклад, TLS_AES_256_GCM_SHA384), розташованих у порядку пріоритетності. Сервер обере найбільш безпечний варіант, який він також підтримує.

4. Поле Extensions

Це найбільш гнучка та важлива частина сучасного TLS-квітування. Розширення дозволяють додавати нові функції без зміни основного протоколу. Ключові розширення включають:

- Server Name Indication (SNI) - повідомляє серверу ім'я хоста (наприклад, v2.e-health.com), до якого звертається клієнт. Це критично для серверів, що хостять кілька сайтів на одній IP-адресі.

- Supported Versions - у TLS 1.3 це розширення вказує на перелік версій протоколу, які підтримує клієнт. Саме тут клієнт заявляє про готовність працювати з TLS 1.3.

- Key Share - містить відкриті ключі клієнта для алгоритму Діффі-Геллмана. Це дозволяє серверу обчислити спільний секрет уже після першої

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

відповіді, що значно пришвидшує з'єднання в TLS 1.3.

- Signature Algorithms - список алгоритмів цифрового підпису, які клієнт готовий перевіряти (наприклад, RSA-PSS або ECDSA).

Аналіз повідомлення Client Hello у даному трафіку дозволяє підтвердити, що додаток моніторингу здоров'я використовує сучасні методи захисту. Наявність розширення Key Share свідчить про використання TLS 1.3, що мінімізує затримки та підвищує стійкість до перехоплення порівняно з TLS 1.2.

Сервер відповідає повідомленням Server Hello, обираючи один із наборів шифрів (cipher suites), який він також здатний підтримувати. У всіх зафіксованих сесіях використовувався один із двох різних наборів шифрів. Набір TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 застосовується у випадках, коли комунікація здійснюється за протоколом TLSv1.2, а TLS_AES_256_GCM_SHA384 — при використанні протоколу TLSv1.3. Це продемонстровано на рисунках 3.9 та 3.10. Згідно зі стандартами, перший набір класифікується як «достатній» (sufficient), а другий — як «належний» (good), що підтверджує відповідність алгоритмів шифрування, хешування, перевірки сертифікатів та обміну ключами сучасним вимогам безпеки.

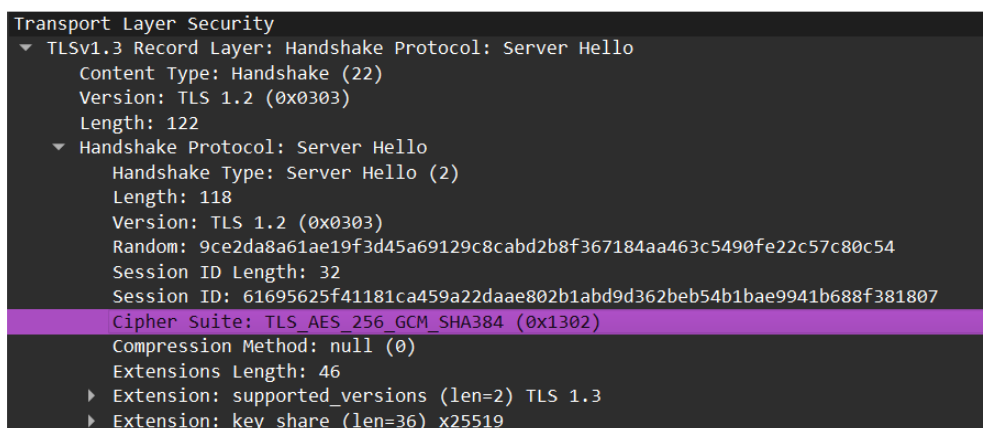


Рисунок 3.9 - Повідомлення Server Hello для протоколу TLSv1.3

Сервер незмінно обирає набір шифрів TLS_AES_256_GCM_SHA384 для цієї версії TLS.

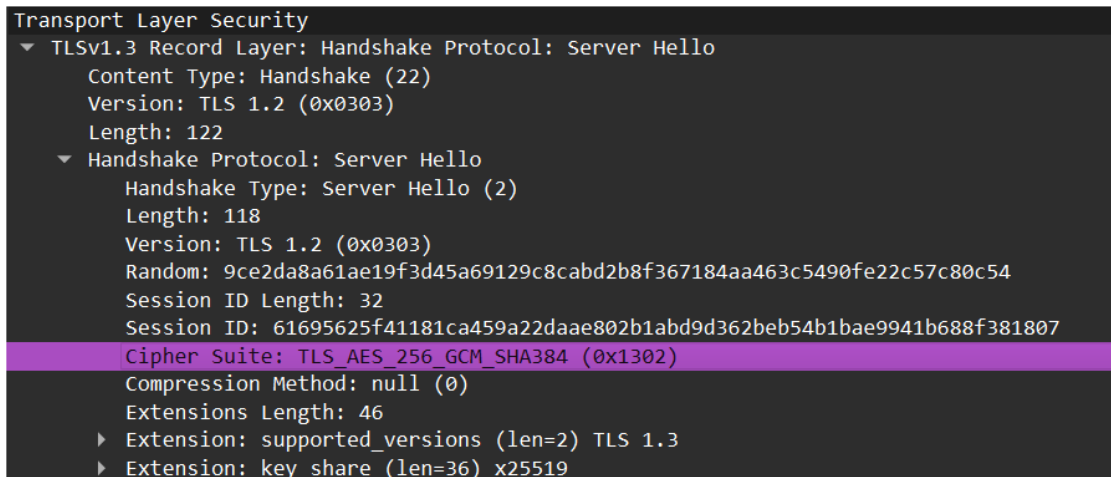


Рисунок 3.10 - Повідомлення Server Hello для протоколу TLSv1.2

Сервер незмінно обирає набір шифрів TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 для цієї версії TLS.

ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) забезпечує властивість Perfect Forward Secrecy (ідеальна пряма секретність). Це означає, що навіть якщо майбутній закритий ключ сервера буде скомпрометовано, минулі сесії не зможуть бути розшифровані. AES 256 GCM - сучасний стандарт симетричного шифрування, який одночасно забезпечує конфіденційність та автентичність даних (Authenticated Encryption). SHA384 - криптографічна хеш-функція, що використовується для перевірки цілісності повідомлень та підписів.

Під час процедури встановлення з'єднання (handshake) сторони, що взаємодіють, обмінюються випадковими значеннями (random values). У разі повторного використання цих значень зломисники можуть отримати можливість обійти механізми захисту TLS, наприклад, шляхом реалізації атаки повторного відтворення (replay attack). У всіх зафіксованих сесіях було передано 320 випадкових значень. Жодного дублювання виявлено не було, що підтверджує використання унікальних значень для кожної окремої сесії.

Після цього сервер надає свій сертифікат, який має бути підписаний довіреним центром сертифікації (Certificate Authority), як зазначалося у другому розділі.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

На рисунку 3.6 показано, що після обміну сертифікатами здійснюється процедура обміну ключами. Сервер і клієнт обмінюються своїми відкритими (публічними) ключами, крім того, сервер надає цифровий підпис. На рисунку 3.11 представлено повідомлення про обмін ключами від сервера, а на рисунку 3.12 — повідомлення про обмін відкритими ключами від сторони клієнта.

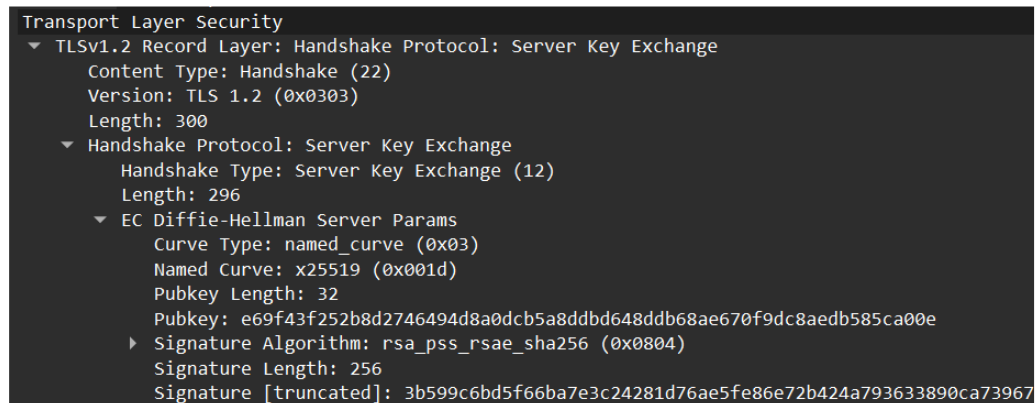


Рисунок 3.11 - Сервер передає клієнту свій відкритий ключ та цифровий підпис

Після того як клієнт передав свій ключ, він надсилає повідомлення Change Cipher Spec, що сигналізує про те, що всі наступні повідомлення будуть зашифровані з використанням узгоджених параметрів. Далі клієнт надсилає Encrypted Handshake Message, яке є зашифрованим повідомленням Finished. Сервер відповідає аналогічним повідомленням, а також надсилає власне зашифроване повідомлення про завершення (Encrypted Handshake Message). На цьому процедура встановлення зв'язку (handshake) завершується, після чого ініціюється протокол прикладних даних (application data protocol), як також продемонстровано на рисунку 3.6.

Параметри безпеки, що застосовувалися для TLS-з'єднання, відповідають стандартам, викладеним у другому розділі. Це свідчить про те, що протокол TLS забезпечує належний рівень захисту комунікації між застосунком електронної охорони здоров'я (e-health) та серверами.

```

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 37
  ▼ Handshake Protocol: Client Key Exchange
    Handshake Type: Client Key Exchange (16)
    Length: 33
    ▼ EC Diffie-Hellman Client Params
      Pubkey Length: 32
      Pubkey: e1d5d51394e7e3396e34b9ec56309058f1fe74918500bdb9a17b24b94328b809

```

Рисунок 3.12 - Клієнт передає свій відкритий ключ серверу

3.3. Дослідження комунікації за протоколом Bluetooth Low Energy

Детальний аналіз трафіку в межах технології Bluetooth не дозволив отримати вичерпних даних щодо прикладного рівня взаємодії. Це зумовлено технічними обмеженнями обраного методичного підходу, який базувався на використанні апаратного сніфера.

У ході експерименту вдалося зафіксувати мережеву активність виключно на каналному рівні (Link Layer). Отримані дампи трафіку підтверджують ініціацію процедури встановлення з'єднання з боку годинника, проте подальша передача пакетів, що стосуються безпосередньої роботи пристрою, не була детермінована в межах поточної конфігурації аналізатора.

Незважаючи на обмеженість перехоплених даних, було ідентифіковано критично важливий аспект безпеки — використання механізму парування за методом Passkey Entry. Згідно з отриманими даними, обидва вузли (смартфон із застосунком та годинник) мають відповідні I/O-можливості (Input/Output capabilities): пристрої здатні до візуалізації числового коду та підтримки інтерфейсу для його введення користувачем.

Застосування даного методу автентифікації значно підвищує стійкість комунікаційного каналу до атак типу «людина посередині» (Man-in-the-Middle, MitM), відповідно до теоретичних положень, викладених у другому розділі, оскільки виключає можливість несанкціонованого перехоплення ключа без фізичного доступу до інтерфейсів пристроїв.

Неможливість детального аналізу пакетів прикладного рівня після ініціації з'єднання між смартфоном та смарт-годинником зумовлена специфікою архітектури безпеки стека протоколів Bluetooth 5.x та апаратними обмеженнями використовуваного аналізатора. Основними чинниками, що перешкоджали дешифруванню трафіку, є:

1. Адаптивна зміна частот

Протокол BLE використовує 40 каналів у діапазоні 2,4 ГГц, з яких 37 призначені для передачі даних. Після встановлення з'єднання пристрої переходять у режим псевдовипадкової зміни частот.

Проблема полягає в тому, що якщо сніфер не перехопив пакет CONNECT_IND, що містить параметри Hop Increment та Channel Map, він не здатний синхронізуватися з послідовністю перемикання каналів, що призводить до повної втрати зв'язку з цільовою сесією на фізичному рівні.

2. Шифрування на рівні контролера

Використання методу парування Passkey Entry активує механізм безпечного з'єднання (LE Secure Connections), що базується на алгоритмі Діффі-Геллмана на еліптичних кривих (ECDH). Після успішної автентифікації генерується довгостроковий ключ (Long Term Key, LTK), який використовується для створення сеансових ключів шифрування. Оскільки шифрування відбувається на рівні контролера (Link Layer) за стандартом AES-CCM, дані стають недоступними для зовнішнього спостерігача. Без знання LTK або можливості перехопити процедуру обміну ключами в момент парування (що неможливо при використанні ECDH), сніфер бачить лише зашифровані PDU, які сприймаються як білий шум або некоректні пакети.

3. Використання приватних адрес

Для запобігання відстеженню пристрої застосовують механізм конфіденційності, що полягає в регулярній зміні MAC-адреси. Відповідно, якщо адреса змінилася під час експерименту, апаратний аналізатор, налаштований на конкретний ідентифікатор, втрачає цільовий пристрій,

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						61
Змн.	Арк.	№ докум.	Підпис	Дата		

фіксуючи лише загальний ефірний фон без прив'язки до досліджуваної сесії.

4. Апаратні обмеження

Хоча використовуваний пристрій є потужним інструментом, він має один радіомодуль. У щільному радіоефірі (за наявності інших Wi-Fi та Bluetooth пристроїв) ймовірність пропуску критично важливого пакета синхронізації значно зростає. Втрата лише одного пакета керування призводить до того, що аналізатор не може коректно інтерпретувати наступний потік даних.

Таким чином, відсутність даних прикладного рівня у захопленому BLE-трафіку є непрямим підтвердженням високої стійкості системи. Це свідчить про коректну імплементацію шифрування на рівні каналного рівня та ефективне використання механізмів автентифікації, що унеможливорює пасивне перехоплення конфіденційної медичної інформації за допомогою стандартного обладнання.

3.4. Систематизація кіберзагроз медичних даних на основі STRIDE моделі

На основі результатів мережевого аналізу, викладених у попередніх пунктах, розроблено модель загроз для екосистеми. На рисунку 3.13 представлено архітектурну схему системи, що включає пристрій, мобільний застосунок та серверну інфраструктуру. Комунікація між компонентами здійснюється за протоколами DNS, TLS та TCP.

На схемі (рис. 3.13) ідентифіковано критичні точки експлуатації:

Точка 1 - безпосередній вплив на апаратне забезпечення смарт-годинника.

Точка 2 - компрометація Bluetooth-з'єднання (BLE) між годинником та смартфоном.

Точка 3 - атака на рівні операційної системи або пам'яті смартфона.

Точка 4 - вплив на мережеву комунікацію між смартфоном та

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		62

серверами.

Точка 5 - пряма атака на серверну інфраструктуру виробника.

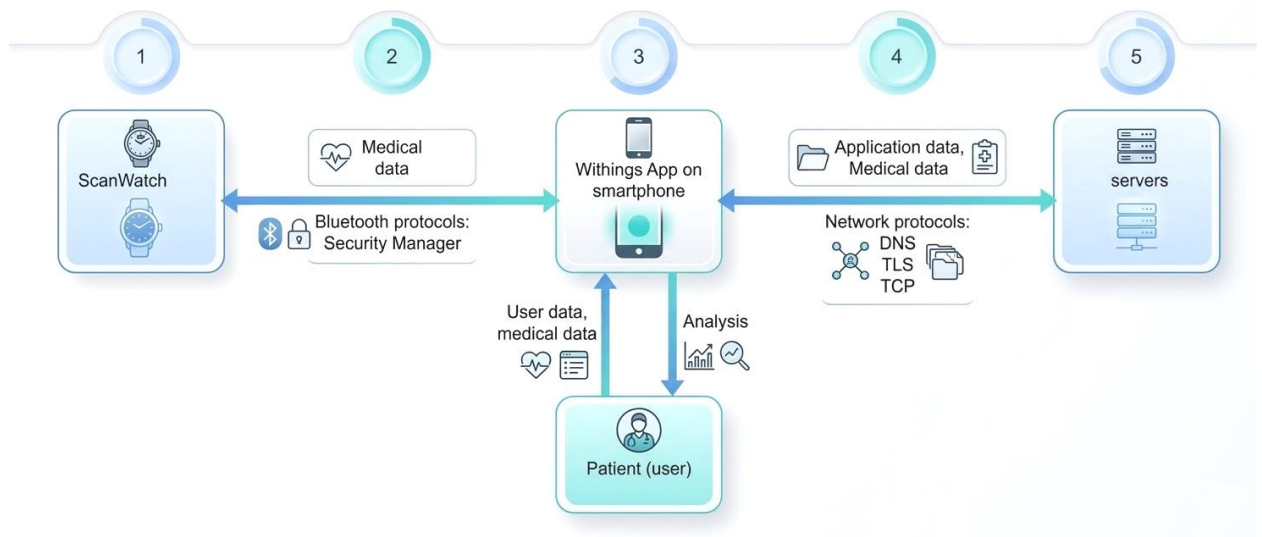


Рисунок 3.13 - Архітектурна схема системи обробки медичних даних

Для систематизації потенційних загроз використано методологію STRIDE, яка класифікує атаки за шістьма категоріями:

- Spoofing (Спуфінг) - фальсифікація ідентифікатора користувача або пристрою.
- Tampering (Підробка) - Несанкціонована модифікація даних або коду.
- Repudiation (Відмова) - Заперечення факту виконання операції.
- Information Disclosure (Розголошення інформації) - Порухення конфіденційності даних.
- Denial of Service (DoS) - Порухення доступності сервісів для легітимних користувачів.
- Elevation of Privilege (Підвищення привілеїв) - Отримання несанкціонованого рівня доступу.

У таблиці 3.1 наведено результати оцінки вразливості системи до різних типів атак з урахуванням захисних властивостей впровадженого протоколу TLS.

Таблиця 3.1 - Аналіз типів атак на мережеві комунікації екосистеми обробки медичних даних

Тип атаки	Категорія STRIDE	Точки експлуатації	Захист TLS
Атака через побічні канали	T	1, 3, 5	×
Фізична атака	T	1, 3, 5	×
Атака зі зниженням рівня	T	2, 4	✓
Атака методом «грубої сили»	R, I	2, 3, 4, 5	×
Перехоплення даних	I	2, 4	✓
Атака «людина посередині»	S, T, I	2, 4	✓
Радіоперешкоди	D	2, 4	×
Атаки повторного відтворення	T, R	2, 4	✓
Маршрутні атаки	T, D	4	×
Шкідливе ПЗ	T, D	1, 3, 5	×

Символ «✓» позначає наявність вбудованого механізму протидії в протоколі, «×» — вразливість на рівні протоколу (потребує додаткових заходів).

Проведемо аналітичний огляд результатів моделювання.

1. Фізичний та апаратний рівні. Атаки через побічні канали та пряме фізичне втручання вимагають безпосереднього доступу до обладнання. Згідно з деклараціями безпеки, центри обробки даних мають багаторівневий фізичний захист, що мінімізує ризики для точки 5. Дослідження стійкості апаратного забезпечення годинника (точка 1) до таких атак виходить за межі поточної роботи.

2. Мережева доступність. Атаки типу Jamming (радіоперешкоди) критично впливають на доступність (категорія D), проти якої TLS не забезпечує захисту. Однак реалізація таких атак потребує спеціалізованого радіообладнання та географічної близькості до об'єкта.

3. Роль TLS та набори шифрів. Впровадження TLS суттєво нівелює загрози перехоплення та підробки даних у каналах зв'язку (точки 2, 4). Стійкість до атак «грубої сили» прямо корелює з довжиною ключа та алгоритмом шифрування. Виявлене використання TLS 1.3 з наборами шифрів на базі AES-256 відповідає сучасним криптографічним стандартам.

Окрему увагу слід приділити атакам зі зниженням рівня (Downgrade). Їх запобігання можливе лише за умови повної деактивації застарілих алгоритмів на стороні сервера. Оскільки алгоритми на базі RSA для обміну ключами класифікуються NCSC як такі, що підлягають виведенню з експлуатації, очікується їх повне видалення з конфігурацій системи у найближчій перспективі для посилення безпеки.

4. Інфраструктурний захист. Протидія вірусному ПЗ та маршрутним атакам потребує інтеграції систем виявлення вторгнень (IDS/IPS), що є вектором для подальших досліджень у сфері безпеки IT-інфраструктури медичного призначення.

3.5. Оцінка відповідності системи обробки медичних даних принципам кібербезпеки та нормативним директивам

Основною метою проведеного кейс-стаді було комплексне дослідження механізмів автентифікації, шифрування та забезпечення цілісності даних у системі. У цьому підрозділі здійснюється верифікація теоретичних властивостей кібербезпеки та нормативних актів на основі отриманих експериментальних даних.

У таблиці 3.2 систематизовано аспекти кібербезпеки, що безпосередньо реалізовані в екосистемі.

Таблиця 3.2

Верифікація аспектів кібербезпеки в системі

Аспект кібербезпеки	Стан	Технічне обґрунтування та реалізація
Конфіденційність	✓	Забезпечується наскрізним шифруванням трафіку

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		65

		протоколом TLS. Використання виключно стійких наборів шифрів (наприклад, AES-256-GCM) гарантує захист від несанкціонованого дешифрування повідомлень.
Цілісність	✓	Реалізується через використання режиму автентифікованого шифрування з асоційованими даними (AEAD) в алгоритмі AES-GCM, що дозволяє виявляти будь-які модифікації пакетів.
Доступність	×	Безпосередньо не гарантується мережевими протоколами TLS/TCP, проте TLS опосередковано сприяє стійкості до атак Downgrade та MitM, що запобігає розриву сесій.
Автентифікація	✓	Здійснюється на основі сертифікатів, виданих довіреним центром (CA). Це дозволяє клієнту верифікувати справжність сервера та його відкритого ключа.
Авторизація	×	Визначається політиками доменного адміністрування та доступу до облікових записів, що не є предметом аналізу мережевого трафіку.
Відповідальність	×	Забезпечується на рівні прикладного ПЗ та ведення системних журналів (логів), для яких TLS слугує захищеним транспортом.
Симетричне шифрування	✓	Базується на галузевому стандарті AES-256-GCM, що є оптимальним за критеріями швидкодії та безпеки.
Хешування	✓	Використовується алгоритм SHA-384, що відповідає вимогам NIST щодо стійкості до колізій та знаходження прообразу.
Асиметричне шифрування	✓	Застосовується для безпечного обміну ключами через алгоритми ECDHE та RSA (у версії TLS 1.2).
Аспект кібербезпеки	Стан	Технічне обґрунтування та реалізація

Слід зазначити, що такі аспекти, як доступність, авторизація та відповідальність, виходять за межі функціоналу транспортних протоколів, проте імплементація TLS створює необхідний базис для їх коректного функціонування.

Наступним кроком є оцінка відповідності системи міжнародним та галузевим стандартам (таблиця 3.3).

Відповідність системи досліджуваної системи обробки медичних
даних міжнародним нормативним директивам

Директива / Стандарт	Стан відповідності
GDPR	Наявність сертифікації підтверджує впровадження організаційних та технічних заходів захисту персональних даних від несанкціонованого доступу.
MDR	Виконано вимоги щодо забезпечення цілісності та конфіденційності медичних даних. ПЗ відповідає критерію «state-of-the-art» завдяки використанню TLS версій 1.2 та 1.3.
NIS2	Реалізовано політику криптографічного захисту через TLS. Компанія декларує наявність плану відновлення (disaster recovery), проте відсутність обов'язкової двофакторної автентифікації (MFA) є потенційним вектором для покращення.
NCSC	Набори шифрів класифікуються як «Good» та «Sufficient». Використані криптографічні примітиви для обміну ключами, хешування та верифікації сертифікатів відповідають рекомендаціям щодо безпеки зв'язку.

Результати проведеного аналізу свідчать про те, що досліджувана система демонструє високий рівень відповідності сучасним вимогам кібербезпеки. Використання актуальних версій протоколу TLS та стійких криптографічних алгоритмів дозволяє ефективно нейтралізувати більшість мережових загроз, ідентифікованих у моделі STRIDE, забезпечуючи надійний захист конфіденційної інформації користувачів.

3.6. Інтеграція факторів кібербезпеки в модель HHQA

Метою даної роботи є розробка та обґрунтування детермінант кібербезпеки для їх подальшої інтеграції в модель HHQA (Home Healthcare Quality Assessment), зокрема в межах кластера «Застосунок е-охорони здоров'я». Ключовий акцент при формуванні цих факторів було зроблено на забезпеченні безпеки мережових комунікацій.

Запропоновані критерії базуються на результатах проведеного кейс-стаді, аналізі моделі загроз екосистеми додатку обробки медичних даних. Розроблені рекомендації у формі контрольного списку покликані надати

організаціям сфери охорони здоров'я інструментарій для верифікації мінімальних вимог безпеки, що безпосередньо корелює з підвищенням загальної якості медичних послуг.

Контрольний список факторів кібербезпеки для моделі ННQA:

- Використання криптографічних алгоритмів, стійких до відомих методів криптоаналізу.
- Забезпечення регулярного оновлення системного та прикладного програмного забезпечення.
- Впровадження валідованих сертифікатів відкритих ключів від довірених центрів сертифікації (CA).
- Наявність механізмів автентифікації під час процедури парування (pairing) периферійних пристроїв.
- Підтримка багатофакторної автентифікації (MFA) для доступу до конфіденційних даних.

Проведемо обґрунтування розроблених рекомендацій.

1. Стійкість криптографічних алгоритмів. Враховуючи динамічний характер кіберзагроз, криптографічна стійкість не є статичною властивістю. Як було показано на прикладі хеш-функції SHA-1, алгоритми з часом втрачають актуальність через виявлені вразливості. Аналіз трафіку підтвердив критичну важливість використання актуальних версій протоколу TLS (v1.3) та сучасних наборів шифрів. Підтримка сервером найвищої доступної версії протоколу є ключовим індикатором безпеки комунікаційного каналу.

2. Життєвий цикл програмного забезпечення. Регулярне оновлення ПЗ є обов'язковим індикатором адаптивності системи до стану «state-of-the-art» у криптографії. Це дозволяє вчасно усувати zero-day вразливості та оновлювати криптографічні бібліотеки відповідно до нових стандартів.

3. Автентифікація серверної інфраструктури. Довіра між мобільним застосунком та серверною частиною базується на процедурі TLS Handshake. Критичним аспектом тут є перевірка сертифіката відкритого ключа.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		68

Використання сертифікатів, підтверджує легітимність вузла зв'язку та мінімізує ризики підміни сервера.

4. Безпека локальних інтерфейсів зв'язку. Для взаємодії з носійними пристроями необхідно впроваджувати надійні методи автентифікації на етапі парування. У ході дослідження було ідентифіковано використання методу числового порівняння (Passkey Entry/Numeric Comparison), що, як зазначено у другому розділі, значно підвищує стійкість до активних атак типу «людина посередині» (MitM) у порівнянні зі спрощеними методами (Just Works).

5. Багатофакторна автентифікація (MFA). Дана рекомендація безпосередньо впливає з вимог директиви NIS2. Впровадження MFA (наприклад, поєднання пароля та одноразового коду) забезпечує додатковий рівень захисту особистої медичної інформації, гарантуючи доступ до системи лише авторизованим суб'єктам навіть у разі компрометації одного з ідентифікаторів.

3.7 Висновки по розділу

У третьому розділі проведено експериментальні дослідження мережових комунікацій та змодельовано загрози безпеки застосувань електронних медичних сервісів. Виконано аналіз мережевого та DNS-трафіку, що дозволило ідентифікувати потенційні точки компрометації та особливості взаємодії між компонентами системи. Дослідження протоколу Bluetooth Low Energy показало наявність вразливостей, пов'язаних із недостатнім рівнем автентифікації та захисту переданих даних. Систематизація загроз на основі моделі STRIDE дала змогу структурувати ризики та визначити відповідні механізми протидії. У підсумку інтеграція факторів кібербезпеки в модель оцінки якості підтвердила доцільність комплексного підходу до забезпечення безпеки та надійності електронних медичних сервісів.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У результаті виконання бакалаврської роботи було здійснено дослідження теоретичних, технологічних та прикладних аспектів забезпечення кібербезпеки застосувань електронних медичних сервісів, що функціонують у межах сучасної цифрової екосистеми охорони здоров'я. Отримані результати дозволяють сформулювати такі узагальнені висновки.

У першому розділі проведено системний аналіз предметної області захисту даних в електронних медичних сервісах. Встановлено, що впровадження гібридних моделей у сфері охорони здоров'я, які поєднують централізовані та розподілені підходи до обробки даних, супроводжується суттєвими викликами у сфері інформаційної безпеки, масштабованості та забезпечення якості сервісів. Запропонована методологія оцінки якості гібридних систем дозволяє враховувати як функціональні, так і нефункціональні характеристики, зокрема надійність, безпеку та продуктивність. У роботі детально розглянуто теоретичні аспекти кібербезпеки та мережевих комунікацій, що лежать в основі функціонування електронних медичних сервісів. Особливу увагу приділено криптографічним методам захисту інформації. Встановлено, що ефективне забезпечення конфіденційності, цілісності та автентичності медичних даних досягається шляхом комбінованого використання симетричного шифрування (для швидкої обробки великих обсягів даних), асиметричного шифрування (для безпечного обміну ключами) та криптографічного хешування.

У другому розділі досліджено технологічні засади мережевої взаємодії, архітектуру протоколів та нормативне регулювання у сфері електронних медичних сервісів. Встановлено, що базові мережеві протоколи, такі як TCP/IP, DNS та TLS, формують фундамент комунікаційної інфраструктури, проте одночасно є потенційними точками виникнення вразливостей. Проведений аналіз показав, що найбільш критичними є загрози, пов'язані з підміною DNS-запитів, перехопленням трафіку та атаками на транспортному

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						70
Змн.	Арк.	№ докум.	Підпис	Дата		

рівні. Особливу увагу приділено протоколу TLS як ключовому механізму захисту транспортного рівня. Доведено, що коректна конфігурація TLS, використання сучасних криптографічних алгоритмів та відмова від застарілих версій протоколу є критично важливими для забезпечення безпеки медичних сервісів. Також досліджено специфіку використання технології Bluetooth Low Energy, яка широко застосовується в медичних пристроях. Виявлено, що незважаючи на енергоефективність, BLE має ряд вразливостей, пов'язаних з автентифікацією та захистом каналів передачі даних.

У третьому розділі виконано експериментальні дослідження мережових комунікацій та змодельовано загрози безпеки застосувань електронних медичних сервісів. Проведений аналіз мережевого трафіку дозволив ідентифікувати ключові параметри взаємодії між компонентами системи та виявити потенційні точки компрометації. Дослідження DNS-трафіку підтвердило можливість використання методів аналізу доменних запитів для виявлення підозрілої активності та ідентифікації вузлів.

Систематизація кіберзагроз на основі моделі STRIDE дозволила структурувати потенційні ризики за категоріями та визначити відповідні заходи протидії. Це забезпечило формування комплексної моделі загроз, адаптованої до специфіки медичних інформаційних систем. Проведена оцінка відповідності системи принципам кібербезпеки та нормативним директивам підтвердила необхідність інтеграції безпеки на всіх етапах життєвого циклу програмного забезпечення.

Важливим результатом роботи є інтеграція факторів кібербезпеки в модель HHQA, що дозволяє підвищити рівень якості медичних сервісів шляхом врахування безпекових характеристик поряд із функціональними показниками. Це забезпечує комплексний підхід до оцінки ефективності системи та сприяє підвищенню довіри користувачів до електронних медичних сервісів

					БР.ІП – 12.00.00.000 ПЗ	Арк.
						71
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mansfield-Devine, S., & Godfrey, A. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, 48–52. Elsevier, Amsterdam. <https://doi.org/10.1016/j.maturitas.2018.04.008>
2. Abuabed, S., Naik, N., & Sharma, R. (2023). STRIDE-based threat modeling for healthcare systems. *Journal of Global Humanities and Social Sciences*, 6(3), 112–124. Bon Future Press, London.
3. Shahzadi, S., Khan, M., & Ahmad, R. (2025). Ransomware detection and prevention in healthcare systems. *PeerJ Computer Science*, 11, e3073, 1–38. PeerJ Inc., California. <https://doi.org/10.7717/peerj-cs.3073>
4. Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2021). Cyber risk in health facilities: A systematic literature review. *International Journal of Environmental Research and Public Health*, 18(4), 1–18. MDPI, Basel.
5. Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2019). HealthGuard: A machine learning-based security framework for smart healthcare systems. *IEEE Access*, 7, 135977–135991. IEEE, New York.
6. Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2024). Machine learning for healthcare-IoT security: A review and risk mitigation. *IEEE Internet of Things Journal*, 11(3), 1–20. IEEE, New York.
7. ElSayed, Z., Elsayed, N., & Bay, S. (2024). A novel zero-trust machine learning architecture for healthcare IoT cybersecurity. *Future Internet*, 16(2), 1–22. MDPI, Basel.
8. Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment. *IEEE Access*, 5, 186–202. IEEE, New York.
9. Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2017). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal*, 11(1), 88–95. IEEE, New York.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		72

10. Radanliev, P., De Roure, D., Walton, R., & Montalvo, R. M. (2020). Cyber risk in IoT healthcare systems. *Computers & Security*, 93, 101–118. Elsevier, Amsterdam.
11. Koufi, V., Malamateniou, F., & Vassilacopoulos, G. (2019). Security challenges in healthcare cloud computing. *Journal of Medical Systems*, 43(3), 1–12. Springer, New York.
12. Sun, J., & Zhang, Y. (2018). Security and privacy in cloud-based healthcare systems. *IEEE Communications Magazine*, 56(4), 38–44. IEEE, New York.
13. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access*, 3, 678–708. IEEE, New York.
14. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*, 13(2), 113–170. Springer, Berlin.
15. Roman, R., Najera, P., & Lopez, J. (2013). Securing the Internet of Things. *Computer*, 44(9), 51–58. IEEE, New York.
16. Tully, J., Dameff, C., Chan, T. C., & Castillo, E. M. (2023). Ransomware attack disruptions in emergency departments. *JAMA Network Open*, 6(5), e231245. AMA, Chicago.
17. Goebel, M., Dameff, C., & Tully, J. (2019). Hacking 9-1-1: Infrastructure vulnerabilities and attack vectors. *Journal of Medical Internet Research*, 21(7), e123–e130. JMIR Publications, Toronto.
18. Coravos, A., Tully, J., Doerr, M., & Dameff, C. (2020). Cybersecurity informed consent in connected medical technology. *Journal of Medical Internet Research*, 22(3), e156–e165.
19. Maggio, L. A., Dameff, C., Kanter, S. L., Woods, B., & Tully, J. (2021). Cybersecurity challenges in academic health centers. *Academic Medicine*, 96(6), 870–876. AAMC, Washington.

20. Wright, J. (2023). Healthcare cybersecurity and supply chain risk management. *Health Economics and Management Review*, 4(4), 17–27.
21. Oche, J. O., Ololade, E. O., & Adefunmilola, A. O. (2024). Protecting patient privacy in smart healthcare. *World Journal of Advanced Research and Reviews*, 23(1), 3047–3050.
22. Prawiyogi, A. G., & Meria, L. (2023). Cognitive cybersecurity in healthcare CPS-IoT systems. *International Transactions on Artificial Intelligence*, 2(1), 24–32.
23. Tsikteris, S., Pantaleon, O. D., & Tsiropoulou, E. E. (2024). Cybersecurity certification frameworks. *Energies*, 17(19), 5017. MDPI, Basel.
24. Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things. *Journal of Cyber Security*, 1(1), 65–77. Oxford University Press.
25. Behl, A., & Behl, K. (2017). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press, Oxford, 1–312.
26. Stallings, W. (2017). *Cryptography and network security: Principles and practice*. Pearson, London, 1–768.
27. Kahn, J. M., & Li, X. (2020). TLS security analysis in modern web systems. *IEEE Security & Privacy*, 18(4), 12–20.
28. Rescorla, E. (2018). The transport layer security (TLS) protocol version 1.3. IETF RFC 8446, 1–160.
29. Postel, J. (1981). Transmission Control Protocol. RFC 793, DARPA, 1–85.
30. Mockapetris, P. (1987). Domain names – implementation and specification. RFC 1035, IETF, 1–55.
31. Bluetooth SIG. (2021). Bluetooth Core Specification Version 5.2. Bluetooth SIG, Kirkland, 1–3500.
32. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey. *Computer Networks*, 88, 96–119. Elsevier.

33. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in IoT. *Computer Networks*, 76, 146–164.
34. Dworkin, M. (2001). Recommendation for block cipher modes of operation. NIST Special Publication 800-38A, 1–66.
35. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
36. Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures. *Communications of the ACM*, 21(2), 120–126.

					БР.ІП – 12.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		75

БІБЛІОГРАФІЧНА ДОВІДКА

Тема бакалаврської роботи: “Розробка та тестування безпеки застосувань електронних медичних сервісів”

Обсяг пояснювальної записки: 71 аркушів.

Дата закінчення роботи: 9 червня 2026 р.

Підпис студента _____