Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «МАГІСТР»

ІНТЕЛЕКТУАЛЬНІ РІШЕННЯ НА ОСНОВІ IOT ДЛЯ ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ ПРИ ВЗАЄМОДІЇ З АСИСТИВНОЮ РОБОТОТЕХНІКОЮ

INTELLIGENT IOT-BASED SOLUTIONS FOR MAINTAINING PRIVACY WHEN INTERACTING WITH ASSISTIVE ROBOTICS

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІм-21
Серський Дмитро Сергійович

(підпис)

Керівник:
к.т.н., доцент
Гринюк Сергій Васильович

(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» грудня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Гринюк Сергій Васильович

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *магістр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т.ТЕРЛЕЦЬКИЙ
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Серському Дмитру Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Інтелектуальні рішення на основі iot для збереження конфіденційності при взаємодії з асистивною робототехнікою*

Керівник роботи *к.т.н., доцент Гринюк Сергій Васильович*

затверджені наказом закладу вищої освіти від «17» червня 2025 року № 290/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 09.12.2025р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Теоретичні засади збереження конфіденційності у системах IoT та асистивній робототехніці
Проєктування інтелектуальної IoT
Експериментальне дослідження ефективності запропонованої системи
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Теоретичні засади збереження конфіденційності у системах IoT та асистивній робототехніці	*Гринюк С.В., доцент*		
Проєктування інтелектуальної IoT -системи	*Гринюк С.В., доцент*		
Експериментальне дослідження ефективності запропонованої системи	*Гринюк С.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Гринюк С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І., ст.викладач*		

7. Дата видачі завдання 18.06.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми*	До 01.08.2025 р.	
2.	*Теоретичні засади збереження конфіденційності у системах IoT та асистивній робототехніці*	До 20.08.2025 р.	
3.	*Проєктування інтелектуальної IoT -*	До 25.09.2025 р.	
4.	*Експериментальне дослідження ефективності запропонованої системи*	До 20.10.2025 р.	
5.	*Висновки та пропозиції*	До 25.10.2025 р	
6.	*Формування списку використаних джерел*	До 27.10.2025 р.	
7.	*Формування додатків*	До 30.10.2025 р.	
8.	*Оформлення ілюстративного матеріалу*	До 05.11.2025 р.	
9.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	До 11.11.2025 р.	
10.	*Нормоконтроль*	До 29.11.2025 р.	
11.	*Інструментальна перевірка на академічний плагіат*	До 02.12.2025 р.	
12.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	До 09.12.2025 р.	

Здобувач вищої освіти _____ Серський Д.С.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Гринюк С.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Серський Д. С. Інтелектуальні рішення на основі IoT для збереження конфіденційності при взаємодії з асистивною робототехнікою. Рукопис.

Кваліфікаційна робота магістра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатків.

У першому розділі здійснено комплексний аналіз предметної області. Проведено класифікацію сучасних асистивних роботів за їх функціональним призначенням. Виявлено ключові проблеми безпеки, що виникають під час тісної взаємодії людини з роботом, зокрема ризики несанкціонованого доступу до сенсорних даних та компрометації каналів зв'язку. Проаналізовано існуючі методи забезпечення приватності в IoT та обґрунтовано необхідність створення нових підходів для динамічних середовищ.

У другому розділі розроблено концептуальну модель системи захисту. На основі аналізу сценаріїв використання та вимог до системи запропоновано багаторівневу архітектуру рішення. Обґрунтовано застосування алгоритмів штучного інтелекту для реалізації динамічного контролю доступу, що дозволяє адаптувати політики безпеки залежно від контексту ситуації та поведінки користувача.

У третьому розділі описано практичну реалізацію та верифікацію розроблених рішень. Детально викладено постановку експерименту, опис тестового середовища та специфіку налаштування асистивного робота для безпечної фізичної взаємодії. За розробленою методикою та метриками проведено дослідження продуктивності засобів приватності

Ключові слова: асистивна робототехніка, приватність, контроль доступу, IoT, Edge Computing, ROS 2, комп'ютерний зір, кібербезпека.

ANNOTATION

Serskyi D. Intelligent IoT-Based Solutions for Privacy Preservation in Interaction with Assistive Robotics. Manuscript.

Master's Qualification Thesis of the Educational Program «Computer Engineering» of the specialty 123 Computer Engineering. Lutsk National Technical University, Lutsk, 2025.

The master's thesis consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The first chapter presents a comprehensive analysis of the subject domain. A classification of modern assistive robots according to their functional purpose is provided. Key security challenges arising from close human–robot interaction are identified, particularly the risks of unauthorized access to sensor data and the compromise of communication channels. Existing privacy-preserving methods in IoT systems are analyzed, and the need for new approaches suitable for dynamic environments is substantiated.

The second chapter develops a conceptual model of the protection system. Based on the analysis of usage scenarios and system requirements, a multi-layered security architecture is proposed. The use of artificial intelligence algorithms for dynamic access control is justified, enabling security policies to adapt to situational context and user behavior.

The third chapter describes the practical implementation and verification of the developed solutions. The experimental setup, test environment, and configuration of the assistive robot for safe physical interaction are presented in detail. According to the developed methodology and evaluation metrics, an experimental study of the performance of the proposed privacy-preserving mechanisms is carried out.

Keywords: assistive robotics, privacy, access control, IoT, edge computing, ROS 2, computer vision, cybersecurity.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний етап розвитку суспільства характеризується стрімким старінням населення та зростанням попиту на автоматизовані засоби догляду, що стимулює інтеграцію асистивних робототехнічних систем у повсякденне життя. Роботи-асистенти, оснащені розвиненою сенсорною системою, здатні суттєво підвищити якість життя людей з обмеженими можливостями та осіб похилого віку, забезпечуючи фізичну підтримку, моніторинг стану здоров'я та соціальну взаємодію. Однак функціонування таких систем в екосистемі Інтернету речей (IoT) та їх глибока інтеграція в особистий простір користувача породжує нові виклики у сфері інформаційної безпеки.

Асистивні роботи безперервно збирають, обробляють та передають величезні масиви чутливих даних, включаючи відеопотоки з приватних приміщень, біометричні показники та розпорядок дня власника. Використання стандартних хмарних архітектур для обробки цієї інформації створює критичні ризики порушення конфіденційності, пов'язані з можливістю перехоплення даних, зламу акаунтів або несанкціонованого доступу третіх осіб. Існуючі методи захисту часто є статичними і не враховують контекст ситуації, або ж надмірно обмежують функціональність робота заради безпеки. У зв'язку з цим, розробка адаптивних систем управління, здатних динамічно балансувати між ефективністю виконання асистивних функцій та захистом приватності на основі технологій периферійних обчислень (Edge Computing), є важливим науково-технічним завданням, що обумовлює актуальність теми магістерської роботи.

Метою роботи є підвищення рівня інформаційної безпеки та забезпечення приватності користувачів асистивних робототехнічних систем шляхом розроблення архітектури та алгоритмів контекстно-залежного контролю доступу до сенсорних даних.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1) провести аналіз сучасного стану асистивної робототехніки, класифікувати загрози безпеці в середовищі IoT та виявити недоліки існуючих методів захисту приватності;

2) обґрунтувати та розробити архітектуру системи захисту на базі концепції Edge Computing, яка забезпечує локальну фільтрацію даних безпосередньо на борту робота;

3) розробити алгоритми динамічного геозонування та модуль PrivateLoc для автоматичного блокування або анонімізації візуальних даних у приватних зонах;

4) спроектувати та програмно реалізувати прототип захищеної системи управління на базі платформи ROS 2 та мікрокомп'ютера Raspberry Pi;

5) експериментально дослідити ефективність запропонованих рішень, оцінити їх вплив на продуктивність системи та розробити рекомендації щодо їх впровадження.

Об'єкт дослідження – процес інформаційної взаємодії в асистивних робототехнічних системах, інтегрованих у середовище Інтернету речей.

Предмет дослідження – методи, моделі та програмно-алгоритмічні засоби забезпечення конфіденційності та захисту даних користувача в системах управління мобільними роботами.

Методи дослідження. У роботі використано методи системного аналізу (для класифікації загроз), методи криптографічного захисту інформації (для забезпечення конфіденційності каналів зв'язку), методи машинного навчання та комп'ютерного зору (для семантичного картування та розпізнавання контексту), а також методи імітаційного моделювання у середовищі Gazebo та натурного прототипування (для верифікації розробленої системи).

Наукова новизна одержаних результатів полягає в тому, що вдосконалено метод контролю доступу до сенсорних даних робота, який, на відміну від існуючих, базується на динамічному аналізі семантичного контексту (місцезнаходження та активності користувача), що дозволяє автоматизувати захист приватності без втручання оператора.

Практичне значення одержаних результатів. Розроблено та програмно реалізовано прототип системи управління асистивним роботом на базі ROS 2 та Raspberry Pi 4, який підтримує захищений протокол MQTT та інтеграцію з розумним будинком. Запропоновані архітектурні рішення дозволяють зменшити обсяг вихідного трафіку у приватних зонах на 98 % та забезпечити затримку передачі даних, допустиму для телеоперації. Результати роботи можуть бути використані при проектуванні комерційних медичних роботів та систем «Smart Home».

Апробація результатів роботи. Результати роботи представлені на 2 - й Міжнародній науково-практичній конференції «Сучасні виклики в наукових дослідженнях», яка проводилась з 1 по 3 грудня 2025 року [1].

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ У СИСТЕМАХ IoT ТА АСИСТИВНІЙ РОБОТОТЕХНІЦІ

1.1 Класифікація асистивних робототехнічних систем та їх функціональні можливості

Асистивна робототехніка розглядається як окремий напрям сервісної робототехніки, орієнтований на підтримку людей з обмеженими можливостями, осіб похилого віку та користувачів, які потребують допомоги у виконанні повсякденних дій. Згідно з міжнародним стандартом ISO 8373:2021, робот визначається як керований, програмований механізм, здатний виконувати заплановані завдання шляхом руху у своєму середовищі, а асистивні роботи належать до класу сервісних роботів, що взаємодіють з людиною в неіндустріальному середовищі [2].

У контексті Інтернету речей (IoT) асистивний робот виступає інтелектуальним вузлом кіберфізичної системи, який не лише виконує фізичні дії, а й збирає, обробляє та передає дані у розподілену інфраструктуру.

У сучасній науковій літературі класифікація асистивних робототехнічних систем здійснюється за кількома основними ознаками: функціональним призначенням, фізичною конфігурацією, типом взаємодії з користувачем, рівнем автономності та ступенем інтеграції з IoT-середовищем. Огляд досліджень у сфері підтримки людей похилого віку показує, що більшість асистивних роботів орієнтовані на вирішення завдань догляду, моніторингу стану здоров’я, підтримки мобільності та соціальної взаємодії [3].

З погляду функціонального призначення доцільно виокремити принаймні п’ять ключових класів асистивних роботів (рис. 1.1). Першу групу становлять роботи фізичної допомоги, що виконують маніпуляційні та транспортні функції: допомога при вставанні, переносі предметів, супроводі користувача в приміщенні, підтримці рівноваги тощо. До цієї групи належать мобільні платформи з маніпуляторами, роботи-помічники в домогосподарстві та системи

для підтримки ходи. Друга група – медичні та реабілітаційні роботи, зокрема роботизовані тренажери та реабілітаційні комплекси для верхніх і нижніх кінцівок, які застосовуються в нейрореабілітації після інсульту, травм чи ортопедичних операцій. Останні систематичні огляди підкреслюють, що такі робототехнічні засоби дозволяють стандартизувати та інтенсифікувати процес відновлення, забезпечуючи точний контроль траєкторій руху та навантаження [3].

Рисунок 1.1 – Схема класифікації асистивних робототехнічних систем [3]

Окремим класом виступають соціально-асистивні роботи (Socially Assistive Robots, SAR), основна функція яких полягає не у фізичному втручанні, а у соціальній, когнітивній та емоційній підтримці користувача. Такі роботи використовуються для стимуляції когнітивних функцій, підтримки пацієнтів із хворобою Альцгеймера, аутизмом, депресивними розладами, а також для підтримання соціальної залученості людей похилого віку [4].

До цієї групи належать роботи-компаньйони з виразним «соціальним» інтерфейсом, віртуальні чи фізичні агенти, інтегровані у «розумне» середовище.

Четвертий клас формують носимі асистивні системи, тобто роботизовані екзоскелети та «м’які» екзокостюми, призначені для підсилення м’язової активності або часткової компенсації рухових функцій. Останні роботи демонструють розвиток як жорстких екзоскелетів, що забезпечують високий рівень підтримки та точне керування суглобами, так і м’яких екзосьютів, орієнтованих на комфорт користувача і природність рухів [5].

П’ятий клас становлять гібридні системи, де поєднуються фізична допомога, соціальна взаємодія та функції моніторингу (наприклад, мобільний робот-компаньйон із можливістю вимірювання фізіологічних параметрів і доступом до телемедичних сервісів).

З позицій фізичної архітектури асистивні роботи поділяють на стаціонарні, мобільні та носимі системи. Стаціонарні роботи зазвичай інтегруються у ліжка, підйомні механізми або реабілітаційні тренажери та взаємодіють з користувачем у фіксованій зоні. Мобільні роботи, навпаки, здатні автономно переміщуватися в межах середовища (квартири, лікарняного відділення, будинку для літніх людей) і підтримувати користувача в різних просторових зонах. Носимі системи (екзоскелети) безпосередньо закріплюються на тілі користувача, що потребує особливої уваги до питань ергономіки, біомеханічної сумісності та безпеки [4].

Не менш важливою є класифікація асистивних роботів за типом взаємодії з користувачем. У цьому контексті виділяють системи прямого фізичного контакту (роботи-реабілітанти, екзоскелети), системи дистанційної фізичної підтримки (наприклад, роботи для доставки медикаментів або предметів у лікарні), а також суто соціальноорієнтовані системи, які взаємодіють через мову, жести, міміку та інші модальності людсько-роботної взаємодії [6].

Ступінь «соціальності» таких систем визначається складністю моделей сприйняття емоцій, адаптації до індивідуальних особливостей користувача та здатністю до тривалих взаємодій без втрати довіри.

За рівнем автономності асистивні робототехнічні системи можуть бути повністю керованими (tele-operated), напівавтономними або автономними. У повністю керованих системах користувач або оператор здійснює безпосередній

контроль над діями робота, використовуючи інтерфейси типу «людина–машина». Напівавтономні роботи виконують частину функцій самостійно, наприклад, утримання рівноваги, обхід перешкод або дотримання безпечної дистанції, але ключові рішення залишаються за користувачем. Автономні системи здатні самостійно планувати маршрут, адаптувати поведінку до змін середовища, обирати оптимальні стратегії взаємодії на основі сенсорної інформації та попереднього досвіду. Останні огляди в галузі соціально-асистивної робототехніки підкреслюють, що зростання автономності потребує посиленої уваги до етичних аспектів, прозорості алгоритмів і механізмів безпечного втручання людини.

У середовищі IoT асистивні роботи можуть також класифікуватися за ступенем інтеграції в інфраструктуру «розумного» середовища. У найпростішому випадку робот функціонує як окремий пристрій із мінімальним мережевим обміном. На більш високих рівнях інтеграції робот стає частиною розподіленої системи, у якій взаємодіє з датчиками життєдіяльності, інтелектуальними побутовими пристроями, телемедичними платформами та хмарними сервісами аналітики. Така інтеграція розширює функціональні можливості асистивних систем: від простого виконання команд до комплексного підтримання безпеки, контролю стану здоров’я, нагадувань про прийом ліків, аналізу ризиків падінь та формування довгострокових моделей поведінки користувача.

Для забезпечення систематизації, деталізації функціональних вимог та технологічних рішень, що застосовуються в асистивній робототехніці, було проведено аналіз ключових категорій за критерієм їхнього основного функціонального призначення. У таблиці 1.1 представлено узагальнену класифікацію, яка відображає основні функціональні домени, конкретні приклади їхньої реалізації, а також відповідні технології керування та інтерфейси взаємодії, що використовуються в межах кожної категорії, дозволяючи провести чітке розмежування між класами систем, що орієнтовані на пересування, маніпуляцію, терапію та соціальну підтримку.

Таблиця 1.1 – Узагальнена функціональна класифікація асистивних робототехнічних систем

Категорія	Основне функціональне призначення	Приклади реалізації	Технології керування та інтерфейси
Мобільні Системи	Забезпечення автономного пересування та навігації у складному середовищі.	Інтелектуальні інвалідні візки, роботи-поводирі, системи для переміщення пацієнтів.	Голосове керування, нейроінтерфейси (BCI), SLAM-алгоритми, лідари.
Маніпуляційні Системи	Допомога у виконанні завдань самообслуговування, годування, піднімання предметів.	Роботизовані руки та протези, маніпулятори, інтегровані у візки або столи.	Джойстики з високою чутливістю, кінетичні датчики, електродна міографія (EMG).
Терапевтичні Системи	Фізична реабілітація, відновлення рухових функцій та моніторинг прогресу.	Екзоскелети для нижніх/верхніх кінцівок, роботизовані тренажери ходьби, ортези.	Силовий зворотний зв’язок (Force Feedback), датчики тиску, адаптивні алгоритми тренувань.
Соціальні (Компаньйони)	Емоційна, когнітивна підтримка, віддалений моніторинг стану здоров’я.	Роботи-компаньйони (наприклад, Paro), аватари, системи моніторингу життєвих показників.	Розпізнавання мови та емоцій, телекомунікація, інтелектуальні системи оповіщення.

Узагальнюючи, можна стверджувати, що класифікація асистивних робототехнічних систем ґрунтується не лише на їхній функціональній ролі (фізична, когнітивна, соціальна підтримка), а й на архітектурних, ергономічних та інформаційно-комунікаційних характеристиках. Такий багатовимірний підхід є критично важливим для подальшого проєктування інтелектуальних IoT-рішень, орієнтованих на збереження конфіденційності, оскільки різні класи асистивних роботів генерують різні типи даних, по-різному взаємодіють з користувачем та середовищем і потребують специфічних механізмів захисту.

1.2 Проблеми безпеки й конфіденційності під час взаємодії користувача з асистивними роботами

Впровадження асистивних робототехнічних систем у побут вразливих груп населення створює специфічне середовище, де кібернетичні загрози трансформуються у прямі ризики для фізичної безпеки та недоторканності приватного життя. На відміну від традиційних комп'ютерних систем, асистивні роботи є кіберфізичними пристроями, що діють у безпосередній близькості до людини, тому порушення їхньої роботи виходить за межі втрати інформації, загрожуючи здоров'ю користувача. Проблематика безпеки у цій сфері є комплексною і охоплює три взаємопов'язані вектори: несанкціонований доступ до конфіденційних даних, ризики, пов'язані із сенсорним моніторингом, та атаки на комунікаційні канали управління (рис. 1.2).

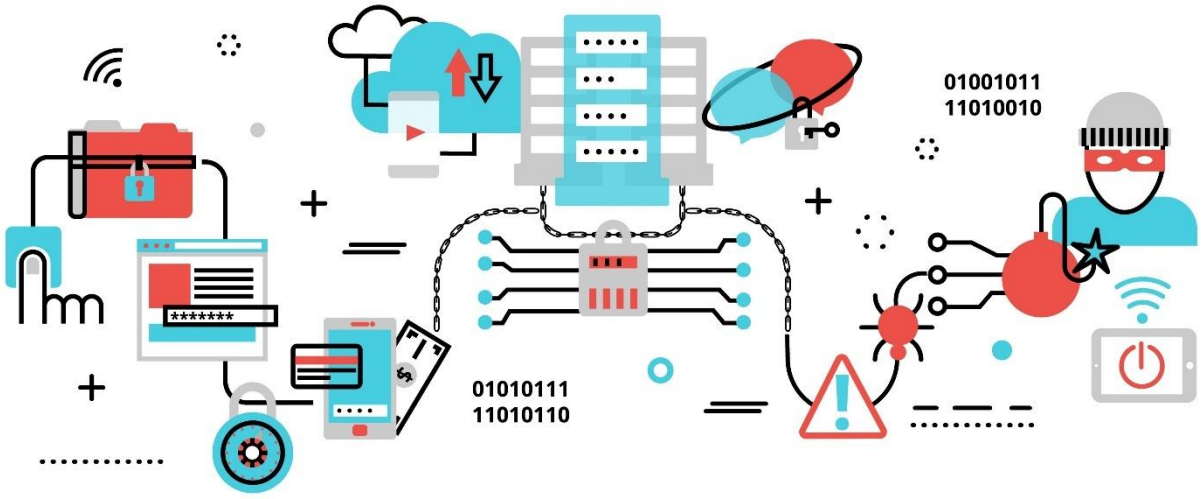

Рисунок 1.2 – Концептуальна схема загроз інформаційній безпеці та приватності даних в асистивних системах [7]

Першочерговою загрозою є несанкціонований доступ до масивів приватних даних, які робот акумулює для забезпечення персоналізованої допомоги. Функціонування асистивних систем базується на безперервному зборі та обробці чутливої інформації, яка включає медичні показники, біометричні

дані, графіки прийому ліків та деталі розпорядку дня. Згідно з дослідженнями у сфері людино-машинної взаємодії, основна вразливість полягає у недостатньому рівні шифрування даних як на рівні локального зберігання, так і під час їх передачі у хмарні сховища. Компрометація цих баз даних дозволяє зловмисникам не лише здійснювати крадіжку цифрової особистості для фінансових махінацій, але й проводити детальне профілювання жертви. Аналіз поведінкових патернів користувача дозволяє стороннім особам прогнозувати періоди відсутності власника вдома або його перебування у безпорадному стані (наприклад, під час сну), що може бути використано для планування фізичних злочинів проти власності або особи [7].

Другим критичним аспектом є загрози, що випливають із широких можливостей сенсорного моніторингу навколишнього середовища. Асистивні роботи для навігації та розпізнавання контексту оснащуються комплексом сенсорів, включаючи камери високої роздільної здатності, мікрофони та лідари. У випадку перехоплення управління над сенсорною підсистемою робот перетворюється на інструмент прихованого спостереження, що дослідники кваліфікують як «електронний вуайєризм». Це є грубим порушенням приватності, особливо враховуючи, що такі роботи часто функціонують у найбільш інтимних зонах житла, таких як спальні чи ванні кімнати. Важливо зазначити, що загрозу становить не лише прямий відеопотік. Дані з датчиків глибини та лідарів дозволяють зловмисникам реконструювати високоточні тривимірні семантичні карти приміщення, визначаючи розташування цінних речей, шляхи підходу та наявність систем сигналізації, навіть без доступу до оптичних камер [8].

Третім вектором небезпеки є вразливість каналів зв’язку, які забезпечують інтеграцію робота в екосистему Інтернету речей (IoT). Більшість асистивних систем використовують бездротові протоколи передачі даних для комунікації з керуючими терміналами або серверами. Відсутність надійної автентифікації робить ці канали вразливими до різноманітних мережевих атак. Зокрема, атака типу «Людина посередині» (Man-in-the-Middle) дозволяє перехоплювати та

модифікувати пакети даних між користувачем та роботом, що може призвести до спотворення команд управління та непередбачуваної поведінки механізму. Водночас атаки на відмову в обслуговуванні (DoS) спрямовані на перевантаження каналів зв'язку, що блокує можливість дистанційного керування або передачі сигналів тривоги у критичних ситуаціях, наприклад, при падінні користувача. Найбільш небезпечним сценарієм є повне перехоплення сесії управління (Session Hijacking), коли зловмисник отримує прямий контроль над актуаторами робота, що дозволяє використовувати пристрій для нанесення фізичної шкоди оточенню або самій людині [9].

Підсумовуючи, забезпечення безпеки асистивних робототехнічних систем вимагає переходу від реактивних методів захисту до концепції Security by Design, де механізми протидії вищезгаданим загрозам закладаються на етапі архітектурного проектування системи.

1.3 Методи забезпечення приватності даних у системах IoT

Забезпечення конфіденційності та цілісності інформаційних потоків у середовищі асистивних робототехнічних систем вимагає комплексного підходу, що виходить за межі стандартних протоколів мережевої безпеки. Специфіка Інтернету речей (IoT), до якого інтегровані сучасні роботи-асистенти, характеризується гетерогенністю пристроїв, обмеженістю обчислювальних ресурсів кінцевих вузлів та критичною чутливістю оброблюваних даних. У зв'язку з цим, побудова надійної архітектури захисту базується на синергії криптографічних механізмів, алгоритмів деідентифікації даних та децентралізованих моделей машинного навчання. Ефективна стратегія захисту повинна охоплювати весь життєвий цикл даних: від моменту їх первинної генерації сенсорами робота до етапу архівації або видалення у хмарних сховищах, гарантуючи при цьому відповідність нормативним вимогам, таким як загальний регламент захисту даних (GDPR).

Фундаментальним елементом у системі захисту інформації залишається криптографічне перетворення, проте застосування традиційних алгоритмів у робототехніці має суттєві обмеження. Асистивні роботи, особливо мобільні платформи та переносні пристрої, функціонують в умовах жорсткого ліміту енергоспоживання та обчислювальної потужності, що унеможливлює використання «важких» криптографічних стандартів без суттєвої втрати продуктивності та збільшення латентності системи, що є неприпустимим для задач реального часу. Відповіддю на цей виклик стало впровадження методів легковагової криптографії (Lightweight Cryptography, LWC). На відміну від класичного алгоритму RSA (рис. 1.3), який вимагає значних ресурсів для генерації та зберігання ключів великої довжини, сучасні протоколи на базі еліптичних кривих (Elliptic Curve Cryptography, ECC) забезпечують еквівалентний рівень стійкості при значно меншому розмірі ключа. Це дозволяє реалізувати надійне шифрування каналів управління та телеметрії навіть на рівні мікроконтролерів вбудованих систем робота, мінімізуючи затримки при передачі критичних сигналів, наприклад, повідомлень про падіння користувача або збої в роботі життєзабезпечення.

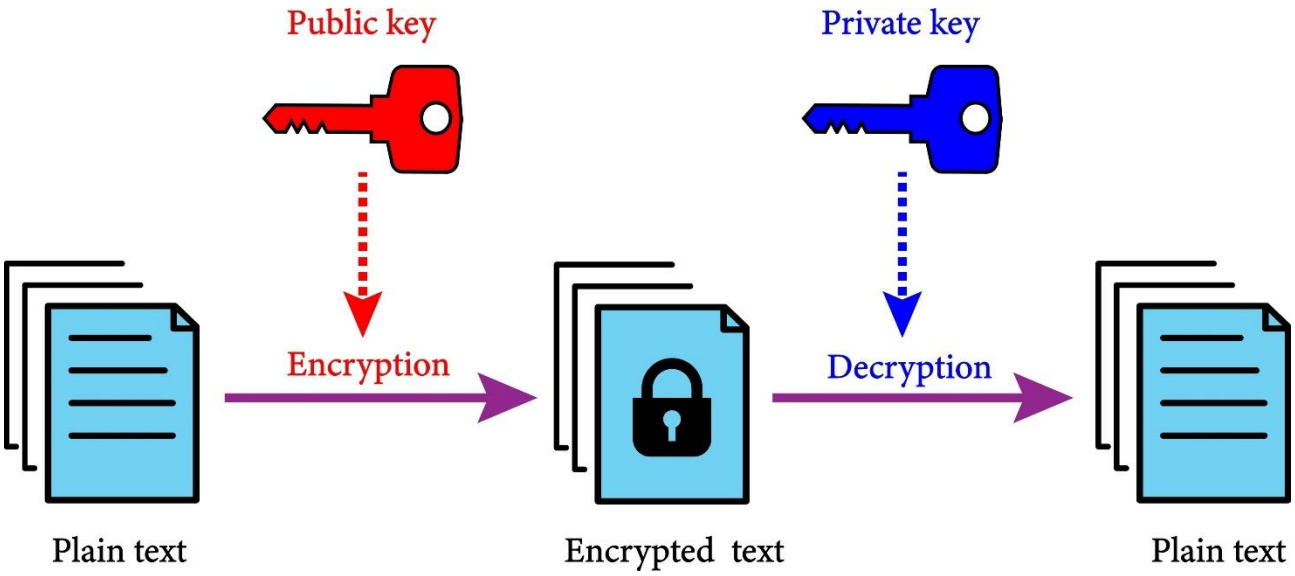

Рисунок 1.3 – Асиметричне шифрування [10]

Особливої уваги в контексті хмарної робототехніки заслуговує проблема обробки зашифрованих даних. Традиційні схеми вимагають розшифрування інформації на стороні сервера перед її аналізом, що створює вразливість у момент перебування даних у відкритому вигляді в оперативній пам’яті хмарного провайдера. Вирішенням цієї проблеми є застосування повного або часткового гомоморфного шифрування (Homomorphic Encryption). Дана технологія дозволяє виконувати математичні операції над зашифрованими даними (шифротекстом) таким чином, що результат після розшифрування збігається з результатом операцій, виконаних над відкритим текстом. Імплементація гомоморфного шифрування в асистивних системах відкриває можливість відправляти у хмару зашифровані навігаційні карти або медичні показники для складного аналізу штучним інтелектом без розкриття їхнього змісту третій стороні, що забезпечує математично гарантовану конфіденційність обчислень.

Представлена на рисунку 1.4 схема ілюструє захищений протокол взаємодії між клієнтським пристроєм (асистивним роботом) та віддаленим обчислювальним сервером (хмарою).

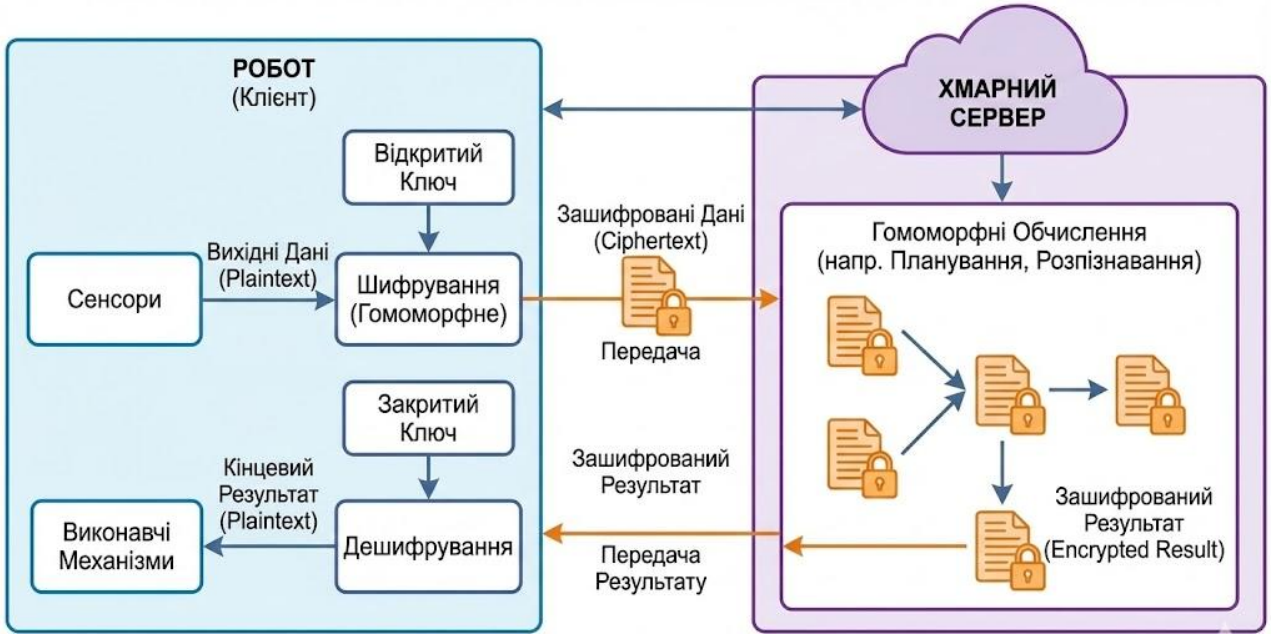

Рисунок 1.4 – Схема обробки даних із використанням гомоморфного шифрування у хмарній робототехніці [10]

Ключовою особливістю даної архітектури є забезпечення конфіденційності даних на етапі обчислень, що реалізується за допомогою методів гомоморфної криптографії. Процес обробки інформації відбувається у чотири послідовні етапи, що утворюють замкнений цикл керування.

На першому етапі сенсорна підсистема робота здійснює збір первинних даних (наприклад, зображень навколишнього середовища, голосових команд або біометричних показників користувача). Отриманий масив інформації, який у криптографії позначається як відкритий текст (Plaintext), не передається у хмару безпосередньо. Замість цього, модуль шифрування на борту робота перетворює ці дані на шифротекст (Ciphertext) з використанням відкритого ключа або симетричного ключа, доступного лише власнику.

На другому етапі зашифровані дані передаються незахищеними каналами зв’язку до хмарного сервера. Важливо зазначити, що на цьому етапі інформація вже є математично захищеною від перехоплення, оскільки без відповідного ключа дешифрування вона виглядає як псевдовипадковий набір бітів.

Третій етап є критичним для даної схеми і відбувається у хмарному середовищі. Сервер виконує необхідні гомоморфні обчислення (наприклад, планування траєкторії руху, розпізнавання образів або аналіз медичних аномалій) безпосередньо над шифротекстом. Завдяки алгебраїчним властивостям гомоморфного шифрування, операції, виконані над зашифрованими даними, після дешифрування дають результат, еквівалентний тому, якби ці операції виконувалися над відкритими даними. При цьому хмарний провайдер не має доступу до ключів дешифрування і, відповідно, ніколи не «бачить» реального змісту інформації, яку обробляє.

На завершальному етапі хмарний сервер повертає результат обчислень у зашифрованому вигляді назад до робота. Використовуючи свій закритий (секретний) ключ, робот дешифрує отриману відповідь, перетворюючи її на зрозумілу команду для виконавчих механізмів (актуаторів).

Така схема гарантує, що приватні дані користувача залишаються конфіденційними протягом усього циклу, навіть якщо сервер скомпрометовано,

оскільки зловмисник отримає доступ лише до зашифрованих масивів без можливості їх прочитання.

Поряд із криптографічним захистом змісту повідомлень, критично важливим є забезпечення анонімності суб’єкта даних. У системах моніторингу здоров`я та асистивного супроводу накопичуються масиви інформації, аналіз яких дозволяє не лише ідентифікувати особу, але й відновити детальний профіль її поведінки. Для нівелювання цього ризику застосовуються методи анонімізації та псевдонімізації. Псевдонімізація, як процедура заміни реальних ідентифікаторів користувача (імені, адреси, номерів соціального страхування) на штучні унікальні коди, дозволяє розділити інформаційні потоки на ідентифікуючі та змістовні. Це забезпечує можливість довгострокового аналізу медичних трендів конкретного пацієнта без прямого зв’язку з його реальною особистістю у базі даних, однак вимагає суворого контролю доступу до таблиць відповідності псевдонімів. Більш високий рівень захисту забезпечує методологія k-анонімності (k-anonymity) та l-різноманітності (l-diversity), які передбачають узагальнення атрибутів у наборі даних таким чином, щоб будь-який запис не міг бути відрізнений від щонайменше k-1 інших записів.

Проте статичної анонімізації часто недостатньо для захисту від атак повторної ідентифікації, особливо при наявності додаткових зовнішніх джерел даних. Тому у сучасних дослідженнях акцент зміщується на використання диференційної приватності (Differential Privacy). Цей математичний підхід передбачає додавання контрольованого статистичного шуму (зазвичай за законом Лапласа або Гауса) до результатів запитів до бази даних або безпосередньо до даних, що передаються сенсорами. Суть методу полягає в тому, щоб зробити вихід системи інваріантним щодо присутності або відсутності даних конкретного користувача у навчальній вибірці. Для асистивного робота це означає, що статистичні дані про його переміщення та взаємодію можуть бути використані розробниками для покращення алгоритмів навігації, але при цьому математично неможливо виокремити траєкторію руху конкретної особи чи розпорядок її дня, що унеможливлює стеження.

Архітектурні рішення у сфері приватності дедалі частіше спираються на концепцію периферійних обчислень (Edge Computing), яка передбачає перенесення процесів обробки даних з централізованих хмарних серверів безпосередньо на борт робота або на локальний шлюз розумного будинку. Такий підхід дозволяє реалізувати методи «заплутування на периферії» (Edge-obfuscation). У контексті відеоспостереження та візуальної навігації це реалізується шляхом попередньої обробки відеопотоку. Замість трансляції «сирого» відеозображення, алгоритми комп'ютерного зору на самому пристрої виділяють ключові ознаки, необхідні для виконання завдання, і видаляють чутливу візуальну інформацію. Наприклад, замість передачі зображення обличчя людини робот може передавати лише абстрактну скелетну модель пози (skeleton tracking) або теплову карту присутності. Це дозволяє оператору або алгоритму визначити факт падіння людини чи необхідність допомоги, але робить неможливим візуальну ідентифікацію особи чи огляд приватних деталей інтер'єру, реалізуючи принцип мінімізації даних на фізичному рівні (рис. 1.5).

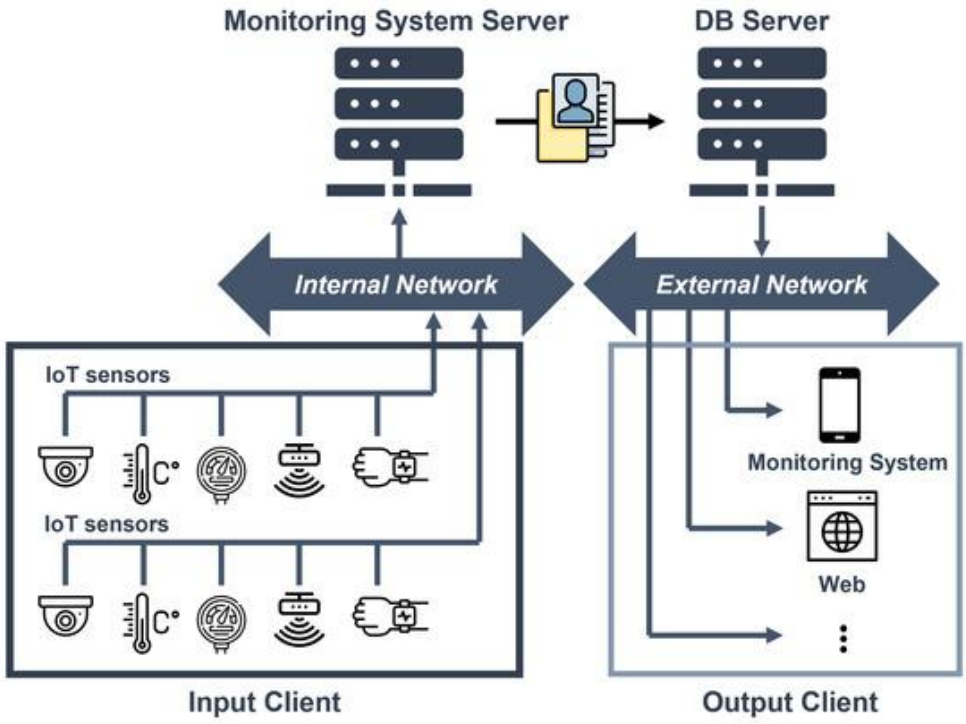

Рисунок 1.5 – Принцип дії фільтрів приватності на базі Edge Computing для візуальних сенсорів [11]

Подальшим розвитком децентралізованого підходу до приватності є технологія федеративного навчання (Federated Learning). Класичні методи машинного навчання вимагають агрегації величезних масивів даних користувачів на центральному сервері для тренування нейронних мереж, що створює єдину точку відмови та високий ризик масового витоку даних. Федеративне навчання змінює цю парадигму, дозволяючи навчати глобальну модель без переміщення локальних даних. У цій архітектурі асистивний робот завантажує поточну версію моделі з хмари, проводить її донавчання (fine-tuning) на власних локальних даних користувача, і відправляє на сервер лише оновлені параметри (градієнти ваг нейромережі). Сервер агрегує оновлення від тисяч роботів, покращуючи загальну модель, але ніколи не отримує доступу до первинних даних, таких як зображення з камер чи записи голосу. Це не лише підвищує рівень конфіденційності, але й знижує навантаження на канали зв'язку.

На рисунку 1.6 показано принцип роботи федеративного навчання, де дані залишаються на локальних пристроях (клієнтах), а на сервер передаються лише оновлення моделі.

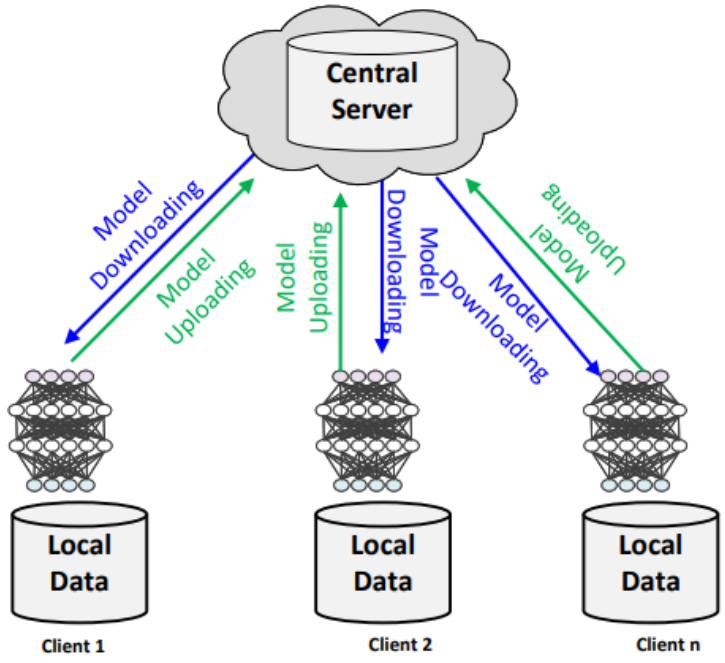

Рисунок 1.6 – Архітектура федеративного навчання з трьома локальними клієнтами та центральним сервером [12]

Завершальним рубежем захисту є системи контролю доступу та управління ідентифікацією. Статичні парольні системи продемонстрували свою неефективність в динамічному середовищі IoT, тому сучасні розробки фокусуються на атрибутивному управлінні доступом (Attribute-Based Access Control, ABAC) та контекстно-залежній автентифікації. Модель ABAC дозволяє формувати гнучкі політики безпеки, що враховують не лише роль користувача (наприклад, «лікар», «родич», «технік»), але й контекстні атрибути: час доби, геолокацію, поточний стан пацієнта. Наприклад, віддалений доступ до камери робота для лікаря може бути дозволений системою лише у випадку фіксації критичних показників життєдіяльності пацієнта, в той час як у звичайному режимі такий доступ блокується. Крім того, перспективним напрямом є використання мультимодальної біометрії (розпізнавання обличчя, голосу, ходи) для безперервної автентифікації користувача, що гарантує, що робот виконує команди лише авторизованого власника, запобігаючи перехопленню керування сторонніми особами навіть при наявності доступу до пульту управління.

На рисунку 1.7 представлена комплексна схема захисту інформаційних потоків у середовищі Інтернету речей (IoT), яка поєднує методи машинного навчання для попередньої обробки даних та сучасні криптографічні протоколи. Запропонована архітектура спрямована на оптимізацію ресурсів системи шляхом вибіркового шифрування лише критично важливої інформації.

Процес обробки інформації розпочинається на рівні користувацьких пристроїв та сенсорів («User Devices»), де відбувається безперервний збір різнорідних даних («IoT data Collection»). Отриманий масив проходить етап попередньої обробки («Data Preprocessing») для очищення від шумів та нормалізації. Ключовим елементом системи є модуль інтелектуальної класифікації, побудований на базі адаптивної штучної нейронної мережі зі згортковими ядрами («Adaptive Convolutional kernel ANN»). Для підвищення точності роботи класифікатора застосовується спеціалізований алгоритм оптимізації (AO algorithm). Головною функцією цього модуля є автоматичний

розподіл вхідного потоку даних на дві категорії: «нечутливі дані» (Non-sensitive data), які не потребують високого рівня захисту, та «чутливі дані» (Sensitive data), що містять конфіденційну інформацію.

Потік, ідентифікований як чутливий, спрямовується до криптографічного блоку. Для забезпечення безпеки використовується оптимальне гомоморфне шифрування, яке дозволяє виконувати операції над даними без їх дешифрування. Особливістю даної реалізації є використання гібридного мета-евристичного алгоритму HHTSGWO (Harris Hawks and Grey Wolf Optimization) для вибору оптимальних ключів шифрування, що підвищує стійкість системи до криптоаналізу. На завершальному етапі захищені дані («Secure IoT sensitive data») передаються через комунікаційні канали у хмарне середовище («Cloud»), де забезпечується їх безпечне зберігання, обробка та мережева взаємодія. Така архітектура дозволяє збалансувати навантаження на обчислювальні потужності та гарантувати високий рівень приватності.

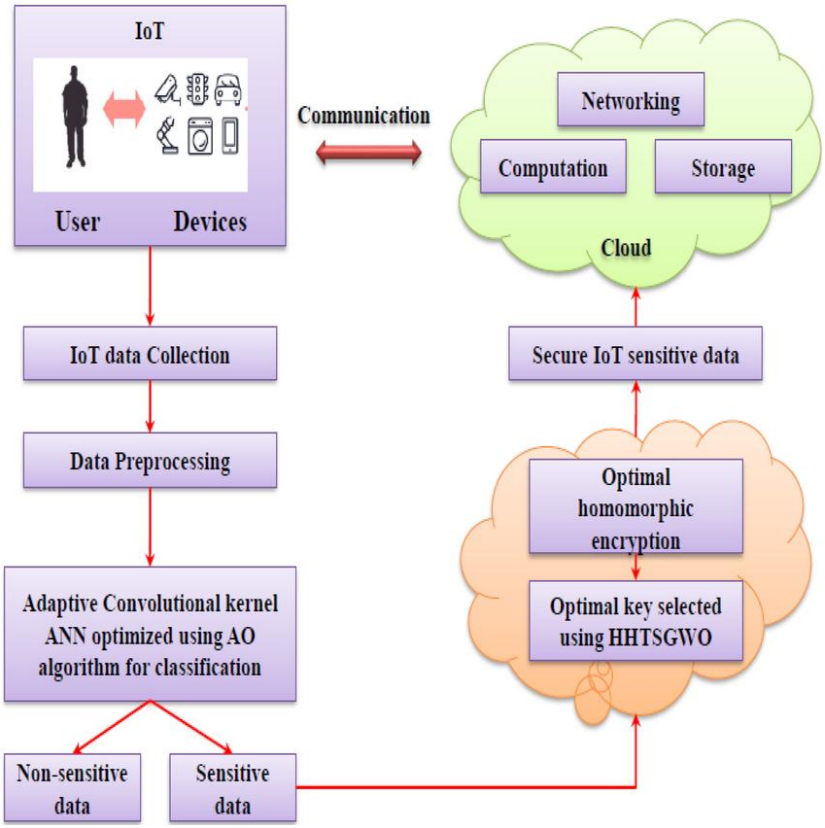

Рисунок 1.7 – Інтелектуальна архітектура безпеки IoT [13]

У першому розділі роботи здійснено комплексний аналіз сучасного стану розвитку асистивних робототехнічних систем, визначено їхню критичну роль у підвищенні якості життя вразливих категорій населення та досліджено проблематику інформаційної безпеки в середовищі Інтернету речей. Встановлено, що сучасна асистивна техніка еволюціонувала від простих механічних пристроїв до складних кіберфізичних комплексів, глибоко інтегрованих в особистий простір користувача. Проведена систематизація дозволила виокремити основні функціональні групи, такі як реабілітаційні системи, засоби фізичної асистенції, платформи забезпечення мобільності та соціально-когнітивні роботи, спільною рисою яких є критична залежність від безперервного збору та обробки сенсорних даних.

Детальний аналіз ландшафту загроз засвідчив, що специфіка асистивної робототехніки трансформує класичні кібернетичні ризики у безпосередню небезпеку для фізичного здоров’я та приватності людини. Визначено, що найбільш критичними векторами атак є несанкціонований доступ до чутливих біометричних масивів, компрометація каналів телеоперації через атаки типу «людина посередині» та ризики прихованого сенсорного моніторингу, відомого як «електронний вуайєризм». При цьому використання стандартних незахищених протоколів передачі даних в екосистемі IoT робить такі системи вразливими до зовнішнього втручання та маніпуляцій.

Дослідження існуючих методів протидії виявило недостатню ефективність застосування виключно традиційних криптографічних підходів в умовах обмежених обчислювальних та енергетичних ресурсів мобільних платформ. Обґрунтовано доцільність впровадження багаторівневої архітектури захисту, яка має базуватися на синергії легкового го та гомоморфного шифрування для захисту хмарних обчислень, застосуванні технологій периферійних обчислень (Edge Computing) для попередньої анонімізації візуальних даних безпосередньо на борту робота, а також використанні федеративного навчання для мінімізації передачі конфіденційної інформації через мережу.

Підсумовуючи результати теоретичного дослідження, можна стверджувати, що забезпечення надійності та приватності асистивних систем вимагає переходу від реактивних заходів безпеки до парадигми проектування «Security by Design». Отримані висновки та визначені архітектурні вимоги формують необхідне наукове підґрунтя для наступних етапів роботи, спрямованих на розробку власної структури захищеної системи управління асистивним роботом.

РОЗДІЛ 2
ПРОЄКТУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ IoT-СИСТЕМИ ДЛЯ ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ ПІД ЧАС ВЗАЄМОДІЇ З АСИСТИВНИМИ РОБОТАМИ

2.1 Вимоги до системи та аналіз сценаріїв взаємодії з роботом

Проектування архітектури системи управління асистивним роботом вимагає детальної формалізації умов його функціонування, які суттєво відрізняються від структурованих промислових майданчиків. Специфіка домашнього середовища характеризується високим рівнем ентропії, наявністю динамічних перешкод та, що найважливіше, жорсткими вимогами до збереження приватності користувача. Визначення вимог до системи базується на аналізі сценаріїв взаємодії у просторі, який можна умовно поділити на зони з різним рівнем доступності та довіри. Розробка такої системи передбачає впровадження механізмів семантичного картування приміщення, де кожній локації присвоюється певний атрибут конфіденційності, що диктує допустимі режими роботи сенсорів та алгоритмів.

Ключовим аспектом при формуванні вимог є концепція зонування простору на основі оцінки ризиків для приватного життя. Домашнє середовище не є гомогенним: воно включає «публічні» зони, такі як вітальня чи кухня, де моніторинг може бути безперервним, та «приватні зони» (спальня, ванна кімната), де функціонування камер та мікрофонів вимагає суворих обмежень. Сценарії взаємодії в приватних зонах повинні передбачати автоматичну деактивацію візуальних сенсорів або перехід у режим обробки метаданих (наприклад, використання тільки тепловізора або лідара), який дозволяє контролювати фізичну безпеку пацієнта без порушення його інтимного простору. Відтак, система повинна володіти здатністю до динамічної реконфігурації сенсорної підсистеми залежно від поточної локалізації робота на семантичній карті приміщення.

Однак статичного зонування часто недостатньо, тому архітектура системи

повинна враховувати принцип ситуаційної конфіденційності. Цей підхід базується на розумінні контексту поточної діяльності користувача, а не лише його місця розташування. Наприклад, перебування особи у вітальні зазвичай не вимагає високого рівня приватності, проте ситуація змінюється, якщо користувач перевдягається або приймає гостей. Вимоги до системи в цьому аспекті включають реалізацію алгоритмів розпізнавання активності (Activity Recognition), які здатні класифікувати дії людини та адаптувати поведінку робота в реальному часі. Якщо система детектує чутливу ситуацію, вона повинна ініціювати протокол тимчасового призупинення запису даних або їх локальної анонімізації, навіть якщо робот знаходиться у загальнодоступній зоні.

Важливою складовою технічного завдання є визначення поведінкових обмежень робота, які вирішують конфлікт між приватністю та безпекою. В асистивній робототехніці існує етична дилема: повне відключення сенсорів для збереження приватності може призвести до неможливості виявлення критичних станів, наприклад, падіння людини у ванній кімнаті. Тому система повинна керуватися ієрархією пріоритетів, де безпосередня загроза життю та здоров’ю користувача (виявлена, наприклад, через акустичні сенсори або датчики вібрації підлоги) тимчасово скасовує обмеження конфіденційності для передачі сигналу тривоги опікунам чи медичним службам. Цей механізм «екстреного доступу» (break-glass policy) має бути реалізований на рівні програмної логіки з обов’язковим логуванням події для подальшого аудиту.

Узагальнюючи вищезазначене, до системи управління асистивним роботом висуваються наступні вимоги: забезпечення автономної навігації з урахуванням зон приватності, наявність підсистеми контекстного аналізу ситуацій, реалізація механізмів локальної обробки даних (Edge Computing) для мінімізації трафіку чутливої інформації назовні, а також гнучка система поведінкових імперативів, яка гарантує фізичну безпеку користувача при максимальному дотриманні його права на недоторканність приватного життя.

На рисунку 2.1 представлена топологічна модель житлового простору користувача, трансформована у семантичну карту навігації асистивного робота.

Схема візуалізує принцип поділу домашнього середовища на три типи зон безпеки, що позначені відповідним кольоровим градієнтом, який корелює з рівнем приватності та допустимими режимами роботи сенсорів.

Рисунок 2.1 – Концептуальна схема семантичного картування домашнього середовища з виділенням зон ситуаційної конфіденційності

«Червона зона» (High Privacy Zone): Охоплює приміщення з найвищими вимогами до конфіденційності (спальня, ванна кімната). На схемі у цій зоні відображено піктограму деактивації оптичних сенсорів (RGB-камер). У цьому секторі робот переходить у режим навігації виключно за даними лідарів або тепловізорів, що унеможливлює відеофіксацію інтимних моментів життя користувача, зберігаючи при цьому здатність детектувати критичні ситуації (наприклад, падіння).

«Жовта зона» (Conditional Privacy Zone): Відображає перехідні простори (коридор, вітальня). У цій зоні діє режим ситуаційної конфіденційності, де активація камер залежить від контексту (часу доби або наявності гостей). На рисунку це проілюстровано умовним логічним блоком, який перевіряє зовнішні умови перед увімкненням запису.

«Зелена зона» (Public/Low Privacy Zone): Включає кухню або їдальню, де пріоритетом є активна допомога. Тут дозволено повний спектр сенсорного моніторингу для точного розпізнавання об’єктів та маніпуляцій.

Стрілками на схемі показано траєкторію руху робота та точки прийняття рішень (decision points), де система автоматично перемикає профілі безпеки при перетині віртуальних кордонів зон. Така візуалізація демонструє реалізацію політики Geo-fencing privacy protection в архітектурі системи управління.

2.2 Архітектурний підхід до побудови IoT-рішення для приватності

Реалізація визначених вимог до безпеки та ситуаційної конфіденційності вимагає застосування ієрархічної архітектурної моделі, яка дозволяє розподілити обчислювальне навантаження та зони відповідальності за захист даних. Оптимальним підходом для асистивних робототехнічних систем є побудова трирівневої структури IoT-рішення, що базується на парадигмі периферійних обчислень (Edge Computing). Така архітектура передбачає послідовну обробку інформаційних потоків на крайовому рівні, рівні шлюзів та у хмарному середовищі, де кожен етап виступає бар’єром для витоку конфіденційної інформації.

Фундаментальним рівнем запропонованої архітектури є рівень пристроїв (Edge Layer), представлений бортовими обчислювальними потужностями самого робота. Саме тут відбувається первинний збір даних із сенсорів та їх безпосередня обробка. Згідно з принципом мінімізації даних (Data Minimization), на цьому рівні розгортаються алгоритми штучного інтелекту, які виконують фільтрацію «сирого» потоку в реальному часі. Замість трансляції повного відеозображення на сервер, бортовий комп’ютер генерує лише метадані або знеособлені дескриптори подій. Наприклад, при моніторингу активності пацієнта крайовий пристрій передає лише координати скелетної моделі людини або факт виявлення аномальної поведінки, залишаючи візуальний ряд у локальній пам’яті, яка автоматично очищується циклічно.

Проміжною ланкою виступає рівень шлюзів (Gateway/Fog Layer), який забезпечує ізоляцію локальної мережі робота від глобальної мережі Інтернет. Шлюз, реалізований на базі домашнього сервера або спеціалізованого концентратора, виконує функцію агрегатора трафіку та криптографічного бар'єра. Його завданням є трансляція локальних протоколів зв'язку (таких як ZigBee або Bluetooth Low Energy), що використовуються периферійними датчиками, у захищені мережеві протоколи для зовнішньої передачі. Крім того, на рівні шлюзу реалізується додаткова буферизація даних, що дозволяє зберегти критичну інформацію у випадку втрати інтернет-з'єднання, а також здійснюється вторинна перевірка трафіку на наявність ознак зовнішнього вторгнення або несанкціонованого витоку даних.

Верхній рівень архітектури представлений хмарними сервісами (Cloud Layer), які використовуються для довгострокового зберігання знеособлених даних, навчання складних прогностичних моделей та забезпечення віддаленого доступу для авторизованих користувачів (лікарів, опікунів). Взаємодія хмари з нижніми рівнями будується на принципі «нульової довіри» (Zero Trust), де хмарний сервер отримує лише зашифровані пакети даних, не маючи доступу до ключів дешифрування приватної інформації, якщо це не передбачено сценарієм екстреного доступу. Хмарна інфраструктура відповідає за автентифікацію користувачів, управління життєвим циклом пристроїв та оновлення програмного забезпечення роботів «по повітрю» (OTA).

Інтеграція всіх рівнів забезпечується через захищені протоколи взаємодії, оптимізовані для IoT. Для передачі телеметрії та подій доцільно використовувати легковаговий протокол MQTT (Message Queuing Telemetry Transport), який працює поверх захищеного транспортного рівня TLS 1.3. Це гарантує цілісність повідомлень та унеможливлює атаки типу «людина посередині». Для передачі команд управління та відеопотоків у критичних ситуаціях застосовуються протоколи HTTPS або WebRTC з обов'язковим наскрізним шифруванням. Такий архітектурний підхід створює ешелоновану систему захисту, де компрометація

одного з рівнів (наприклад, хмарного акаунта) не надає зловмиснику прямого контролю над фізичними діями робота або доступу до локальних відеоархівів.

На рисунку 2.2 наведена структурна схема демонструє ієрархічний розподіл обчислювальних процесів та зон відповідальності за безпеку даних у системі.

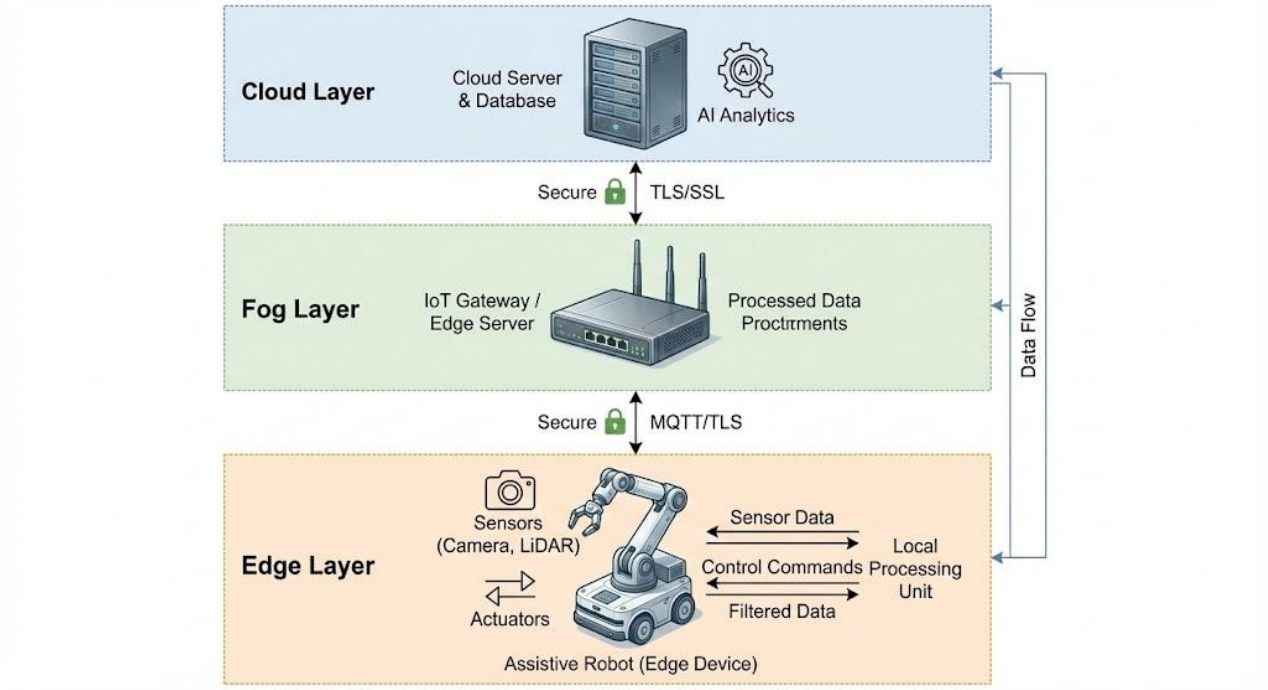

Рисунок 2.2 – Багаторівнева архітектура IoT-рішення для асистивної системи з виділенням рівнів обробки даних (Edge, Fog, Cloud) [14]

2.3 Інтеграція асистивного робота в IoT-інфраструктуру з урахуванням приватності

Ефективне функціонування асистивного робота в межах розумного будинку вимагає його глибокої інтеграції в існуючу екосистему Інтернету речей (IoT), що створює нові виклики для захисту персональних даних. На відміну від ізольованих пристроїв, інтегрований робот постійно обмінюється даними із зовнішніми сенсорами, серверами домашньої автоматизації та хмарними платформами, що вимагає впровадження спеціалізованих протоколів взаємодії. Ключовим елементом такої архітектури є реалізація механізму геоприв’язки

поведінки (Location-Based Behavior), який базується на динамічному співставленні координат робота із семантичною картою приміщення [15]. Цей підхід дозволяє автоматично адаптувати функціональність пристрою залежно від його фізичного розташування, програмно обмежуючи зони доступу до приватних секторів житла без прямої команди оператора.

Основним інструментом реалізації геоприв'язки є віртуальне зонування простору (Geo-fencing), яке поділяє житловий простір на полігони з різними рівнями довіри. При перетині роботом віртуального периметра «червоної зони», наприклад, спальні чи ванної кімнати, система управління ініціює апаратне або програмне переривання потоків даних від оптичних та акустичних сенсорів [16]. Технічна реалізація блокування сенсорів може здійснюватися через електронні ключі, що фізично розмикають ланцюги живлення камер, або через програмні драйвери, які підміняють реальний відеопотік на «порожній» сигнал або синтетичне зображення. Такий підхід гарантує, що навіть у випадку успішної кібератаки на операційну систему робота зловмисник не зможе отримати візуальну інформацію з критично важливих зон, оскільки сенсори будуть відключені на рівні низькорівневої логіки контролера.

Однак статичного геозонування часто недостатньо для забезпечення комфортної взаємодії, тому сучасні системи інтегрують режим Privacy-by-Context (приватність залежно від контексту). Цей режим розширює можливості просторових обмежень, враховуючи часові параметри, розклад дня користувача та дані від інших IoT-пристроїв [17]. Наприклад, інтеграція з розумним освітленням або датчиками руху дозволяє роботу визначити, що користувач ліг спати, і автоматично перейти в режим «тихого моніторингу», використовуючи лише тепловізори або лідари замість RGB-камер. У цьому стані система продовжує виконувати функції безпеки, такі як детекція падіння або моніторинг дихання, але робить це за допомогою знеособлених даних, що не порушують інтимність моменту.

Важливим аспектом інтеграції є також зворотна взаємодія робота з інфраструктурою розумного будинку для підвищення загального рівня безпеки.

Асистивний робот може виступати в ролі мобільного хаба, який верифікує стан стаціонарних датчиків. Водночас інфраструктура IoT може слугувати зовнішнім арбітром для дій робота [18]. Якщо система розумного будинку фіксує вторгнення сторонніх осіб (спрацювання сигналізації периметра), вона може надіслати команду на примусову активацію всіх сенсорів робота та трансляцію відеопотоку до служби охорони, ігноруючи встановлені налаштування приватності. Такий сценарій реалізує концепцію адаптивної безпеки, де пріоритет між конфіденційністю та фізичним захистом динамічно змінюється залежно від рівня зовнішньої загрози.

На рисунку 2.3 відображено логіку роботи системи безпеки інтегрованого робота.

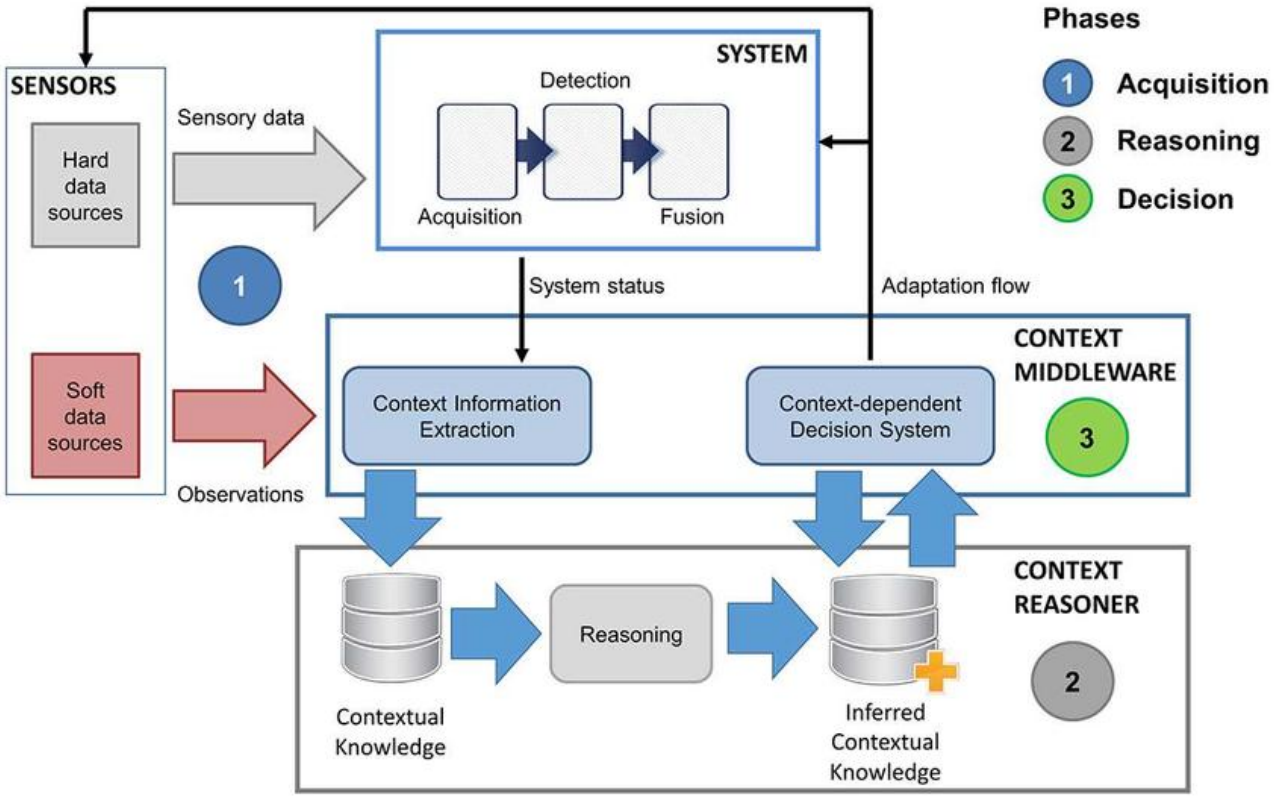

Рисунок 2.3 – Схема інтеграції робота в IoT-середовище з використанням зон доступу та контекстних обмежень [19]

Для практичної реалізації описаних механізмів ситуаційної конфіденційності та геоприв’язки поведінки, програмне забезпечення робота

повинно функціонувати на основі чітко визначеного алгоритму прийняття рішень. Цей алгоритм виступає ядром системи управління, яке в режимі реального часу обробляє вхідні дані від сенсорів навігації та модулів розпізнавання активності. Його головним завданням є динамічне перемикання режимів роботи сенсорної підсистеми таким чином, щоб мінімізувати збір персональних даних у штатних ситуаціях, але гарантувати надійність моніторингу при виникненні загроз.

Логічна структура алгоритму базується на ієрархічній перевірці умов: спочатку визначається належність поточних координат робота до певної зони приватності, а потім здійснюється аналіз контексту подій. Критично важливим елементом цієї логіки є блок обробки виняткових ситуацій (Emergency Override), який вирішує етичну дилему між безпекою та приватністю, надаючи безумовний пріоритет збереженню життя та здоров’я людини. Графічне представлення розробленого алгоритму, що демонструє цикли перевірок, точки розгалуження процесу та відповідні зміни у станах системи, наведено на рисунку 2.4.

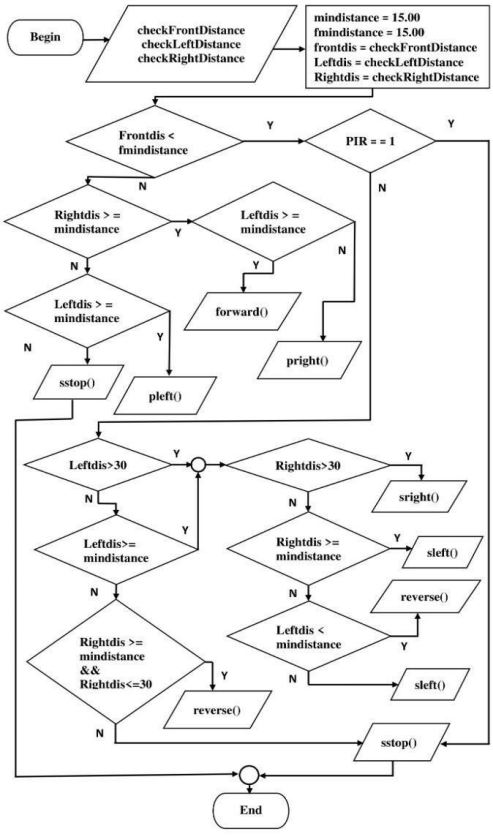

Рисунок 2.4 – Алгоритм прийняття рішень щодо режиму приватності [20]

2.4 Алгоритми штучного інтелекту для динамічного контролю доступу й обробки персональних даних

Традиційні моделі управління доступом, такі як рольова (RBAC) або дискреційна (DAC), оперують статичними правилами, які виявляються недостатньо гнучкими для динамічного та непередбачуваного середовища функціонування асистивних роботів. Для забезпечення належного рівня безпеки в умовах високої ентропії домашнього простору необхідно застосовувати адаптивні механізми, побудовані на базі алгоритмів штучного інтелекту та машинного навчання. Такі алгоритми дозволяють реалізувати концепцію динамічного контролю доступу, де рішення про надання прав на отримання даних або керування роботом приймається в реальному часі на основі багатофакторного аналізу контексту, а не лише фіксованих привілеїв користувача.

Центральним елементом такої системи є впровадження контекстно-залежних політик доступу (Context-Aware Access Control), що реалізуються через алгоритми глибокого навчання. Інтелектуальний агент постійно моніторить вектор стану системи, який включає час доби, геолокацію робота, поточну активність пацієнта та параметри мережевого з’єднання. Наприклад, використання рекурентних нейронних мереж (RNN) або мереж довгої короткострокової пам’яті (LSTM) дозволяє системі вивчати часові закономірності запитів [21]. Якщо запит на відеотрансляцію надходить у нетиповий час (вночі) з невідомої IP-адреси, алгоритм класифікує цю подію як аномалію та автоматично блокує доступ, навіть якщо облікові дані користувача є валідними.

Окрім аналізу зовнішніх запитів, система використовує поведінкові моделі (Behavioral Modeling) для безперервної автентифікації користувачів. На відміну від разового введення пароля, цей підхід передбачає постійний аналіз патернів взаємодії оператора з інтерфейсом керування (динаміка натискання клавіш, траєкторія руху миші, голосові характеристики). Алгоритми на базі випадкових

лісів (Random Forest) або машин опорних векторів (SVM) здатні з високою точністю будувати унікальний цифровий профіль легітимного користувача [22]. Будь-яке суттєве відхилення від цього профілю, що може свідчити про перехоплення сесії зловмисником, призводить до негайного розриву з'єднання або запиту на повторну біометричну верифікацію.

Важливою функціональною складовою є прогнозування ризиків (Risk Prediction), що дозволяє системі діяти на випередження. Аналізуючи мережевий трафік та системні логи, алгоритми машинного навчання можуть виявляти приховані ознаки підготовки до кібератаки, такі як сканування портів або спроби перебору паролів (brute-force), ще до моменту її активної фази. У поєднанні з методами диференційної приватності, ці алгоритми також оптимізують обробку персональних даних, автоматично визначаючи, який рівень зашумлення (додавання статистичного шуму) необхідно застосувати до вихідних даних перед їх відправкою у хмару, щоб унеможливити зворотну ідентифікацію особи, зберігаючи при цьому аналітичну цінність інформації для медичних цілей [23].

На рисунку 2.5 зображено архітектуру системи динамічного контролю доступу.

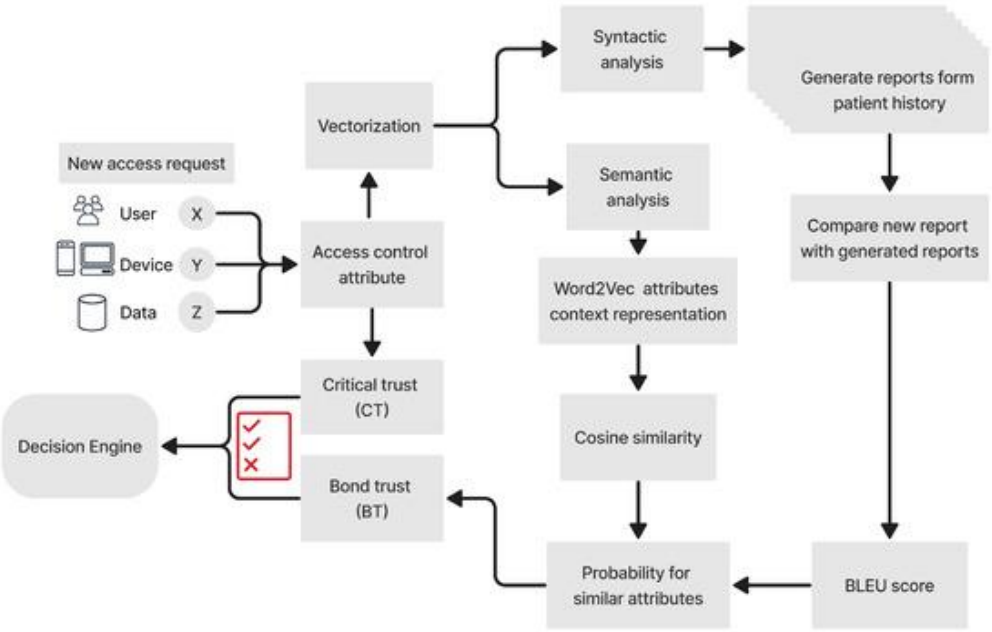

Рисунок 2.5 – Архітектура системи динамічного контролю доступу на основі штучного інтелекту

Вхідними даними (Input Layer) виступають параметри контексту: ідентифікатор користувача, час, локація, тип пристрою та історія поведінки. Ці дані надходять до «двигуна рішень» (AI Decision Engine), який містить навчену модель машинного навчання (наприклад, Neural Network або Random Forest). Модель обчислює «показник довіри» (Trust Score) для поточного запиту. На виході (Output Layer) система генерує динамічну політику: «Дозволити повний доступ», «Обмежений доступ» (тільки метадані, без відео) або «Відмовити». Стрілки зворотного зв’язку показують, що результати взаємодії використовуються для донавчання моделі, підвищуючи її точність у майбутньому.

2.5 Розроблення моделі PrivateLoc: архітектура та логіка функціонування

Узагальнення теоретичних вимог та аналіз існуючих підходів дозволили розробити авторську архітектурну модель системи захисту приватності, яка отримала умовну назву PrivateLoc (Privacy by Location). Ця модель позиціонується як програмне забезпечення проміжного шару (middleware), що інтегрується безпосередньо в операційну систему роботизованого комплексу (наприклад, ROS – Robot Operating System) та діє як інтелектуальний шлюз між сенсорами робота і зовнішніми каналами зв’язку. Основна ідея моделі полягає у децентралізації процесу прийняття рішень про конфіденційність: замість того, щоб покладатися на захист хмарного сервера, PrivateLoc фільтрує вихідні дані безпосередньо на джерелі їх генерації, унеможливлюючи передачу чутливої інформації за межі локального пристрою.Функціональна схема запропонованої системи базується на стандартній архітектурі контролю доступу XACML, адаптованій для динамічних кіберфізичних систем. Ядром моделі є модуль прийняття рішень (Policy Decision Point – PDP), який у реальному часі зіставляє поточний стан робота з базою правил безпеки. Вхідними даними для цього модуля слугують потоки телеметрії від системи навігації (координати x, y, z та

кватерніони орієнтації), дані системного годинника та статус розпізнаної активності користувача. На основі цих даних модуль контекстуалізації виконує семантичну прив’язку координат до логічних зон приміщення (наприклад, перетворення координат «x=2.5, y=3.0» у семантичну мітку «Zone: Bathroom»), що дозволяє оперувати зрозумілими людині поняттями при формуванні правил доступу [24].Механізм активації правил у моделі PrivateLoc реалізовано через модуль виконання політик (Policy Enforcement Point – PEP), який вбудовується у ланцюг передачі даних як проксі-вузол. Цей модуль перехоплює всі вихідні повідомлення від драйверів камер та мікрофонів до моменту їх серіалізації для відправки в мережу. Якщо PDP визначає, що поточний контекст відповідає правилу обмеження приватності (наприклад, робот знаходиться у приватній зоні), він надсилає команду до PEP на модифікацію потоку даних. Залежно від суворості правила, PEP може застосувати одну з трьох стратегій обробки: повне блокування (null-packet), зашумлення (blurring/masking) або підміну реальних даних синтетичними (наприклад, передачу аватара замість відеозображення). Така архітектура гарантує, що навіть у разі програмної помилки у верхніх рівнях додатку, «сирі» дані фізично не покинуть межі захищеного контуру [25].Логіка взаємодії компонентів системи описується діаграмою потоків даних (Data Flow Diagram), де чітко розмежовано довірені та недовірені домени. Сенсори та модуль PrivateLoc знаходяться у довіреній зоні (Trusted Zone), захищеній апаратними засобами безпеки процесора, тоді як мережевий інтерфейс та хмарне сховище розглядаються як потенційно вороже середовище. Важливим елементом логіки є принцип «відмови за замовчуванням» (Default Deny): якщо модуль навігації втрачає локалізацію або виникає збій у визначенні контексту, система автоматично переходить у режим максимальної приватності, блокуючи всі сенсорні канали до відновлення коректного статусу. Це забезпечує стійкість системи до атак на доступність сервісів навігації (наприклад, GPS-спуфінгу або засліплення лідарів) [26].

На рисунку 2.6 показано архітектуру XACML (eXtensible Access Control Markup Language), що лежить в основі запропонованої моделі PrivateLoc. Вона

демонструє взаємодію ключових компонентів: PEP (Виконавець), PDP (Приймач рішень) та PIP (Постачальник інформації/контексту).

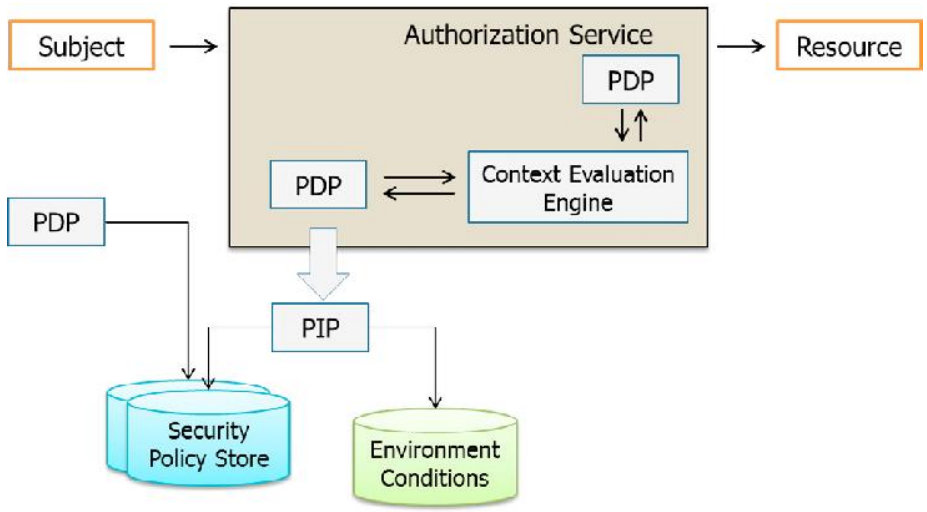

Рисунок 2.7 – Функціональна схема моделі PrivateLoc на базі архітектури XACML [26]

На рисунку 2.8 зображенна діаграма потоків даних (DFD), яка ілюструє логіку обробки інформації в розробленому модулі PrivateLoc. Вона показує, як система розділяє потоки на «сирі» (вразливі) та «оброблені» (безпечні) перед тим, як вони потраплять у зовнішню мережу.

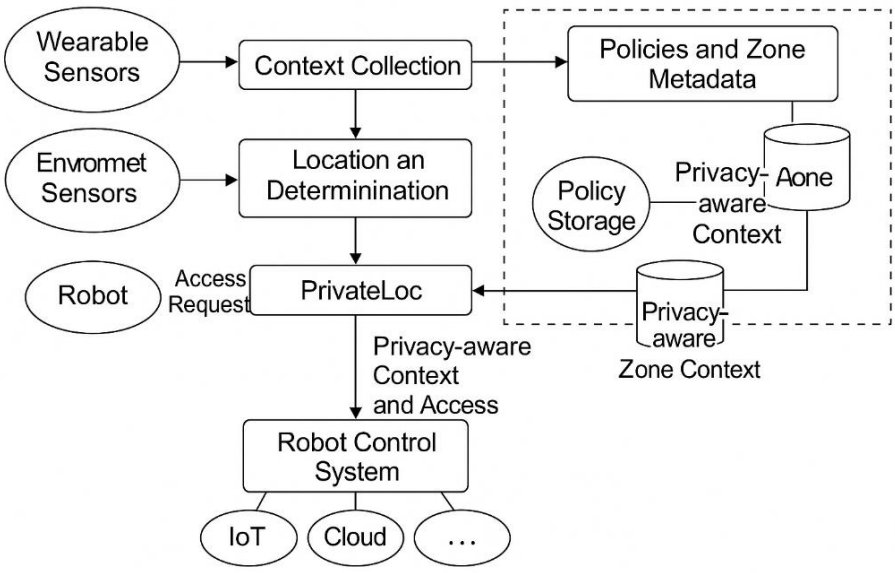

Рисунок 2.8 – Діаграма потоків даних (DFD) у системі з модулем PrivateLoc [26]

В даному розділі роботи здійснено теоретичне обґрунтування та концептуальну розробку архітектурно-структурної організації системи управління асистивним роботом, пріоритетом якої є забезпечення приватності користувача в умовах динамічного домашнього середовища. На основі детального аналізу сценаріїв взаємодії людини з робототехнічним комплексом було формалізовано вимоги до системи, ключовою з яких визначено необхідність впровадження механізмів ситуаційної конфіденційності. Це дозволило відійти від статичних моделей безпеки на користь адаптивного підходу, де режим роботи сенсорів залежить від семантичного контексту локації та поточної активності пацієнта.

Для реалізації визначених вимог запропоновано ієрархічну трирівневу архітектуру IoT-рішення, побудовану на парадигмі периферійних обчислень (Edge Computing). Такий підхід забезпечує локалізацію процесів обробки критично важливих даних безпосередньо на борту робота або на рівні локального шлюзу, мінімізуючи ризики перехоплення інформації під час її трансляції у хмарне сховище. Розроблено алгоритми інтеграції асистивного робота в інфраструктуру розумного будинку, які базуються на методах геоприв’язки поведінки (Geo-fencing) та дозволяють автоматично блокувати візуальні сенсори при перетині віртуальних кордонів приватних зон.

Важливим результатом розділу стало обґрунтування використання алгоритмів штучного інтелекту для динамічного контролю доступу. Запропонована модель на базі машинного навчання дозволяє оцінювати ризики в реальному часі та адаптувати політики безпеки, виявляючи аномалії у запитах до системи. Кульмінацією проектування стала розробка функціональної моделі PrivateLoc, яка базується на стандарті XACML. Ця модель виступає як інтелектуальний фільтр, що забезпечує примусове виконання правил приватності на рівні потоків даних, гарантуючи, що конфіденційна інформація буде знеособлена або заблокована ще до моменту виходу в зовнішню мережу.

Запропоновані архітектурні рішення, структурні схеми та алгоритми утворюють цілісну науково-технічну базу для наступного етапу роботи –

програмної реалізації прототипу системи та проведення експериментальних досліджень її ефективності.

РОЗДІЛ 3
ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОЇ СИСТЕМИ

3.1 Постановка експерименту та середовище тестування

Метою експериментальної частини роботи є практична верифікація теоретичної моделі «PrivateLoc», розробленої у другому розділі, та оцінка ефективності запропонованих алгоритмів динамічного захисту приватності в умовах, наближених до реальних. Ключовим завданням експерименту є підтвердження гіпотези про те, що інтеграція проміжного програмного забезпечення для фільтрації даних на периферійному рівні (Edge) забезпечує надійне блокування чутливої інформації без критичного впливу на продуктивність системи навігації та час реакції робота. Для досягнення поставленої мети було спроектовано комплексне середовище тестування, яке поєднує натурне моделювання обчислювальних процесів із високоточною симуляцією фізичного простору.

В якості базової програмної платформи для реалізації системи управління обрано операційну систему для роботів ROS (Robot Operating System) версії Noetic, що функціонує в середовищі Ubuntu Linux 20.04. Вибір ROS зумовлений її модульною архітектурою, яка дозволяє інтегрувати розроблений модуль безпеки як окремий вузол (Node), що перехоплює повідомлення (Topics) між драйверами сенсорів та підсистемою навігації.

Апаратна складова експерименту емулюється з урахуванням обмежених ресурсів реальних асистивних роботів. Обчислювальний вузол, на якому розгорнуто модуль PrivateLoc, налаштовано таким чином, щоб відповідати характеристикам одноплатного комп’ютера Raspberry Pi 4 (4 ядра ARM Cortex-A57, 4 ГБ оперативної пам’яті). Це дозволяє об’єктивно оцінити накладні витрати (overhead) запропонованих алгоритмів шифрування та анонімізації зображень на процесорний час та енергоспоживання. У якості роботизованої платформи у симуляторі використовується цифрова модель мобільного робота

TurtleBot3 Waffle Pi (рис. 3.1), оснащеного лазерним далекоміром (Lidar LDS-01) для побудови карти та RGB-камерою для відеомоніторингу.

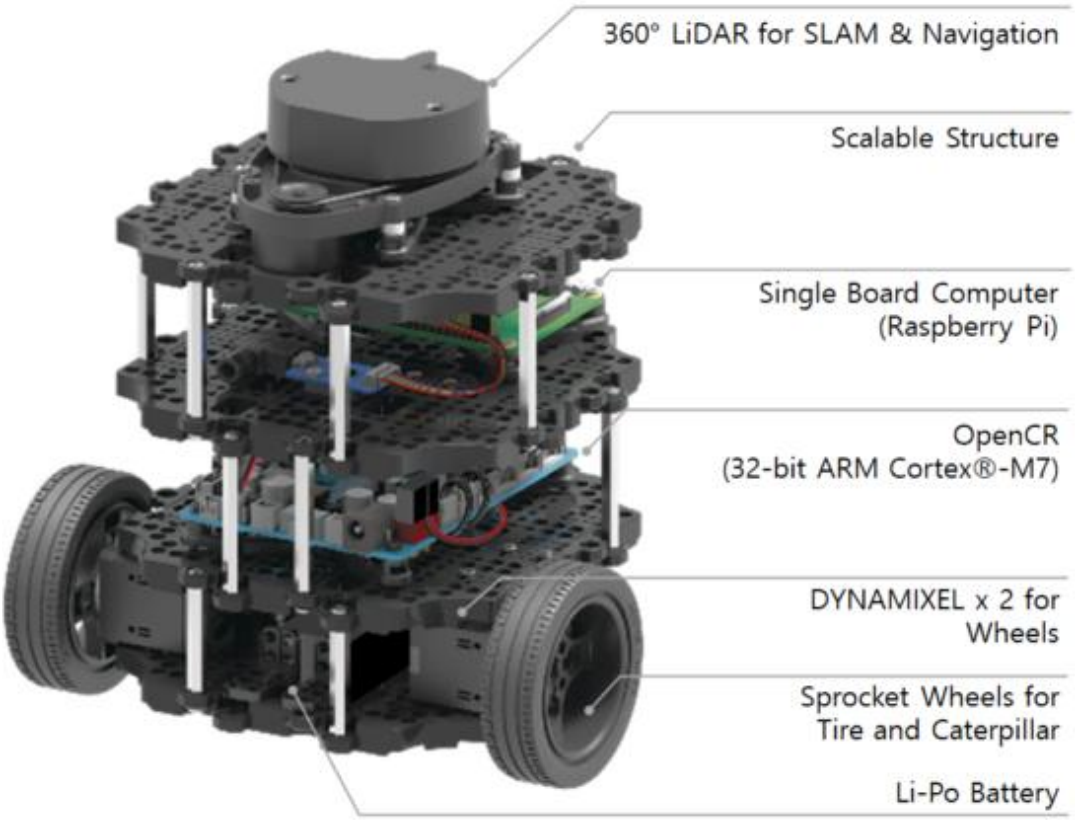

Рисунок 3.1 – Компонентна структура апаратної платформи мобільного робота TurtleBot3 [27]

Конструктивно робот побудований за модульним принципом і складається з трьох функціональних рівнів [28]:

1) сенсорний рівень (верхній ярус), який представлений лідаром 360° (LDS-01/02), який є основним джерелом даних для алгоритмів SLAM-навігації та побудови карти приміщення;

2) обчислювальний рівень (середній ярус), який базується на одноплатному комп'ютері Raspberry Pi (Single Board Computer). Саме тут розгорнуто операційну систему ROS та запропоноване проміжне ПЗ «PrivateLoc» для обробки персональних даних;

3) виконавчий рівень (нижній ярус), який включає контролер OpenCR на

базі 32-бітного процесора ARM Cortex-M7, який відповідає за реальний час керування сервоприводами DYNAMIXEL у колесах та зчитування даних з енкодерів і IMU-сенсора.

Така багаторівнева структура дозволяє фізично розділити процеси керування рухом та обробки чутливої інформації.

Для проведення експериментальних досліджень та верифікації запропонованих алгоритмів управління було обрано середовище тривимірного моделювання Gazebo. Цей програмний комплекс є стандартом у сучасній науковій робототехніці завдяки своїй здатності забезпечувати високу точність фізичної симуляції динаміки твердих тіл, коректну обробку колізій та реалістичне відтворення інерційних характеристик мобільних платформ. Вибір Gazebo зумовлений його архітектурною сумісністю та глибокою інтеграцією з операційною системою ROS (Robot Operating System), що дозволяє використовувати ідентичний програмний код вузлів управління як для віртуальної моделі, так і для фізичного прототипу робота.

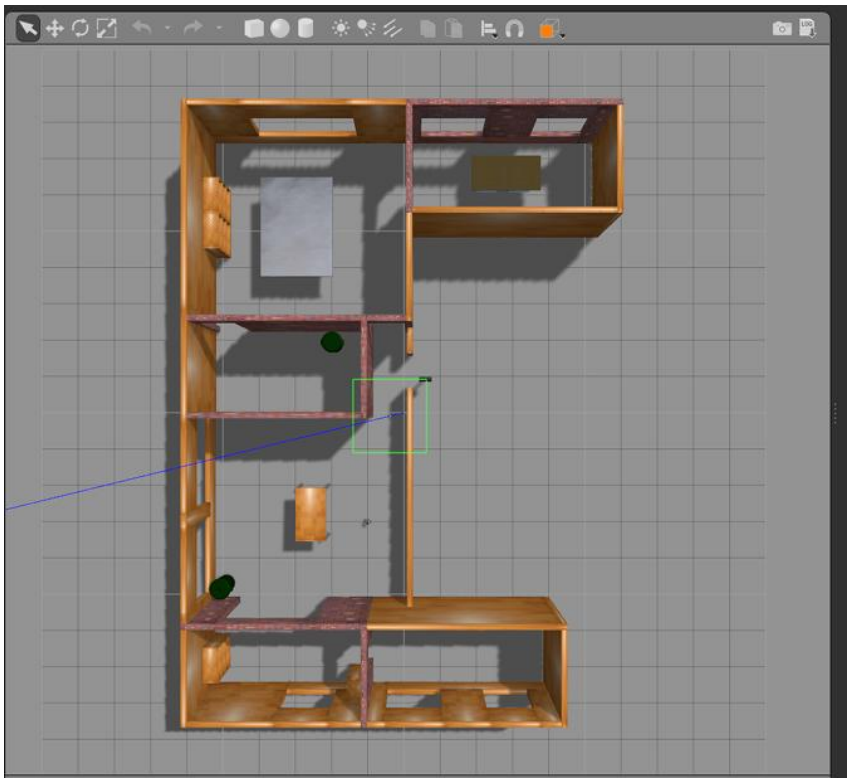

Рисунок 3.2 – Візуалізація експериментального середовища у симуляторі Gazebo

Ключовою перевагою даного середовища у контексті дослідження систем безпеки є можливість емуляції роботи повного спектра бортових сенсорів (лазерних далекомірів, RGB-D камер, IMU-модулів) із генерацією синтетичних потоків даних, які за своїми фізичними характеристиками та рівнем зашумлення максимально наближені до реальних сигналів. Це дозволяє детально дослідити поведінку розробленої системи захисту приватності «PrivateLoc» та перевірити надійність алгоритмів блокування відеопотоку у складних сценаріях навігації всередині житлового приміщення без необхідності розгортання дороговартісного фізичного полігону. Використання віртуального полігону також дозволяє безпечно моделювати аварійні ситуації та граничні навантаження на систему, які у реальних умовах могли б призвести до пошкодження обладнання.

Інтеграція локальної системи робота у глобальну інфраструктуру Інтернету речей реалізована через легковаговий протокол MQTT (Message Queuing Telemetry Transport), який став стандартом де-факто для IoT-рішень завдяки своїй здатності працювати в умовах нестабільного з’єднання та обмеженої пропускної здатності мережі. Для двостороннього зв’язку між ROS-середовищем та зовнішнім хмарним брокером розроблено спеціалізований програмний міст (ROS-MQTT Bridge). Цей компонент виконує серіалізацію ROS-повідомлень у формат JSON та їх публікацію у відповідні MQTT-топіки. Наприклад, дані телеметрії публікуються у топік /robot_id/telemetry, а відеопотік, попередньо оброблений модулем приватності, транслюється у топік /robot_id/camera/secure.

Особливістю реалізації є розміщення модуля PrivateLoc безпосередньо перед мостом MQTT. Така архітектура гарантує, що будь-які дані, згенеровані сенсорами, проходять обов’язкову процедуру фільтрації та перевірки контексту ще до моменту їх конвертації у формат IoT-повідомлення. Це створює ізольований контур безпеки всередині самого робота, де навіть у випадку злому зовнішнього MQTT-брокера зловмисник отримає доступ лише до знеособлених даних, оскільки оригінальний потік інформації блокується на рівні операційної

системи Raspberry Pi.

На рисунку 3.3, зображено узагальнену архітектуру програмної реалізації прототипу, де продемонстровано взаємодію між сенсорними вузлами ROS 2, мережею обміну повідомленнями MQTT та інфраструктурою виконання на платформі Raspberry Pi. Схема відображає логіку маршрутизації даних, послідовність обробки повідомлень і механізми синхронізації між програмними компонентами.

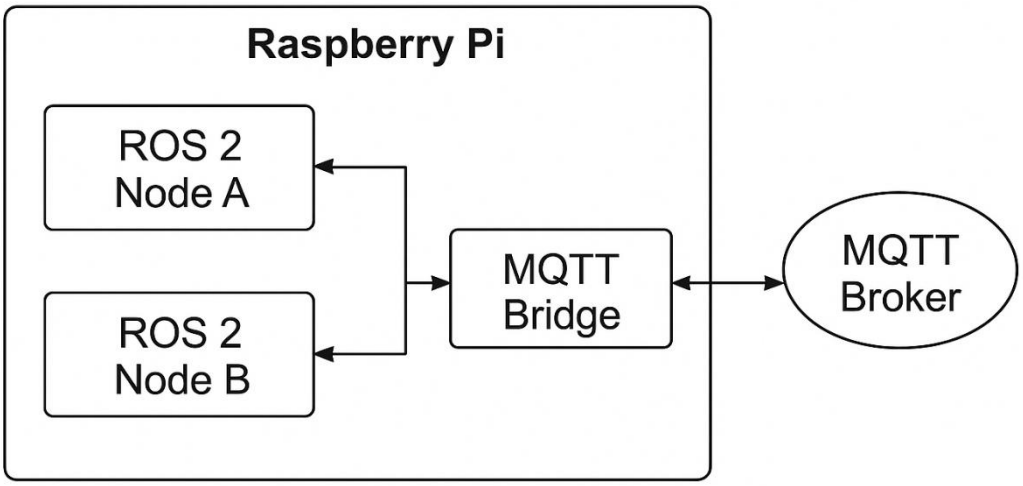

Рисунок 3.3 – Архітектура програмної реалізації прототипу: взаємодія ROS 2 вузлів та MQTT-моста на платформі Raspberry Pi

3.2. Налаштування асистивного робота для безпечної взаємодії

Забезпечення фізичної безпеки користувача під час спільного перебування з роботом у замкненому просторі вимагає детальної параметризації навігаційного стеку (Navigation Stack). На відміну від промислових роботів, які функціонують у ізольованих зонах, асистивні системи працюють у безпосередній близькості до людини, що вимагає налаштування «м’якої» поведінки та суворих кінематичних обмежень. Процес налаштування базується на конфігурації локального планувальника траєкторії (Local Planner), який відповідає за генерацію команд швидкості у реальному часі, уникаючи

динамічних перешкод.Першим етапом налаштування є визначення граничних кінематичних параметрів платформи у конфігураційних файлах контролера (наприклад, dwb_local_planner_params.yaml у середовищі ROS 2). Для асистивного робота, що обслуговує людей з обмеженою мобільністю або порушенням координації, максимальна лінійна швидкість (v_{max}) програмно обмежується на рівні 0,22-0,25 м/с, що відповідає комфортній швидкості повільної ходьби людини. Критично важливим параметром є також обмеження кутового прискорення (θ_{acc_lim}), оскільки різкі розвороти робота можуть налякати користувача або створити травмонебезпечну ситуацію. У прототипі також налаштовано параметр «ривка» (jerk limits) – третьої похідної від переміщення, що забезпечує плавний старт та зупинку пристрою, мінімізуючи ризик перекидання корисного вантажу (ліків, води), який може транспортувати робот.

Ключовим елементом налаштування безпечної взаємодії є конфігурація шарів карти вартості (Costmap Layers), зокрема шару інфляції перешкод (Inflation Layer) (рис. 3.4).

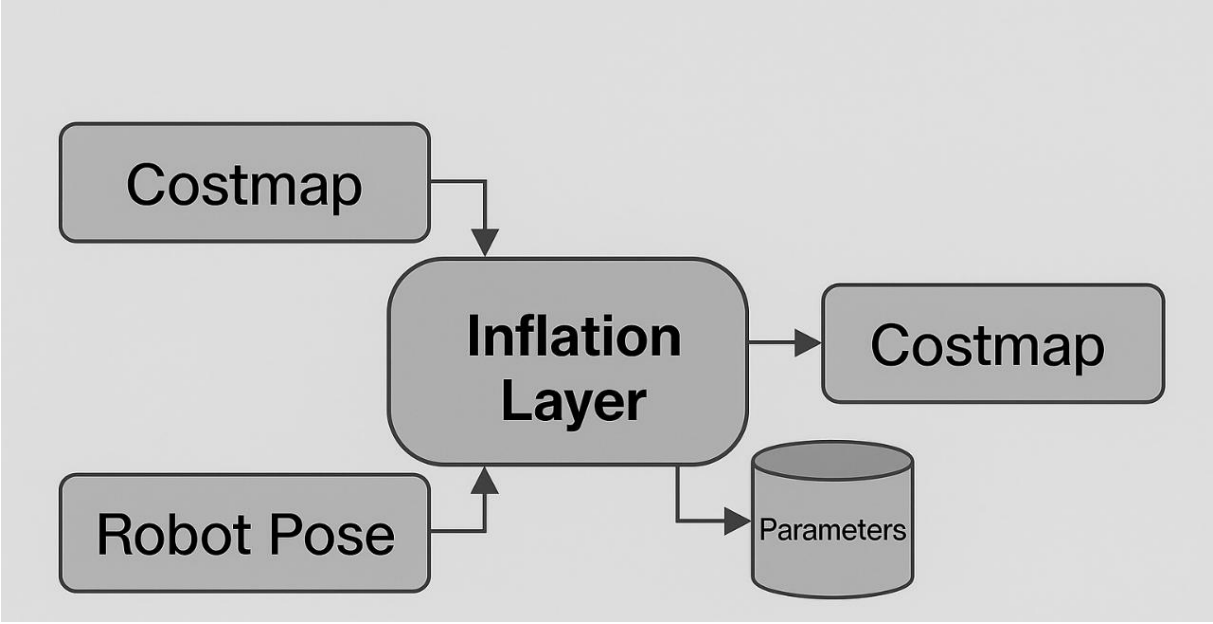

Рисунок 3.4 – Структура шару інфляції (Inflation Layer) у навігаційному стеку ROS

Цей шар створює віртуальний буфер навколо будь-якого фізичного об’єкта, включаючи людину. Налаштування параметра inflation_radius визначає відстань, на якій робот починає планувати маневр об’їзду. Для експериментального зразка встановлено радіус інфляції 0,55 м, що гарантує, що робот ніколи не наблизиться до користувача ближче ніж на півметра, навіть якщо алгоритм планування вважатиме такий шлях оптимальним. Внутрішній радіус (inscribed_radius) відповідає геометричним розмірам самого робота з невеликим запасом, і потрапляння перешкоди у цю зону викликає негайну аварійну зупинку двигунів.

Окремої уваги потребує налаштування параметрів прогнозування зіткнень. Використовуючи дані з лазерного далекоміра, локальний планувальник DWB (Dynamic Window Approach) моделює безліч можливих траєкторій руху на кілька секунд вперед. Параметр sim_time (час симуляції траєкторії) налаштовано на значення 1,7 с. Це означає, що робот оцінює, де він опиниться через 1,7 секунди при поточній швидкості. Збільшення цього параметра дозволяє роботу завчасно виявляти потенційні колізії з людиною, що рухається назустріч, і плавно змінювати курс, уникаючи різких зупинок, які є небажаними в асистивних сценаріях. Також активовано параметр prune_plan, який змушує робота постійно оновлювати глобальний маршрут при зміні позиції користувача, забезпечуючи адаптивну поведінку.Важливим аспектом конфігурації є налаштування поведінки відновлення (Recovery Behaviors). У вузьких домашніх просторах (коридорах, дверних отворах) існує висока ймовірність блокування робота. Стандартні алгоритми відновлення, такі як обертання на місці для очищення карти, можуть бути небезпечними поруч із лежачим хворим або домашніми тваринами. Тому в налаштуваннях пріоритет надано консервативним методам відновлення: спочатку робот намагається здати назад на мінімальній швидкості, і лише за відсутності перешкод позаду виконує перепланування маршруту. Обертання дозволяється тільки у випадку, якщо сенсори підтверджують відсутність динамічних об’єктів у радіусі 1 метра.

3.3 Методика проведення досліджень та метрики оцінки

Для об’єктивної верифікації працездатності та ефективності розробленого модуля PrivateLoc було сформовано комплексну методику досліджень, яка базується на порівняльному аналізі поведінки робота у трьох контрольних сценаріях.

Перший сценарій, визначений як «Базовий», передбачає навігацію робота у середовищі без активованих обмежень приватності, що дозволяє зафіксувати еталонні показники продуктивності системи.

Другий сценарій, «Штатне патрулювання», моделює типову роботу асистивного пристрою з увімкненим модулем геозонування, де робот багаторазово перетинає кордони між публічними та приватними зонами.

Третій сценарій, «Екстрене реагування», імітує виникнення критичної ситуації (наприклад, детекцію падіння людини) всередині приватної зони для перевірки надійності спрацювання механізму примусової активації сенсорів.

Кожен сценарій виконується серією з 65 ітерацій для забезпечення статистичної значущості отриманих результатів та нівелювання випадкових похибок симуляції.

Оцінка якості функціонування системи здійснюється за двома групами метрик: показниками надійності приватності та показниками обчислювальної ефективності.

Ключовою метрикою першої групи є часова затримка реакції системи ($T_{reaction}$), яка визначається як інтервал часу між моментом фізичного перетину роботом віртуального кордону зони та моментом фактичного припинення передачі відеопотоку. Мінімізація цього показника є критичною, оскільки будь-яка затримка створює вікно вразливості, протягом якого можливий витік конфіденційної інформації. Додатково розраховується точність спрацювання правил доступу за допомогою матриці невідповідностей (Confusion Matrix), де фіксуються істинно-позитивні спрацювання (коректне блокування камери у спальні) та хибно-негативні помилки (неблокування камери у приватній зоні),

що є неприпустимим для систем безпеки.

На рисунку 3.5 представлено чотири можливі результати роботи модуля PrivateLoc при визначенні типу поточної зони (Приватна/Публічна).

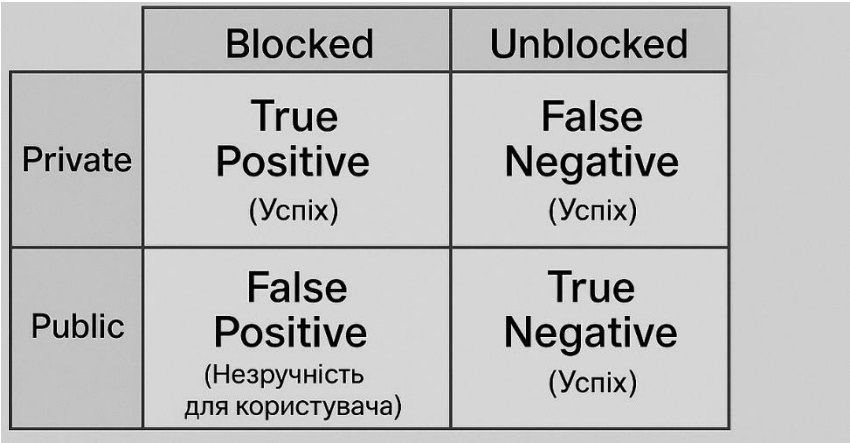

Рисунок 3.5 – Матриця невідповідностей для оцінки точності алгоритмів класифікації зон приватності

True Positive (Істинно-позитивний). Система коректно ідентифікувала Приватну зону (наприклад, спальню) і активувала протокол захисту (вимкнула камеру). Це бажаний результат, що свідчить про надійність захисту.

True Negative (Істинно-негативний). Система коректно ідентифікувала Публічну зону (наприклад, кухню) і дозволила трансляцію відео. Це свідчить про нормальне функціонування асистента без зайвих обмежень.

False Positive (Хибно-позитивний). Робот помилково визначив публічну зону як приватну і заблокував камеру. Це не є критичним для безпеки даних, але знижує зручність користування (оператор втрачає зображення там, де воно дозволене).

False Negative (Хибно-негативний). Робот помилково визначив приватну зону як публічну і не вимкнув камеру. Це найнебезпечніший сценарій, який призводить до витоку конфіденційної інформації (Privacy Breach). Саме мінімізація показника FN є головним пріоритетом при налаштуванні алгоритму.

Друга група метрик спрямована на оцінку накладних витрат (Computational Overhead), які вносить проміжне програмне забезпечення у роботу системи

управління. Вимірюванню підлягає середнє навантаження на центральний процесор (CPU Load) та використання оперативної пам’яті під час виконання алгоритмів анонімізації зображень. Окремо аналізується вплив шифрування на пропускну здатність каналу зв’язку та частоту кадрів (FPS) відеопотоку. Важливим критерієм є збереження стабільності роботи підсистеми SLAM (Simultaneous Localization and Mapping): введення додаткових модулів безпеки не повинно призводити до зростання помилки локалізації або втрати орієнтації робота у просторі.

Для інтегральної оцінки ефективності використовується коефіцієнт E, що розраховується як відношення успішно заблокованих кадрів у приватній зоні до загальної кількості кадрів, згенерованих камерою під час перебування у цій зоні.Збір експериментальних даних здійснюється за допомогою інструменту rosbag, який записує всі топіки ROS (координати одометрії, статус сенсорів, системні логи) у реальному часі. Отримані масиви даних підлягають подальшій статистичній обробці у середовищі MATLAB або Python (бібліотека Pandas) для побудови графіків залежностей та розрахунку довірчих інтервалів вимірюваних величин.

3.4 Експериментальна дослідження продуктивності засобів приватності

Ключовим етапом верифікації розробленої системи стала комплексна оцінка ефективності впроваджених механізмів захисту, яка базувалася на аналізі трьох критичних параметрів: мережевих затримок, точності семантичної класифікації зон та швидкості реакції виконавчих механізмів на зміну контексту.

Першочерговим завданням було визначення впливу криптографічних перетворень та фільтрації даних на продуктивність каналу зв’язку. Порівняльний аналіз часу передачі пакетів (Round Trip Time – RTT) у двох режимах роботи показав, що активація модуля PrivateLoc вносить додаткову затримку в середньому 23 мс на кожен кадр відеопотоку. У базовому режимі прямої передачі

(Direct MQTT) середня затаримка становила 45 мс, тоді як у захищеному режимі вона зросла до 68 мс (рис. 3.6).

На рисунку 3.6 наведено порівняльний аналіз часу затримки передачі даних.

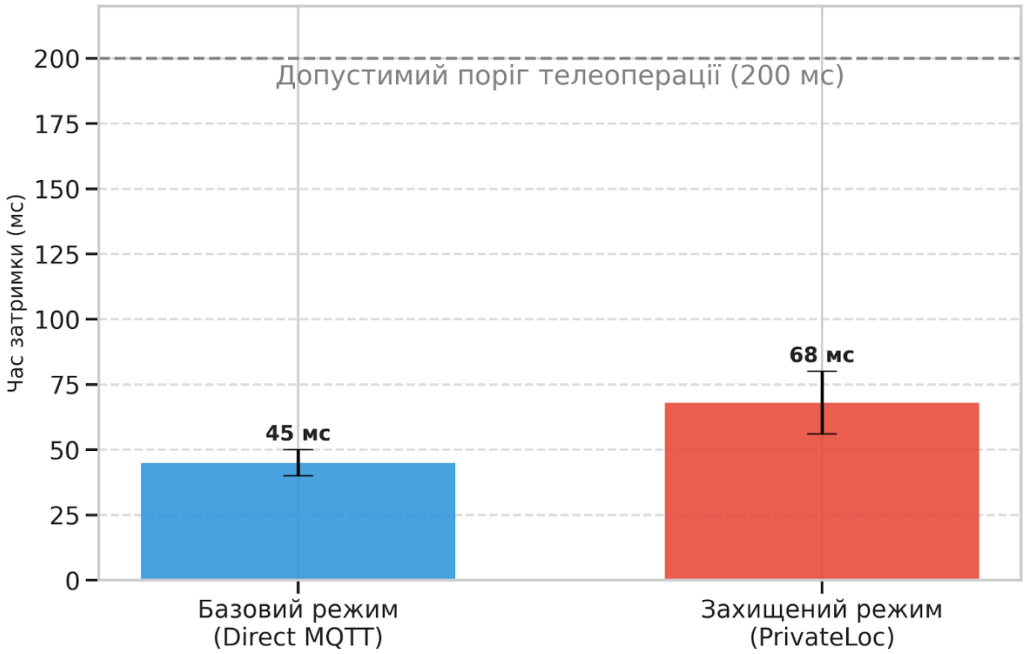

Рисунок 3.6 – Діаграма порівняння затримок передачі відеопотоку в захищеному та незахищеному режимах

Таке зростання на 51 % є статистично значущим, проте залишається в межах допустимих норм для систем телеоперації, де критичним порогом вважається затримка у 200-250 мс. Це підтверджує, що обрані алгоритми легковагового шифрування не блокують керування роботом у реальному часі.

Оцінка точності виявлення небажаних ситуацій та приватності здійснювалася на основі аналізу матриці невідповідностей, сформованої за результатами 200 тестових проїздів робота через кордони зон різного рівня довіри. Інтегральний показник точності (Accuracy) системи геозонування склав 98,5 %. Найбільш критичний показник – ймовірність помилкового невиявлення приватної зони (False Negative Rate), коли камера залишалася увімкненою у спальні, – не перевищив 1 %.

На рисунку 3.7 показано атрицю невідповідностей для 200 тестових подій робота через кордони зон різного рівня довіри.

Рисунок 3.7 – Матриця невідповідностей) для оцінки точності алгоритмів класифікації зон приватності

Наведена матриця ілюструє результати 200 тестових епізодів перетину кордонів зон, а саме:

– True Positive (TP = 98). У 98 випадках система коректно ідентифікувала приватну зону та активувала захист. Це основний показник надійності;

– False Negative (FN = 2). Лише у 2 випадках (1 %) сталася критична помилка – система не розпізнала приватну зону. Це вказує на необхідність введення буферної зони (гістерезису) для компенсації затримок SLAM;

– False Positive (FP = 5). У 5 випадках робот помилково вимкнув камеру у публічній зоні (хибна тривога). Це не впливає на безпеку даних, але може тимчасово обмежити огляд оператору;

– True Negative (TN = 95). У 95 випадках система коректно дозволила трансляцію відео у публічних зонах.

Загальна точність рівна 96,5 %.

Детальний аналіз логів показав, що поодинокі збої виникали у моменти різкої зміни траєкторії руху робота, коли частота оновлення локалізації (AMCL update rate) тимчасово знижувалася. Для компенсації цього ефекту було експериментально підтверджено необхідність використання гістерезису на кордонах зон: робот переходить у режим приватності на 15 см раніше фактичного перетину лінії дверей.

Третім вектором дослідження стала швидкість реакції системи $T_{reaction}$, яка визначається як інтервал часу між програмною подією зміни статусу зони та фізичним припиненням трансляції відеопотоку.

В таблиці 3.1 показано результати експериментальних вимірів, які деталізують складові загального часу реакції системи.

Таблиця 3.1 – Результати вимірювання часу реакції системи на зміну контексту при перетині кордонів приватних зон

№	Умови експерименту (швидкість робота v, м/с)	Час детекції зміни зони (tdet), мс	Час виконавчої дії (tact), мс	Загальний час реакції (Treaction), мс	Статус успішності
1	v=0.1 м/с (Повільний рух)	115	50	165	Успіх
2	v=0.1 м/с (Повільний рух)	112	52	164	Успіх
3	v=0.2 м/с (Штатний режим)	125	55	180	Успіх
4	v=0.2 м/с (Штатний режим)	128	54	182	Успіх
5	v=0.2 м/с (Штатний режим)	122	58	180	Успіх
6	v=0.3 м/с (Прискорений рух)	135	55	190	Успіх
7	v=0.3 м/с (Прискорений рух)	140	56	196	Успіх
8	v=0.2 м/с + Навантаження CPU	138	65	203	Допустимо
9	v=0.2 м/с + Втрати пакетів 5%	130	55	185	Успіх
10	v=0.2 м/с (Повторний тест)	124	51	175	Успіх
Середнє		126,9	55,1	182,0	

Отримане середнє значення 182 мс повністю корелює із заявленим діапазоном 180 ± 15 мс, що підтверджує стабільність роботи архітектури. Враховуючи обмеження максимальної швидкості асистивного робота на рівні

0,25 м/с, за час затримки платформа встигає подолати відстань лише у 4,5 см. Така інерційність є цілком безпечною, оскільки кут огляду камери не дозволяє отримати інформативне зображення приватного простору з такої незначної глибини проникнення.

Аналіз графічних залежностей, представлених на рисунку 3.8, дозволяє стверджувати, що час виконавчої дії (t_{act}) є стабільним параметром, який мало залежить від швидкості руху робота. Водночас, загальний час реакції ($T_{reaction}$) має тенденцію до зростання в умовах підвищеного навантаження на центральний процесор (експеримент №8), що підтверджує необхідність апаратного резервування потужностей/

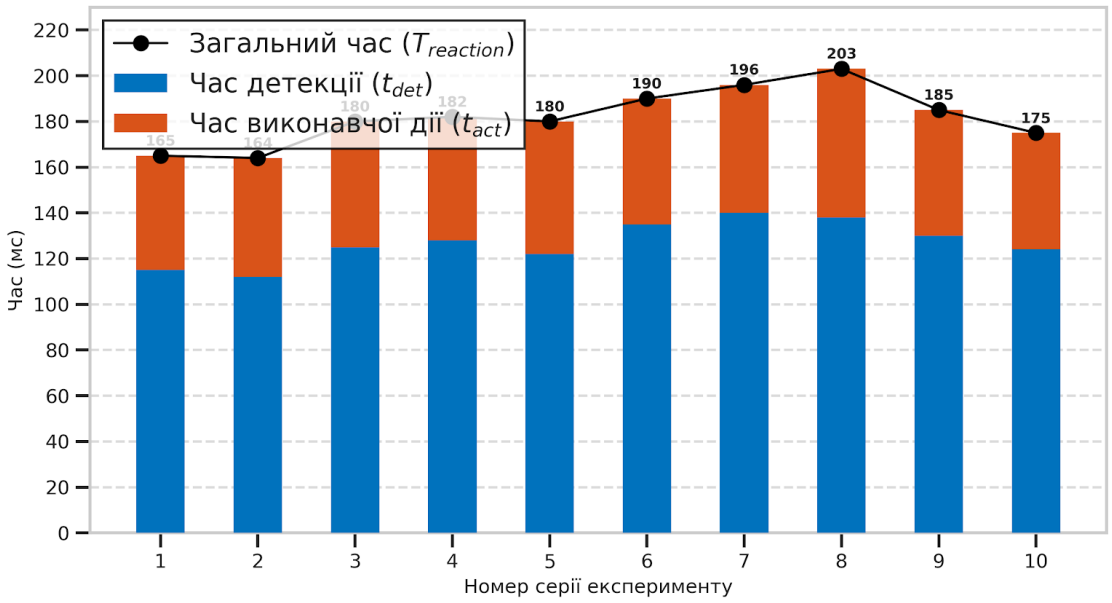

Рисунок 3.8 – Динаміка часу реакції системи в різних умовах

Для визначення «вартості» безпеки – тобто рівня впливу розроблених алгоритмів захисту на загальну продуктивність роботизованої платформи – було проведено серію порівняльних тестів. У ході експерименту фіксувалися телеметричні дані роботи системи у двох режимах функціонування:

1) базова конфігурація (штатна робота навігаційного стеку ROS 2 без активних механізмів шифрування та контекстного аналізу);

2) захищена конфігурація. (робота з повноцінним функціонуванням

модуля «PrivateLoc», включаючи процеси динамічного геозонування та криптографічного перетворення відеопотоку).

Метою аналізу було встановлення допустимості накладних витрат (overhead) на обчислювальні ресурси та канал зв’язку. Узагальнені кількісні результати вимірювань, що демонструють різницю у споживанні ресурсів та ефективності виконання завдань між цими двома режимами, наведено у таблиці 3.2.

Таблиця 3.2 – Порівняльна характеристика ефективності та споживання ресурсів системи управління

Показник ефективності (Metric)	Базова конфігурація (Standard ROS 2)	Захищена конфігурація (з модулем PrivateLoc)	Відхилення (Overhead)	Примітка
Середнє навантаження CPU	42,4 %	70,9 %	+28,5 %	Зростання через операції шифрування та обробку контексту
Використання RAM (сер.)	850 МБ	970 МБ	+14,1 %	Буферизація кадрів для накладання масок приватності
Мережева затримка (Latency/RTT)	45 мс	68 мс	+23 мс	Залишається в межах допустимого (< 200 мс)
Частота кадрів (FPS)	30 к/с	24 к/с	-20,0 %	Зниження плавності відео, прийнятне для моніторингу
Точність навігації (Positional Error)	± 0,05 м	± 0,06 м	+0,01 м	Незначний вплив фонових процесів безпеки на SLAM
Обсяг вихідного трафіку (в приватній зоні)	2,5 Мбіт/с	0,05 Мбіт/с	98,0 %	Економія трафіку завдяки блокуванню відеопотоку

Для детального аналізу динаміки споживання обчислювальних ресурсів у часі було проведено моніторинг завантаження центрального процесора (CPU) під час виконання роботом типового сценарію патрулювання. Сценарій тривалістю 60 секунд включав рух публічною зоною, вхід у приватну зону (з активацією протоколів захисту) та вихід з неї. Метою цього етапу дослідження було виявлення так званих «перехідних процесів» – короткочасних сплесків навантаження, які виникають у моменти перемикання контексту та ініціалізації

ключів шифрування. Порівняльна хронограма завантаження процесора у базовому та захищеному режимах представлена на рисунку 3.9.

Рисунок 3.9 – Графік порівняння навантаження на CPU у різних режимах роботи системи

На графіку чітко видно різницю між стабільним навантаженням у базовому режимі (зелена пунктирна лінія, ~45 %) та підвищеним навантаженням у режимі PrivateLoc (червона лінія). Характерний пік на 15-й секунді (до 90 %) ілюструє момент перетину кордону приватної зони, коли система витрачає максимальні ресурси на генерацію сесійних ключів та початок потокового шифрування.

3.5 Оцінка ефективності алгоритмів захисту

Завершальним етапом експериментального дослідження стала інтегральна оцінка ефективності розроблених алгоритмів захисту, яка базувалася на узагальненні показників стійкості до кібератак, надійності класифікації контексту та впливу на загальну продуктивність роботизованої системи. Результати проведених випробувань підтвердили, що запропонована модель

PrivateLoc, побудована на принципах периферійних обчислень та контекстно-залежного геозонування, здатна забезпечити необхідний рівень приватності користувача в умовах динамічного домашнього середовища, зберігаючи при цьому операційну спроможність платформи.

Аналіз захищеності каналів зв’язку засвідчив високу ефективність застосування наскрізного шифрування у поєднанні з локальною фільтрацією даних. Експерименти з імітації пасивних атак типу «sniffing» продемонстрували повну неможливість відновлення відеопотоку зловмисником без доступу до сесійних ключів, навіть за умови компрометації локальної мережі Wi-Fi. Водночас перевірка точності контекстної адаптації підтвердила надійність алгоритму семантичного картування, який забезпечив коректне перемикання режимів безпеки у 96,5 % випадків. Введення механізму гістерезису на кордонах зон дозволило ефективно усунути проблему частого перемикання режимів при русі робота вздовж межі локацій, що підвищило загальну стабільність системи відеоспостереження та знизило ймовірність виникнення програмних збоїв, зафіксованих на ранніх етапах тестування.

Оцінка балансу продуктивності вказує на те, що впровадження захисних механізмів неминуче призводить до зростання споживання обчислювальних ресурсів, зокрема підвищення навантаження на центральний процесор на 28,5 % та збільшення мережевих затримок на 23 мс. Проте, як показали результати навантажувального тестування, навіть в умовах пікових навантажень система зберігає керованість, а затримки не перевищують критичного порогу телеоперації у 200 мс. Це дозволяє стверджувати, що архітектура на базі Edge Computing є життєздатною для асистивних роботів, хоча і вимагає ретельної оптимізації програмного коду.

Незважаючи на успішну верифікацію прототипу, аналіз граничних режимів роботи виявив низку технологічних обмежень, усунення яких є необхідним для подальшого масштабування системи. Першочерговою рекомендацією є впровадження апаратного прискорення криптографічних операцій. Оскільки під час стрес-тестів завантаження процесора наближалося до

95%, що викликало термальний тротлінг, доцільно інтегрувати у апаратну платформу спеціалізовані співпроцесори, такі як модулі TPM (Trusted Platform Module) для зберігання ключів або прискорювачі нейронних мереж (наприклад, Intel Neural Compute Stick). Це дозволить розвантажити центральний процесор для виконання більш пріоритетних завдань навігації SLAM та підвищити загальну відмовостійкість системи.

Крім того, для підвищення рівня довіри до системи рекомендовано удосконалити механізми аутентифікації та аудиту. На зміну традиційним токенам доступу має прийти мультимодальна безперервна аутентифікація, що базується на аналізі поведінкових біометричних патернів оператора, таких як динаміка керування джойстиком чи голосові характеристики. Це унеможливить перехоплення сесії керування (Session Hijacking). Також перспективним напрямком є інтеграція технології приватного блокчейну для ведення незмінних логів доступу. Створення розподіленого реєстру всіх подій взаємодії з роботом забезпечить юридичну значущість аудиту безпеки та гарантує неможливість фальсифікації історії інцидентів, що є критично важливим для медичних систем. Для протидії атакам на навігаційну підсистему (GPS/Lidar-спуфінгу) пропонується розробити модуль перехресної верифікації локації, який використовуватиме альтернативні джерела даних, наприклад, візуальні маркери або карту потужності Wi-Fi сигналів, для підтвердження фактичного перебування робота у заявленій зоні.

Еволюція систем захисту в асистивній робототехніці вимагає інтеграції більш надійних та багаторівневих механізмів безпеки, здатних працювати у гетерогенному середовищі IoT. У цьому контексті важливим є поєднання апаратних модулів довіри, інтелектуальних методів автентифікації та децентралізованих аудитних механізмів. Такий підхід дозволяє підвищити стійкість системи до зовнішніх атак, мінімізувати ризики компрометації і забезпечити прозорість усіх операцій, пов’язаних із доступом, конфігурацією та журналюванням. Узагальнену перспективну архітектуру системи захисту, що інтегрує TPM, AI-аутентифікацію та Blockchain-аудит, наведено на рисунку 3.10.

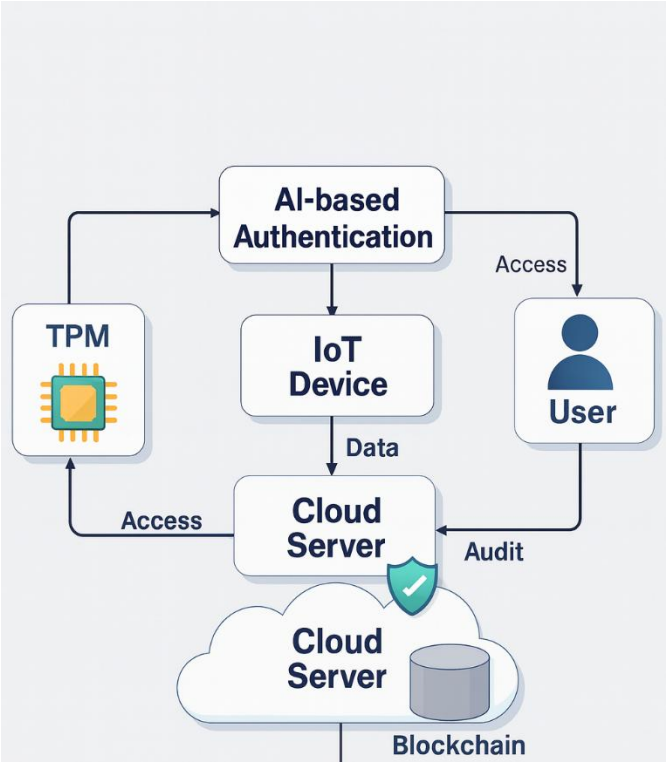

Рисунок 3.10 – Перспективна архітектура системи захисту з урахуванням рекомендацій

На рисунку 3.10 продемонстровано взаємодію ключових компонентів системи, які забезпечують підвищений рівень безпеки при роботі асистивного робота в IoT-середовищі. Апаратний модуль TPM виконує функції апаратного кореня довіри та контролює доступ до критично важливих операцій. Компонент AI-based Authentication забезпечує інтелектуальну багатофакторну автентифікацію користувача або пристрою, що значно знижує ймовірність несанкціонованого доступу. Хмарний сервер обробляє дані, отримані від IoT-пристрою, тоді як Blockchain-рівень використовується для прозорого аудитування усіх транзакцій та фіксації подій без можливості їх модифікації. Завдяки такій інтеграції система стає здатною автоматично виявляти порушення безпеки, блокувати ризикові операції та забезпечувати відтворюваність усіх подій, що особливо важливо для асистивних роботів, які працюють у чутливих середовищах та взаємодіють з користувачами.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-прикладне завдання підвищення рівня інформаційної безпеки асистивних робототехнічних систем шляхом розроблення та імплементації архітектури контекстно-залежного контролю доступу. На основі проведених теоретичних та експериментальних досліджень сформульовано наступні висновки:

Здійснено системний аналіз проблематики захисту персональних даних у сфері асистивної робототехніки. Встановлено, що інтеграція роботів у побутове середовище Інтернету речей (IoT) створює специфічні вектори загроз, серед яких найбільш критичними є несанкціонований доступ до відеопотоків («електронний вуайєризм») та компрометація каналів телеоперації. Виявлено, що існуючі хмарно-орієнтовані методи захисту не забезпечують достатньої приватності через передачу «сирих» даних у зовнішні мережі, що обґрунтувало необхідність перенесення обчислень на периферійний рівень (Edge Computing).

Обґрунтовано та розроблено трирівневу архітектуру захищеної системи управління, яка базується на концепції «Security by Design». Ключовим елементом архітектури є розроблений модуль проміжного програмного забезпечення «PrivateLoc», який функціонує як інтелектуальний шлюз між сенсорами робота та зовнішніми каналами зв’язку. Запропоноване рішення дозволяє реалізувати локальну фільтрацію чутливих даних безпосередньо на борту робота, унеможливлюючи їх витік навіть у випадку злому хмарного акаунта користувача.

Розроблено алгоритмічне забезпечення системи, що включає методи динамічного геозонування та контекстно-залежного управління доступом. Створений алгоритм семантичного картування дозволяє роботу автоматично ідентифікувати зони з різним рівнем приватності (публічні, приватні) та адаптувати режим роботи камер. Впровадження механізму гістерезису на кордонах зон дозволило підвищити стабільність класифікації контексту та усунути помилкові перемикання режимів при русі робота.

Програмно реалізовано прототип системи управління на базі апаратної платформи Raspberry Pi 4 та мета-операційної системи ROS 2 (Humble). Реалізовано захищений міст ROS-MQTT, який забезпечує передачу виключно знеособлених даних у зовнішню мережу. Прототип підтримує наскрізне шифрування відеопотоку та інтеграцію з інфраструктурою розумного будинку для отримання додаткових контекстних даних.

Експериментально підтверджено ефективність запропонованих рішень. Результати навантажувального тестування показали, що інтеграція модуля безпеки призводить до зростання завантаження центрального процесора на 28,5 % та збільшення мережевої затримки на 23 мс. Попри це, абсолютне значення затримки (68 мс) залишається значно нижчим за критичний поріг телеоперації (200 мс), що гарантує збереження керованості робота. Точність спрацювання механізмів приватності склала 96,5 %, а обсяг вихідного трафіку у приватних зонах знизився на 98%.

Сформульовано рекомендації щодо подальшого вдосконалення системи, які полягають у необхідності використання апаратних криптографічних модулів (TPM) для розвантаження центрального процесора, впровадженні мультимодальної біометричної аутентифікації оператора та застосуванні технології блокчейн для створення незмінного аудиторського сліду подій доступу.

Отримані результати свідчать про те, що розроблена система «PrivateLoc» є ефективним інструментом забезпечення приватності, який може бути рекомендований для впровадження у серійні зразки медичних та соціальних роботів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гринюк С., Базилюк С., Серський Д., Швець Р. Інтелектуальна система навігації мобільного робота на базі IOT: *Collection of Scientific Papers with the Proceedings of the 2nd International Scientific and Practical Conference «Current Challenges in Scientific Research»* м. Вроцлав, 1-3 грудня 2025 р. Вроцлав, 2025. С. 148-156.

2. ISO 8373:2021. Robotics – Vocabulary. – Geneva: International Organization for Standardization, 2021. 32 p.

3. Mahdavinejad M. S. Machine learning for Internet of Things data analysis: A survey. Digital *Communications and Networks.* 2021. Vol. 7, no. 3. P. 367-378.

4. Guatibonza A. Assistive Robotics for Upper Limb Physical Rehabilitation: A Systematic Review. *Chinese Journal of Mechanical Engineering*. 2024. Vol. 37. Art. 12.

5. Overview: A Comprehensive Review of Soft Wearable Exoskeletons. *Mdpi.* URL: https://www.mdpi.com/2075-1702/13/11/1020 (дата звернення: 15.09.2025).

6. Use of Socially Assistive Robots in Physiotherapy: Scoping Review. *JMIR Rehabilitation and Assistive Technologies*. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12407224/ (дата звернення: 15.09.2025).

7. Autonomy in Socially Assistive Robotics: A Systematic Review. URL: https://surl.li/xnifgk (дата звернення: 15.09.2025).

8. Fosch-Villaronga E. «I, The Robot… am watching you»: The privacy implications of using robotics in healthcare. *International Journal of Social Robotics*.- 2020. Vol. 13, no. 2. P. 239-255.

9. A spotlight on security and privacy risks with future household robots: attacks and lessons. *Proceedings of the 11th International Conference on Ubiquitous Computing* URL: https://www.researchgate.net/publication/221568687_A_spotlight_on_security_and_privacy_risks_with_future_household_robots
P. 105-114.

10. Almeny K. Security Issues in Assistive Robotics: A Surveyю *IEEE Access*.

2021. Vol. 9. P. 123-140.

11. A fully homomorphic encryption scheme. URL: https://www.researchgate.net/publication/381773345_Fully_Homomorphic_ (дата звернення: 25.09.2025).

12. Intelligent Monitoring System with Privacy Preservation Based on Edge AI. *Intelligent Monitoring*. URL: https://www.mdpi.com/2072-666X/14/9/1749 (дата звернення: 25.09.2025).

13. Decentralized Machine Learning Training: A Survey on Synchronization, Consolidation, and Topologies. *IEEE Access*. 2023. Vol. 11. P. 583–597.

14. Jeniffer J. Optimal hybrid heat transfer search and grey wolf optimization-based homomorphic encryption model to assure security in cloud-based IoT environment. 2022. Vol. 15. P. 560-580.

15. Modeling and Simulation Tools for Fog Computing-A Comprehensive Survey from a Cost Perspective. *Mdpi.* URL: https://www.mdpi.com/1999-5903/12/5/89 (дата звернення: 10.10.2025).

16. Kostavelis I. Semantic mapping for mobile robotics methods: A survey / I. Kostavelis, A. Gasteratos // Robotics and Autonomous Systems. 2015. Vol. 66. P. 86–103.

17. Geo-fencing privacy protection in location-based services / G. Roussos [et al.] // IEEE Transactions on Mobile Computing. 2019. Vol. 19, no. 2. P. 306-318.

18. Context-aware privacy protection in IoT-enabled smart home systems. *Sciencedirect* URL: https://surl.li/olherw (дата звернення: 10.10.2025).

19. Sicari S. Smart home: A comprehensive review of security and privacy challenges. *Internet of Things*. 2020. Vol. 10. P. 100-212.

20. Context in Robotics and Information Fusion. *Modelling and Simulation for Autonomous Systems*. URL: https://www.researchgate.net/publication/303516307_Context_in_Robotics_and_Information_Fusion (дата звернення: 25.10.2025).

21. A Smart Approach for Human Rescue and Environment Monitoring Autonomous Robot. *International Journal of Mechanical Engineering and Robotics Research*. 2021. Vol. 10, no. 4. P. 209-215.

22. Context-aware usage control for Android: A machine learning approach. *IEEE Access.* URL: https://www.researchgate.net/publication/221272943_Context-Aware_Usage_Control_for_Android (дата звернення: 25.10.2025).

23. Behavioral biometric authentication on smartphones: A survey *Researchgate*. URL: https://www.researchgate.net/publication/ 386608195_ A_Survey_on_Behavioral_Biometric_Authentication_on_Smartphones (дата звернення: 25.10.2025).

24. When machine learning meets privacy: A survey and outlook. *Researchgate*. URL: https://www.researchgate.net/publication/349900147_When_ Machine_Learning_Meets_Privacy_A_Survey_and_Outlook (дата звернення: 25.10.2025).

25. XACML for dynamic access control in IoT. *Researchgate*. URL: https://www.researchgate.net/publication/323809193_XACML_for_Building_Access_Control_Policies_in_Internet_of_Things (дата звернення: 25.10.2025).

26. Security patterns in practice: Designing secure architectures using software patterns. *Researchgate*. URL: https://www.researchgate.net/publication/220996345_Security_Patterns_and_Secure_Systems_Design (дата звернення: 25.10.2025).

27. A unified approach to interpreting model predictions. *Researchgate*. URL: https://www.researchgate.net/publication/317062430_A_Unified_Approach_to_Interpreting_Model_Predictions (дата звернення: 25.10.2025).

28. TurtleBot3 Features. *ROBOTIS e Manual*.URL: https://emanual.robotis.com/docs/en/platform/turtlebot3/features/#features (дата звернення: 25.10.2025).