Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта»
Назва теми

Рівень вищої освіти *другий (магістерський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 240239.10.02.38 ПЗ

Виконав здобувач ІІ курсу, група КІ2м-24-2 _____ Іван КРОТЕВИЧ
Підпис Ініціали, прізвище

Керівник канд.-техн. наук, доцент _____ Володимир ГРИГА
Науковий ступінь, учене звання Підпис Ініціали, прізвище

Нормоконтролер д. техн. наук, професор _____ Сергій ЛИСЕНКО
Науковий ступінь, учене звання Підпис Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС _____ Ольга ПАВЛОВА
«01» травня 2026 р. підпис Ініціали, прізвище
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Рівень вищої освіти другий (магістерський)

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
Ольга ПАВЛОВА

" 12 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кротевичу Івану Леонідовичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта»
Керівник проекту (роботи) Грига Володимир Михайлович, к.т.н., доц.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 12.01.2026 р. № 6

2. Термін подання здобувачем роботи на кафедру 01.05.2026 р.

3. Вихідні дані до роботи Завдання на кваліфікаційну роботу

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

Аналіз предметної галузі та існуючих рішень ідентифікації особи для автоматизації роботи «розумного ліфта»
Моделювання кіберфізичної системи ідентифікації особи
Методи та алгоритми ідентифікації особи та адаптивного керування для автоматизації роботи «розумного ліфта
Проектування кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта»

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

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання «_12_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	12.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	12.01.2026	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	20.01.2026	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	01.02.2026	виконано
5	Робота над науковою статтею	01.03.2026	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.03.2026	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.04.206	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2026	виконано
9	Попередній захист ДРМ	29.04.2026	виконано
10	Захист ДРМ на засіданні ЕК	До 20.05.2026	

Здобувач _____ Іван КРОТЕВИЧ
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Володимир ГРИГА
Підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта»

Автор роботи: Іван КРОТЕВИЧ

Керівник роботи: Володимир ГРИГА

Пояснювальна записка: 92 с., 11 рис., 4 табл., 2 дод., 80 джерел.

КІБЕРФІЗИЧНІ СИСТЕМИ, ІДЕНТИФІКАЦІЯ ОСОБИ, РОЗУМНИЙ ЛІФТ, АДАПТИВНЕ КЕРУВАННЯ, КОНВЕЄР ОБРОБКИ, ВБУДОВАНІ СИСТЕМИ, БІОМЕТРИЧНІ ДАНІ.

Об’єктом дослідження є процеси апаратно-програмної взаємодії та передачі керуючих сигналів у кіберфізичних системах ідентифікації особи.

Предметом дослідження є архітектурні рішення, методи та апаратні інтерфейси для автоматизації роботи «розумного ліфта» на основі біометричних даних.

Мета дослідження – забезпечення автоматизованого та безпечного керування «розумним» ліфтом на основі ідентифікації особи в кіберфізичному середовищі.

Для розв’язання поставлених задач використовувалися принципи системного проектування, методи комп’ютерного зору, теорію оцінювання стану динамічних систем та методи проектування вбудованих систем.

Наукова новизна:

- запропоновано архітектурне рішення кіберфізичної системи, що базується на інтеграції сенсорів глибини та edge-обчислювачів, що, на відміну від хмарних аналогів, забезпечує детермінований час відгуку системи.
- дістав подальшого розвитку метод адаптивного керування ліфтовим обладнанням, який враховує не лише ідентифікатор особи, а й апаратний стан системи та контекстні параметри.

Практична значимість отриманих результатів полягає у полягає у розробленій архітектурі кіберфізичної системи, яка базується на використанні edge-обчислень. Такий підхід дозволяє реалізувати обробку біометричних даних безпосередньо на локальному пристрої, що забезпечує мінімальні затримки, підвищену надійність та зменшення залежності від мережевої інфраструктури. Це особливо важливо для систем реального часу, де швидкість реакції є критичною. Також є можливість інтеграції запропонованого рішення з існуючими ліфтовими системами через стандартні інтерфейси (GPIO, промислові протоколи, релейні модулі). Це значно спрощує впровадження розробки у реальні об’єкти без необхідності повної заміни обладнання, що знижує економічні витрати.

У першому розділі проведено аналіз предметної галузі де визначено, що «розумний ліфт» є складною кіберфізичною системою, де надійність функціонування залежить від швидкодії обчислювальних вузлів та стабільності каналів передачі даних. Обґрунтовано доцільність використання вбудованих систем (Edge AI) для локальної ідентифікації особи, що дозволяє уникнути затримок хмарної інфраструктури та підвищити безпеку персональних даних.

Аналіз існуючих рішень показав відсутність уніфікованих апаратних інтерфейсів для зв’язку КФС із застарілими контролерами ліфтів, що робить розробку релейних та протокольних вузлів сполучення критично важливою.

У другому розділі виконано моделювання кіберфізичної системи ідентифікації особи як багаторівневої інтегрованої структури, що поєднує фізичні процеси збору даних та їх інтелектуальну обробку.

Сформована концептуальна модель дозволила представити процес ідентифікації як послідовність взаємопов’язаних перетворень, від отримання сирих біометричних даних до прийняття рішення. Це дало змогу формалізувати систему у вигляді математичних відображень, що є важливим для подальшого аналізу, оптимізації та програмної реалізації.

У третьому розділі розроблено та обґрунтовано методи і алгоритми ідентифікації особи, а також підходи до адаптивного керування ліфтовою системою. Проведений аналіз існуючих підходів показав, що класичні статистичні

методи поступаються сучасним нейромережевим архітектурам за точністю та стійкістю до шумів.

Розроблений конвеєр обробки біометричних даних включає етапи детекції, відстеження, нормалізації та класифікації, що забезпечує комплексний підхід до ідентифікації. Особливістю запропонованих рішень є їх орієнтація на роботу в реальному часі з урахуванням обмежених ресурсів edge-пристроїв.

Значним результатом є розробка методу адаптивного керування ліфтом, який враховує не лише факт ідентифікації користувача, але й контекстні параметри (стан системи, пріоритети, середовище). Це дозволяє перейти від статичних алгоритмів до інтелектуального керування, що підвищує ефективність роботи ліфтової системи. Також у розділі реалізовано механізм прийняття рішень, який інтегрує результати біометричного аналізу з керуючими алгоритмами. Це забезпечує автоматизацію процесу вибору поверху, оптимізацію маршрутів і підвищення рівня персоналізації.

У четвертому розділі виконано проєктування кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» та реалізовано її архітектурні й програмно-апаратні рішення.

Розроблена архітектура системи базується на принципах розподілених обчислень із використанням edge-пристроїв, що дозволяє забезпечити низьку затримку обробки даних та незалежність від хмарної інфраструктури. Це є критично важливим для систем реального часу, зокрема ліфтових комплексів.

У процесі проєктування обґрунтовано вибір апаратної платформи та сенсорної підсистеми, що забезпечують необхідну продуктивність для виконання алгоритмів комп’ютерного зору. Запропоновані рішення дозволяють реалізувати повноцінний цифровий конвеєр обробки даних безпосередньо на вбудованому пристрої.

Окрему увагу приділено розробці інтерфейсу взаємодії з ліфтовою автоматикою, що забезпечує інтеграцію з існуючими системами керування через стандартні апаратні інтерфейси. Це підвищує універсальність і практичну застосовність розробленого рішення.

ЗМІСТ

Скорочення та умовні познаки 5
Вступ 6
1 Аналіз предметної галузі та існуючих рішень 10
1.1 Особливості функціонування «розумних» ліфтових систем 10
1.2 Методи ідентифікації особи в автоматизованих системах 12
1.3 Огляд сучасних наукових досліджень у сфері кіберфізичних систем ідентифікації особи для «розумних» ліфтів 16
1.4 Апаратні засоби кіберфізичних систем ідентифікації особи для автоматизації роботи «розумного» ліфта 21
1.5 Постановка задачі 23
1.6 Висновки до першого розділу 24
2 Моделювання кіберфізичної системи ідентифікації особи 25
2.1 Концептуальна модель кіберфізичної системи ідентифікації особи 25
2.2 Інтеграція кіберфізичної системи ідентифікації особи в систему автоматизації «розумного ліфта» 28
2.3 Моделювання процесу прийняття рішень у кіберфізичній системі на основі ідентифікації особи 32
2.4 Структура процесу прийняття рішень 37
2.6 Висновки 45
3 Методи та алгоритми ідентифікації особи та адаптивного керування для автоматизації роботи «розумного ліфта» 46
3.1 Архітектура конвеєра обробки біометричних даних 46
3.2 Метод детекції облич 49
3.3 Метод відстеження обличчя 56
3.4 Метод адаптивного керування ліфтовим обладнанням на основі ідентифікації особи та контекстних параметрів 59
3.5 Прийняття рішень в кіберфізичній системі ідентифікації особи для автоматизації роботи «розумного ліфта» 61

3.6 Висновки 67
4 Проектування кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» 69
4.1 Архітектура кіберфізичної системи 69
4.2 Проектування інтерфейсу взаємодії з розумним ліфтом 79
4.3 Перевірка справжності біометричного об’єкта 83
4.4 Обґрунтування вибору апаратної платформи та сенсорної підсистеми з урахуванням побудови цифрового конвеєра обробки даних 87
4.5 Висновки 94
Висновки 96
Перелік джерел посилань 98
Додаток А. Тези доповіді 106
Додаток Б. Презентація 108

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БД - база даних

КФС - кіберфізична система

ПЗ - програмне забезпечення

IoT - Internet of Things (інтернет речей)

FSM - Finite State Machine (скінченний автомат)

GPIO - General-Purpose Input/Output (інтерфейс введення-виведення загального призначення)

GPU - Graphics Processing Unit (графічний процесор)

RGB-D - Red, Green, Blue + Depth (колірна модель з даними про глибину)

ВСТУП

Сучасний розвиток галузі кіберфізичних систем характеризується переходом від автономних обчислювальних систем до розгалужених кіберфізичних комплексів. У контексті «інтелектуальних будівель» особливої ваги набуває завдання створення інтегрованих систем вертикального транспорту, де цифрові обчислювальні вузли безпосередньо взаємодіють із силовими виконавчими механізмами. Традиційні мікропроцесорні системи керування ліфтами, що базуються на перериваннях від механічних кнопок, не дозволяють реалізувати принципи адаптивного управління та інтелектуального доступу.

Розвиток концепції «розумних» будівель передбачає інтеграцію різнорідних інженерних підсистем, таких як енергозабезпечення, безпеки, клімат-контролю, відеоспостереження та транспортних систем у єдину інформаційно-керуючу інфраструктуру. У такому середовищі ліфт перестає бути ізольованим механічним пристроєм і трансформується у повноцінний кіберфізичний модуль, який обмінюється даними з іншими системами будівлі та адаптує свою поведінку відповідно до поточних умов експлуатації. Це вимагає переходу від централізованих схем керування до розподілених обчислювальних архітектур, у яких значна частина функцій реалізується на рівні периферійних (edge) пристроїв.

Така трансформація обумовлює необхідність переосмислення підходів до проєктування апаратно-програмних комплексів. Зокрема, зростає роль вбудованих систем, що забезпечують обробку сигналів у реальному часі, взаємодію з сенсорними підсистемами та формування керуючих впливів на виконавчі механізми. При цьому критичними параметрами стають не лише продуктивність обчислень, але й детермінованість виконання, затримки передачі даних, надійність апаратних компонентів та стійкість до відмов.

Однією з ключових тенденцій є використання розподілених обчислювальних вузлів, розташованих безпосередньо у фізичному середовищі системи. Такі вузли виконують функції локальної обробки даних, фільтрації та агрегації інформації, що дозволяє зменшити навантаження на центральні сервери та забезпечити

мінімальні затримки при прийнятті керуючих рішень. У системах вертикального транспорту це має особливе значення, оскільки затримки в обробці сигналів можуть безпосередньо впливати на безпеку та комфорт користувачів.

Іншою важливою складовою сучасних кіберфізичних систем є сенсорні підсистеми, які забезпечують безперервний моніторинг стану об’єкта. У випадку ліфтових систем це включає контроль положення кабіни, швидкості руху, навантаження, стану дверей, а також параметрів навколишнього середовища. Отримані дані використовуються для формування керуючих алгоритмів, діагностики технічного стану та забезпечення безпечної експлуатації. Водночас зростає кількість сенсорів та складність їх інтеграції, що вимагає використання стандартизованих інтерфейсів і протоколів обміну даними.

Особливе місце у структурі сучасних «розумних» ліфтових систем займають підсистеми ідентифікації особи. Вони забезпечують не лише контроль доступу до окремих зон будівлі, але й реалізацію персоналізованих сценаріїв обслуговування. Наприклад, система може автоматично визначати поверх призначення користувача, оптимізувати маршрути руху кабін або надавати пріоритет певним категоріям пасажирів. З технічної точки зору це означає необхідність інтеграції додаткових сенсорів, обчислювальних модулів та каналів зв’язку у загальну архітектуру системи.

Разом із розширенням функціональності зростають і вимоги до інформаційної безпеки. Кіберфізичні системи є вразливими до різноманітних атак, що можуть призвести як до витоку даних, так і до порушення фізичних процесів. Тому при проєктуванні таких систем необхідно враховувати механізми захисту на всіх рівнях, від апаратного до мережевого. Це включає аутентифікацію пристроїв, шифрування каналів зв’язку, контроль цілісності даних та моніторинг аномалій у роботі системи.

Не менш важливим аспектом є забезпечення масштабованості та гнучкості архітектури. «Розумні» будівлі постійно модернізуються, доповнюються новими підсистемами та пристроями, що вимагає можливості їх інтеграції без суттєвої перебудови існуючої інфраструктури. Це досягається за рахунок модульного

підходу до проєктування, використання відкритих стандартів та уніфікованих інтерфейсів.

Таким чином, сучасні кіберфізичні системи вертикального транспорту є складними багаторівневими комплексами, що поєднують апаратні засоби, програмне забезпечення та мережеву інфраструктуру. У цьому контексті актуальним є дослідження та розробка архітектурних рішень для кіберфізичних систем ідентифікації особи, інтегрованих у «розумні» ліфтові комплекси.

Актуальність роботи зумовлена необхідністю автоматизації «розумного ліфта» на основі біометричної ідентифікації особи. Це потребує вирішення складних інженерних задач, від організації високошвидкісного захоплення потокових даних сенсорами глибини до забезпечення real-time обробки на вбудованих (edge) платформах з обмеженими ресурсами. Застосування біометричної ідентифікації дозволяє замінити фізичні рівні інтерфейсу користувача на цифрові аналоги, що підвищує надійність системи та забезпечує безконтактне керування.

Мета дослідження – забезпечення автоматизованого та безпечного керування «розумним» ліфтом на основі ідентифікації особи в кіберфізичному середовищі.

Для досягнення мети необхідно вирішити такі завдання:

− проаналізувати архітектурні особливості сучасних комп’ютерних систем керування ліфтами та методи біометричної ідентифікації;

− розробити структурну модель КФС як багаторівневу ієрархію фізичного, мережевого та обчислювального рівнів;

− обґрунтувати вибір апаратної платформи (Edge AI) та сенсорної підсистеми для забезпечення низької затримки обробки;

− спроектувати цифровий конвеєр обробки біометричних даних та інтерфейс взаємодії з ліфтовою автоматикою (GPIO, релейні модулі, промислові протоколи).

Об’єктом дослідження є процеси апаратно-програмної взаємодії та передачі керуючих сигналів у кіберфізичних системах ідентифікації особи.

Предметом дослідження є архітектурні рішення, методи та апаратні інтерфейси для автоматизації роботи «розумного ліфта» на основі біометричних даних.

Наукова новизна:

− запропоновано архітектурне рішення КФС, що базується на інтеграції сенсорів глибини та edge-обчислювачів, що, на відміну від хмарних аналогів, забезпечує детермінований час відгуку системи.

− дістав подальшого розвитку метод адаптивного керування ліфтовим обладнанням, який враховує не лише ідентифікатор особи, а й апаратний стан системи та контекстні параметри.

Практична значимість отриманих результатів полягає у полягає у розробленій архітектурі кіберфізичної системи, яка базується на використанні edge-обчислень. Такий підхід дозволяє реалізувати обробку біометричних даних безпосередньо на локальному пристрої, що забезпечує мінімальні затримки, підвищену надійність та зменшення залежності від мережевої інфраструктури. Це особливо важливо для систем реального часу, де швидкість реакції є критичною. Також є можливість інтеграції запропонованого рішення з існуючими ліфтовими системами через стандартні інтерфейси (GPIO, промислові протоколи, релейні модулі). Це значно спрощує впровадження розробки у реальні об’єкти без необхідності повної заміни обладнання, що знижує економічні витрати.

Для розв’язання поставлених задач використовувалися принципи системного проектування, методи комп’ютерного зору, теорію оцінювання стану динамічних систем та методи проектування вбудованих систем.

За темою кваліфікаційної роботи опубліковано одну публікацію [80] у збірнику наукових праць за студентської науково-технічної конференції «Перспективні мережні та комп’ютерні технології» ПЕРСИК-2026, Харків.

1 АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ ТА ІСНУЮЧИХ РІШЕНЬ

1.1 Особливості функціонування «розумних» ліфтових систем

«Розумні» ліфтові системи є невід'ємною складовою сучасних інтелектуальних будівель і реалізують принципи кіберфізичних систем, що передбачають тісну інтеграцію фізичних процесів із цифровими технологіями керування.

На відміну від традиційних ліфтів, які функціонують за фіксованими алгоритмами виклику та обслуговування, «розумні» ліфти використовують дані в реальному часі, аналітичні моделі та адаптивні алгоритми для підвищення ефективності роботи. Основною метою таких систем є оптимізація перевезення пасажирів, зменшення часу очікування, підвищення рівня комфорту та забезпечення безпеки.

Функціонування «розумного» ліфта базується на багаторівневій архітектурі, яка включає сенсорний рівень, рівень обробки даних, рівень керування та комунікаційний рівень.

Сенсорний рівень забезпечує збір інформації про стан системи та навколишнє середовище за допомогою різноманітних датчиків, таких як датчики положення кабіни, навантаження, присутності, а також відеокамери та біометричні сенсори.

Отримані дані передаються до обчислювальних модулів, де здійснюється їх обробка, аналіз та формування керуючих впливів. Для цього використовуються як вбудовані контролери, так і edge- або хмарні обчислювальні ресурси.

Ключову роль у роботі системи відіграють алгоритми керування, які визначають логіку обслуговування викликів.

У будівлях із декількома ліфтами застосовуються алгоритми групового керування, що дозволяють ефективно розподіляти запити між кабінами. Такі алгоритми можуть бути реалізовані на основі евристичних методів, правил пріоритетів або моделей машинного навчання.

Значного поширення набула концепція керування за пунктом призначення,

яка передбачає введення користувачем необхідного поверху ще до входу в кабіну. Це дозволяє групувати пасажирів із подібними маршрутами, зменшувати кількість зупинок і підвищувати пропускну здатність системи.

Важливою особливістю «розумних» ліфтів є здатність до адаптивного керування. Система аналізує статистичні та історичні дані про використання ліфта, враховує часові закономірності (наприклад, години пік) та динамічно змінює параметри своєї роботи. Це дозволяє прогнозувати навантаження та оптимізувати роботу системи без втручання оператора.

Інтеграція ліфтової системи у загальну інфраструктуру будівлі забезпечує взаємодію з іншими підсистемами, такими як системи контролю доступу, відеоспостереження, пожежної безпеки та управління енергоспоживанням. Така інтеграція реалізується за допомогою сучасних мережевих протоколів і забезпечує централізований моніторинг та керування.

Особливе значення у функціонуванні «розумного» ліфта має ідентифікація користувачів. Вона дозволяє реалізувати персоналізовані сценарії обслуговування, такі як автоматичний виклик ліфта, попередній вибір поверху призначення, обмеження доступу до певних зон будівлі.

Це не лише підвищує комфорт користування, але й суттєво покращує рівень безпеки. Наприклад, система може надавати різні права доступу для співробітників, відвідувачів або технічного персоналу.

Разом із численними перевагами, «розумні» ліфтові системи мають і певні недоліки. До них належать висока вартість впровадження, складність налаштування та обслуговування, залежність від інформаційної інфраструктури, а також ризики, пов’язані з кібербезпекою.

Незважаючи на це, розвиток технологій Інтернету речей, штучного інтелекту та кіберфізичних систем сприяє широкому впровадженню таких рішень у сучасних будівлях.

Таблиця 1.1 містить характеристики основних компонентів «розумної» ліфтової системи.

Таблиця 1.1 – Характеристики основних компонентів «розумної» ліфтової системи

Компонент системи	Основні функції	Приклади реалізації	Значення для системи
Сенсорний рівень	Збір даних про стан ліфта та середовища	Датчики, камери, біометричні сенсори	Забезпечує вхідні дані
Обчислювальний рівень	Обробка та аналіз інформації	PLC, edge-пристрої, сервери	Формує рішення
Рівень керування	Прийняття керуючих рішень	Алгоритми, AI-моделі	Оптимізує роботу
Комунікаційний рівень	Передача даних між компонентами	Ethernet, Wi-Fi, IoT-протоколи	Забезпечує інтеграцію
Інтерфейс користувача	Взаємодія з користувачем	Панелі, мобільні додатки, голосові системи	Забезпечує зручність
Система ідентифікації	Розпізнавання та авторизація користувачів	Face ID, RFID, біометрія	Підвищує безпеку і персоналізацію

1.2 Методи ідентифікації особи в автоматизованих системах

Ідентифікація особи є однією з ключових функцій сучасних автоматизованих та кіберфізичних систем, оскільки забезпечує коректну взаємодію між користувачем і технічним середовищем, контроль доступу до ресурсів, а також персоналізацію сервісів.

У контексті інтелектуальних систем управління, зокрема «розумних» ліфтів, ідентифікація користувача виступає базовим механізмом прийняття рішень, що визначають сценарії роботи системи, рівень доступу та пріоритет обслуговування.

Під ідентифікацією особи розуміють процес встановлення унікальної відповідності між користувачем і записом у базі даних системи на основі певних ознак або атрибутів.

При цьому слід розрізняти три взаємопов’язані, але функціонально різні процеси: ідентифікацію, аутентифікацію та авторизацію.

Ідентифікація передбачає визначення особи серед множини користувачів,

аутентифікація – це підтвердження заявленої особи шляхом перевірки її автентичності, тоді як авторизація визначає права доступу до ресурсів після успішного встановлення особи. У складних кіберфізичних системах ці процеси часто реалізуються як єдиний безперервний цикл обробки даних.

Методи ідентифікації класифікуються за типом використовуваних факторів, які поділяються на три основні категорії: знання, володіння та властивості користувача.

Перший тип базується на інформації, відомій лише користувачеві, такій як паролі або PIN-коди. Незважаючи на простоту реалізації, такі методи мають низький рівень безпеки через можливість підбору, перехоплення або соціальної інженерії.

Другий тип передбачає використання фізичних носіїв, таких як RFID-карти, електронні ключі або мобільні пристрої. Ці методи є більш зручними у використанні, однак залишаються вразливими до втрати або крадіжки ідентифікаційного засобу.

Найбільш перспективними є методи третьої групи, що базуються на біометричних характеристиках людини, які є унікальними та важко підроблюваними.

Біометричні методи ідентифікації поділяються на фізіологічні та поведінкові.

Фізіологічні методи базуються на аналізі статичних характеристик організму, таких як риси обличчя, відбитки пальців, структура райдужної оболонки ока або геометрія руки.

Поведінкові методи враховують динамічні характеристики, зокрема голос, манеру ходи, підпис або стиль взаємодії з пристроями. У сучасних автоматизованих системах найбільшого поширення набули фізіологічні методи, оскільки вони забезпечують вищу стабільність і точність розпізнавання.

Особливе місце серед біометричних методів займає технологія розпізнавання обличчя, яка є найбільш придатною для інтеграції у кіберфізичні системи типу «розумного» ліфта. Це зумовлено її безконтактністю, швидкістю

роботи та можливістю використання стандартних відеокамер.

Процес розпізнавання обличчя включає кілька послідовних етапів: детекцію обличчя на зображенні, нормалізацію та вирівнювання, виділення характерних ознак і порівняння отриманого вектора ознак із шаблонами в базі даних. Сучасні підходи до розпізнавання обличчя базуються на методах глибокого навчання, зокрема згорткових нейронних мережах, які дозволяють досягати високої точності навіть за складних умов освітлення, часткових перекриттів або змін ракурсу.

Іншим поширеним методом є ідентифікація за відбитками пальців, яка характеризується високою точністю та зрілістю технології. Однак у контексті ліфтових систем цей метод має обмеження через необхідність фізичного контакту з сенсором, що може знижувати гігієнічність та швидкість обслуговування. Ідентифікація за райдужною оболонкою ока забезпечує ще вищу точність, проте вимагає дорогого обладнання та спеціальних умов зчитування, що обмежує її практичне застосування в масових системах.

Голосова ідентифікація, яка базується на аналізі акустичних характеристик мовлення, може використовуватися як додатковий або альтернативний метод, особливо в системах із голосовим інтерфейсом. Водночас вона є чутливою до шумів, змін голосу користувача та потенційно вразливою до атак відтворення записаного голосу.

Важливим аспектом оцінки ефективності методів ідентифікації є використання кількісних показників, таких як коефіцієнт хибного прийняття (false acceptance rate, FAR) та коефіцієнт хибного відхилення (false rejection rate, FRR). FAR характеризує ймовірність того, що система помилково визнає неавторизованого користувача, тоді як FRR відображає ймовірність відмови в доступі легітимному користувачеві. Баланс між цими показниками визначає загальну надійність системи та налаштовується залежно від вимог до безпеки. У практичних застосуваннях також використовується показник рівності помилок (equal error rate, EER), який відповідає точці, де FAR і FRR є однаковими.

Сучасні тенденції розвитку систем ідентифікації спрямовані на використання мультифакторних підходів, які поєднують кілька методів для

підвищення рівня безпеки та надійності. Наприклад, поєднання розпізнавання обличчя з використанням мобільного пристрою або RFID-карти дозволяє зменшити ймовірність несанкціонованого доступу та підвищити стійкість системи до атак. У кіберфізичних системах такий підхід також сприяє більш гнучкій адаптації до різних сценаріїв використання.

Разом із перевагами, впровадження систем ідентифікації супроводжується низкою викликів. Одним із ключових є забезпечення захисту персональних даних, особливо у випадку використання біометричної інформації, яка є незмінною та унікальною для кожної особи. Це вимагає застосування сучасних криптографічних методів, а також дотримання нормативно-правових вимог щодо обробки персональних даних. Іншим важливим аспектом є стійкість до атак підміни (spoofing), коли зловмисник намагається обманути систему за допомогою фотографій, відео або інших засобів імітації. Для протидії таким загрозам використовуються методи визначення справжності об’єкта, які аналізують динамічні характеристики об’єкта.

Не менш важливим є питання обчислювальної ефективності, оскільки системи ідентифікації в реальному часі повинні забезпечувати мінімальні затримки обробки. Це особливо актуально для «розумних» ліфтів, де швидкість прийняття рішень безпосередньо впливає на комфорт користувачів. Тому при проєктуванні системи необхідно враховувати баланс між точністю, швидкодією та ресурсними витратами.

Таким чином, аналіз методів ідентифікації показує, що для кіберфізичних систем, орієнтованих на взаємодію з великою кількістю користувачів у реальному часі, найбільш доцільним є використання біометричних технологій, зокрема розпізнавання обличчя, доповненого мультифакторними механізмами. Це забезпечує оптимальне поєднання зручності, швидкості та рівня безпеки, що є критично важливим для ефективного функціонування «розумних» ліфтових систем.

1.3 Огляд сучасних наукових досліджень у сфері кіберфізичних систем

ідентифікації особи для «розумних» ліфтів

Упродовж останніх років спостерігається активний розвиток досліджень у сфері кіберфізичних систем, інтелектуальних будівель, комп'ютерного зору та біометричної ідентифікації.

Значна частина наукових праць присвячена інтеграції технологій штучного інтелекту, edge-computing, Internet of Things (IoT) та методів глибокого навчання у системи автоматизації ліфтового транспорту.

Основною тенденцією є перехід від традиційних ліфтових систем до адаптивних кіберфізичних платформ, здатних аналізувати поведінку користувачів, оптимізувати маршрути руху кабін та забезпечувати персоналізовану взаємодію з пасажирами.

Автори дослідження [10] запропонували концепцію Digital Triplet для ліфтової системи, яка поєднує фізичний ліфт, цифровий двійник та інтелектуальний модуль прийняття рішень.

Система реалізована із використанням OPC-UA, PLC-контролерів Siemens та алгоритму YOLOv3 для розпізнавання об'єктів. Автори продемонстрували можливість інтеграції комп'ютерного зору у кіберфізичне середовище ліфта з метою підвищення рівня безпеки та автоматизації прийняття рішень. Особливу увагу приділено синхронізації фізичної та цифрової моделей у реальному часі.

Важливий внесок у розвиток кіберфізичних систем із біометричною ідентифікацією зроблено у статті [11]. У дослідженні автори запропонували реконфігуровану CPS-архітектуру для систем відеоспостереження у «розумних» містах із підтримкою розпізнавання облич та edge-обробки відеоданих. Система використовує локальні edge-вузли для виконання нейромережевої обробки відео у реальному часі та центральний сервер для біометричної ідентифікації та відстеження користувачів. Дослідники показали, що використання адаптивної передачі відеоданих дозволяє зменшити навантаження на мережу приблизно на 75% без втрати точності розпізнавання. Дана робота є важливою для проєктування «розумних» ліфтів, оскільки демонструє ефективність поєднання edge-computing

та біометричної ідентифікації у кіберфізичних системах.

Автори роботи [12] представили дослідження, у якому запропоновано edge-орієнтовану систему моніторингу ліфтів із використанням технологій штучного інтелекту. Метою роботи було автоматичне виявлення електромотоциклів у ліфтах житлових будинків для запобігання пожежній небезпеці. Автори наголошують, що локальна обробка відеоданих на edge-пристроях дозволяє суттєво знизити ризики витоку персональних даних і підвищити кібербезпеку системи. У роботі також розглядаються загрози інформаційній безпеці та методи їх нейтралізації у CPS-середовищі.

Подальший розвиток технологій комп'ютерного зору для ліфтових систем представлено у роботі [13]. У даному дослідженні запропоновано інтелектуальну інформаційну систему ліфта (IEIS), яка використовує комп'ютерний зір для аналізу пасажиропотоку, визначення завантаженості кабіни та прогнозування попиту. Система виконує розпізнавання пасажирів, підрахунок людей та аналіз переміщення користувачів для оптимізації роботи ліфта. Автори показали, що використання відеоаналітики дозволяє суттєво знизити енергоспоживання та покращити ефективність роботи будівлі.

Важливим напрямом сучасних досліджень є застосування edge-computing для локальної обробки відеоданих. У роботі [14] автори запропонували систему підрахунку людей у ліфті на основі нейромережі MobileNet-SSD. Обробка даних виконується безпосередньо на edge-пристроях, що дозволяє забезпечити роботу системи в реальному часі та зменшити затримки передачі даних. Результати дослідження підтвердили ефективність використання lightweight-моделей глибокого навчання для задач інтелектуального моніторингу ліфтових систем.

У роботі [15] автори запропонували інтелектуальну ліфтову систему на базі YOLOv3, що використовує комп'ютерний зір для виявлення пасажирів та прийняття рішень щодо зупинок ліфта. Дослідження показало скорочення часу очікування приблизно на 15% та зменшення енергоспоживання на 20% порівняно з традиційними алгоритмами керування. У роботі також розглянуто використання камер, вагових сенсорів та edge-обчислень як складових кіберфізичної

архітектури.

У роботі [16] представлено дослідження, у якому запропоновано IoT-платформу для моніторингу та предиктивного обслуговування ліфтів. Автори інтегрували WebSocket-комунікацію, сенсори IoT та алгоритми машинного навчання (XGBoost, LSTM) для прогнозування несправностей ліфтового обладнання. Отримані результати продемонстрували можливість зниження кількості відмов та підвищення ефективності технічного обслуговування.

У дослідженні [17] представлено IoT-систему моніторингу ліфтів ElevatorTalk-M. Автори запропонували модель на основі скінченних автоматів для адаптивного формування логіки моніторингу залежно від конфігурації сенсорів. У дослідженні використано датчики струму, руху та вібрації для аналізу стану ліфта в реальному часі. Особливістю роботи є можливість масштабування та автоматичної адаптації системи до зміни апаратної конфігурації.

Автори роботи [18] запропонували безконтактну інтелектуальну систему ліфта на основі технологій AIoT та розпізнавання обличчя. Основною метою роботи було зменшення фізичного контакту користувачів із панелями керування ліфтом після пандемії COVID-19. Система автоматично ідентифікує мешканця будівлі за допомогою камери та виконує вибір поверху без натискання кнопок. Автори відзначають скорочення часу очікування ліфта та підвищення зручності використання у багатоповерхових житлових будинках. Особливу увагу приділено інтеграції Artificial Intelligence of Things (AIoT) та безконтактних інтерфейсів у кіберфізичну інфраструктуру будівлі.

У роботі [19] запропоновано інтелектуальну систему попереднього бронювання та диспетчеризації ліфтів. Система дозволяє користувачам резервувати ліфт через мобільний додаток ще до прибуття до ліфтового холу. Архітектура SmartRide поєднує IoT, edge-computing та елементи біометричної ідентифікації, включаючи розпізнавання обличчя для автоматичного підтвердження особи пасажира. Автори показали, що використання прогнозування пасажиропотоку та попереднього планування маршрутів дозволяє суттєво зменшити середній час очікування й оптимізувати навантаження на

ліфтову систему.

У роботі [20] запропоновано модель інтелектуального моніторингу та диспетчеризації ліфтів із використанням біометричних даних користувачів. Для аналізу відеопотоку застосовано модифіковану нейромережу YOLO з інтеграцією Ghost-модулів та механізмів CBAM attention. Система здатна виявляти користувачів із особливими потребами, дитячі візки та інші критичні об’єкти, що дозволяє динамічно адаптувати роботу ліфта. Дослідники акцентують увагу на можливості використання біометричних характеристик для підвищення безпеки та оптимізації групового керування ліфтами у реальному часі.

У роботі [21] автори розглянули перспективи використання Brain–Computer Interface (BCI) у системах керування ліфтами. Дослідження орієнтоване насамперед на користувачів із обмеженими фізичними можливостями. Запропонована система дозволяє здійснювати виклик ліфта та вибір поверху за допомогою сигналів мозкової активності. Хоча дана технологія перебуває на ранньому етапі розвитку, автори наголошують, що Brain–Computer Interface може стати важливим елементом майбутніх кіберфізичних систем доступності та персоналізованого керування у «розумних» будівлях.

Напрям інтелектуального моніторингу ліфтів представлено у статті [22]. Автори запропонували систему безконтактного оптичного аналізу вібрацій ліфта із використанням лазерних сенсорів та двогілкової нейронної мережі CNN-LSTM. Розроблена модель дозволяє здійснювати високоточну діагностику несправностей ліфтового обладнання у режимі реального часу. Досягнута точність класифікації становила 99,97%, що демонструє перспективність застосування глибокого навчання та безконтактних сенсорних технологій у кіберфізичних системах моніторингу ліфтів.

Окрему увагу дослідники приділяють розвитку алгоритмів комп’ютерного зору для задач безпеки у ліфтах. У статті [23] запропоновано модифікований алгоритм YOLOv10 для автоматичного виявлення електровелосипедів у ліфтах житлових будинків. Необхідність такого дослідження пов’язана зі зростанням кількості пожеж, спричинених акумуляторами електротранспорту. Автори

реалізували покращені механізми self-attention та calibration-модулі для підвищення точності виявлення об’єктів у складних умовах ліфтового простору. Результати дослідження підтвердили ефективність використання сучасних моделей комп’ютерного зору для забезпечення безпеки «розумних» ліфтових систем.

Окремий напрям наукових досліджень стосується проблем кібербезпеки та захисту персональних даних у CPS-системах.

У роботах авторів [24] розглядаються основні типи атак на кіберфізичні системи, включаючи підміну сенсорних даних, атаки на канали зв’язку та порушення роботи систем ідентифікації. Автори підкреслюють необхідність використання криптографічного захисту, edge-обробки та багаторівневої аутентифікації для забезпечення безпеки CPS-середовищ.

Проведений аналіз наукових джерел показує, що сучасні дослідження у сфері «розумних» ліфтів зосереджені на таких основних напрямах:

- інтеграція комп’ютерного зору та біометричної ідентифікації;
- використання edge-computing та IoT;
- оптимізація енергоспоживання;
- предиктивне технічне обслуговування;
- забезпечення кібербезпеки та захисту персональних даних;
- застосування штучного інтелекту для адаптивного керування.

Незважаючи на значну кількість досліджень, проблема комплексної реалізації кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного» ліфта залишається актуальною. Особливої уваги потребують питання інтеграції біометричної ідентифікації з системами керування ліфтом у режимі реального часу, забезпечення конфіденційності персональних даних та підвищення стійкості системи до кіберзагроз.

1.4 Апаратні засоби кіберфізичних систем ідентифікації особи для автоматизації роботи «розумного» ліфта

У кіберфізичних системах «розумних» будівель ключову роль відіграють апаратні компоненти, що забезпечують безпосередню взаємодію із фізичним середовищем, збір даних, їх попередню обробку та передачу до вищих рівнів системи. До таких компонентів належать периферійні (edge) пристрої, сенсорні підсистеми та виконавчі механізми [25]. Саме ці елементи формують основу для реалізації функціональності системи в реальному часі, забезпечують детермінованість обробки та впливають на загальну надійність і продуктивність.

Периферійні або edge-пристрої являють собою обчислювальні вузли, розташовані безпосередньо поблизу джерел даних. Вони виконують функції збору, фільтрації, агрегації та часткової обробки інформації до її передачі у центральні системи. Такий підхід дозволяє суттєво зменшити затримки, знизити навантаження на мережу та підвищити автономність системи. У «розумних» ліфтах edge-пристрої можуть бути представлені одноплатними комп’ютерами (наприклад, на базі ARM-архітектури), промисловими контролерами або спеціалізованими вбудованими модулями [26].

З точки зору апаратної організації, edge-пристрої характеризуються наявністю процесора (CPU), оперативної пам’яті, інтерфейсів введення/виведення, мережевих модулів та, у деяких випадках, апаратних прискорювачів обчислень. Важливими параметрами є енергоспоживання, тепловиділення, надійність роботи в умовах обмеженого простору та підтримка промислових стандартів. У задачах реального часу перевага надається платформам, що підтримують операційні системи реального часу або оптимізовані Linux-дистрибутиви [27].

Сенсорні підсистеми є джерелом первинної інформації про стан системи та навколишнього середовища. У ліфтових кіберфізичних системах використовуються різні типи сенсорів, які можна класифікувати за функціональним призначенням. До основних належать датчики положення (енкодери, кінцеві вимикачі), що визначають координати кабіни; датчики швидкості та прискорення, які забезпечують контроль руху; датчики навантаження, що дозволяють оцінювати масу пасажирів і запобігати перевантаженню; а також датчики відкривання дверей і присутності.

Окрему групу становлять сенсори безпеки, які забезпечують контроль аварійних ситуацій [28]. До них належать інфрачервоні бар'єри, датчики перешкод, датчики вібрації та температури. Вони дозволяють виявляти нестандартні режими роботи та ініціювати аварійні алгоритми керування. У сучасних системах дедалі частіше застосовуються багатофункціональні сенсорні модулі, що поєднують кілька типів вимірювань.

У контексті систем ідентифікації особи важливу роль відіграють спеціалізовані сенсори, зокрема відеокамери, інфрачервоні камери та мікрофони. Відеокамери забезпечують отримання зображень для подальшої обробки, тоді як інфрачервоні сенсори дозволяють працювати в умовах недостатнього освітлення. З точки зору комп'ютерної інженерії важливими є параметри роздільної здатності, частоти кадрів, інтерфейсу підключення (USB, CSI, Ethernet) та підтримки апаратного кодування відео [29].

Виконавчі механізми є елементами, що реалізують фізичний вплив на систему. У ліфтах до них належать електродвигуни, приводи дверей, гальмівні системи та інші пристрої. Керування виконавчими механізмами здійснюється через силові модулі та драйвери, які взаємодіють із контролерами через цифрові або аналогові інтерфейси. Важливим аспектом є забезпечення точності керування та швидкої реакції на зміну команд.

Інтеграція сенсорів і виконавчих механізмів із edge-пристроями здійснюється через різноманітні апаратні інтерфейси [30]. Найбільш поширеними є GPIO для цифрових сигналів, ADC для аналогових вимірювань, а також серійні інтерфейси, такі як UART, SPI та I2C. У промислових системах широко застосовуються також інтерфейси CAN та RS-485, які забезпечують високу завадостійкість і надійність передачі даних.

Однією з ключових вимог до апаратних засобів кіберфізичних систем є забезпечення роботи в реальному часі [31]. Це означає, що обробка сигналів і формування керуючих впливів повинні відбуватися з гарантованими часовими обмеженнями. Для цього використовуються апаратні переривання, таймери, DMA-контролери та інші механізми, що дозволяють мінімізувати затримки та

забезпечити детермінованість виконання.

Важливим аспектом є також масштабованість і модульність апаратної платформи. Система повинна забезпечувати можливість підключення додаткових сенсорів і пристроїв без суттєвої зміни архітектури. Це досягається за рахунок використання стандартизованих інтерфейсів і протоколів, а також модульного підходу до проєктування.

Окрім функціональних характеристик, значну увагу приділяють питанням надійності та відмовостійкості. Апаратні компоненти повинні працювати в умовах підвищених навантажень, температурних коливань та електромагнітних завад. Для цього використовуються промислові компоненти, механізми резервування та системи діагностики.

Таким чином, периферійні (edge) пристрої та сенсорні підсистеми є критично важливими елементами кіберфізичних систем «розумних» будівель. Вони забезпечують зв’язок між фізичним середовищем і обчислювальною частиною системи, визначають швидкодію, точність і надійність роботи, а також створюють основу для реалізації функцій ідентифікації особи та автоматизації роботи «розумного» ліфта.

1.5 Постановка задачі

Проведений аналіз наукових робіт показує, що розвиток «розумних» ліфтових систем відбувається у напрямі глибокої інтеграції технологій штучного інтелекту, біометричної ідентифікації, edge-computing, IoT та комп’ютерного зору. Основними тенденціями є безконтактна взаємодія з користувачем, персоналізація роботи системи, підвищення рівня безпеки, предиктивний моніторинг технічного стану обладнання та адаптивне керування на основі аналізу даних у реальному часі.

Отже, для досягнення мети магістерської роботи необхідно розв’язати наступні завдання:

- проаналізувати архітектурні особливості сучасних комп’ютерних

систем керування ліфтами та методи біометричної ідентифікації;

- розробити структурну модель КФС як багаторівневу ієрархію фізичного, мережевого та обчислювального рівнів;
- обґрунтувати вибір апаратної платформи (Edge AI) та сенсорної підсистеми для забезпечення низької затримки (latency) обробки;
- спроектувати цифровий конвеєр обробки біометричних даних та інтерфейс взаємодії з ліфтовою автоматикою (GPIO, релейні модулі, промислові протоколи).

1.6 Висновки до першого розділу

У першому розділі проведено аналіз предметної галузі де визначено, що «розумний ліфт» є складною кіберфізичною системою, де надійність функціонування залежить від швидкодії обчислювальних вузлів та стабільності каналів передачі даних.

Обґрунтовано доцільність використання вбудованих систем (Edge AI) для локальної ідентифікації особи, що дозволяє уникнути затримок хмарної інфраструктури та підвищити безпеку персональних даних.

Аналіз існуючих рішень показав відсутність уніфікованих апаратних інтерфейсів для зв’язку КФС із застарілими контролерами ліфтів, що робить розробку релейних та протокольних вузлів сполучення критично важливою.

2 МОДЕЛЮВАННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ОСОБИ

2.1 Концептуальна модель кіберфізичної системи ідентифікації особи

Кіберфізична система ідентифікації особи (КФСІО) є складною інтегрованою системою, яка поєднує фізичні процеси спостереження за людиною з інформаційними та обчислювальними процесами аналізу біометричних даних. Така система реалізує безперервний цикл взаємодії між фізичним середовищем і цифровою обчислювальною інфраструктурою, забезпечуючи автоматизоване визначення або підтвердження особи користувача.

Концептуально КФСІО розглядається як динамічна система, що функціонує в умовах невизначеності, обмежених ресурсів та необхідності обробки даних у реальному часі. На відміну від традиційних систем, вона має тісний зв’язок із фізичним середовищем, що обумовлює необхідність врахування впливу зовнішніх факторів, таких як освітлення, положення об’єкта, наявність шумів та інших перешкод.

Загальна структура КФСІО базується на принципах системного аналізу та передбачає декомпозицію на функціональні підсистеми, кожна з яких виконує визначену роль у загальному процесі ідентифікації. Такий підхід дозволяє забезпечити модульність, гнучкість і масштабованість системи, а також спрощує її математичне моделювання та програмну реалізацію.

У найзагальнішому вигляді КФСІО можна представити як систему, що реалізує відображення вхідних біометричних даних у множину ідентифікаторів користувачів виду 2.1:

$$Y = F(X), \tag{2.1}$$

де X – простір вхідних даних;

Y – множина можливих рішень щодо ідентифікації особи;

F – функція, що є складною композицією взаємопов’язаних перетворень, що реалізуються на різних рівнях системи.

Першим етапом функціонування КФСІО є взаємодія з фізичним середовищем, яка реалізується через сенсорну підсистему. Ця підсистема виконує перетворення реальних біометричних характеристик людини у цифрову форму. Важливо відзначити, що цей процес супроводжується появою шумів та спотворень, які можуть бути викликані як апаратними обмеженнями, так і зовнішніми умовами.

У загальному вигляді процес формування вхідних даних можна описати у вигляді 2.2:

$$x(t) = H(s(t), n(t)), \tag{2.2}$$

де $s(t)$ – реальний стан об’єкта;

$n(t)$ – випадкові збурення;

H – оператор вимірювання.

Таким чином, вже на початковому етапі виникає задача підвищення якості даних та мінімізації впливу шумів.

Отримані дані передаються на рівень попередньої обробки, який виконує їх нормалізацію та підготовку до подальшого аналізу. На цьому рівні здійснюється усунення або зменшення впливу факторів, що не несуть корисної інформації для ідентифікації, таких як неоднорідність освітлення, фонові об’єкти або геометричні спотворення.

Попередня обробка дозволяє привести всі вхідні дані до єдиного стандарту, що є критично важливим для стабільної роботи алгоритмів розпізнавання.

Наступним ключовим компонентом концептуальної структури є підсистема виділення ознак. Саме на цьому етапі відбувається перехід від сирих даних до їх абстрактного представлення у вигляді векторів ознак. Ці вектори повинні зберігати суттєві характеристики обличчя людини та бути інваріантними до змін зовнішніх умов.

Формально цей процес можна описати як перетворення виду 2.3:

$$z = \Phi(x), \tag{2.3}$$

де Ф – функція виділення ознак.

Вибір цієї функції є одним із найважливіших аспектів побудови системи, оскільки саме вона визначає якість подальшої ідентифікації.

Рівень ідентифікації є центральним елементом КФСІО, на якому здійснюється прийняття рішення щодо належності вхідних даних до певного користувача. Цей процес може бути реалізований у вигляді задачі пошуку найближчого елемента в просторі ознак або як задача класифікації.

Важливою особливістю цього рівня є необхідність роботи з великими обсягами даних, що потребує оптимізації алгоритмів з точки зору швидкодії та використання пам’яті.

Результат ідентифікації має ймовірнісний характер, що обумовлено наявністю шумів і неповноти інформації. Тому наступним етапом є рівень прийняття рішень, на якому враховується не лише сам результат, але й ступінь його достовірності. Це дозволяє підвищити надійність системи та зменшити кількість помилкових спрацьовувань.

Завершальним елементом концептуальної структури є підсистема взаємодії із зовнішніми системами. Вона забезпечує передачу результатів ідентифікації у прикладні системи, які використовують ці дані для реалізації власних функцій. У контексті даної роботи такою системою є система автоматизації роботи «розумного ліфта». При цьому КФСІО виконує роль інформаційного постачальника і не бере участі у формуванні логіки керування.

Важливою характеристикою КФСІО є наявність зворотного зв’язку, який дозволяє адаптувати систему до змін умов функціонування. Наприклад, результати ідентифікації можуть використовуватися для оновлення бази даних або корекції параметрів моделей. Це забезпечує здатність системи до самонавчання та підвищення точності з часом.

Крім того, концептуальна структура повинна враховувати вимоги до роботи

в реальному часі. Це означає, що всі етапи обробки даних повинні виконуватися з обмеженою затримкою, яка не перевищує допустимого порогу. Таким чином, при проектуванні системи необхідно враховувати компроміс між точністю і швидкодією.

Ще одним важливим аспектом є забезпечення безпеки біометричних даних. Оскільки система працює з персональною інформацією, необхідно передбачити механізми її захисту від несанкціонованого доступу, включаючи шифрування, аутентифікацію та контроль доступу.

Таким чином, концептуальна структура кіберфізичної системи ідентифікації особи являє собою багаторівневу ієрархічну систему, що забезпечує повний цикл обробки біометричних даних, від їх отримання до формування результату, придатного для використання у зовнішніх системах.

Запропонована структура дозволяє врахувати особливості реального середовища, забезпечити високу точність і швидкодію, а також створює основу для подальшого математичного моделювання та реалізації системи.

2.2 Інтеграція кіберфізичної системи ідентифікації особи в систему автоматизації «розумного ліфта»

Кіберфізична система ідентифікації особи, розглянута в попередньому підрозділі, є самостійною функціональною підсистемою, яка забезпечує отримання достовірної інформації про користувача. Однак практична цінність такої системи реалізується лише за умови її інтеграції з прикладними системами автоматизації. Одним із перспективних напрямів застосування є використання результатів ідентифікації для автоматизації роботи «розумного ліфта».

Структурна схема кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» представлена на рисунку 2.1.

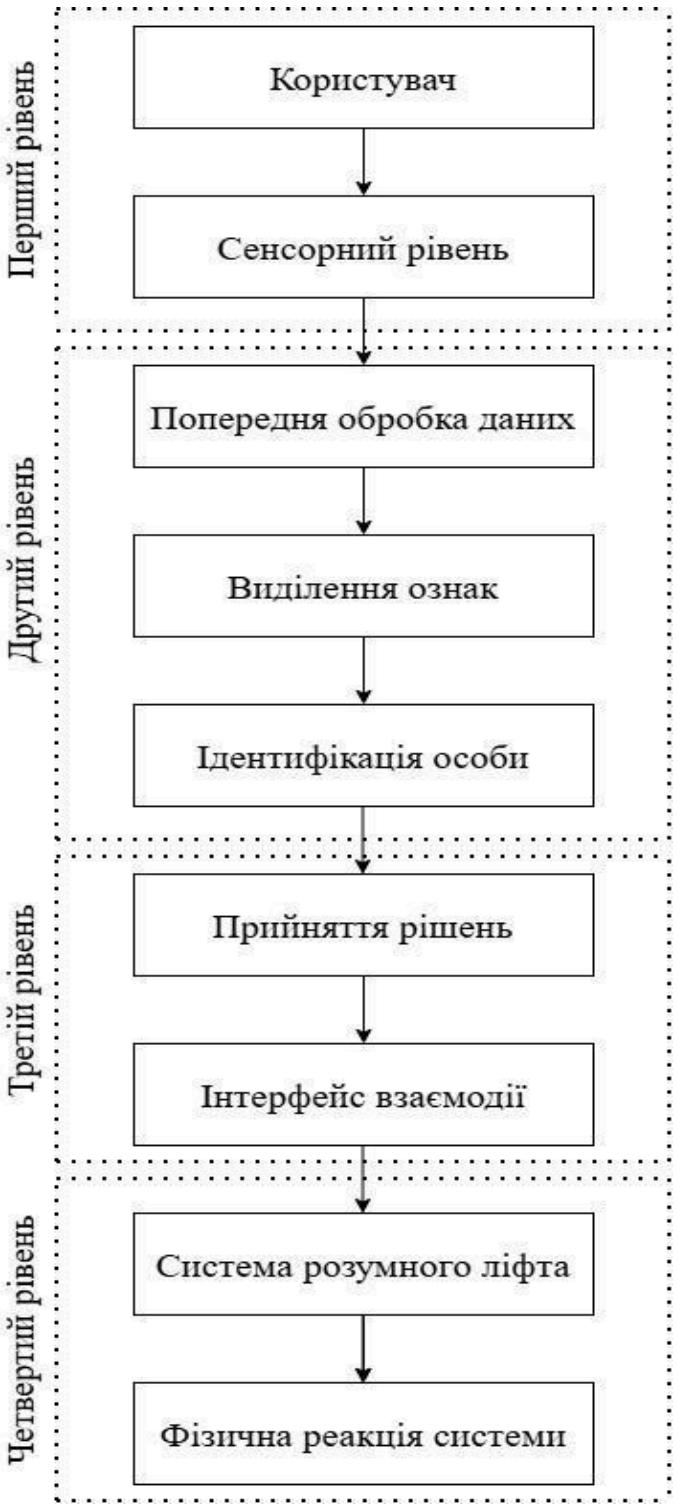


Рисунок 2.1 – Структурна схема кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта»

Подана структурна схема відображає багаторівневу архітектуру кіберфізичної системи ідентифікації особи та її інтеграцію із системою автоматизації «розумного ліфта». Система побудована за принципом послідовного

перетворення фізичних даних у керуючі впливи з урахуванням етапів обробки, аналізу та прийняття рішень.

На відміну від традиційних систем керування ліфтами, де взаємодія з користувачем здійснюється через механічні або сенсорні інтерфейси (кнопки виклику та вибору поверху), у системах нового покоління передбачається мінімізація прямої взаємодії людини з інтерфейсом. Це досягається за рахунок використання даних про користувача, отриманих автоматично, зокрема за допомогою біометричної ідентифікації.

На першому рівні знаходиться сенсорний рівень, який забезпечує первинне отримання інформації про користувача. Основними елементами цього рівня є камера відеоспостереження, датчик присутності, датчик освітлення та модуль реального часу. Камера виконує захоплення зображення користувача, який входить у зону дії системи, тоді як додаткові сенсори фіксують контекстні умови, що можуть впливати на якість ідентифікації. Датчик присутності дозволяє визначити факт появи користувача, а годинник реального часу забезпечує часову прив’язку подій.

Другий рівень представлений кіберфізичною системою ідентифікації особи (КФСІО). На цьому етапі здійснюється комплексна обробка отриманих даних. Спочатку виконується попередня обробка зображення, яка включає нормалізацію, вирівнювання та підвищення якості вхідних даних. Далі відбувається етап виділення ознак, де за допомогою нейронної моделі формується компактне векторне представлення (embedding) обличчя користувача. Отримані ознаки порівнюються з базою даних еталонних зразків, що дозволяє визначити ідентифікатор особи ууу та рівень достовірності qqq. Результатом роботи цього рівня є структурований вихідний сигнал, що містить параметри ідентифікації та передається до наступного рівня системи.

Третій рівень відповідає за прийняття рішень. На цьому етапі здійснюється аналіз достовірності результату ідентифікації шляхом порівняння показника q із заданим порогом q_{min}.

У випадку, якщо рівень достовірності є недостатнім, система ініціює

відхилення доступу або повторну ідентифікацію.

Якщо ж результат є валідним, виконується перевірка прав доступу користувача на основі його ідентифікатора. Далі враховується контекстна інформація, така як час доби, режим роботи системи та інші умови експлуатації. На основі цих даних формується множина допустимих дій, з якої обирається оптимальне рішення, що і визначає подальшу поведінку системи.

Четвертий рівень становить система керування ліфтом, яка отримує керуючий сигнал від блоку прийняття рішень. До складу цього рівня входить контролер ліфта (PLC або мікроконтролер), а також виконавчі механізми. Вони забезпечують фізичну реалізацію команд, таких як виклик кабіни, вибір поверху, відкриття або закриття дверей, а також керування приводами руху. Таким чином, цей рівень перетворює цифрові рішення у фізичні дії.

Окремо на схемі виділено інформаційну інфраструктуру, яка забезпечує взаємодію між усіма рівнями системи. Вона включає базу даних користувачів, сервер обробки та зберігання даних, а також мережеву інфраструктуру (LAN, Wi-Fi або Ethernet). База даних містить біометричні шаблони та інформацію про права доступу користувачів. Сервер забезпечує обробку запитів, збереження журналів подій та координацію роботи підсистем. Мережевий рівень відповідає за передачу даних між компонентами системи.

Схема також містить позначення потоків даних і керуючих сигналів. Суцільні стрілки відображають основний інформаційний потік від сенсорного рівня до виконавчих механізмів, тоді як пунктирні лінії позначають зворотний зв’язок, який використовується для журналювання подій, фіксації помилок та уточнення результатів роботи системи.

Таким чином, представлена схема демонструє повний цикл функціонування кіберфізичної системи від збору даних про користувача до формування керуючого впливу на фізичний об’єкт, тобто ліфт. Це дозволяє реалізувати інтелектуальну, адаптивну та безконтактну систему керування доступом у будівлі.

2.3 Моделювання процесу прийняття рішень у кіберфізичній системі на основі ідентифікації особи

Розглянемо поняття біометричної ідентифікації особи. Під біометричною ідентифікацією особи розуміється процес автоматизованого встановлення або підтвердження особи користувача на основі його унікальних фізіологічних або поведінкових характеристик. На відміну від традиційних методів аутентифікації, таких як використання паролів, карт доступу або PIN-кодів, біометричні підходи базуються на властивостях, які є невід'ємними для конкретної людини та складними для підробки або передачі іншій особі.

До основних фізіологічних біометричних характеристик належать геометрія обличчя, відбитки пальців, райдужна оболонка ока, структура вен, тоді як поведінкові характеристики включають особливості голосу, динаміку набору тексту або характер рухів. У контексті даної роботи основна увага приділяється ідентифікації за зображенням обличчя, що є найбільш зручним і безконтактним методом для інтеграції в кіберфізичні системи.

Процес біометричної ідентифікації складається з кількох етапів.

На першому етапі здійснюється захоплення біометричних даних за допомогою сенсорних пристроїв. Далі виконується попередня обробка, яка спрямована на підвищення якості даних та їх нормалізацію.

Наступним кроком є виділення ознак, у результаті чого формується компактне цифрове представлення біометричного образу.

На завершальному етапі відбувається порівняння отриманого представлення з еталонними даними, що зберігаються в базі, та прийняття рішення про ідентифікацію.

Суттєвою особливістю біометричної ідентифікації є її ймовірнісний характер. Через наявність шумів, змін умов зйомки та внутрішньої варіативності біометричних характеристик результат ідентифікації не є абсолютно точним і описується через показники достовірності. Це обумовлює необхідність використання порогових критеріїв і оцінки ризиків помилок, таких як помилкове

прийняття або відхилення користувача.

Важливою перевагою біометричної ідентифікації є можливість її безконтактної реалізації, що підвищує зручність використання та швидкість взаємодії з системою. Це робить її особливо актуальною для застосування в кіберфізичних системах автоматизації, де необхідна мінімізація участі користувача у процесі керування. Зокрема, у системах «розумного ліфта» біометрична ідентифікація дозволяє автоматично визначати користувача та формувати керуючі дії без використання традиційних інтерфейсів.

Таким чином, біометрична ідентифікація виступає ключовим інструментом для побудови інтелектуальних систем доступу та автоматизації, забезпечуючи поєднання високого рівня безпеки, зручності та адаптивності.

Інтеграція КФСІО із системою «розумного ліфта» передбачає організацію інформаційного обміну, при якому результат ідентифікації використовується як вхідний параметр для алгоритмів керування.

Формально цей процес можна представити у вигляді 2.4:

$$U = G(I,\ Q,\ C), \tag{2.4}$$

де U – керуючий вплив на систему ліфта;

G – функція прийняття рішень, тобто формалізований алгоритм, який перетворює результат ідентифікації особи у керуючу дію системи;

I – ідентифікатор особи;

Q – достовірність ідентифікації;

C – контекст.

Дана формула описує загальний принцип формування керуючого впливу в системі на основі результатів ідентифікації особи. Вона відображає залежність вихідного сигналу від трьох основних параметрів: ідентифікатора користувача, рівня достовірності розпізнавання та контекстної інформації.

Функція G реалізує логіку прийняття рішень, яка може включати як детерміновані правила, так і інтелектуальні алгоритми. Такий підхід дозволяє

враховувати не лише факт ідентифікації, але й якість цього процесу та зовнішні умови. У результаті формується адаптивна модель керування, здатна працювати в умовах невизначеності.

Таким чином, ідентифікація особи виступає джерелом інформації, необхідної для формування керуючих рішень.

Функція прийняття рішень у кіберфізичній системі ідентифікації особи являє собою формалізований алгоритм, який забезпечує перетворення результатів розпізнавання користувача у відповідні керуючі дії системи. Її основне призначення полягає у встановленні однозначного зв’язку між отриманою інформацією про особу та подальшою реакцією системи автоматизації. Така функція виступає проміжною ланкою між підсистемою ідентифікації та виконавчими механізмами, забезпечуючи узгодженість їх взаємодії.

На відміну від простих логічних схем, функція прийняття рішень враховує не лише сам факт ідентифікації, але й якісні характеристики цього процесу, зокрема рівень достовірності отриманого результату. Це обумовлено тим, що біометрична ідентифікація має ймовірнісний характер, і тому кожне рішення повинно прийматися з урахуванням ризику помилки. У зв’язку з цим функція прийняття рішень включає механізми оцінювання надійності даних та застосування порогових критеріїв, які визначають допустимість використання результату ідентифікації.

Крім того, важливим компонентом вхідних даних для функції є контекстна інформація, яка може включати часові параметри, стан системи, рівень завантаженості, а також індивідуальні характеристики користувача. Урахування контексту дозволяє перейти від статичної моделі керування до адаптивної, що змінює свою поведінку залежно від умов функціонування. Це особливо важливо для кіберфізичних систем, які працюють у динамічному середовищі.

Функція прийняття рішень може бути реалізована різними способами залежно від складності системи.

У найпростішому випадку вона представляє собою набір детермінованих правил типу «якщо–то», що задають відповідність між ідентифікатором

користувача та дією системи. У більш складних реалізаціях можуть використовуватися методи оптимізації, які дозволяють обирати найкраще рішення за певними критеріями, такими як мінімізація часу обслуговування або енергоспоживання.

Також можливе застосування ймовірнісних моделей або методів машинного навчання, що забезпечують адаптацію системи до змін умов експлуатації.

Суттєвою характеристикою функції прийняття рішень є її робота в умовах обмеженого часу. У кіберфізичних системах затримка між моментом ідентифікації та формуванням керуючого сигналу повина бути мінімальною, що накладає обмеження на складність алгоритмів. Це вимагає оптимального поєднання швидкодії та точності, а також ефективної організації обчислювальних процесів.

З практичної точки зору функція прийняття рішень визначає, яким чином система буде реагувати на появу конкретного користувача.

Наприклад, у випадку успішної ідентифікації вона може ініціювати виконання певної дії, тоді як при недостатньому рівні достовірності може відмовити у виконанні або запустити повторний процес розпізнавання. Таким чином, саме ця функція забезпечує інтелектуальну поведінку системи та її здатність до автономного функціонування.

Отже, функція прийняття рішень є ключовим елементом кіберфізичної системи ідентифікації особи, оскільки вона забезпечує перехід від інформаційного рівня до рівня керування. Її правильна побудова визначає ефективність, надійність та адаптивність усієї системи в цілому.

Процес взаємодії між КФСІО та системою автоматизації можна описати як послідовність етапів.

Спочатку користувач потрапляє в зону дії сенсорної підсистеми, де відбувається захоплення його зображення. Далі КФСІО виконує всі етапи обробки, від попередньої обробки до ідентифікації, і формує результат у вигляді ідентифікатора та рівня достовірності.

Отриманий результат передається до системи керування ліфтом через відповідний інтерфейс взаємодії. На основі цієї інформації система автоматизації

визначає подальші дії, які можуть включати:

- автоматичний виклик ліфта на поверх користувача;
- вибір цільового поверху на основі профілю користувача;
- встановлення пріоритету обслуговування;
- обмеження доступу до певних поверхів.

Важливо підкреслити, що КФСІО не бере участі у формуванні логіки керування ліфтом, а лише надає вхідні дані. Це забезпечує слабку зв’язаність між підсистемами та дозволяє використовувати систему ідентифікації незалежно від конкретної реалізації ліфтового обладнання.

З точки зору кіберфізичних систем, інтеграція відбувається через замкнений контур взаємодії, у якому фізичні дії користувача (поява перед ліфтом) призводять до формування цифрового сигналу (результату ідентифікації), який, у свою чергу, викликає фізичну реакцію системи (рух ліфта). Такий підхід дозволяє забезпечити високий рівень автоматизації та адаптивності системи.

Однією з ключових переваг використання ідентифікації особи є можливість персоналізації роботи системи. На основі історичних даних про користувача можуть формуватися індивідуальні сценарії, що дозволяє скоротити час обслуговування та підвищити комфорт.

Наприклад, система може автоматично визначати найбільш ймовірний поверх призначення залежно від часу доби.

Разом з тим інтеграція КФСІО із системою «розумного ліфта» накладає додаткові вимоги до якості ідентифікації. Зокрема, помилки розпізнавання можуть призводити до некоректних дій системи, що знижує її ефективність. У зв’язку з цим необхідно враховувати ймовірнісні характеристики системи та впроваджувати механізми перевірки достовірності результатів. Ще одним важливим аспектом є забезпечення роботи в реальному часі. Загальний час від моменту появи користувача до формування керуючого сигналу повинен бути мінімальним, щоб система виглядала для користувача миттєвою та інтуїтивною. Це вимагає оптимізації як алгоритмів ідентифікації, так і каналів передачі даних між підсистемами.

Крім того, інтеграція повинна враховувати питання безпеки. Оскільки система використовує персональні біометричні дані, необхідно забезпечити їх захист при передачі та зберіганні. Це досягається за рахунок використання криптографічних методів, а також розмежування доступу до інформації.

Таким чином, інтеграція кіберфізичної системи ідентифікації особи із системою автоматизації «розумного ліфта» забезпечує перехід від традиційного керування до інтелектуального, орієнтованого на користувача. Ідентифікація виступає ключовим елементом, що дозволяє реалізувати автоматичне, персоналізоване та безконтактне управління.

Запропонований підхід створює основу для подальшого моделювання процесів прийняття рішень та оптимізації роботи системи в цілому.

2.4 Структура процесу прийняття рішень

Процес прийняття рішень у кіберфізичній системі ідентифікації особи реалізується як послідовність етапів, що перетворюють результат розпізнавання користувача у керуючий сигнал. Кожен етап виконує окрему функцію обробки інформації та зменшує невизначеність, що виникає під час ідентифікації.

На першому етапі система аналізує результат біометричної ідентифікації користувача, який отримується після обробки зображення. Через те, що процес розпізнавання обличчя є ймовірнісним, отриманий результат не може вважатися абсолютно точним. На нього впливають різні фактори, зокрема освітлення, ракурс, часткове перекриття обличчя або наявність шумів у зображенні.

Саме тому система повинна оцінити, наскільки отриманий результат є достовірним і чи можна його використовувати для автоматичного керування ліфтом. Для цього вводиться числовий показник достовірності, який відображає ступінь відповідності поточного зображення еталонним даним у базі.

Якщо рівень достовірності є недостатнім, система не повинна виконувати автоматичні дії, оскільки це може призвести до помилкового вибору поверху або надання доступу сторонній особі. У такому випадку система або переходить у

режим очікування, або пропонує користувачу скористатися стандартними елементами керування.

В таблиці 2.1 відображено послідовність етапів процесу прийняття рішень у системі «розумного ліфта», а також відповідні вхідні та вихідні дані кожного етапу. Така структуризація дозволяє чітко визначити логіку обробки інформації та взаємозв’язок між підсистемами.

Таблиця 2.1 – Структура процесу прийняття рішень у КФС ідентифікації особи для автоматизації роботи «розумного ліфта»

№	Етап процесу	Вхідні дані	Вихідні дані
1	Оцінка достовірності ідентифікації	Зображення користувача, вектор ознак, база даних	Ідентифікатор особи, рівень достовірності
2	Перевірка прав доступу	Ідентифікатор користувача, база прав доступу	Множина дозволених дій (наприклад, доступні поверхи)
3	Аналіз контексту	Час, стан системи, історія використання	Уточнена множина дій
4	Вибір допустимих дій	Множина дій	Остаточна множина допустимих дій
5	Генерація керуючого сигналу	Ідентифікатор, достовірність, контекст, множина	Керуючий сигнал uuu (виклик ліфта, вибір поверху тощо)

Після підтвердження достовірності ідентифікації система переходить до перевірки прав доступу користувача. Цей етап є необхідним, оскільки навіть правильно ідентифікований користувач не завжди має право виконувати всі можливі дії у системі ліфта.

У контексті «розумного ліфта» права доступу визначають, які поверхи доступні конкретному користувачу, а також які режими роботи системи він може

використовувати. Наприклад, мешканець будинку може мати доступ лише до свого поверху, тоді як технічний персонал може мати доступ до всіх.

Перевірка прав доступу здійснюється шляхом звернення до бази даних, де для кожного користувача зберігається перелік дозволених дій. Якщо користувач не має необхідних прав, система не виконує автоматичний вибір поверху і може обмежити функціональність.

На третьому етапі система враховує контекстні умови, у яких відбувається її робота. Контекст у кіберфізичній системі ідентифікації особи для автоматизації роботи «розумного ліфта» є одним із ключових факторів, що визначає адаптивність і інтелектуальність функціонування системи. Його врахування дозволяє перейти від жорстко заданих алгоритмів до гнучкої моделі прийняття рішень, яка здатна змінювати свою поведінку залежно від поточних умов експлуатації. На відміну від традиційних систем керування, де рішення приймаються за фіксованими правилами, у кіберфізичній системі контекст забезпечує динамічну корекцію цих правил.

Контекст представляє собою сукупність параметрів, які описують як зовнішнє середовище, так і внутрішній стан системи в конкретний момент часу. До основних складових контексту належать часові характеристики, зокрема час доби, день тижня або календарні особливості. Ці параметри дозволяють системі враховувати режим функціонування об’єкта, наприклад розмежування робочого та неробочого часу. У робочі години система може функціонувати у режимі максимального обслуговування користувачів, тоді як у нічний період у режимі підвищеної безпеки з обмеженням доступу до окремих поверхів.

Важливим елементом контексту є поточний стан ліфтової системи. Він включає інформацію про положення кабіни, напрямок її руху, кількість активних викликів, а також рівень завантаженості. Наприклад, якщо ліфт вже рухається у напрямку, який відповідає потребам користувача, система може не викликати нову кабіну, а оптимізувати існуючий маршрут. У випадку високого навантаження, коли кількість викликів перевищує певний поріг, система може змінювати алгоритм обслуговування, наприклад групувати користувачів за напрямками руху або

змінювати пріоритети обробки запитів.

Окрему роль відіграє інформація про історію використання системи конкретним користувачем. Аналізуючи попередні дії, система може формувати типові сценарії поведінки, що дозволяє прогнозувати майбутні запити. Наприклад, якщо користувач регулярно використовує ліфт для поїздки на певний поверх у визначений час, система може автоматично пропонувати або навіть виконувати відповідну дію без додаткового підтвердження. Такий підхід значно підвищує комфорт користування та зменшує час взаємодії із системою.

Крім того, контекст може включати зовнішні умови, такі як освітлення, що впливає на якість ідентифікації, або технічний стан обладнання. У випадку зниження якості розпізнавання система може змінювати порогові значення або вимагати додаткового підтвердження особи. Це дозволяє підтримувати стабільність роботи навіть за несприятливих умов.

Урахування контексту також забезпечує підвищення рівня безпеки. Наприклад, у нічний час або в умовах підвищеного ризику система може вимагати більш високий рівень достовірності ідентифікації або обмежувати автоматичні дії. Таким чином, контекст використовується не лише для оптимізації роботи, але й для запобігання потенційним загрозам.

Формально контекст можна розглядати як набір змінних, які впливають на процес прийняття рішень, і які використовуються для модифікації множини допустимих дій. Це означає, що одна й та сама ідентифікована особа може отримувати різні варіанти поведінки системи залежно від умов, у яких відбувається взаємодія.

Отже, контекст є невід’ємною складовою кіберфізичної системи ідентифікації особи для «розумного ліфта», оскільки він забезпечує адаптивність, інтелектуальність та ефективність функціонування. Його врахування дозволяє не лише підвищити якість обслуговування користувачів, але й оптимізувати роботу всієї системи в умовах реального часу.

Контекст можна подати у вигляді вектору параметрів виду 2.5:

$$\mathrm{C} = G(t,\ d,\ s,\ l,\ h), \tag{2.5}$$

де t – час доби;

d – день тижня;

s – стан ліфта;

l – рівень завантаженості;

h – історія використання користувача.

Контекст безпосередньо впливає на формування множини допустимих дій системи. У класичному випадку множина дій залежить лише від користувача, однак у кіберфізичній системі вона уточнюється з урахуванням певних умов.

Це означає, що навіть для одного і того ж користувача набір доступних дій може змінюватися залежно від часу, стану системи або інших факторів.

Наприклад:

- у денний час користувач може мати доступ до всіх дозволених поверхів;
- у нічний час доступ обмежується;
- при перевантаженні ліфта змінюється логіка обслуговування.

2.5 Модель станів та переходів системи у КФС ідентифікації особи для «розумного ліфта»

Модель скінченного автомата (FSM) є одним із базових інструментів проєктування кіберфізичних систем, оскільки дозволяє формалізувати поведінку системи у вигляді набору станів, подій та переходів між ними. Для задачі автоматизації роботи «розумного ліфта» з функцією ідентифікації особи FSM відіграє ключову роль, забезпечуючи передбачуваність, керованість та безпечність функціонування системи.

У контексті даної системи FSM описує логіку взаємодії між користувачем, сенсорною підсистемою, модулем ідентифікації (наприклад, на основі комп’ютерного зору чи RFID) та виконавчими механізмами ліфта. Кожен стан відображає певний етап роботи системи, а переходи між станами ініціюються

подіями (наприклад, появою користувача, завершенням розпізнавання, натисканням кнопки або сигналом від контролера).

FSM дозволяє:

- чітко розділити функціональні етапи роботи системи;
- уникнути неоднозначних сценаріїв поведінки;
- спростити відлагодження та тестування;
- забезпечити реакцію в реальному часі.

Розглянемо базовий набір станів для КФС ідентифікації особи в «розумному ліфті» (рис. 2.2).

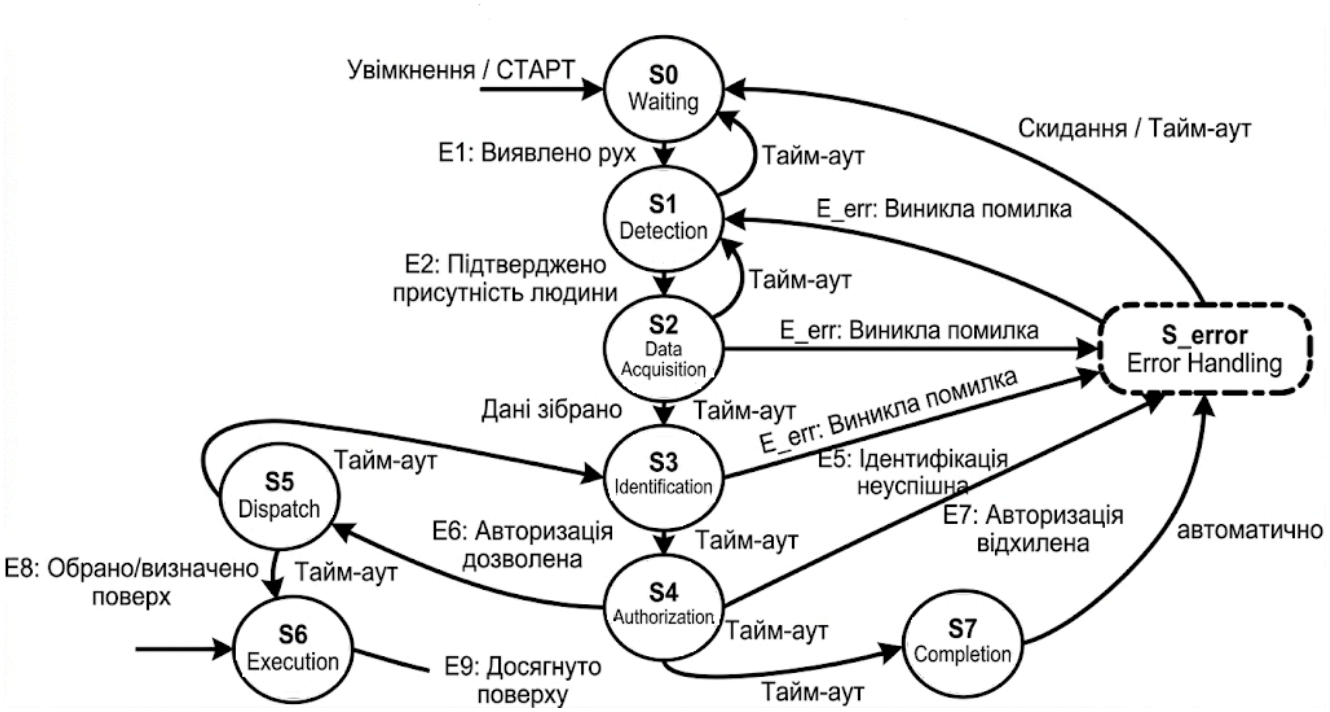


Рисунок 2.2 – Граф станів скінченного автомата «розумного» ліфта

Наведений граф описує логіку роботи системи керування доступом до ліфта у вигляді послідовності станів. Вона охоплює весь цикл взаємодії з користувачем, від пасивного очікування та виявлення людини до ідентифікації, перевірки прав доступу й виконання поїздки, а також передбачає обробку помилок.

Розглянемо детальніше стани системи.

Стан S0 – очікування, коли система перебуває у пасивному режимі,

очікуючи на появу користувача. Сенсори (камера, датчики руху) працюють у режимі моніторингу з мінімальним енергоспоживанням. У цьому стані не відбувається активної обробки даних, окрім базового детектування активності.

Стан S1 – виявлення користувача. Після фіксації руху або появи об'єкта система переходить до стану детекції. Використовуються алгоритми комп'ютерного зору для визначення наявності людини в зоні доступу до ліфта. Якщо об'єкт не підтверджується як людина, то система повертається в стан очікування.

Стан S2 – захоплення даних. На цьому етапі відбувається збір біометричних або ідентифікаційних даних, зокрема зображення обличчя, RFID-мітка, мобільний ідентифікатор тощо. Важливо забезпечити достатню якість даних для подальшого розпізнавання.

Стан S3 – ідентифікація. Отримані дані передаються в модуль обробки, де відбувається порівняння з базою користувачів. Це може бути локальна або хмарна обробка. Результатом є визначення особи або відмова в ідентифікації.

Стан S4 – авторизація. Після успішної ідентифікації система перевіряє права доступу користувача: дозволені поверхи, часові обмеження, рівень доступу. Якщо користувач не має прав, то формується відмова.

Стан S5 – призначення маршруту. Система автоматично визначає потрібний поверх (наприклад, за профілем користувача) або очікує вибір. Далі формується команда для виклику ліфта та оптимізації маршруту.

Стан S6 виконання. Ліфт рухається відповідно до отриманої команди. Система може продовжувати моніторинг для додаткових подій (наприклад, нових користувачів).

Стан S7 завершення. Після досягнення потрібного поверху цикл завершується, система повертається до стану Idle.

Стан S_error помилка. Окремий стан для обробки виключних ситуацій: збій сенсора, відмова ідентифікації, мережеві проблеми тощо.

Переходи між станами відбуваються на основі подій.

Матриця переходів скінченного автомата наведена в таблиці 2.2.

Таблиця 2.2 – Матриця переходів скінченного автомата

Початковий стан	Подія-тригер	Цільовий стан	Виконувана дія (Action)
S0 (Idle)	E1 (Рух)	S1 (Detection)	Активація камери, старт CPU детектора.
S1 (Detection)	E2 (Людина)	S2 (Acquisition)	Старт буферизації RGB-D потоку.
S1 (Detection)	Не E2 / Тайм-аут	S0 (Idle)	Деактивація камери, очищення буфера.
S2 (Acquisition)	E3 (Дані є)	S3 (Identification)	Активація GPU, інференс нейромережі.
S3 (Identification)	E4 (Успіх ID)	S4 (Authorization)	Пошук прав у БД для ID.
S3 (Identification)	E5 (Неуспіх)	S_error (Error)	Відмова, індикація «Невідомий».
S4 (Authorization)	E6 (Дозвіл)	S5 (Dispatch)	Запуск прогнозного алгоритму
S4 (Authorization)	E7 (Відмова)	S_error (Error)	Відмова, індикація «Доступ заборонено».
S5 (Dispatch)	E8 (Поверх є)	S6 (Execution)	Формування команди (GPIO/Modbus).
S6 (Execution)	E9 (Фініш)	S7 (Completion)	Логування успішного маршруту.
S7 (Completion)	(автоматично)	S0 (Idle)	Очищення контексту, Fail-safe перевірка.
Будь-який стан	S_error (Помилка)	S_error (Error)	Зупинка конвеєра, Fail-safe, Reset.

У кіберфізичних системах FSM має враховувати реальні фізичні процеси та обмеження:

- часові обмеження де кожен перехід має виконуватись у визначений час, інакше система може втратити актуальність даних;
- асинхронність подій, оскільки події можуть виникати незалежно одна від одної (наприклад, одночасна поява кількох користувачів);
- FSM повинна мати механізми відновлення після помилок;
- безпека є особливо важливою для систем ідентифікації тому, що необхідно запобігати несанкціонованому доступу.

2.6 Висновки

У другому розділі виконано моделювання кіберфізичної системи ідентифікації особи як багаторівневої інтегрованої структури, що поєднує фізичні процеси збору даних та їх інтелектуальну обробку.

Сформована концептуальна модель дозволила представити процес ідентифікації як послідовність взаємопов’язаних перетворень, від отримання сирих біометричних даних до прийняття рішення. Це дало змогу формалізувати систему у вигляді математичних відображень, що є важливим для подальшого аналізу, оптимізації та програмної реалізації.

Ключовим результатом є декомпозиція системи на функціональні підсистеми: сенсорну, попередньої обробки, виділення ознак, ідентифікації та прийняття рішень. Такий підхід забезпечує модульність архітектури, спрощує масштабування системи та дозволяє незалежно вдосконалювати окремі компоненти без порушення цілісності всієї КФС.

Особливу увагу приділено врахуванню впливу зовнішніх факторів (шумів, освітлення, перешкод), що підтверджує реалістичність моделі та її придатність для роботи в умовах реального середовища. Формалізація процесу прийняття рішень дала можливість інтегрувати результати ідентифікації з логікою керування «розумним» ліфтом.

3 МЕТОДИ ТА АЛГОРИТМИ ІДЕНТИФІКАЦІЇ ОСОБИ ТА АДАПТИВНОГО КЕРУВАННЯ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИ «РОЗУМНОГО ЛІФТА»

3.1 Архітектура конвеєра обробки біометричних даних

У кіберфізичній системі ідентифікації особи ключову роль відіграє не лише вибір окремих алгоритмів комп'ютерного зору, а й їх узгоджена організація у вигляді обчислювального конвеєра. Саме конвеєрна структура дозволяє забезпечити обробку відеопотоку в режимі реального часу, мінімізувати затримки та гарантувати стабільність роботи системи в умовах змінного середовища. Для задач комп'ютерної інженерії це є принципово важливим, оскільки мова йде не про ізольовані алгоритми, а про їх ефективну інтеграцію в єдину систему з чітко визначеними етапами обробки даних.

Конвеєр складається з послідовності взаємопов'язаних етапів: попередня обробка зображення, детекція обличчя, перевірка справжності біометричного об'єкта, нормалізація та ідентифікація (рис.3.1).

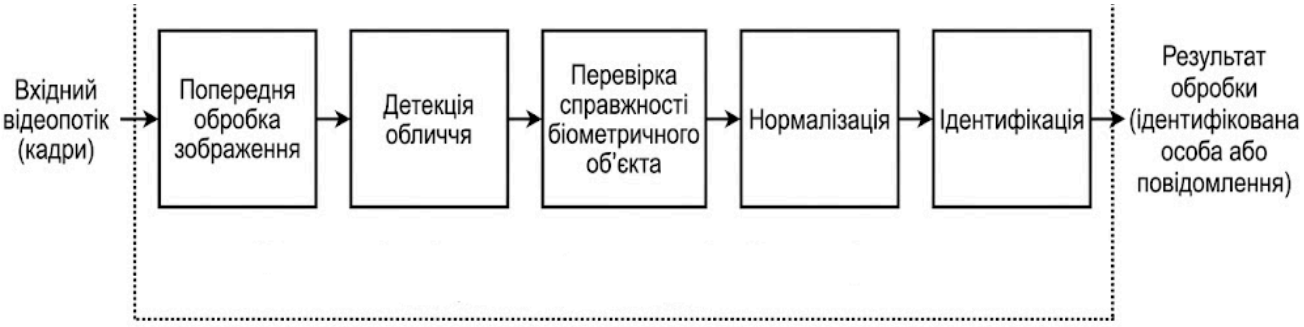


Рисунок 3.1 – Структурна схема конвеєра обробки біометричних даних

Кожен із цих етапів виконує окрему функцію, але водночас впливає на точність і швидкодію всієї системи. Важливою особливістю є те, що обробка даних відбувається потоково, тобто кожен кадр відео проходить через усі етапи незалежно, що дозволяє досягти паралелізму та ефективного використання обчислювальних ресурсів.

Формально конвеєр обробки можна представити як композицію функцій виду 3.1:

$$Y = F(X) = f_n(f_{n-1}(\dots f_1(X))), \quad (3.1)$$

де X – вхідний відео потік;

f_i – окремі етапи обробки;

Y – результат ідентифікації користувача.

Першим етапом є захоплення відеопотоку з камери, зокрема з використанням глибинного сенсора Intel RealSense D435. На цьому етапі система отримує синхронізовані потоки RGB-зображення, карти глибини та інфрачервоного сигналу. Важливою задачею є забезпечення стабільної частоти кадрів (FPS) та мінімальної затримки, що досягається шляхом використання буферизації кадрів і низькорівневих драйверів доступу до камери. Отримані дані формують первинний вхід, який передається до наступного етапу обробки.

Попередня обробка зображення спрямована на покращення якості вхідних даних та підвищення стійкості алгоритмів детекції. На цьому етапі виконуються операції нормалізації яскравості, корекції контрасту, фільтрації шумів та масштабування зображення. Також можливе застосування гістограмного вирівнювання або адаптивних фільтрів для компенсації нерівномірного освітлення.

У контексті роботи в реальному часі важливо мінімізувати обчислювальні витрати, тому обробка виконується з урахуванням компромісу між якістю та швидкодією. Результатом є підготовлене зображення, придатне для ефективної роботи алгоритмів комп’ютерного зору.

Наступним етапом є детекція обличчя, яка полягає у визначенні області інтересу (ROI), що містить обличчя користувача. Для цього застосовуються сучасні методи, зокрема нейромережева архітектура MTCNN або алгоритми бібліотеки Dlib. У процесі детекції виконується аналіз зображення з метою

виявлення характерних ознак обличчя, після чого формується прямокутна область та визначаються ключові точки. Цей етап є критично важливим, оскільки точність локалізації обличчя безпосередньо впливає на якість подальшої ідентифікації.

Для підвищення ефективності системи використовується відстеження обличчя, яке дозволяє уникнути повторної повної детекції на кожному кадрі. Алгоритм відстеження прогнозує положення обличчя на основі попередніх кадрів, що може бути реалізовано за допомогою фільтра Калмана або методів оптичного потоку. Це дозволяє значно зменшити обчислювальне навантаження та підвищити стабільність визначення ROI, особливо при плавних рухах користувача. Відстеження також забезпечує часову узгодженість даних, що важливо для наступних етапів аналізу.

Перевірка справжності біометричного об’єкта є одним із ключових елементів забезпечення безпеки системи. Вона виконується із використанням даних глибини та інфрачервоного випромінювання, отриманих від камери Intel RealSense D435. Алгоритм аналізує просторову структуру обличчя, визначаючи наявність характерних перепадів глибини, що відрізняють реальне обличчя від плоских зображень.

Додатково використовується аналіз ІЧ-відбиття, який дозволяє розрізняти матеріали за їх спектральними характеристиками. У деяких випадках також враховуються мікрорухи обличчя. Результатом цього етапу є коефіцієнт достовірності біометричного об’єкта, який визначає, чи буде обличчя допущене до подальшої обробки.

Після підтвердження справжності об’єкта виконується нормалізація зображення обличчя. Цей етап передбачає приведення зображення до стандартного вигляду, що включає вирівнювання по ключових точках (очі, ніс), масштабування до фіксованого розміру та корекцію орієнтації. Метою є зменшення впливу варіацій положення голови, освітлення та інших факторів на результати ідентифікації. Нормалізація забезпечує інваріантність подальших ознак до зовнішніх умов.

Наступним етапом є вилучення ознак, яке полягає у перетворенні

зображення обличчя у компактне числове представлення, тобто вектор ознак. Для цього використовуються методи глибокого навчання, які дозволяють виділити найбільш інформативні характеристики обличчя. Отриманий вектор має високу дискримінативну здатність і дозволяє ефективно порівнювати різні обличчя між собою. Саме на цьому етапі відбувається перехід від зображення до формалізованого опису особи.

Завершальним етапом є ідентифікація користувача, яка полягає у порівнянні отриманого вектора ознак із базою даних. Для цього застосовуються алгоритми пошуку найближчих сусідів або інші методи класифікації. Результатом є визначення найбільш ймовірного користувача та рівня достовірності ідентифікації. У разі перевищення заданого порогу система формує позитивне рішення та передає його до модуля прийняття рішень, який ініціює відповідну дію у фізичній системі, зокрема виклик ліфта.

Таким чином, кожен етап конвеєра виконує чітко визначену функцію, а їх послідовна інтеграція забезпечує ефективну, надійну та безпечну ідентифікацію користувача в межах кіберфізичної системи.

3.2 Метод детекції облич

Детекція обличчя є базовим етапом, що визначає область інтересу для подальшої обробки. Для реалізації цього етапу застосовуються сучасні методи, зокрема MTCNN або Dlib.

Метод детекції облич є одним із ключових етапів у конвеєрі обробки біометричних даних, оскільки саме на цьому рівні здійснюється первинне виділення області інтересу, що містить обличчя користувача.

Якість виконання цього етапу безпосередньо впливає на точність подальших процедур, а саме перевірки справжності об’єкта, нормалізації, вилучення ознак та ідентифікації.

У контексті кіберфізичної системи «розумного ліфта» детекція облич повинна відповідати вимогам реального часу, бути стійкою до змін освітлення,

ракурсу та часткових перекриттів, а також ефективно працювати на вбудованих обчислювальних платформах.

В основі реалізації методу детекції облич лежить застосування сучасних алгоритмів комп'ютерного зору, зокрема глибоких нейронних мереж. Одним із найбільш доцільних підходів є використання архітектури MTCNN, яка представляє собою каскад із трьох згорткових нейронних мереж: Proposal Network (P-Net), Refine Network (R-Net) та Output Network (O-Net). Така каскадна структура дозволяє поступово уточнювати результати детекції, починаючи з грубого пошуку потенційних областей облич і завершуючи точною локалізацією та визначенням ключових точок.

На першому етапі (P-Net) виконується швидкий аналіз зображення з метою виявлення потенційних кандидатів на обличчя. Для цього зображення масштабується до кількох рівнів (image pyramid), що дозволяє знаходити обличчя різного розміру. Результатом роботи P-Net є набір прямокутних областей із відповідними оцінками ймовірності наявності обличчя. На наступному етапі (R-Net) ці області уточнюються: відсіюються помилкові спрацьовування, коригуються координати рамок та підвищується точність локалізації. Завершальний етап (O-Net) забезпечує остаточну перевірку та визначення ключових точок обличчя, таких як положення очей, носа та рота, що є критично важливим для подальшої нормалізації.

Альтернативним підходом є використання бібліотеки Dlib, яка реалізує детекцію облич на основі гістограм орієнтованих градієнтів (HOG) або згорткових нейронних мереж. HOG-підхід є менш обчислювально затратним і може бути ефективним у системах з обмеженими ресурсами, однак поступається нейромережевим методам за точністю в складних умовах. У свою чергу, CNN-моделі Dlib забезпечують вищу точність, але потребують більше обчислювальних ресурсів.

Перед виконанням детекції облич здійснюється попередня обробка зображення, яка включає нормалізацію освітлення, зменшення шуму та масштабування. Це дозволяє підвищити стабільність роботи алгоритму та

зменшити кількість помилкових спрацьовувань. Важливим аспектом є також оптимізація обробки для роботи в режимі реального часу. Зокрема, використовується зменшення роздільної здатності кадру, обробка кожного n-го кадру та апаратне прискорення на графічних процесорах, наприклад, на платформі NVIDIA Jetson Nano.

Результатом роботи алгоритму детекції є координати прямокутної області, що містить обличчя, а також набір ключових точок, які описують його геометрію. Ці дані передаються на наступні етапи конвеєра, зокрема для відстеження обличчя та нормалізації. Важливо, що точність визначення ROI має вирішальне значення для ефективності всієї системи: навіть незначні помилки на цьому етапі можуть призвести до зниження якості ідентифікації. Для підвищення швидкодії використовується масштабування зображення та оптимізація обчислень, що дозволяє досягти продуктивності 15–25 FPS на пристроях типу NVIDIA Jetson Nano.

Таким чином, метод детекції облич у запропонованій системі базується на використанні сучасних нейромережевих підходів, оптимізованих для роботи в реальному часі, і забезпечує надійне та точне виділення обличчя користувача в умовах реального середовища. Це створює основу для подальших етапів біометричної обробки та прийняття рішень у кіберфізичній системі.

У контексті кіберфізичної системи «розумного ліфта» вимоги до детекції облич значно виходять за межі класичних задач комп’ютерного зору, оскільки алгоритм працює не ізольовано, а як частина реального керуючого контуру, де затримки, нестабільність або помилки безпосередньо впливають на фізичну поведінку системи. З такої позиції це означає необхідність одночасного врахування часових, обчислювальних та апаратних обмежень.

Першою критичною вимогою є забезпечення роботи в режимі реального часу. У даній системі це означає, що повний цикл обробки одного кадру (від захоплення до прийняття рішення) повинен укладатися в часовий інтервал, який не перевищує приблизно 40–70 мс, що відповідає частоті 15–25 кадрів на секунду.

З інженерної точки зору це накладає жорсткі обмеження на часову складність алгоритмів.

З точки зору архітектури обчислювальної системи, важливо забезпечити ефективне використання апаратних ресурсів. На платформах типу NVIDIA Jetson Nano використовується гетерогенна обчислювальна модель, яка включає центральний процесор (CPU) та графічний процесор (GPU). CPU доцільно використовувати для керування потоками даних, обробки вводу-виводу та виконання легких операцій, тоді як GPU застосовується для виконання згорткових нейронних мереж, таких як MTCNN. Такий розподіл дозволяє реалізувати паралельну обробку даних і значно скоротити час виконання.

Ще одним важливим аспектом є організація пам’яті та обміну даними. Відеопотік являє собою безперервний потік великих масивів даних, тому ефективна буферизація є критичною. Використовується кільцевий буфер, який дозволяє уникнути втрати кадрів при пікових навантаженнях. Крім того, важливо мінімізувати копіювання даних між CPU та GPU, використовуючи механізми zero-copy або unified memory, що зменшує затримки доступу до пам’яті. Його основна перевага полягає у фіксованому розмірі пам’яті та циклічному перезаписі даних. Це означає, що нові кадри записуються поверх найстаріших, якщо буфер заповнений, що дозволяє уникнути переповнення пам’яті та втрати стабільності системи.

З інженерної точки зору кільцевий буфер вирішує проблему дисбалансу між швидкістю надходження даних із камери та швидкістю їх обробки. У випадку пікових навантажень, коли модулі детекції або ідентифікації тимчасово не встигають обробляти всі кадри, буфер виконує роль «амортизатора», згладжуючи потік даних. Це дозволяє системі зберігати безперервність роботи без критичних втрат інформації, хоча частина старих кадрів може бути замінена новими.

Додатково, у сучасних архітектурах з GPU-обчисленнями, важливим фактором продуктивності є мінімізація копіювання даних між CPU та GPU. У традиційній моделі дані спочатку передаються з пам’яті CPU у відеопам’ять GPU, що створює додаткові затримки через операції копіювання та синхронізації. Для

усунення цього вузького місця використовуються оптимізовані механізми доступу до пам’яті.

Одним із таких підходів є zero-copy memory, який дозволяє GPU напряму звертатися до системної пам’яті CPU без необхідності створення окремих копій даних у відеопам’яті. Це значно зменшує затримки передачі, особливо при роботі з великими потоками відеоданих. Проте цей підхід може мати обмеження по пропускній здатності пам’яті, оскільки CPU та GPU ділять одну і ту ж фізичну пам’ять.

Іншим більш сучасним підходом є використання unified memory, яка забезпечує єдиний адресний простір для CPU та GPU. У такій архітектурі система автоматично керує міграцією даних між різними типами пам’яті, що спрощує програмну реалізацію та підвищує ефективність використання ресурсів. Це особливо важливо для вбудованих платформ, таких як NVIDIA Jetson Nano, де апаратні ресурси є обмеженими, а вимоги до real-time обробки залишаються високими.

У поєднанні кільцевий буфер і механізми оптимізації пам’яті формують ефективну підсистему обробки даних, яка забезпечує стабільну роботу відеоконвеєра навіть при змінному навантаженні. Це дозволяє досягти балансу між швидкодією, надійністю та використанням ресурсів, що є критично важливим для кіберфізичних систем реального часу.

Стійкість до змін освітлення є ще одним ключовим фактором. У реальних умовах експлуатації ліфта освітлення може суттєво змінюватися залежно від часу доби, положення дверей або наявності зовнішнього світла. Для компенсації цих факторів застосовуються алгоритми нормалізації яскравості, такі як гістограмне вирівнювання або адаптивне коригування контрасту. Крім того, використання додаткових каналів даних, зокрема інфрачервоного сигналу від камери Intel RealSense D435, дозволяє підвищити інваріантність системи до умов освітлення, оскільки ІЧ-діапазон менш чутливий до змін видимого світла.

Стійкість до змін ракурсу та часткових перекриттів досягається за рахунок використання багатомасштабних та багатокутових моделей детекції. У випадку

MTCNN це реалізується через побудову піраміди зображень, що дозволяє знаходити обличчя різних розмірів і під різними кутами. Додатково визначення ключових точок дозволяє оцінити орієнтацію обличчя та виконати його геометричну нормалізацію. У випадках часткового перекриття (наприклад, коли користувач носить маску або окуляри) алгоритм повинен залишатися достатньо чутливим до доступних ознак, що досягається завдяки навчанню моделей на різноманітних наборах даних.

З точки зору системного проєктування важливо також враховувати адаптивність алгоритму. У реальних умовах навантаження на систему може змінюватися, наприклад, при появі кількох користувачів одночасно. У таких випадках система може динамічно змінювати параметри обробки, зменшуючи роздільну здатність кадру або частоту виконання детекції, щоб зберегти стабільність роботи.

Не менш важливим є питання енергоспоживання, особливо для вбудованих систем. Інтенсивне використання GPU може призводити до значного споживання енергії, тому необхідно застосовувати енергозберігаючі режими, такі як динамічне масштабування частоти (DVFS) або адаптивне вимкнення модулів, що не використовуються.

Кіберфізична система ідентифікації особи для керування «розумним ліфтом» може бути формалізована як замкнена система автоматичного керування із зворотним зв’язком (рис.3.2), у якій інформаційні та фізичні процеси інтегруються в єдиний керуючий контур. Такий підхід дозволяє застосувати апарат теорії керування для аналізу стійкості, швидкодії та точності системи.

Об’єктом керування в даній системі виступає ліфт як фізична динамічна система, що характеризується інерційністю, обмеженнями по швидкості руху, положенню кабіни та стану дверей. Саме цей об’єкт підлягає регулюванню, а його поведінка повинна відповідати прийнятим рішенням системи ідентифікації та керування.

Вимірювальний пристрій представлений сенсорною підсистемою, яка включає камери (RGB, інфрачервоні та глибинні сенсори), а також додаткові

датчики присутності та руху. Цей блок забезпечує збір інформації про фізичне середовище, зокрема про наявність користувача, його біометричні характеристики та загальний контекст події. Отримані дані формують вхідний інформаційний потік для подальшої цифрової обробки.

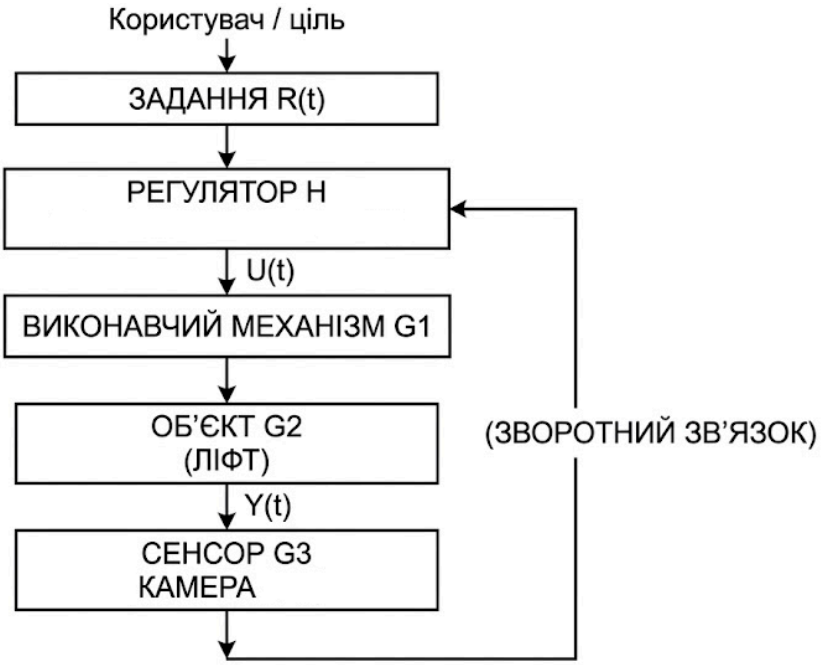


Рисунок 3.2 – Структурна схема системи керування розумним ліфтом із зворотним зв'язком

Регулятором у системі виступає алгоритмічний модуль прийняття рішень, який реалізує логіку ідентифікації користувача та визначення дозволу на доступ. Цей модуль включає методи комп'ютерного зору, перевірку справжності обєкта, зіставлення біометричних ознак та логіку доступу. На основі оброблених даних формується керуюче рішення, яке визначає подальшу поведінку системи, зокрема дозвіл або заборону на виконання дій ліфтом.

Виконавчий механізм реалізує фізичне втілення сформованих рішень у вигляді керуючих сигналів для ліфтового обладнання. Він включає інтерфейси зв'язку, такі як релейні модулі, GPIO або промислові протоколи передачі даних, наприклад RS-485 або Modbus. Саме цей блок забезпечує перетворення цифрових команд у фізичні дії , а саме виклик кабіни, вибір поверху або блокування доступу.

Таким чином, взаємодія між зазначеними блоками формує замкнений контур керування, у якому сенсорна система забезпечує зворотний зв’язок, регулятор приймає рішення на основі оброблених даних, а виконавчий механізм реалізує ці рішення на фізичному рівні. Це дозволяє розглядати систему як класичну кіберфізичну архітектуру з тісною інтеграцією інформаційних та фізичних процесів.

3.3 Метод відстеження обличчя

Відстеження облич є важливим етапом оптимізації конвеєра біометричної обробки, який дозволяє суттєво зменшити обчислювальне навантаження на систему та забезпечити стабільність локалізації користувача у відеопотоці. Основна ідея полягає у тому, що повна процедура детекції обличчя не виконується на кожному кадрі відео. Замість цього система один раз виконує детекцію, а в подальшому використовує алгоритм прогнозування положення об’єкта.

Задача відстеження обличчя розглядається як задача оцінювання стану динамічної системи у часі.

Стан об’єкта (обличчя користувача) описується вектором виду 3.2:

$$x_t = \left(x,\ y,\ w,\ h,\ v_x,\ v_y\right), \tag{3.2}$$

де $x,\ y$ – координати центру обличчя;

$w,\ h$ – розміри bounding box;

$v_x,\ v_y$ – швидкість руху обличчя.

Bounding box (обмежувальна рамка) – це прямокутна область на зображенні або відеокадрі, яка використовується для позначення місця розташування об’єкта, зокрема обличчя, людини або будь-якого іншого елемента, який потрібно виділити для подальшої обробки в системах комп’ютерного зору.

У контексті задачі детекції облич bounding box визначає координати

мінімального прямокутника, який повністю охоплює знайдене обличчя. Зазвичай він задається чотирма параметрами: координатами верхнього лівого кута (x, y), а також шириною та висотою (w, h). У деяких випадках замість цього використовуються дві точки, верхня ліва та нижня права.

Основна функція bounding box полягає у виділенні області інтересу, що дозволяє системі зосередити обчислювальні ресурси лише на релевантній частині зображення. Це суттєво підвищує ефективність подальших етапів обробки, таких як перевірка «живості», нормалізація або вилучення ознак.

З інженерної точки зору bounding box є результатом роботи алгоритмів детекції, наприклад нейронних мереж або класичних методів комп'ютерного зору. Його точність безпосередньо впливає на якість всієї системи, оскільки неточне визначення меж може призвести до втрати частини об'єкта або включення зайвих елементів фону, що знижує ефективність ідентифікації.

У сучасних системах bounding box часто супроводжується додатковим параметром, а саме confidence score, який показує ймовірність того, що виявлений об'єкт дійсно є обличчям. Це дозволяє відфільтровувати помилкові спрацювання та підвищувати надійність системи в умовах реального середовища.

Найчастіше в таких системах використовується фільтр Калмана, який дозволяє оптимально оцінювати стан об'єкта на основі зашумлених вимірювань. Він поєднує прогноз моделі руху та фактичні вимірювання з детектора облич.

Фільтр Калмана є одним із базових математичних інструментів теорії оцінювання стану динамічних систем і широко застосовується в задачах комп'ютерного зору, робототехніки та кіберфізичних систем. У контексті системи «розумного ліфта» він використовується для задачі відстеження обличчя користувача у відеопотоці, що дозволяє зменшити обчислювальне навантаження та підвищити стабільність роботи алгоритму детекції.

З формальної точки зору фільтр Калмана вирішує задачу рекурсивного оцінювання прихованого стану системи на основі зашумлених вимірювань.

Блок-схема алгоритму відстеження обличчя представлена на рисунку 3.3.

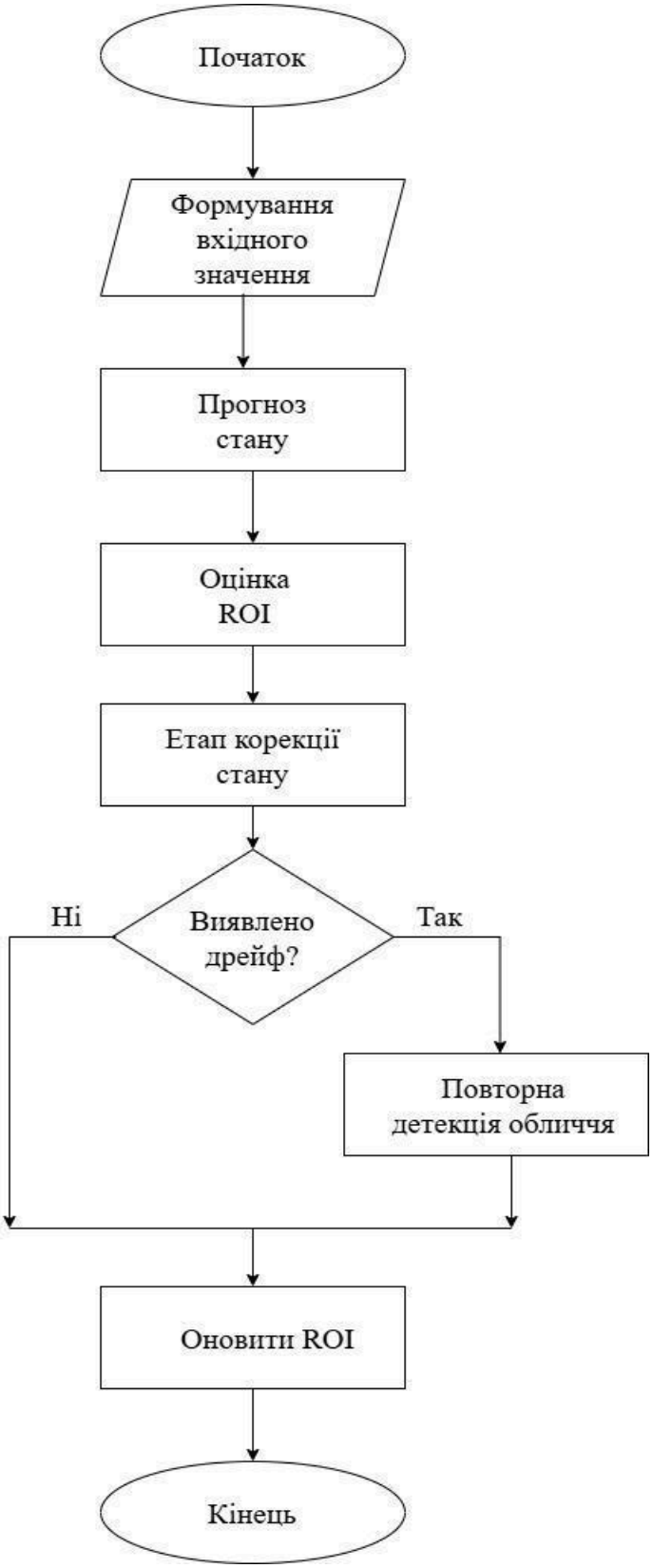


Рисунок 3.3 – Блок-схема алгоритму відстеження обличчя

Алгоритм фільтра Калмана працює у два основні етапи: прогнозування та корекція.

На етапі прогнозування система оцінює новий стан об’єкта на основі попереднього стану та моделі руху.

На етапі корекції отримані вимірювання використовуються для уточнення прогнозу з урахуванням похибки моделі. Таким чином формується оптимальна оцінка стану, яка мінімізує середньоквадратичну похибку.

У задачі відстеження облич у кіберфізичній системі цей підхід дозволяє значно зменшити потребу у повторному виконанні ресурсоємної детекції на кожному кадрі. Замість цього детекція виконується періодично, а між цими моментами положення обличчя прогнозується фільтром Калмана. Це забезпечує стабільність ROI, зменшує кількість обчислень та підвищує загальну продуктивність системи.

Використання фільтра Калмана є прикладом інтеграції методів теорії керування та обробки сигналів у задачі комп’ютерного зору, що дозволяє ефективно реалізувати реальний час роботи системи в умовах шумних та неповних вимірювань.

3.4 Метод адаптивного керування ліфтовим обладнанням на основі ідентифікації особи та контекстних параметрів

У межах розроблюваної кіберфізичної системи процес формування керуючого впливу на ліфтове обладнання реалізується не як статична реакція на подію, а як адаптивний метод, що враховує ідентифікатор особи, апаратний стан системи та динамічний контекст середовища.

Суть методу полягає у переході від традиційного реактивного керування (натискання кнопки) до проактивної генерації команд на основі прогнозування намірів користувача.

Математично метод описується функцією G, яка описана формулою 3.3, що трансформує результати біометричної обробки та контекстні дані у керуючий сигнал U:

$$U = G(I, Q, C), \tag{3.3}$$

де I – ідентифікатор особи;

Q – рівень достовірності розпізнавання;

C – вектор контексту.

На відміну від існуючих підходів, вектор контексту C у даному методі розширено апаратними показниками такими як поточний апаратний стан ліфта (положення кабіни, стан дверей) та рівень завантаженості обладнання.

Розглянемо відмінності від існуючих методів.

1. Врахування апаратного фідбеку. Метод аналізує стан (наприклад, ліфт вже рухається у потрібному напрямку з іншим пасажиром), що дозволяє оптимізувати енергоспоживання та уникати зайвих циклів пуску/зупинки двигуна.

2. Динамічне обмеження прав. На відміну від жорстких біометричних замків, цей метод змінює множину дозволених дій залежно від часу t (наприклад, автоматичне обмеження доступу до офісних поверхів у нічний час для певних категорій персоналу).

3. Мінімізація затримок обробки. Завдяки використанню рівня достовірності, система може ініціювати виклик кабіни ще на етапі трекінгу (до завершення повної ідентифікації), якщо впевненість системи перевищує заданий поріг.

Реалізація методу в межах КФС передбачає виконання п'яти послідовних кроків.

1. Оцінка достовірності та ідентифікація. Система отримує вектор ознак із AI-конвеєра, проводить зіставлення з еталонами та визначає ідентифікатор особи та показник впевненості Q.

2. Перевірка прав доступу. На основі ідентифікатора здійснюється звернення до бази прав доступу для формування первинної множини дозволених поверхів.

3. Аналіз контекстного вектора. Система зчитує поточний час t, стан ліфта s та історію h. Якщо користувач регулярно о 9:00 переміщується на 12-й

поверх, цей поверх отримує найвищий пріоритет.

4. Селекція оптимальної дії. Відбувається остаточний вибір цільового поверху на основі перетину прав доступу та прогнозної моделі поведінки.

5. Генерація керуючого сигналу. Рішення транслюється у фізичну дію через інтерфейси GPIO або промислові протоколи (Modbus/RS-485), що замикає контур керування обчислювач – виконавчий механізм.

3.5 Прийняття рішень в кіберфізичній системі ідентифікації особи для автоматизації роботи «розумного ліфта»

Рівень прийняття рішень є ключовим елементом кіберфізичної системи «розумного ліфта», оскільки саме тут відбувається перетворення результатів обробки біометричних даних у конкретні керуючі дії.

Цей рівень виконує функцію програмного регулятора, який працює в замкненому контурі керування та забезпечує узгодження між інформаційною та фізичною (ліфт) частинами системи.

На вхід цього модуля надходить структурована інформація від AI-конвеєра, яка зазвичай включає:

- ідентифікатор користувача;
- ймовірність або впевненість ідентифікації;
- результат перевірки справжності об’єкта;
- координати користувача;
- поточний стан системи.

Схема, зображена на рисунку 3.4 відображає послідовність етапів та логіку перемикання станів кіберфізичної системи в процесі автоматизації роботи розумного ліфта на основі біометричної ідентифікації.

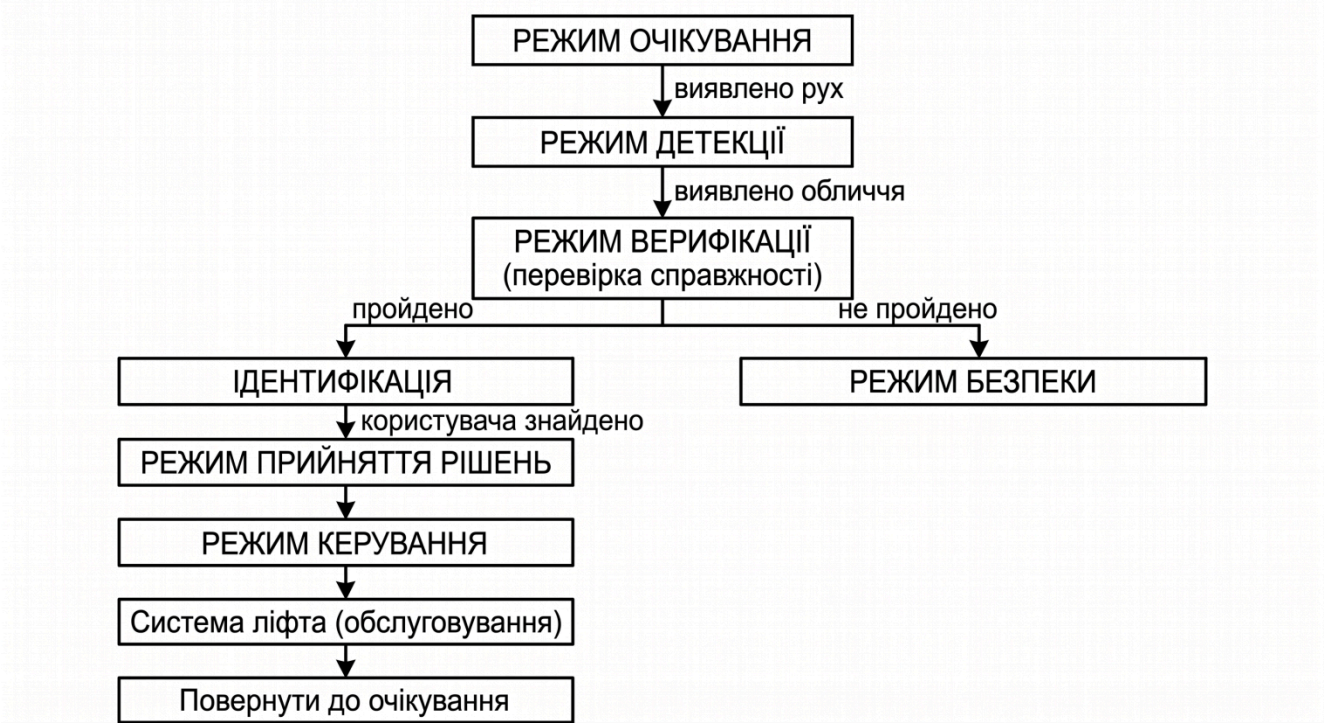


Рисунок 3.4 – Схема перемикання станів кіберфізичної системи в процесі автоматизації роботи розумного ліфта на основі біометричної ідентифікації

У початковому стані система перебуває в режимі очікування, що характеризується низьким споживанням енергії. Цей стан зберігається до моменту, поки програмний модуль, підключений до датчиків (наприклад, камери Intel RealSense), не зафіксує виявлено рух у зоні спостереження.

Після спрацювання тригера руху система переходить у режим детекції. На цьому етапі AI Core активує алгоритми комп'ютерного зору (наприклад, MTCNN або dlib) для аналізу відеопотоку та визначення, чи виявлено обличчя людини. Якщо обличчя успішно локалізоване, розпочинається режим верифікації, який є критично важливим для безпеки КФС. Він передбачає перевірку справжності біометричного об’єкта, використовуючи дані карти глибини та ІЧ-сенсора для відсікання атак підміни (спуфінгу).

Логіка подальшої роботи системи розгалужується залежно від результату перевірки справжності:

− якщо перевірку не пройдено, система класифікує це як потенційну атаку та переходить у режим безпеки для протоколювання події або інформування

служби безпеки, після чого виконується повернути до очікування;

− у випадку, якщо перевірку пройдено, активується етап ідентифікація. AI Core формує вектор біометричних характеристик і співставляє його з базою даних для встановлення особи. Якщо користувача знайдено, система переходить до режиму прийняття рішень. На цьому етапі, використовуючи контекстний вектор та історію переміщень, автоматично визначається цільовий поверх.

Ухвалене рішення передається виконавчим механізмам у режимі керування. Після цього безпосередньо задіюється система ліфта (обслуговування), яка виконує фізичний виклик кабіни та вибір поверху. По завершенні виконання команди система повертається у початковий стан режиму очікування, замикаючи повний цикл функціонування КФС.

Режим очікування є базовим станом роботи кіберфізичної системи «розумного ліфта», у якому система перебуває у пасивному стані до появи зовнішніх подій. У цьому режимі не виконується повний цикл біометричної обробки, а лише здійснюється мінімальний моніторинг середовища для виявлення потенційної активності в зоні контролю.

З інженерної точки зору цей режим є важливим для оптимізації енергоспоживання та обчислювальних ресурсів. Система працює у режимі зниженої частоти обробки кадрів, наприклад 5–10 FPS, що дозволяє зменшити навантаження на CPU та GPU. Активуються лише легкі алгоритми детекції руху або зміни сцени.

Основною задачею Idle Mode є виявлення тригера для переходу у наступний режим. Таким тригером може бути рух у полі зору камери, зміна освітлення або спрацювання сенсора присутності. Після фіксації такої події система переходить у режим детекції.

Таким чином, Idle Mode виконує функцію енергозберігаючого фону та початкового фільтра подій, які потенційно потребують подальшої обробки.

Режим детекції активується у момент виявлення потенційного об’єкта у зоні спостереження. У цьому режимі система переходить до повноцінної обробки відеопотоку з метою локалізації обличчя користувача.

Основним завданням є визначення області інтересу, яка містить обличчя, за допомогою алгоритмів комп’ютерного зору. На цьому етапі застосовуються моделі глибокого навчання або класичні каскадні класифікатори, які дозволяють швидко виявити обличчя навіть у складних умовах освітлення.

Detection Mode є ресурсомістким, оскільки передбачає обробку кожного кадру або кожного N-го кадру з високою точністю. Після успішного виявлення обличчя система ініціює створення bounding box та передає дані до модуля tracking.

Якщо обличчя не виявлено протягом певного часу, система повертається у режим очікування. Таким чином, цей режим виконує роль «фільтра реальних користувачів» серед випадкових змін у сцені.

Цей режим є критичним з точки зору безпеки системи, оскільки саме тут відбувається перевірка того, чи є об’єкт у кадрі реальною живою людиною, а не спробою підміни (фото, відео, маска).

У цьому режимі використовується багатоканальний аналіз даних:

- аналіз глибини сцени;
- інфрачервоний відгук;
- аналіз мікрорухів обличчя;
- перевірка стабільності геометрії обличчя.

Особливістю цього режиму є те, що система працює з кількома потоками даних одночасно, що підвищує обчислювальну складність, але значно збільшує надійність.

Якщо система фіксує ознаки спуфінгу (наприклад, відсутність глибинної структури або аномальну поведінку IR-сигналу), вона негайно блокує подальшу обробку та переходить у режим безпеки.

Успішне проходження цього етапу означає, що користувач є «живим» та може бути переданий на наступний рівень ідентифікації.

Режим ідентифікації відповідає за встановлення особи користувача на основі його біометричних характеристик. На цьому етапі відбувається порівняння ознак обличчя, отриманих з відеопотоку, з базою даних зареєстрованих

користувачів.

Система формує цифровий дескриптор обличчя, який використовується для пошуку найближчого збігу у базі даних. Результатом роботи цього режиму є:

- ідентифікація користувача або його відсутність у базі;
- визначення рівня доступу (роль);
- оцінка впевненості збігу.

У випадку успішної ідентифікації система переходить до логічного модуля прийняття рішень. Якщо користувач не розпізнаний, може бути ініційовано обмежений доступ або блокування.

Цей режим є одним із найважливіших з точки зору точності системи, оскільки помилки на цьому етапі можуть призвести до неправильного керування ліфтом.

У цьому режимі відбувається інтерпретація результатів усіх попередніх етапів у вигляді конкретних керуючих дій. Система аналізує:

- факт ідентифікації користувача;
- результат перевірки справжності об’єкта;
- контекст середовища (стан ліфта, завантаження);
- політику доступу.

На основі цих даних формується рішення:

- дозволити доступ;
- відмовити у доступі;
- викликати ліфт;
- визначити напрям руху;
- або активувати режим безпеки.

Особливістю цього режиму є його логічний характер, він не виконує обробку зображень, а працює з уже сформованими ознаками та правилами.

У цьому режимі прийняті рішення перетворюються у фізичні керуючі сигнали, які передаються до виконавчого рівня системи. Це може бути:

- виклик кабіни ліфта;
- вибір поверху;

- зупинка або зміна напрямку руху;
- блокування доступу.

Передача команд здійснюється через апаратні інтерфейси, такі як GPIO, релейні модулі або промислові протоколи зв’язку. Це програмно керовані цифрові виводи мікрокомп’ютера або мікроконтролера, які можуть встановлювати логічний рівень «0» або «1». У контексті ліфтової системи GPIO використовується для формування простих керуючих сигналів, наприклад активації реле, які, у свою чергу, перемикають силові ланцюги. Перевагою GPIO є мінімальна затримка та простота реалізації, однак він не підходить для складних системного рівня обміну даними.

Наступним рівнем є релейні модулі, які виконують функцію фізичного перемикання електричних кіл. Реле дозволяє ізолювати низьковольтну логіку керуючої системи від високовольтної частини ліфтового обладнання. Це особливо важливо з точки зору електробезпеки та відповідності промисловим стандартам. У системі «розумного ліфта» релейні модулі використовуються для імітації натискання кнопок виклику поверху або керування контактами існуючої ліфтової панелі. Таким чином, програмна система фактично «інтегрується» у вже існуючу інфраструктуру без її повної заміни.

Більш складним рівнем взаємодії є промислові протоколи зв’язку, такі як RS-485 або Modbus. Вони забезпечують цифровий обмін даними між контролером кіберфізичної системи та ліфтовим контролером. На відміну від простих GPIO-сигналів, ці протоколи дозволяють передавати структуровані команди та отримувати зворотну інформацію про стан системи: поточний поверх, швидкість руху, стан дверей, помилки або аварійні події. Це робить систему не лише виконавчим механізмом, а й частково інтегрованою частиною загальної системи керування будівлею.

З точки зору архітектури, ці інтерфейси формують фізичний шар виконавчої підсистеми, який працює під управлінням decision layer. У цьому режимі система повністю припиняє обробку відео- та біометричних даних і переходить у фазу виконання команд. Тобто вся попередня AI-обробка завершується, а результат у

вигляді дискретного керуючого сигналу передається на рівень апаратного виконання.

Таким чином, апаратні інтерфейси забезпечують критично важливий перехід між цифровою логікою та фізичним світом. Вони гарантують, що рішення, прийняті інтелектуальним модулем системи, будуть коректно, швидко та безпечно реалізовані у реальному ліфтовому обладнанні, що є ключовою вимогою для кіберфізичних систем реального часу.

Після завершення виконання команди система повертається у режим очікування.

Режим безпеки є аварійним станом системи, який активується у випадках виявлення загроз або аномальної поведінки. До таких ситуацій належать:

- виявлення spoofing-атаки;
- невідома особа без доступу;
- некоректна робота сенсорів;
- конфлікт даних між модулями системи.

У цьому режимі всі керуючі команди блокуються, а система переходить у захищений стан. Додатково можуть виконуватися такі дії:

- запис інциденту в журнал подій;
- надсилання сигналу до системи безпеки;
- блокування взаємодії з ліфтом.

Security Mode має найвищий пріоритет у системі та може перервати будь-який інший режим роботи.

3.6 Висновки

У третьому розділі розроблено та обґрунтовано методи і алгоритми ідентифікації особи, а також підходи до адаптивного керування ліфтовою системою.

Проведений аналіз існуючих підходів показав, що класичні статистичні методи поступаються сучасним нейромережевим архітектурам за точністю та

стійкістю до шумів.

Розроблений конвеєр обробки біометричних даних включає етапи детекції, відстеження, нормалізації та класифікації, що забезпечує комплексний підхід до ідентифікації. Особливістю запропонованих рішень є їх орієнтація на роботу в реальному часі з урахуванням обмежених ресурсів edge-пристроїв.

Значним результатом є розробка методу адаптивного керування ліфтом, який враховує не лише факт ідентифікації користувача, але й контекстні параметри (стан системи, пріоритети, середовище). Це дозволяє перейти від статичних алгоритмів до інтелектуального керування, що підвищує ефективність роботи ліфтової системи.

Також у розділі реалізовано механізм прийняття рішень, який інтегрує результати біометричного аналізу з керуючими алгоритмами. Це забезпечує автоматизацію процесу вибору поверху, оптимізацію маршрутів і підвищення рівня персоналізації.

4 ПРОЕКТУВАННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ОСОБИ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИ «РОЗУМНОГО ЛІФТА»

4.1 Архітектура кіберфізичної системи

Реалізація кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» базується на принципах інтеграції фізичних процесів, обчислювальних модулів та систем керування в єдиному інформаційно-керуючому середовищі.

Основною особливістю запропонованої архітектури є наявність замкненого контуру, в якому результати обробки даних безпосередньо впливають на фізичний стан об’єкта керування ліфта.

Архітектура кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» представлена на рисунку 4.1.

Сенсорний рівень кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» є базовим рівнем, який забезпечує безпосередню взаємодію із зовнішнім середовищем. Його основна функція полягає у зборі первинних даних про користувача, їх первинній обробці, передачі в обчислювальний модуль та реалізації керуючих впливів на виконавчі механізми ліфта.

Особливістю кіберфізичних систем є тісна інтеграція фізичних процесів (рух людини, виклик ліфта, переміщення кабіни) з цифровими алгоритмами обробки інформації. У даному випадку фізичний рівень виступає джерелом даних для алгоритмів комп’ютерного зору та одночасно виконавчим елементом, що реалізує рішення системи.

До складу сенсорного рівня входять:

- підсистема візуального спостереження (камери);
- обчислювальний модуль;
- сенсорна підсистема;
- інтерфейс взаємодії з ліфтовим обладнанням;
- система електроживлення.

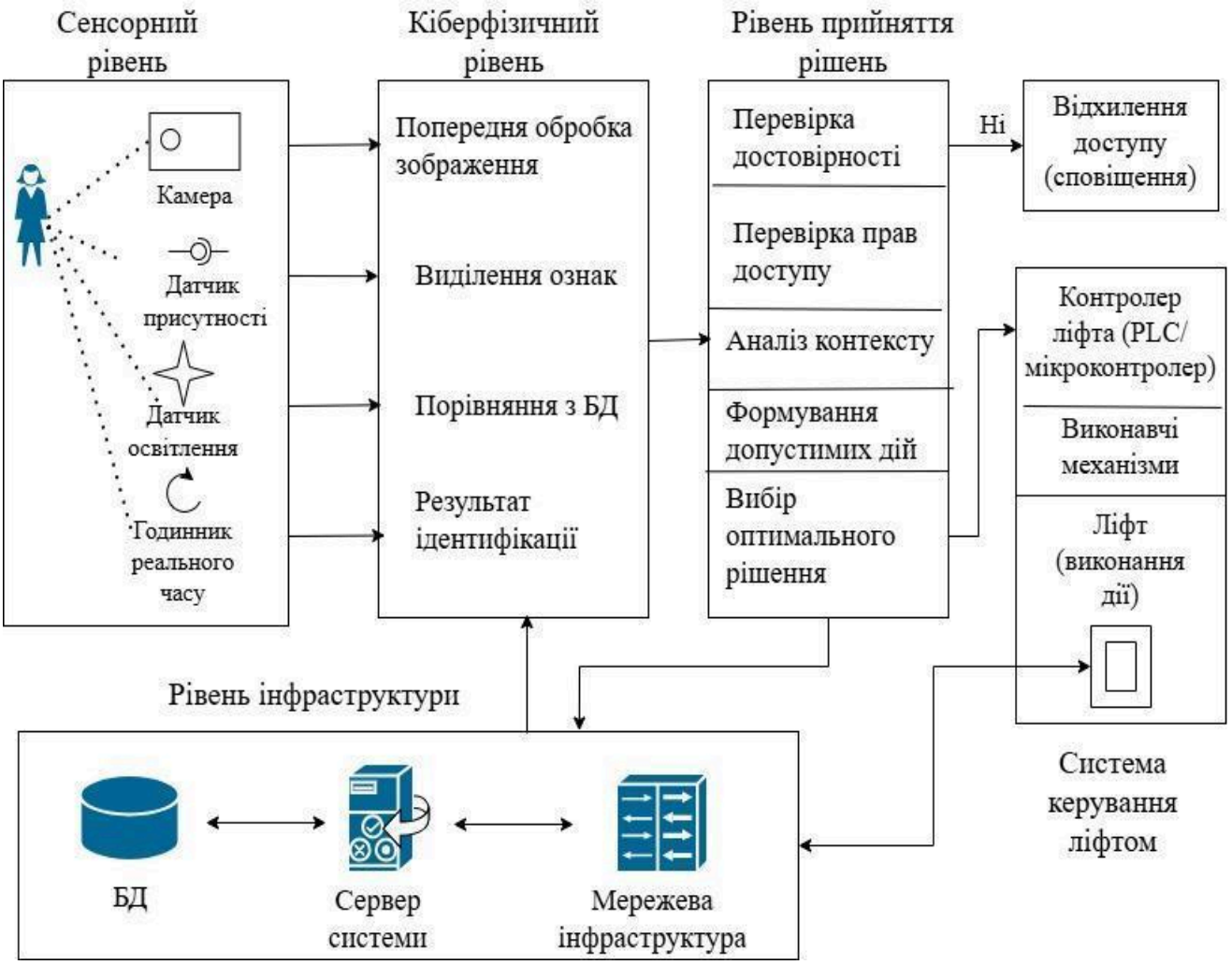


Рисунок 4.1 – Архітектура кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта»

Камера є ключовим елементом системи, оскільки саме вона формує вхідні дані для алгоритмів ідентифікації. Від її характеристик залежить точність, швидкість та надійність роботи всієї системи.

Основні технічні вимоги до камери:

- достатня роздільна здатність (не менше 720p);
- стабільна робота при різному освітленні;
- низька затримка передачі відео;
- можливість інтеграції з обчислювальним модулем;
- підтримка потокового відео в реальному часі.

Як базове рішення розглядається Raspberry Pi Camera Module v2, яка

використовує стандартний CMOS-сенсор та працює у видимому спектрі.

Принцип роботи RGB-камери полягає у перетворенні світлового потоку в електричний сигнал за допомогою фоточутливих елементів. Зображення формується у трьох кольорових каналах (червоний, зелений, синій), що дозволяє отримати повнокольорову картину сцени.

Перевагами такого рішення є низька вартість та доступність, простота інтеграції з одноплатними комп'ютерами, достатня якість зображення для базових алгоритмів розпізнавання.

Однак існують суттєві обмеження такі як значна залежність від освітлення (погіршення якості при слабкому світлі), відсутність інформації про глибину приміщення, вразливість до атак підміни (наприклад, використання фотографій).

Таким чином, RGB-камера може використовуватись у прототипах або бюджетних рішеннях, але не забезпечує високого рівня безпеки.

Інфрачервоні камери, зокрема NoIR Camera Module v2, не мають ІЧ-фільтра та здатні працювати в умовах низького освітлення.

Принцип роботи базується на реєстрації інфрачервоного випромінювання, яке відбивається від об'єктів. При використанні ІЧ-підсвітки камера може формувати зображення навіть у повній темряві.

До переваг можна віднести стабільність роботи незалежно від освітлення, можливість цілодобового використання, краща контрастність облич у темряві.

До недоліків відносяться нижча деталізація текстур, складність кольорового аналізу, обмеженість застосування для складних моделей розпізнавання.

Інфрачервоні камери доцільно використовувати як допоміжні.

Найбільш ефективним рішенням є використання Intel RealSense D435.

Ця камера використовує технологію стереозору або структурованого світла для побудови карти глибини. Вона формує тривимірне представлення сцени, що дозволяє точно визначати форму обличчя.

До переваг відносяться можливість отримання 3D-даних, можливість реалізації алгоритмів перевірки «живості», значне підвищення точності ідентифікації, стійкість до атак підміни.

До недоліків належать вища вартість, складність інтеграції, підвищене енергоспоживання.

Обчислювальний модуль є центральним елементом фізичного рівня кіберфізичної системи, оскільки саме він забезпечує виконання всіх алгоритмів обробки даних, отриманих від сенсорів, та прийняття рішень у реальному часі. У контексті системи ідентифікації особи для «розумного ліфта» на обчислювальний модуль покладаються такі функції: обробка відеопотоку з камери, виконання алгоритмів детекції та розпізнавання облич, аналіз результатів ідентифікації, взаємодія з базою даних користувачів, а також формування керуючих сигналів для виконавчих пристроїв (інтерфейсу ліфта).

Основною вимогою до обчислювального модуля є забезпечення обробки даних у режимі реального часу. Це означає, що затримка між моментом появи користувача в полі зору камери та реакцією системи (наприклад, викликом ліфта) повинна бути мінімальною, зазвичай не перевищувати 1–2 секунд. Для досягнення цього необхідна достатня обчислювальна потужність, особливо з урахуванням використання сучасних алгоритмів глибокого навчання для розпізнавання облич.

Як базове рішення може використовуватись одноплатний комп’ютер Raspberry Pi 4, який характеризується низькою вартістю, компактними розмірами та широкими можливостями підключення периферійних пристроїв. Він оснащений багатоядерним ARM-процесором та достатнім обсягом оперативної пам’яті (до 8 ГБ), що дозволяє виконувати базові алгоритми комп’ютерного зору з використанням бібліотек, таких як OpenCV. Однак через відсутність спеціалізованих апаратних засобів прискорення обчислень, таких як графічний процесор для обробки нейронних мереж, його можливості є обмеженими при реалізації складних моделей глибокого навчання. Це може призводити до зниження швидкодії та точності системи, особливо при роботі з високою роздільною здатністю відео або при необхідності обробки кількох потоків одночасно.

Більш ефективним рішенням є використання спеціалізованих платформ для

задач штучного інтелекту, таких як NVIDIA Jetson Nano. Дана платформа оснащена вбудованим графічним процесором (GPU), який підтримує технологію CUDA та оптимізований для виконання операцій над матрицями, що є основою роботи нейронних мереж. Це дозволяє значно прискорити виконання алгоритмів розпізнавання облич і забезпечити обробку відеопотоку в режимі реального часу без суттєвих затримок. Крім того, Jetson Nano підтримує спеціалізовані бібліотеки для глибинного навчання, що спрощує розробку та інтеграцію системи.

Для систем з підвищеними вимогами до продуктивності, наприклад у великих бізнес-центрах або об’єктах із високим потоком людей, доцільно використовувати більш потужні рішення, такі як NVIDIA Jetson Xavier NX. Ця платформа забезпечує значно більшу обчислювальну потужність, що дозволяє одночасно обробляти декілька відеопотоків, використовувати складніші моделі нейронних мереж і реалізовувати додаткові функції, такі як аналіз поведінки користувачів або інтеграція з іншими системами безпеки.

Важливим аспектом вибору обчислювального модуля є також енергоспоживання та тепловиділення. Оскільки система встановлюється у замкненому просторі (наприклад, у ліфтовому холі або технічній шафі), необхідно забезпечити ефективне відведення тепла та стабільне живлення. У цьому контексті одноплатні комп’ютери мають перевагу завдяки низькому енергоспоживанню, однак при використанні більш продуктивних платформ може знадобитися додаткове охолодження.

Отже, вибір обчислювального модуля є компромісом між вартістю, продуктивністю та енергоефективністю. Для навчальних або прототипних систем достатньо використання Raspberry Pi 4, тоді як для практичної реалізації доцільно застосовувати платформи сімейства NVIDIA Jetson, які забезпечують необхідний рівень продуктивності для роботи системи в реальному часі.

Сенсорна підсистема кіберфізичної системи ідентифікації особи для «розумного ліфта» виконує критично важливу функцію виявлення присутності користувача та ініціації роботи всієї системи. Її основне призначення полягає в тому, щоб забезпечити активацію обчислювальних процесів лише у момент появи

людини в зоні обслуговування, що дозволяє значно знизити енергоспоживання, зменшити навантаження на обчислювальний модуль та підвищити загальну ефективність функціонування системи. У разі відсутності сенсорної підсистеми обробка відеопотоку здійснювалася б безперервно, що призвело б до перевитрати ресурсів і зниження надійності роботи.

Найбільш доцільним базовим рішенням є використання пасивного інфрачервоного сенсора, зокрема HC-SR501 PIR Motion Sensor, принцип роботи якого ґрунтується на реєстрації змін інфрачервоного випромінювання в зоні контролю. Людське тіло постійно випромінює тепло, і при переміщенні людини відбувається зміна теплового поля, яку фіксує піроелектричний елемент сенсора. Завдяки використанню лінзи Френеля зона огляду розбивається на окремі сегменти, що дозволяє підвищити чутливість до руху. PIR-сенсор характеризується низьким енергоспоживанням, широким кутом огляду (до 120°) та достатньою дальністю виявлення (до 5–7 метрів), що робить його оптимальним для первинної активації системи. Разом із тим, він не здатний визначати кількість людей, точну відстань або статичну присутність, а також може реагувати на сторонні теплові впливи, що є його основними обмеженнями.

Для розширення функціональних можливостей системи можуть використовуватись ультразвукові сенсори, такі як HC-SR04 Ultrasonic Sensor, які працюють за принципом випромінювання ультразвукових хвиль та вимірювання часу їх повернення після відбиття від об’єкта. Це дозволяє визначати відстань до користувача з точністю до кількох міліметрів у межах діапазону до 4 метрів. Проте в умовах реального середовища, зокрема у ліфтових холах з великою кількістю людей та відбивних поверхонь, такі сенсори можуть працювати нестабільно через шум, перешкоди та складність інтерпретації сигналів. Крім того, вони мають обмежений кут огляду і залежать від властивостей поверхонь, від яких відбивається сигнал.

Більш сучасним і технологічно досконалим рішенням є використання сенсорів типу Time-of-Flight, наприклад VL53L0X ToF Sensor. Принцип їх роботи полягає у випромінюванні лазерного імпульсу та вимірюванні часу його

повернення після відбиття від об’єкта. На відміну від ультразвукових сенсорів, ToF використовує світло, що забезпечує значно вищу точність, швидкість та стабільність вимірювань. Такі сенсори дозволяють точно визначати відстань до користувача в межах до 2 метрів, що є достатнім для задач позиціонування перед камерою. Вони мають компактні розміри, низьке енергоспоживання та високу стійкість до зовнішніх впливів, однак їх використання обмежується меншою дальністю дії та вищою вартістю.

Найбільш ефективним підходом до побудови сенсорної підсистеми є комбіноване використання різних типів сенсорів. У такій конфігурації PIR-сенсор виконує функцію первинного детектора руху, активуючи систему лише при появі користувача. Після цього камера переходить у активний режим роботи, а додатковий ToF-сенсор може використовуватись для уточнення відстані до об’єкта та забезпечення оптимальних умов для розпізнавання облич. Така багаторівнева схема дозволяє мінімізувати кількість хибних спрацювань, знизити навантаження на обчислювальний модуль і підвищити точність роботи системи в цілому.

Важливим аспектом є також правильне розміщення сенсорів у просторі. PIR-сенсор доцільно встановлювати над дверима ліфта або на стелі таким чином, щоб він охоплював зону підходу користувача на відстані 3–5 метрів. Це дозволяє завчасно активувати систему до моменту, коли людина стане перед камерою. ToF-сенсор, у свою чергу, доцільно розміщувати ближче до рівня тіла користувача (приблизно 1–1,2 м), що забезпечує точніше вимірювання дистанції. При встановленні необхідно уникати зон із сильними тепловими потоками (наприклад, кондиціонери або опалювальні прилади), які можуть впливати на роботу PIR-сенсора, а також забезпечити відсутність фізичних перешкод у зоні дії сенсорів.

Таким чином, сенсорна підсистема є важливим елементом кіберфізичної системи, який забезпечує ефективну взаємодію з користувачем, оптимізує використання ресурсів та підвищує надійність функціонування всієї системи. Використання комбінованого підходу до вибору сенсорів дозволяє досягти оптимального балансу між точністю, енергоефективністю та вартістю реалізації.

Інтерфейс взаємодії з ліфтовою системою є ключовим компонентом фізичного рівня, оскільки саме він забезпечує передачу керуючих сигналів від кібернетичної частини системи до виконавчих механізмів ліфта. Основною функцією даного інтерфейсу є реалізація автоматичного виклику ліфта та вибору поверху на основі результатів ідентифікації користувача.

Особливістю даного етапу проєктування є необхідність інтеграції з уже існуючою ліфтовою інфраструктурою, яка, як правило, не передбачає відкритих цифрових інтерфейсів для зовнішніх систем. У зв’язку з цим вибір способу взаємодії визначається типом ліфтового обладнання, рівнем доступу до його систем керування та вимогами до безпеки.

Найпростішим і універсальним рішенням є використання релейного інтерфейсу, наприклад 5V Relay Module. Принцип його роботи полягає в електромеханічному замиканні контактів, що імітує натискання фізичних кнопок виклику або вибору поверху. Такий підхід дозволяє інтегрувати систему без внесення змін у штатну електроніку ліфта. Обчислювальний модуль подає сигнал на реле через GPIO-інтерфейс, у результаті чого відбувається короткочасне замикання відповідного ланцюга.

Перевагами релейного підходу є його універсальність, простота реалізації та висока сумісність із різними типами ліфтів. Він не потребує складного налаштування та може бути реалізований навіть у межах навчального проєкту. Однак недоліками є обмежена функціональність, відсутність зворотного зв’язку від ліфта (наприклад, інформації про поточний поверх або стан дверей), а також потенційні проблеми з надійністю при тривалій експлуатації.

Більш досконалим рішенням є використання промислових протоколів зв’язку, таких як Modbus, CAN або RS-485. У цьому випадку система інтегрується безпосередньо в цифрову шину керування ліфтом, що дозволяє не тільки передавати команди, але й отримувати інформацію про його стан. Такий підхід забезпечує більш гнучке керування, можливість реалізації складних алгоритмів оптимізації руху та підвищений рівень безпеки. Однак його застосування потребує доступу до технічної документації ліфта та відповідних дозволів.

У сучасних ліфтових системах деякі виробники, зокрема Otis Elevator Company, надають програмні інтерфейси (API) для інтеграції з зовнішніми системами. Це дозволяє реалізувати повноцінну цифрову взаємодію без фізичного втручання в електричні схеми. Такий підхід є найбільш перспективним, однак доступний лише для сучасного обладнання.

Таким чином, вибір інтерфейсу взаємодії визначається умовами експлуатації: для прототипів і навчальних систем доцільно використовувати релейне керування, тоді як для промислових рішень — цифрові протоколи або API.

Правильне розміщення компонентів фізичного рівня є критично важливим для забезпечення ефективності, точності та надійності роботи всієї системи. Просторове розташування елементів визначає якість збору даних, швидкість реакції системи та зручність взаємодії користувача з ліфтом.

Основним принципом розміщення є орієнтація на природну поведінку користувача. Камера повинна бути встановлена таким чином, щоб забезпечити максимальну ймовірність захоплення обличчя без необхідності спеціальних дій з боку людини. Оптимальною є висота встановлення в межах 1,5–1,7 метра, що відповідає середньому рівню обличчя дорослої людини. Камера орієнтується під невеликим кутом донизу (15–25°), що дозволяє уникнути засвітлення та забезпечити стабільний кут огляду.

Сенсори присутності розміщуються таким чином, щоб забезпечити раннє виявлення користувача. PIR-сенсор доцільно встановлювати над дверима ліфта або на стелі, де він має максимальну зону покриття (до 120°). Це дозволяє активувати систему ще до того, як користувач підійде до камери. Додаткові сенсори, такі як ToF, розміщуються ближче до рівня тіла людини для точного вимірювання відстані.

Обчислювальний модуль встановлюється в захищеному технічному корпусі, зазвичай поблизу ліфтового контролера. Це дозволяє мінімізувати довжину з’єднувальних кабелів, зменшити втрати сигналу та підвищити надійність системи. Корпус повинен забезпечувати захист від пилу, вологи та

несанкціонованого доступу.

Інтерфейс взаємодії з ліфтом розміщується в електрощитовій або іншому технічному приміщенні з обмеженим доступом. Це є важливим з точки зору безпеки, оскільки втручання в роботу ліфта повинно бути строго контрольованим.

При проєктуванні також необхідно враховувати:

- освітлення приміщення;
- можливі перешкоди (стіни, колони);
- потоки людей;
- вимоги до естетики (особливо в сучасних будівлях).

Таким чином, схема розміщення обладнання повинна забезпечувати оптимальні умови для роботи всіх компонентів і водночас не порушувати ергономіку простору.

Система живлення є важливим елементом фізичного рівня, оскільки вона забезпечує стабільну та безперебійну роботу всіх компонентів кіберфізичної системи. Надійність живлення безпосередньо впливає на працездатність системи ідентифікації та її здатність функціонувати в режимі реального часу.

Основним джерелом живлення є електрична мережа змінного струму напругою 220 В. Оскільки більшість компонентів системи працюють на низькій напрузі (5 В або 12 В), необхідно використовувати імпульсні блоки живлення для перетворення напруги. Такі блоки забезпечують високу ефективність, компактність і стабільність вихідних параметрів.

Особливу увагу слід приділити стабілізації напруги, оскільки коливання в мережі можуть негативно впливати на роботу електронних компонентів, особливо обчислювального модуля. Для цього використовуються стабілізатори напруги або джерела живлення з вбудованим захистом.

Для забезпечення безперервності роботи системи доцільно використовувати джерело безперебійного живлення (UPS). Це дозволяє підтримувати роботу системи у випадку короткочасних відключень електроенергії та забезпечує коректне завершення роботи обчислювального модуля. Особливо важливим це є для систем, що працюють у середовищах з підвищеними вимогами до безпеки.

Крім того, система живлення повинна включати засоби захисту від:

- перенапруги;
- короткого замикання;
- перевантаження;
- електромагнітних перешкод.

Не менш важливим є питання розподілу живлення між компонентами. Камера, сенсори та обчислювальний модуль можуть мати різні вимоги до напруги та струму, тому необхідно передбачити окремі лінії живлення або стабілізатори для кожного типу пристроїв.

Також слід враховувати тепловий режим роботи системи. Блоки живлення та обчислювальні модулі можуть виділяти значну кількість тепла, тому необхідно забезпечити належну вентиляцію або використання систем охолодження.

Таким чином, система живлення повинна бути спроєктована з урахуванням вимог до надійності, безпеки та енергоефективності. Її правильна реалізація є запорукою стабільної роботи всієї кіберфізичної системи.

4.2 Проектування інтерфейсу взаємодії з розумним ліфтом

Програмна реалізація кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» базується на багаторівневій архітектурі, яка включає фронтенд-рівень, бекенд-рівень та ядро ідентифікації. Такий підхід дозволяє забезпечити модульність системи, її масштабованість, а також ефективну обробку даних у реальному часі.

Інтерфейс користувача виступає не лише засобом відображення інформації, але й важливим компонентом взаємодії між людиною та кіберфізичною системою, забезпечуючи наочність, контроль та моніторинг процесів.

Фронтенд-рівень реалізується у вигляді веб-інтерфейсу, який відображає результати роботи системи ідентифікації та стан ліфтового обладнання. Для його реалізації використовуються сучасні веб-технології, зокрема HTML5 та CSS3, що забезпечують структуровану розмітку та адаптивний дизайн інтерфейсу. Для

пришвидшення розробки та забезпечення уніфікованого вигляду компонентів можуть застосовуватись CSS-фреймворки, такі як Tailwind або Bootstrap. Динамічна логіка реалізується за допомогою JavaScript із використанням сучасних бібліотек або фреймворків, таких як React або Vue.js, які дозволяють створювати реактивні компоненти та ефективно керувати станом інтерфейсу.

Рис.4.2 – Інтерфейс користувача

Інтерфейс користувача складається з кількох функціональних блоків. Блок «Останній ідентифікований користувач» відображає інформацію про останню успішно розпізнану особу, включаючи ім’я, роль, дозволений поверх та фотографію. Дані для цього блоку надходять із бекенду через API-запити, а зображення може завантажуватись із серверного або хмарного сховища. Блок «Стан ліфта» реалізований як динамічний компонент, що оновлюється у реальному часі через WebSocket-з’єднання. Він відображає поточний поверх, напрямок руху та цільовий поверх, а також дозволяє перемикати режими роботи. Блок відеоспостереження відображає відеопотік із камери, на який накладаються результати обробки (прямокутники ідентифікації, імена користувачів), що формуються на основі даних, отриманих від бекенд-системи. Блок статистики реалізується за допомогою бібліотек візуалізації, таких як Chart.js, і відображає показники ефективності роботи алгоритмів розпізнавання. Журнал доступу

представлений у вигляді таблиці, що регулярно оновлюється на основі даних із бази.

Структура програмної реалізації системи приведена в таблиці 4.1.

Таблиця 4.1 – Структура програмної реалізації системи

Рівень системи	Основні технології	Функції	Вхідні дані	Вихідні дані
Фронтенд	React, Vue.js, HTML, CSS	Відображення даних, інтерфейс користувача	Дані з бекенду, WebSocket	Візуалізація, команди користувача
Бекенд	Node.js, Django, WebSocket	Обробка запитів, API, логіка	Відео, дані користувачів	Дані для UI, команди ліфту
База даних	PostgreSQL, MongoDB	Зберігання даних	Дані від бекенду	Історія, профілі
Ядро AI	OpenCV, Dlib	Розпізнавання облич	Відеопотік	Ідентифікація
Інтеграція	Docker, CI/CD	Розгортання	Конфігурації	Робоча система

Бекенд-рівень виконує функції обробки запитів, управління даними та забезпечення взаємодії між усіма компонентами системи. Він може бути реалізований із використанням серверних технологій, таких як Node.js із фреймворком Express або Django / Flask для мови Python. Для забезпечення обміну даними в реальному часі використовується WebSocket-сервер (наприклад, Socket.io), який передає інформацію про стан ліфта, результати ідентифікації та відеодані на фронтенд. Бекенд також взаємодіє з базами даних: реляційною (наприклад, PostgreSQL) для зберігання журналів подій і NoSQL (наприклад, MongoDB) для зберігання профілів користувачів та біометричних даних.

Основними функціями бекенду є прийом відеопотоку від камери, передача

його в ядро ідентифікації, обробка результатів та їх збереження. Крім того, бекенд забезпечує управління профілями користувачів, включаючи зберігання фотографій, ролей та параметрів доступу, а також ведення журналу доступу, де фіксуються всі події ідентифікації та відповідні дії системи. Окремим завданням є інтеграція з ліфтовою системою: бекенд отримує інформацію про стан ліфта через відповідний інтерфейс і передає команди, сформовані модулем прийняття рішень.

Ядро ідентифікації є найбільш складним компонентом системи, оскільки воно реалізує алгоритми комп'ютерного зору та машинного навчання. Воно може бути побудоване на основі бібліотек, таких як OpenCV, Dlib або спеціалізованих рішень для розпізнавання облич. Основним завданням ядра є аналіз відеопотоку, виявлення облич та їх ідентифікація. На першому етапі виконується детекція облич за допомогою алгоритмів, таких як MTCNN або каскадні класифікатори. Далі для кожного обличчя формується вектор ознак, тобто числове представлення, яке характеризує унікальні риси обличчя. Ці вектори порівнюються з базою даних за допомогою алгоритмів пошуку найближчих сусідів, що дозволяє визначити особу користувача з певною ймовірністю. У випадку успішної ідентифікації результат передається на бекенд разом із координатами обличчя на кадрі.

Важливим етапом є попереднє навчання системи, яке передбачає формування бази даних ознак на основі набору фотографій користувачів. Це забезпечує високу точність подальшої ідентифікації. У разі використання хмарних сервісів (наприклад, Azure або AWS) частина обчислень може виконуватись на віддалених серверах, однак у даній роботі доцільним є локальний підхід для забезпечення конфіденційності даних.

Інтеграція всіх компонентів системи здійснюється з використанням технологій контейнеризації, зокрема Docker, що дозволяє ізолювати окремі сервіси та спростити їх розгортання. Для автоматизації процесів оновлення та розгортання застосовуються підходи CI/CD, які забезпечують безперервну інтеграцію та доставку програмного забезпечення. Система може бути розгорнута як на локальному сервері (edge-рішення), так і в хмарному середовищі, залежно від вимог до масштабованості та доступності.

Запропонована програмна архітектура забезпечує ефективну взаємодію між усіма компонентами кіберфізичної системи та дозволяє реалізувати обробку даних у реальному часі. Використання сучасних технологій фронтенду, бекенду та алгоритмів штучного інтелекту забезпечує високу точність ідентифікації, зручність користування та можливість масштабування системи.

4.3 Перевірка справжності біометричного об’єкта

Однією з критично важливих задач при проєктуванні кіберфізичної системи ідентифікації особи є забезпечення захисту від спуфінг-атак, тобто спроб обману системи за допомогою фотографій, відео або інших підроблених зображень обличчя. У запропонованій системі це завдання вирішується шляхом використання глибинної камери Intel RealSense D435, яка дозволяє отримувати не лише RGB-зображення, але й карту глибини сцени та інфрачервоні (ІЧ) дані. Це забезпечує можливість реалізації багаторівневої перевірки реальності користувача.

Програмна реалізація системи детекції обличчя базується на сучасних алгоритмах комп’ютерного зору, зокрема із використанням бібліотек Dlib або нейромережевих архітектур типу MTCNN. На першому етапі виконується виявлення обличчя у відеопотоці, після чого визначаються ключові точки (landmarks), що описують геометрію обличчя (очі, ніс, рот, контури). Це дозволяє не лише локалізувати обличчя, але й підготувати дані для подальшого аналізу.

Наступним етапом є перевірка «живості» (liveness detection), яка реалізується як комбінація кількох незалежних методів. Першим і найбільш ефективним є аналіз карти глибини. Камера Intel RealSense D435 формує тривимірне представлення обличчя, що дозволяє оцінити його просторову структуру. Для реального обличчя характерна наявність перепадів глибини (ніс виступає вперед, очні западини мають меншу глибину), тоді як фотографія або екран мобільного пристрою є практично плоскими. Програмний модуль аналізує дисперсію значень глибини в області обличчя та порівнює її з пороговими

значеннями. Якщо варіація глибини недостатня, система класифікує об’єкт як підробку.

Другим рівнем захисту є інфрачервоний аналіз. Камера генерує ІЧ-зображення, яке відображає особливості відбиття інфрачервоного випромінювання. Людська шкіра має специфічні спектральні характеристики, які відрізняються від паперу або дисплеїв. Програмний алгоритм аналізує інтенсивність та розподіл ІЧ-сигналу, що дозволяє додатково виявити спроби підміни обличчя.

Ефективність кіберфізичної системи значною мірою залежить від швидкості та надійності обміну даними між її компонентами. У запропонованій архітектурі використовується комбінований підхід до організації мережевої взаємодії, який включає протоколи реального часу, Rest API та низькорівневі інтерфейси керування.

Для забезпечення обміну даними у реальному часі використовується технологія WebSocket, яка дозволяє встановити постійне двостороннє з’єднання між клієнтом і сервером. Це особливо важливо для відображення стану ліфта та трансляції відеопотоку на інтерфейс користувача. Затримка передачі даних у такій конфігурації становить приблизно 45–120 мс, що відповідає вимогам до систем реального часу. WebSocket використовується, зокрема, для передачі координат обличчя, результатів ідентифікації та параметрів стану ліфта.

Для структурованого обміну даними між компонентами системи використовується RESTful API, реалізований на бекенд-рівні (наприклад, на базі Node.js або Django). Через API передаються ідентифікатори користувачів, рівні достовірності, а також службова інформація. Це забезпечує чітке розмежування функцій між модулями та спрощує масштабування системи.

Передача керуючих сигналів до виконавчого рівня здійснюється через інтерфейс GPIO або промислові протоколи, такі як Modbus або RS-485. У випадку використання GPIO обчислювальний модуль безпосередньо керує релейним інтерфейсом, наприклад 5V Relay Module, що дозволяє реалізувати фізичний виклик ліфта. Для промислових рішень більш доцільним є використання

цифрових протоколів, які забезпечують надійність та захист від перешкод.

Важливим аспектом є забезпечення стабільності та ізольованості програмних компонентів. Для цього використовується контейнеризація за допомогою Docker. Кожен сервіс (ядро ідентифікації, бекенд, база даних) розгортається у власному контейнері, що дозволяє уникнути конфліктів залежностей та спростити розгортання системи. Крім того, це забезпечує можливість масштабування окремих компонентів незалежно один від одного.

Структурна схема інформаційних та логічних зв'язків компонентів представлена на рисунку 4.3.

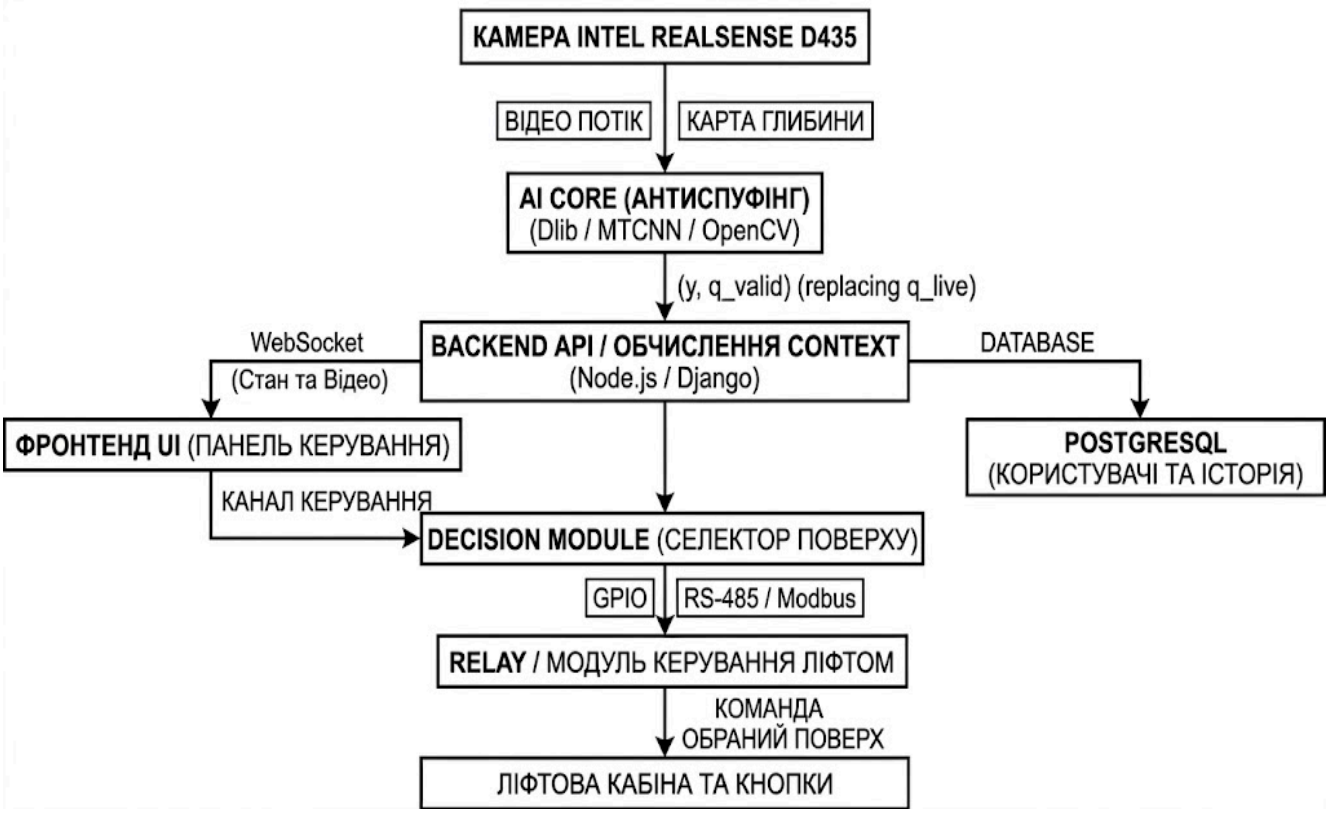


Рисунок 4.3 – Структурна схема інформаційних та логічних зв'язків компонентів

Представлена схема деталізує архітектуру та логіку роботи кіберфізичної системи, призначеної для керування «розумним» ліфтом. Основною метою цієї системи є забезпечення безпечного, безконтактного та автоматизованого доступу до поверхів будівлі, що базується на розпізнаванні облич користувачів та аналізі їхнього поточного контексту. Використання такої технології підвищує рівень

гігієни, комфорту та безпеки, а також оптимізує роботу ліфта за рахунок виключення необхідності ручного вибору поверху та запобігання несанкціонованому доступу.

Функціонування системи розпочинається з верхнього блоку, яким є високотехнологічна камера Intel RealSense D435. Цей пристрій є ключовим сенсорним елементом, що виконує роль джерела вхідних даних. Камера генерує та передає одночасно два інформаційні потоки: стандартний відео потік (кольорове RGB-зображення) та спеціалізовану карту глибини (інформацію про тривимірну структуру простору).

Обидва ці потоки є критично важливими для наступного етапу обробки, який здійснюється програмним модулем AI Core. Головним завданням цього ядра штучного інтелекту є виконання процедури антиспуфінгу, що передбачає перевірку справжності біометричного об’єкта для виключення спроб ідентифікації за допомогою фотографії, відеоекранної атаки або маски.

Для реалізації цієї складної функції AI Core використовує бібліотеки комп'ютерного зору та глибокого навчання, такі як Dlib, MTCNN (для детекції ключових точок обличчя) та OpenCV.

Поєднання аналізу текстури з RGB-потоку та тривимірної форми з карти глибини дозволяє надійно підтвердити, що перед камерою знаходиться жива людина, а не підробка. Результатом роботи AI Core є вектор ідентифікатора користувача та рівень достовірності його фізичної присутності (q_{valid}), які передаються далі за допомогою Rest API до центрального вузла системи Backend API.

Центральний вузол, Backend API, розгорнутий на базі сучасних фреймворків Node.js або Django, виконує функцію координатора всієї системи. Він забезпечує стабільну роботу, логіку обробки даних та мережеву взаємодію. Однією з його основних функцій є обчислення Context (контекстного вектора), що включає аналіз ідентифікованої особи, поточного часу, дня тижня та історії переміщень користувача.

Для зберігання та швидкого доступу до цієї інформації Backend API

взаємодіє з реляційною базою даних POSTGRESQL, де ведеться облік користувачів та історії їхніх поїздок. Одночасно Backend підтримує зв'язок із клієнтським інтерфейсом за допомогою протоколу WebSocket, що дозволяє передавати в реальному часі стан ліфта та відео (трансляцію з камери) на фронтенд UI (панель керування) для моніторингу та візуалізації роботи системи. На основі отриманих біометричних даних та обчисленого контексту Backend API або фронтенД UI (залежно від реалізації) приймає рішення, яке передається до decision module, що виконує роль селектора поверху. Останній, використовуючи канал керування, передає команду на виконавчий рівень. Виконавчий рівень представлений блоком Relay/модуль керування ліфтом, який є фізичним інтерфейсом до штатної автоматики ліфта.

Для надійної передачі сигналів керування використовуються стандартні промислові інтерфейси, такі як GPIO (для дискретних сигналів), RS-485 або протокол Modbus, що гарантує сумісність із широким спектром ліфтового обладнання.

Кінцевим етапом є подача фізичної команди про обраний поверх, яка активує відповідний релейний вихід, симулюючи натискання фізичної кнопки користувачем. завдяки цій послідовності дій ліфтова кабіна та кнопки стають повністю автоматизованими, а користувач отримує можливість дістатися потрібного поверху без будь-якої фізичної взаємодії з кнопковою панеллю, що і є основним досягненням розробленої системи.

4.4 Обґрунтування вибору апаратної платформи та сенсорної підсистеми з урахуванням побудови цифрового конвеєра обробки даних

У процесі проєктування кіберфізичної системи ідентифікації особи для «розумного» ліфта одним із ключових завдань є забезпечення мінімальної затримки обробки даних при збереженні достатньої точності та надійності функціонування. Це обумовлює необхідність обґрунтованого вибору апаратної платформи та сенсорної підсистеми, а також побудови ефективного цифрового конвеєра обробки інформації.

Враховуючи специфіку задачі, до апаратної платформи висуваються

наступні вимоги:

- забезпечення обробки даних у реальному часі;
- мінімізація затримок передачі та обробки;
- підтримка периферійних інтерфейсів для підключення сенсорів;
- енергоефективність та компактність;
- надійність роботи в умовах безперервної експлуатації;
- можливість локальної (edge) обробки без залежності від хмарних сервісів.

Особливістю системи є необхідність виконання обробки біометричних даних безпосередньо на периферійному рівні, що дозволяє уникнути затримок, пов’язаних із передачею даних до віддалених серверів, а також підвищити рівень конфіденційності.

Використання edge-пристроїв з апаратною підтримкою обчислень дозволяє реалізувати обробку даних безпосередньо на місці їх отримання. На відміну від традиційних централізованих систем, у яких обчислення виконуються на сервері, edge-підхід забезпечує:

- зменшення часу реакції системи;
- зниження навантаження на мережу;
- підвищення автономності роботи;
- зменшення ризиків втрати даних при розриві з’єднання.

Такі платформи реалізуються на базі одноплатних комп’ютерів або вбудованих систем із підтримкою апаратного прискорення (GPU, NPU або DSP). Наявність спеціалізованих обчислювальних блоків дозволяє виконувати паралельну обробку потоків даних, що є критично важливим для задач відеоаналізу.

При виборі платформи враховуються:

- продуктивність процесора (кількість ядер, тактова частота);
- обсяг оперативної пам’яті;
- пропускна здатність інтерфейсів введення/виведення;
- підтримка апаратного кодування/декодування відео;

− можливість інтеграції з операційними системами реального часу або оптимізованими Linux-дистрибутивами.

Таким чином, Edge AI платформа виступає центральним вузлом цифрового конвеєра, що забезпечує обробку даних у безпосередній близькості до джерела їх генерації.

Платформа NVIDIA Jetson Orin Nano Developer Kit є спеціалізованим edge-комп'ютером, орієнтованим на виконання задач штучного інтелекту, комп'ютерного зору та обробки потокових даних у режимі реального часу (рис.4.4). Вона базується на енергоефективній ARM-архітектурі та інтегрує графічний процесор архітектури NVIDIA Ampere, що містить CUDA-ядра та тензорні блоки для прискорення паралельних обчислень. Така комбінація апаратних ресурсів дозволяє виконувати складні алгоритми аналізу відеопотоку без необхідності звернення до віддалених серверів, що є критично важливим для кіберфізичних систем, які працюють у режимі реального часу.

Ключовою перевагою Jetson Orin Nano є наявність апаратного прискорення обчислень штучного інтелекту (AI acceleration), яке реалізується через Tensor Cores. Це дозволяє ефективно виконувати операції над великими масивами даних, зокрема обробку зображень, виділення ознак та класифікацію об'єктів. При цьому система забезпечує продуктивність до десятків TOPS (trillions of operations per second), що є достатнім для реалізації задач біометричної ідентифікації в умовах обмеженого часу реакції.

Енергоспоживання платформи знаходиться в діапазоні приблизно 5–15 Вт, що дозволяє використовувати її у вбудованих системах без необхідності складних систем охолодження. Це є важливим фактором для інтеграції у ліфтові шахти або технічні шафи, де простір і енергоресурси обмежені. Підтримка інтерфейсів CSI та USB забезпечує підключення високошвидкісних камер, що дозволяє отримувати відеопотік без значних затримок і втрат якості.

Рисунок 4.4 – Платформа NVIDIA Jetson Orin Nano Developer Kit [75]

Основні апаратні характеристики платформи включають ARM-процесор Cortex-A78AE, графічний процесор архітектури NVIDIA Ampere з до 1024 CUDA-ядер, а також оперативну пам’ять обсягом 8 або 16 ГБ залежно від конфігурації. Така архітектура дозволяє поєднувати загальні обчислення з паралельною обробкою графічних та матричних операцій, що є типовим для алгоритмів комп’ютерного зору.

Інтеграція NVIDIA Jetson Orin Nano у систему ідентифікації особи для «розумного» ліфта реалізується на рівні edge-пристрою, який виконує роль локального обчислювального вузла в кіберфізичній архітектурі. Камера, встановлена у ліфтовому холі або безпосередньо в кабіні, формує відеопотік, який передається на Jetson-платформу через високошвидкісний інтерфейс. Далі відбувається його попередня обробка (нормалізація зображення, виділення області обличчя), після чого система виконує біометричну ідентифікацію користувача.

Схема кіберфізичної системи адаптивного керування ліфтом на основі ідентифікації особи представлена на рисунку 4.5.

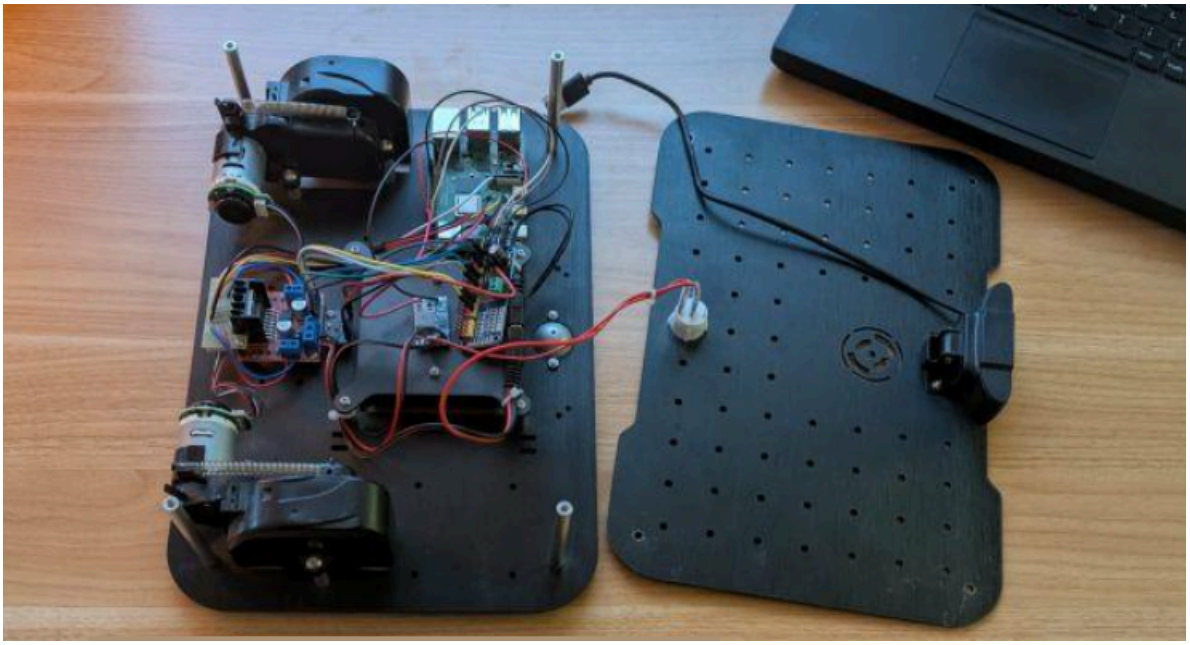


Рисунок 4.5 – Схема кіберфізичної системи адаптивного керування ліфтом на основі ідентифікації особи

Результатом роботи edge-вузла є не сирі дані, а вже оброблена інформація у вигляді ідентифікованої особи або результату перевірки доступу. На основі цього формується керуючий сигнал, який передається до контролера ліфтової системи. Такий підхід дозволяє реалізувати цифровий конвеєр обробки даних із мінімальною затримкою, оскільки всі критичні обчислення виконуються локально, без участі хмарних сервісів.

Завдяки цьому забезпечується висока швидкодія системи, автономність роботи навіть при втраті мережевого з’єднання, а також підвищений рівень безпеки, оскільки біометричні дані не передаються за межі пристрою. У контексті кіберфізичної системи «розумного» ліфта NVIDIA Jetson Orin Nano виконує функцію центрального edge-обчислювального вузла, який поєднує сенсорну підсистему, алгоритми обробки даних та виконавчу частину системи керування в єдиний інтегрований цифровий контур.

Сенсорна підсистема визначає якість та своєчасність отримання первинних даних. У рамках даної системи основним джерелом інформації є відеопотік, що формується за допомогою камери.

До ключових вимог до сенсорів належать:

- достатня роздільна здатність для коректного виділення об’єктів;
- висока частота кадрів для зменшення часових затримок;
- стабільність роботи при змінних умовах освітлення;
- підтримка швидкісних інтерфейсів передачі даних;
- низький рівень шумів.

Вибір відеокамери з інтерфейсом прямого підключення (наприклад, CSI або USB 3.0) дозволяє мінімізувати затримки, пов’язані з передачею відеопотоку. Використання апаратного буферування та потокової передачі даних забезпечує безперервність обробки.

Додатково можуть використовуватися допоміжні сенсори:

- датчики присутності для активації системи;
- інфрачервоні сенсори для роботи в умовах низького освітлення;
- датчики руху для оптимізації енергоспоживання.

Загальна затримка у будь-якій технічній системі формується як сума затримок на кожному етапі проходження сигналу від джерела до виконавчого механізму. Цей процес можна розглядати як послідовний конвеєр, де кожен етап додає свою частку часу.

Першим етапом є затримка сенсора. Вона включає час, необхідний для фізичного вимірювання параметра (наприклад, температури, положення чи зображення), а також час внутрішньої обробки сигналу самим сенсором (оцифрування, фільтрація, підсилення). Наприклад, у камерах це може бути час експозиції та зчитування матриці, а в інерційних датчиках це частота оновлення вимірювань. Чим вища частота дискретизації сенсора, тим менша ця затримка, але це часто збільшує обсяг даних.

Другим компонентом є затримка передачі даних. Вона виникає під час передавання інформації від сенсора до обчислювального вузла. Сюди входять затримки інтерфейсів (наприклад, UART, SPI, Ethernet), мережеві затримки, буферизація та можливі втрати пакетів із повторною передачею. У розподілених системах або хмарних рішеннях цей етап може стати домінуючим через фізичну

відстань і навантаження мережі.

Третім етапом є затримка обробки. Це час, який витрачається на аналіз отриманих даних, виконання алгоритмів (наприклад, фільтрація, комп'ютерний зір, машинне навчання), прийняття рішення. Ця складова сильно залежить від складності алгоритмів, ефективності програмної реалізації та обчислювальних ресурсів (CPU, GPU, FPGA). Наприклад, нейронні мережі можуть давати значні затримки без оптимізації або апаратного прискорення.

До четвертого компонента входить затримка формування та передачі керуючого сигналу.

Після прийняття рішення система повинна сформувати керуючий сигнал і передати його виконавчому механізму (мотору, клапану, дисплею тощо). Це включає час генерації сигналу, можливу цифрово-аналогову конверсію, передачу та фізичну реакцію виконавчого пристрою.

У деяких системах саме цей етап може бути критичним, наприклад у високоточному керуванні.

Щоб зменшити загальну затримку системи, застосовують кілька ключових підходів.

Один із найефективніших способів є використання локальної обробки. Ідея полягає в тому, щоб обробляти дані якомога ближче до джерела їх виникнення, а не передавати їх у віддалені сервери чи хмару.

Це дозволяє суттєво скоротити затримки передачі та підвищити швидкість реакції системи, що критично для задач реального часу (наприклад, автономний транспорт або промислова автоматизація).

Другий підхід полягає оптимізація передачі даних. Використання високошвидкісних інтерфейсів (наприклад, PCIe, Gigabit Ethernet, 5G) та ефективних протоколів дозволяє зменшити час доставки даних. Важливу роль відіграє також мінімізація затримок у мережевому стеку, уникнення зайвої буферизації та використання пріоритетних каналів для критичних даних.

Третій спосіб представляє собою мінімізацію обсягу оброблюваних даних. Замість передачі "сирих" даних (наприклад, повного відеопотоку) можна

використовувати попередню обробку, стиснення або виділення лише важливих ознак (feature extraction). Це зменшує навантаження як на канал передачі, так і на обчислювальні ресурси.

Четвертий напрям полягає у використанні апаратного прискорення. Спеціалізовані обчислювальні пристрої, такі як GPU, FPGA або ASIC, дозволяють значно швидше виконувати обчислення порівняно з універсальними процесорами. Це особливо актуально для задач машинного навчання, обробки сигналів і відео.

П’ятий аспект це оптимізація програмної реалізації. Ефективні алгоритми, оптимізований код, паралелізація обчислень, використання багатопоточності та правильне управління пам’яттю можуть суттєво скоротити час обробки. Навіть без зміни апаратного забезпечення грамотна оптимізація програмного рівня часто дає значний виграш у latency.

У підсумку, загальна затримка системи є комплексною характеристикою, яка залежить від усіх етапів обробки сигналу. Найкращі результати досягаються при системному підході, коли оптимізуються не окремі компоненти, а вся архітектура в цілому.

Таким чином, правильна організація цифрового конвеєра дозволяє досягти необхідного рівня швидкодії системи без втрати її функціональності.

4.5 Висновки

У четвертому розділі виконано проєктування кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» та реалізовано її архітектурні й програмно-апаратні рішення.

Розроблена архітектура системи базується на принципах розподілених обчислень із використанням edge-пристроїв, що дозволяє забезпечити низьку затримку обробки даних та незалежність від хмарної інфраструктури. Це є критично важливим для систем реального часу, зокрема ліфтових комплексів.

У процесі проєктування обґрунтовано вибір апаратної платформи та сенсорної підсистеми, що забезпечують необхідну продуктивність для виконання

алгоритмів комп’ютерного зору. Запропоновані рішення дозволяють реалізувати повноцінний цифровий конвеєр обробки даних безпосередньо на вбудованому пристрої.

Окрему увагу приділено розробці інтерфейсу взаємодії з ліфтовою автоматикою, що забезпечує інтеграцію з існуючими системами керування через стандартні апаратні інтерфейси. Це підвищує універсальність і практичну застосовність розробленого рішення.

Важливим результатом є реалізація механізмів перевірки справжності біометричного об’єкта, що підвищує рівень безпеки системи та захищає її від атак підміни.

Таким чином, у розділі доведено можливість практичної реалізації кіберфізичної системи ідентифікації особи для «розумного ліфта», що поєднує високу швидкодію, точність і надійність, а також відповідає сучасним вимогам до інтелектуальних систем автоматизації.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено кіберфізичну систему ідентифікації особи для автоматизації роботи «розумного ліфта».

Наукова новизна:

− запропоновано архітектурне рішення кіберфізичної системи, що базується на інтеграції сенсорів глибини та edge-обчислювачів, що, на відміну від хмарних аналогів, забезпечує детермінований час відгуку системи.

− дістав подальшого розвитку метод адаптивного керування ліфтовим обладнанням, який враховує не лише ідентифікатор особи, а й апаратний стан системи та контекстні параметри.

Поставлену мету було досягнуто шляхом розв’язання таких завдань:

− проаналізувано архітектурні особливості сучасних комп’ютерних систем керування ліфтами та методи біометричної ідентифікації;

− розроблено структурну модель КФС як багаторівневу ієрархію фізичного, мережевого та обчислювального рівнів;

− обґрунтувано вибір апаратної платформи (Edge AI) та сенсорної підсистеми для забезпечення низької затримки обробки;

− спроектувано цифровий конвеєр обробки біометричних даних та інтерфейс взаємодії з ліфтовою автоматикою (GPIO, релейні модулі, промислові протоколи).

Практична значимість отриманих результатів полягає у розробленій архітектурі кіберфізичної системи, яка базується на використанні edge-обчислень. Такий підхід дозволяє реалізувати обробку біометричних даних безпосередньо на локальному пристрої, що забезпечує мінімальні затримки, підвищену надійність та зменшення залежності від мережевої інфраструктури. Це особливо важливо для систем реального часу, де швидкість реакції є критичною. Також є можливість інтеграції запропонованого рішення з існуючими ліфтовими системами через стандартні інтерфейси (GPIO, промислові протоколи, релейні модулі). Це значно

спрощує впровадження розробки у реальні об’єкти без необхідності повної заміни обладнання, що знижує економічні витрати.

За темою кваліфікаційної роботи опубліковано одну публікацію [80] у збірнику наукових праць за матеріалами студентської науково-технічної конференції «Перспективні мережні та комп’ютерні технології» ПЕРСИК-2026, Харків.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Zhang Z., Pan W. Lift planning and optimization in construction: A thirty-year review. *Automation in Construction*. 2020. Vol. 118. P. 103271.

2. Lăzăroiu G., Kliestik T., Novak A. Internet of things smart devices, industrial artificial intelligence, and real-time sensor networks in sustainable cyber-physical production systems. *Journal of Self-Governance and Management Economics*. 2021. Vol. 9(1). P. 20–30.

3. Khan M. R., Tariq Z., Abdulraheem A. Application of artificial intelligence to estimate oil flow rate in gas-lift wells. *Natural Resources Research*. 2020. Vol. 29(6). P. 4017–4029.

4. Kavitha M., Susitra D., Meenakshi V., Antony A. S. M., Pushpavalli M., Pooja V. R. Smart Lift Technology for Compact Buildings. *2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA)*. 2024. P. 1–5.

5. Verma A., Kavitha M., Kowsalya S., Susitra D., Nayagam V. S., Balasubramanian V. Design and Development of Motor Module for the Advancements in Smartlift. *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*. 2024. P. 1–6.

6. Bhalerao M., Ohol S. Smart vertical lift for disabled person. *Proceedings of the international conference on industrial engineering and operations management*. 2022. Vol. 2022. P.470.

7. Varanasi L. S., Jonnalagadda A. R., Karri S. P. K. Smart edge device utilizing power line communication for energy management and control of electrical appliances. *IEEE Access*. 2024. Vol. 12. P. 37207–37218.

8. Bost S., Searle J. Smart Control: Advancing the Optimization and Control of Artificial Lift Systems. *SPE/AAPG/SEG Unconventional Resources Technology Conference*. 2024. P. D031S069R002.

9. Gichane M. M., Byiringiro J. B., Chesang A. K. та інш. Digital Triplet Approach for Real-Time Monitoring and Control of an Elevator Security System. *Designs*. 2020. Vol. 4(2). P. 9.

10. Isern J., Barranco F., Deniz D., Lesonen J., Hannuksela J., Carrillo R. R. Reconfigurable cyber-physical system for critical infrastructure protection in smart cities via smart video-surveillance. *Pattern Recognition Letters*. 2020. Vol. 140. P. 303–309.

11. Zhu Z., Cao J., Hao T. et al. Highly secure edge-intelligent electric motorcycle management system for elevators. *J Cloud Comp*. 2020. Vol. 9. P. 41.

12. Duidi Wu, Shuangdui Wu, Qianyou Zhao et al. Computer vision-based intelligent elevator information system for efficient demand-based operation and optimization. *Journal of Building Engineering*. 2024. Vol. 81. P. 108126.

13. Shen T.-C., Chu E. T.-H. Edge-Computing-Based People-Counting System for Elevators Using MobileNet–Single-Stage Object Detection. *Future Internet*. 2023. Vol. 15(10). P. 337.

14. Rashed A. N. Z., Yarrarapu M., Prabu R. T. et al. Connected smart elevator systems for smart power and time saving. *Sci Rep*. 2024. Vol. 14. P. 19330.

15. Manekar A., Revankar P. S. Smart elevator systems: An IoT-enabled framework for real-time monitoring and predictive maintenance. *2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA)*. 2025. P. 590–596.

16. Chang I. W., Lin Y. B., Meng H. J., Van L. D. Smart Elevator with Reconfigurable Sensor Monitoring. *IEEE Internet of Things Journal*. 2026.

17. Noh Sun-Kuk. A Study on the Non-Contact Artificial Intelligence Elevator System Due to the Effect of COVID-19. *Electronics*. 2024. Vol. 13(16). P. 3193.

18. Li H.Y., Chu E. T. H. SmartRide: Intelligent reservation and scheduling for elevators. *Journal of Ambient Intelligence and Smart Environments*. 2024. Volume 17. Pp. 1-27.

19. Yu Jie, Hu Bo. Real-Time Monitoring and Safety Scheduling of Intelligent Elevators Based on Biometric Data Analysis. *IEEE Transactions on Consumer Electronics*. 2025. Pp. 1–10.

20. Chatziparasidis I., Sfampa I. K. Residential buildings with brain-computer interface functionality: An elevator case study. *Volume 43, Issue 2*.

21. Jiayu Luo, Yusen Guo, Hongjie Leng et al. Non-contact optical vibration sensing and dual-branch deep learning for intelligent elevator fault diagnosis. *Sensors and Actuators A: Physical*. 2026. Vol. 405. P. 117849.

22. Li T., Lei L., Wang Z., Shi P., Wu Z. An efficient improved YOLOv10 algorithm for detecting electric bikes in elevators. *Electronic Research Archive*. 2025. Vol. 33(6). P. 3673–3698.

23. Yu Z., Kaplan Z., Yan Q., Zhang N. Security and Privacy in the Emerging Cyber-Physical World: A Survey. *arXiv:2105.13347*. 2021.

24. Hossain M., Rahman M., Ramasamy D. Artificial intelligence-driven vehicle fault diagnosis to revolutionize automotive maintenance: A review. *Computer Modeling in Engineering & Sciences*. 2024. Vol. 141(2). P. 951.

25. Vimal G., Verma R. Revolutionizing industries through cyber-physical systems: a systematic review. *Discover Computing*. 2026. Vol. 29. P. 250.

26. Oks S. J., Jalowski M., Lechner M. et al. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. *Information Systems Frontiers*. 2024. Vol. 26. P. 1731–1772.

27. Reddy G. T., Reddy M. P. K., Lakshmanna K. et al. An integrated outlook of Cyber–Physical Systems for Industry 4.0: Topical practices, architecture, and applications. *Green Technologies and Sustainability*. 2022. Vol. 1. P. 100001.

28. Sánchez J. M. G., Jörgensen N., Törngren M. Edge computing for cyber-physical systems: A systematic mapping study emphasizing trustworthiness. *arXiv preprint*. 2021. arXiv:2112.00619.

29. Sabou M., Biffl S., Einfalt A. et al. Semantics for Cyber-Physical Systems: A cross-domain perspective. *Semantic Web Journal*. 2020. Vol. 11(6). P. 1041–1071.

30. Imran M. A., Lateef J. Cyber Physical Security and Interoperability Challenges in IoT Based Smart Building Systems: A Narrative Critical Review. *International Journal of Innovative Science and Research Technology*. 2025. Vol. 10(12).

31. Hu G., Tang L., Lai Z. et al. Battery-free digital twins: A perspective on self-powered sensing for next-generation cyber-physical systems. *Journal of Intelligent*

Material Systems and Structures. 2026.

32. Ali M., Hassan M., Rahman M. Smart grid cyber-physical systems: Components, vulnerabilities, mitigations, opportunities, and conceptual framework. *Energy Reports*. 2026. Vol. 15. P. 109255.

33. Zhang Y., Li H., Wang C. A review of AIoT-enabled cyber-physical systems in building energy management: towards intelligent operation. *Applied Energy*. 2026. Vol. 409. P. 127482.

34. Al-Hwaitat A., Gupta B., Sharma S. Challenges of IoT sensors in smart buildings ecosystems and integration of blockchain for enhanced security and efficiency. *Sustainable Computing: Informatics and Systems*. 2026. Vol. 49. P. 101279.

35. Fraga-Lamas P., Barros D., Lopes S. I., Fernández-Caramés T. M. Mist and Edge Computing Cyber-Physical Human-Centered Systems for Industry 5.0: A Cost-Effective IoT Thermal Imaging Safety System. 2022. arXiv:2212.06294.

36. Xia F., Ma J. Building Smart Communities with Cyber-Physical Systems. *Future Generation Computer Systems*. 2011. Vol. 56. P. 1–11.

37. Radanliev P., De Roure D., Nurse J. R. C. et al. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*. 2020. Vol. 3(13).

38. Ahmad I., Hee L. M., Abdelrhman A. M. et al. Scopes, challenges and approaches of energy harvesting for wireless sensor nodes in machine condition monitoring systems: A review. *Measurement*. 2021. Vol. 183. P. 109856.

39. Saghir F., Gilabert H., Mancuso B. M. Application of Augmented Intelligence and Edge Analytics In Upstream Production Operations: An Innovative Approach for Optimizing Artificial Lift Systems Performance. *SPE Annual Technical Conference and Exhibition*. 2020. P. D031S022R002.

40. Badrinath B., Deepak K., Kavitha M., та інш. Smart Staircase Lift for Assisting Elderly People. *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*. 2024. Vol. 1. P. 483–487.

41. Palermo F., Casciano L., Demagh L. et al. Advancements in context

recognition for edge devices and smart eyewear: Sensors and applications. *IEEE Access*. 2025.

42. Escudero-Santana A., Cortés P., Guadix J., Muñuzuri J., Onieva L. Internet of Lifts: A Cloud Framework for Optimal Elevator Group Control Systems in Smart Cities. *The International Conference on Industrial Engineering and Industrial Management*. 2025. P. 60–65.

43. Pacheco V. Dynamic Lift Control for Improvements in Energy Efficiency. *6th Symposium on Lift and Escalator Technologies*. 2016. Vol. 6(1). P. 159–171.

44. Ebeling T. Lifting Elevators into the Cloud–Permanent Detection of Wear Using Intelligent Sensors. *9th Symposium on Lift and Escalator Technologies*. 2018. Vol. 9(1). P. 139–143.

45. To W. M., Lai L. S., Lam K. H., Chung A. W. Perceived importance of smart and sustainable building features from the users' perspective. *Smart Cities*. 2018. Vol. 1(1). P. 163–175.

46. Serrano W. Digital systems in smart city and infrastructure: Digital as a service. *Smart cities*. 2018. Vol. 1(1). P. 134–154.

47. Erős E., Dahl M., Bengtsson K., Hanna A., Falkman P. A ROS2 based communication architecture for control in collaborative and intelligent automation systems. *Procedia Manufacturing*. 2019. Vol. 38. P. 349–357.

48. Štefanič M., Stankovski V. A review of technologies and applications for smart construction. *Proceedings of the Institution of Civil Engineers-Civil Engineering*. 2019. Vol. 172(2). P. 83–87.

49. Shen T.-C., Chu E. T.-H. Edge-Computing-Based People-Counting System for Elevators Using MobileNet–Single-Stage Object Detection. *Future Internet*. 2023. Vol. 15(10). P. 337.

50. Zhu Z., Cao J., Hao T. et al. Highly Secure Edge-Intelligent Electric Motorcycle Management System for Elevators. *Journal of Cloud Computing*. 2020. Vol. 9. P. 41.

51. Li J. Design and Implementation of Elevator Internet of Things Security Control System based on Cloud Computing. *Proceedings of the 2017 4th International*

Conference on Machinery, Materials and Computer. 2018. P. 80–83.

52. Nikouei S. Y., Chen Y., Song S. et. al. Real-Time Human Detection as an Edge Service Enabled by a Lightweight CNN. *IEEE International Conference on Edge Computing*. 2018.

53. Liu F., Tang G., Li Y. et. al. A Survey on Edge Computing Systems and Tools. *arXiv preprint*. 2019. arXiv:1911.02794.

54. Wang S., Ding C. Mobile Edge Computing-Assisted Biometric Services. *Proceedings of the 11th International Conference on Service Science (ICSS 2018)*. 2018.

55. Ren J., He Y., Huang G. та інш. An Edge-Computing Based Architecture for Mobile Augmented Reality. *IEEE Network*. 2018. Vol. *33*(4). Pp.162-169.

56. Aljoša Vodopija, Stork J., Bartz-Beielstein T., Filipič B. Elevator Group Control as a Constrained Multiobjective Optimization Problem. *Applied Soft Computing*. 2022. Vol. 115. P. 108277.

57. Yamauchi T., Ide R., Sugawara T. Fair and Effective Elevator Car Dispatching Method in Elevator Group Control System Using Cameras. *Procedia Computer Science*. 2019. Vol. 159. P. 455–464.

58. Meribout M., Baobaid A., Khaoua M. O., Tiwari V. K., Pena J. P. State of art IoT and Edge embedded systems for real-time machine vision applications. *IEEE Access*. 2022. Vol. 10. Pp. 58287-58301.

59. Agbo-Ajala J. O., Akinyemi L. A., Ekundayo O. S., Mnkandla E. Biometric-based access control mechanism for edge computing resources and services. In *Cybersecurity Defensive Walls in Edge Computing*. 2026. pp. 317-336. Academic Press.

60. Manekar A., Revankar P. S. Smart elevator systems: An IoT-enabled framework for real-time monitoring and predictive maintenance. In *2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA)*. pp. 590-596. IEEE.

61. Chang I. W., Lin Y.-B., Meng H. J. et. al. Smart Elevator with Reconfigurable Sensor Monitoring. *IEEE Internet of Things Journal*. 2026.

62. Lai L., Ding S., Li Z., Luo Z., Wang H. An Intelligent Micromachine

Perception System for Elevator Fault Diagnosis. *Micromachines*. 2026. Vol. 17(4). P. 401.

63. He T., Tan T., Wu X. et. al. Exploration of Adding Elevators in Existing Residential Buildings to Meet the Challenges of Aging Driven by AI. *International Journal of High Speed Electronics & Systems*. 2026.

64. Roman R., Lopez J., Mambo M. Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges. *Future Generation Computer Systems*. 2018.

65. Cao H., Wachowicz M. An Edge-Fog-Cloud Architecture of Streaming Analytics for Internet of Things Applications. *Sensors*. 2019. Vol. 19(16). P. 3594.

66. George A., Ecabert C., Shahreza H. O. et. al. EdgeFace: Efficient Face Recognition Model for Edge Devices. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. 2024.

67. Khan M. Z., Harous S., Hassan S. et. al. Deep Unified Model For Face Recognition Based on Convolution Neural Network and Edge Computing. *IEEE Access*. 2019. Vol. 7. P. 72622–72633.

68. Xie Y., Li P., Nedjah N. et. al. Privacy Protection Framework for Face Recognition in Edge-Based Internet of Things. *Cluster Computing*. 2023. Vol. 26. P. 3017–3035.

69. Nguyen X. H., Hoang N. D., Nguyen T. H. et. al. An Efficient Face Recognition System Based on Edge Processing Using GPUs. *Smart Systems and Devices*. 2024. Vol. 34(1). P. 1–8.

70. Li J., Wang Y., Wang H. et. al. Real-time Face Recognition System Based on NVIDIA Jetson Nano. *Journal of Physics: Conference Series*. 2021. Vol. 1827. P. 012151.

71. Wen Di, Han H., Jain A. K. Face Liveness Detection with Component Dependent Descriptor. *2015 International Conference on Biometrics (ICB)*. 2015. P. 1–8.

72. Minoli D., Sohraby K., Occhiogrosso B. IoT Considerations, Requirements, and Architectures for Smart Buildings – Energy Optimization and

Next-Generation Building Management Systems. *IEEE Internet of Things Journal*. 2017. Vol. 4(1). P. 269–283.

73. Adamek M., Reznicek M., Pospisilik M., Neumann P. The possibilities of using Bluetooth to control the lift platform used for people with reduced mobility. In *MATEC Web of Conferences. 2019.* Vol. 292. P. 01059. EDP Sciences.

74. Wheeler D., Olszewska J. I. Cross-platform mobile application development for smart services. In *2022 IEEE 22nd International Symposium on Computational Intelligence and Informatics and 8th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Science and Robotics (CINTI-MACRo)*. 2022. pp. 1-6. IEEE.

75. NVIDIA Jetson Orin Nano Developer Kit. URL: https://evo.net.ua/nvidia-jetson-orin-nano-developer-kit/ (дата звернення: 13.04.2026).

76. Wu J., Shino M. Hip lift transfer assistive system for reducing burden on caregiver's waist. *Sensors*. 2021. Vol. *21*(22). P. 7548.

77. Avdagic B., Dewhurst P., Moore G. The potential of digital out-of-home advertising in the lift industry. In *16th Symposium on Lift & Escalator Technologies*. 2025. Vol. 16. №. 1. Pp. 39-47.

78. Wang C., Dong L., Peng D., Pan C. Tactile sensors for advanced intelligent systems. *Advanced Intelligent Systems*. 2019. Vol. 1(8). P. 1900090.

79. D'Almeida A. L., Bergiante N. C. R., de Souza Ferreira G., Leta F. R., de Campos Lima C. B., Lima G. B. A. Digital transformation: a review on artificial intelligence techniques in drilling and production applications. *The International Journal of Advanced Manufacturing Technology*. 2022. Vol. 119(9). P. 5553-5582.

80. Кротевич І. Л., Грига В. М. Метод та кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта». *Перспективні мережні та комп'ютерні технології (ПЕРСИК-2026)*. Харків. 2026. С. 1.

1.

ДОДАТОК А
(обов'язковий)

ТЕЗИ ДОПОВІДІ

ПерСиК 2026. Секція 3. Смарт-системи, ГІС та Інтернет речей (Smart systems, GIS and IoTs)

16:15 – 18:40, Google Meet: meet.google.com/ggg-yosc-cvn

Керівники секції:
д-р. філософії Вдовіченко Олександр Олександрович,
студент Іовенко Іван Євгенович

	Доповідачі	Назва доповіді
Сесія 3.1, 16:15 – 17:25		
1.	*Іовенко Іван*	Аналіз IDOR у сучасних веб-застосунках
2.	*Середюк Артем*	Аналіз хмарно-орієнтованих архітектурних рішень для координації мультиагентних роботизованих систем
3.	*Сніжинський Костянтин*	Розробка системи моніторингу мікроклімату в підземних спорудах подвійного призначення (укриттях)
4.	*Лісовий Вадим*	Система керування мікрокліматом теплиці з прогнозуванням та оптимізацією режимів роботи
5.	*Квітницький Роман*	Моделі та методи інформаційної технології аналізу поведінкових патернів IoT-пристроїв на рівні мережевого протоколу
6.	*Кротевич Іван*	Метод та кіберфізична система ідентифікації особи для автоматизації роботи розумного ліфта
7.	*Федорченко Марк*	Трансформерні моделі для прогнозу врожайності й агрокліматичних ризиків
8.	*Солодовник Микита*	Порівняння методів фільтрації супутникових зображень в умовах шуму
Кава-пауза, 17:25 – 17:30		
Сесія 3.2, 17:30 – 18:40		
9.	*Марчук Юрій*	Метод часової синхронізації у кіберфізичних системах на основі доступності потоків даних
10.	*Міцик Ілля*	Метод виявлення аномальної поведінки об'єктів на основі аналізу фізичних мікро-флуктацій руху з компенсацією динаміки FPV-платформи
11.	*Цибульський Єгор*	Нейромережеве керування сонячними панелями
12.	*Якимовський Валерій*	Кіберфізична система моніторингу метеорологічних параметрів для малих аеродромів
13.	*Черепанов Ілля*	Передбачення оптимального порогового значення DCT-фільтру для SAR-зображень з використанням трансферного навчання на MOBILENETV2
14.	*Прилуцький Роман*	Розробка системи автоматизованого фасування цукру на цукровому заводі

УДК 004.056.5

МЕТОД ТА КІБЕРФІЗИЧНА СИСТЕМА ІДЕНТИФІКАЦІЇ ОСОБИ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИ «РОЗУМНОГО ЛІФТА»

Кротевич І.Л., студент групи КІ2м-24-2

Науковий керівник: к.т.н., доцент Грига В.М.

Хмельницький національний університет

Актуальність. У сучасних умовах цифрової трансформації будівель та розвитку концепції «розумного міста» зростає потреба у впровадженні інтелектуальних систем автоматизації. Ліфтові системи є важливою складовою інфраструктури багатоповерхових будівель, тому підвищення їх ефективності, безпеки та зручності використання є актуальним завданням.

Традиційні методи доступу (картки, коди) мають низку недоліків, зокрема ризик втрати або несанкціонованого використання.

Метою роботи є розробка та аналіз методу і кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта».

Аналіз рішень. Сучасні ліфтові системи поступово впроваджують технології автоматизації та інтелектуального керування. Проте більшість існуючих рішень базуються на традиційних засобах автентифікації, таких як RFID-картки або паролі, що не забезпечують достатнього рівня безпеки. Окремі системи використовують біометричні методи, зокрема розпізнавання обличчя або відбитків пальців, однак їх застосування часто обмежується використанням лише одного типу ідентифікації. Це знижує точність і підвищує ризик помилок. Крім того, не всі рішення передбачають повноцінну інтеграцію з технологіями Інтернету речей та алгоритмами штучного інтелекту, що обмежує можливості адаптивного керування та оптимізації роботи ліфтів.

Результати. У роботі запропоновано кіберфізичну систему «розумного ліфта», яка базується на використанні мультимодальної біометричної ідентифікації. Система поєднує розпізнавання обличчя, відбитків пальців та аналіз поведінкових характеристик користувача.

Розроблена архітектура включає фізичний, обчислювальний і мережевий рівні, що забезпечують збір, обробку та передачу даних у реальному часі. Для підвищення точності ідентифікації використовуються алгоритми машинного навчання та нейронні мережі.

Запропонований підхід дозволяє автоматично визначати права доступу користувача, прогнозувати його маршрут і оптимізувати роботу ліфта. Це сприяє скороченню часу очікування, зменшенню навантаження на систему та підвищенню комфорту користувачів.

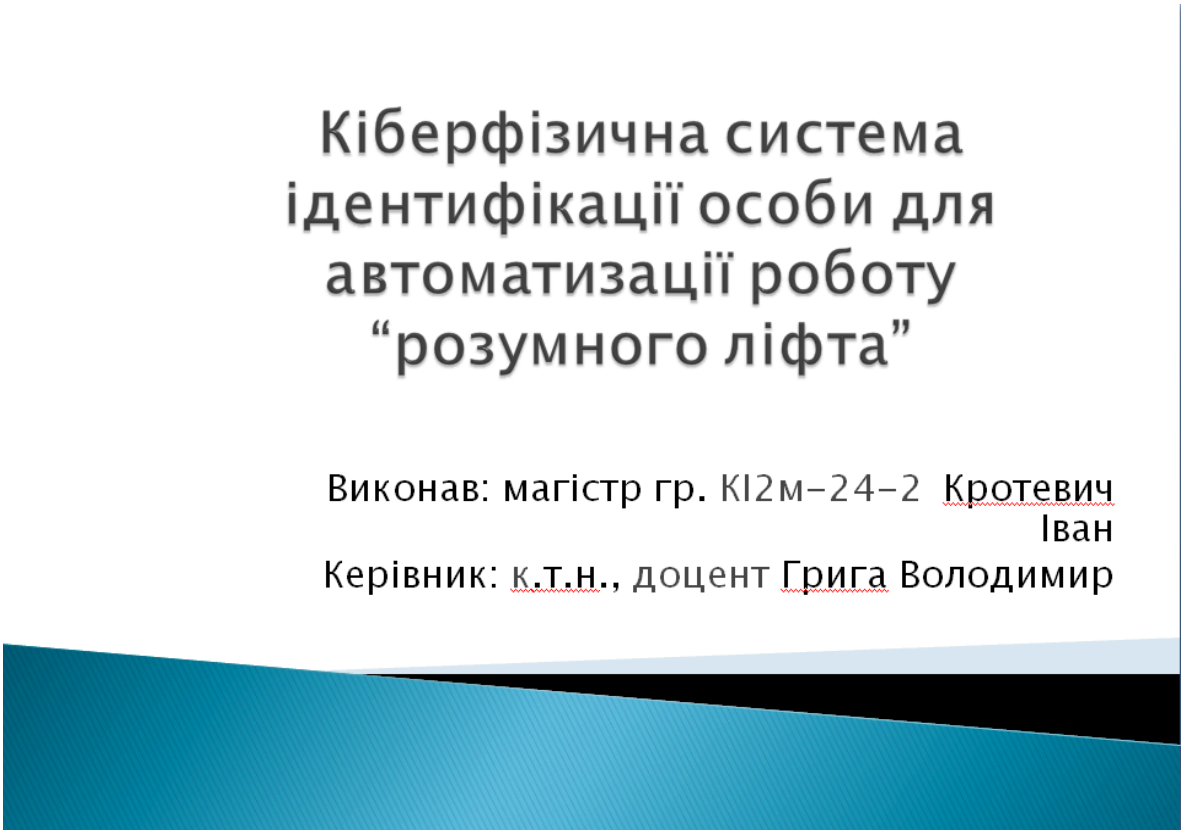
Висновки. У результаті дослідження обґрунтовано доцільність використання кіберфізичних систем і мультимодальної біометричної ідентифікації для автоматизації роботи «розумного ліфта». Запропонований підхід забезпечує підвищення рівня безпеки, точності ідентифікації та ефективності функціонування ліфтових систем. Інтеграція технологій штучного інтелекту та Інтернету речей дозволяє реалізувати адаптивне управління і покращити користувацький досвід.

Подальші дослідження можуть бути спрямовані на розширення функціональних можливостей системи та її інтеграцію в загальну інфраструктуру «розумних будівель»

ДОДАТОК Б

(обов'язковий)

ПРЕЗЕНТАЦІЯ



Актуальність

Розвиток концепції «розумних» будівель передбачає інтеграцію різнорідних інженерних підсистем, таких як енергозабезпечення, безпеки, клімат-контролю, відеоспостереження та транспортних систем у єдину інформаційно-керуючу інфраструктуру. У такому середовищі ліфт перестає бути ізольованим механічним пристроєм і трансформується у повноцінний кіберфізичний модуль, який обмінюється даними з іншими системами будівлі та адаптує свою поведінку відповідно до поточних умов експлуатації. Це вимагає переходу від централізованих схем керування до розподілених обчислювальних архітектур, у яких значна частина функцій реалізується на рівні периферійних (edge) пристроїв.

- Мета дослідження – забезпечення автоматизованого та безпечного керування «розумним» ліфтом на основі ідентифікації особи в кіберфізичному середовищі.

- Об'єктом дослідження є процеси апаратно-програмної взаємодії та передачі керуючих сигналів у кіберфізичних системах ідентифікації особи.
- Предметом дослідження є архітектурні рішення, методи та апаратні інтерфейси для автоматизації роботи «розумного ліфта» на основі біометричних даних.

Задачі дослідження

- проаналізувати архітектурні особливості сучасних комп'ютерних систем керування ліфтами та методи біометричної ідентифікації;
- розробити структурну модель КФС як багаторівневу ієрархію фізичного, мережевого та обчислювального рівнів;
- обґрунтувати вибір апаратної платформи (Edge AI) та сенсорної підсистеми для забезпечення низької затримки обробки;
- спроектувати цифровий конвеєр обробки біометричних даних та інтерфейс взаємодії з ліфтовою автоматикою (GPIO, релейні модулі, промислові протоколи).

Наукова новизна

- запропоновано архітектурне рішення кіберфізичної системи, що базується на інтеграції сенсорів глибини та edge-обчислювачів, що, на відміну від хмарних аналогів, забезпечує детермінований час відгуку системи.
- дістав подальшого розвитку метод адаптивного керування ліфтовим обладнанням, який враховує не лише ідентифікатор особи, а й апаратний стан системи та контекстні параметри.

Практична цінність отриманих результатів

- Практична значимість отриманих результатів полягає у розробленій архітектурі кіберфізичної системи, яка базується на використанні edge-обчислень. Такий підхід дозволяє реалізувати обробку біометричних даних безпосередньо на локальному пристрої, що забезпечує мінімальні затримки, підвищену надійність та зменшення залежності від мережевої інфраструктури. Це особливо важливо для систем реального часу, де швидкість реакції є критичною. Також є можливість інтеграції запропонованого рішення з існуючими ліфтовими системами через стандартні інтерфейси (GPIO, промислові протоколи, релейні модулі). Це значно спрощує впровадження розробки у реальні об'єкти без необхідності повної заміни обладнання, що знижує економічні витрати.

Кіберфізична система ідентифікації особи для автоматизації роботи "розумного ліфта"

Інтеграція КФСІО із системою «розумного ліфта» передбачає організацію інформаційного обміну, при якому результат ідентифікації використовується як вхідний параметр для алгоритмів керування.

Формально цей процес можна представити у вигляді 1:

$$U = G(I, Q, C), \tag{1}$$

де U – керуючий вплив на систему ліфта;

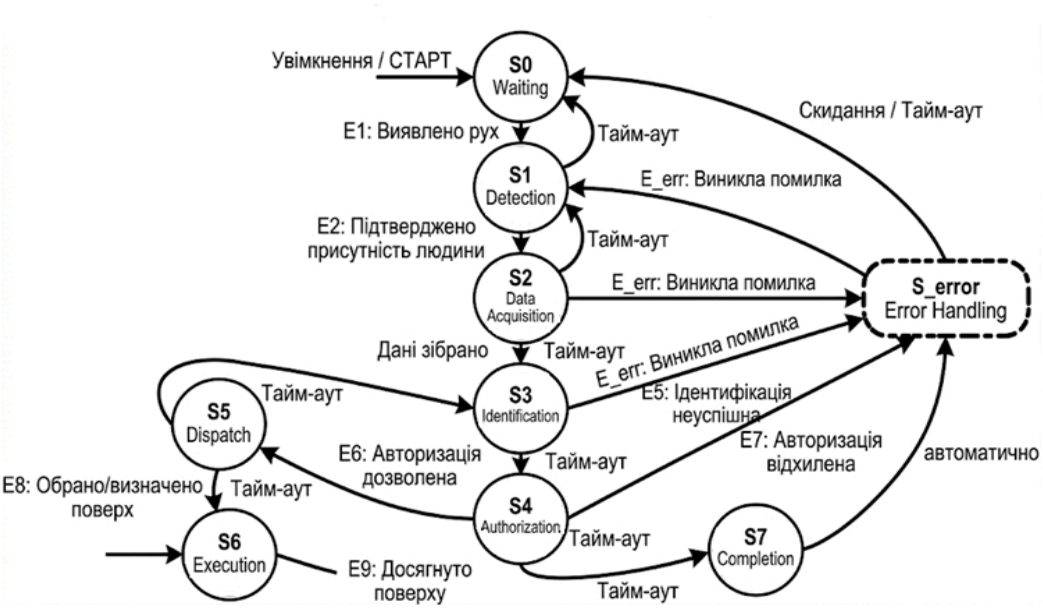
G – функція прийняття рішень, тобто формалізований алгоритм, який перетворює результат ідентифікації особи у керуючу дію системи;

I – ідентифікатор особи;

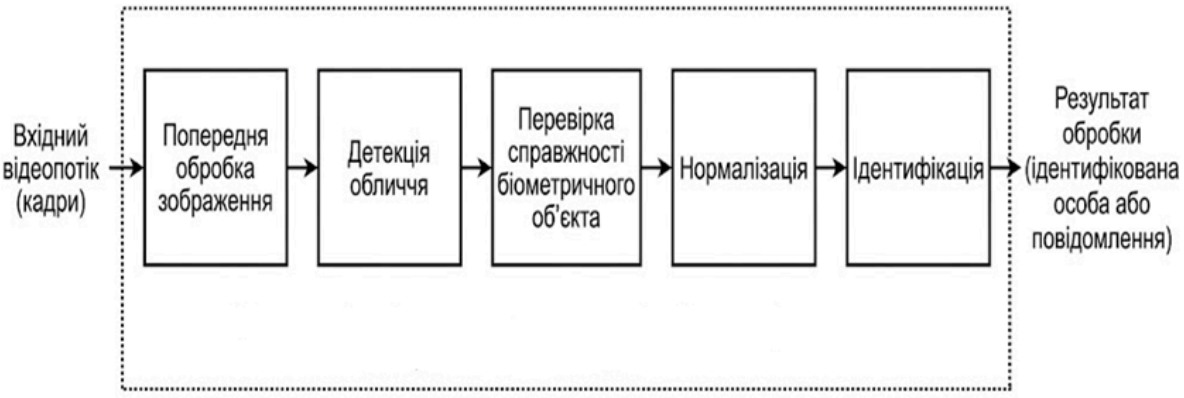
Q – достовірність ідентифікації;

C – контекст.

Граф станів скінченного автомата «розумного» ліфта



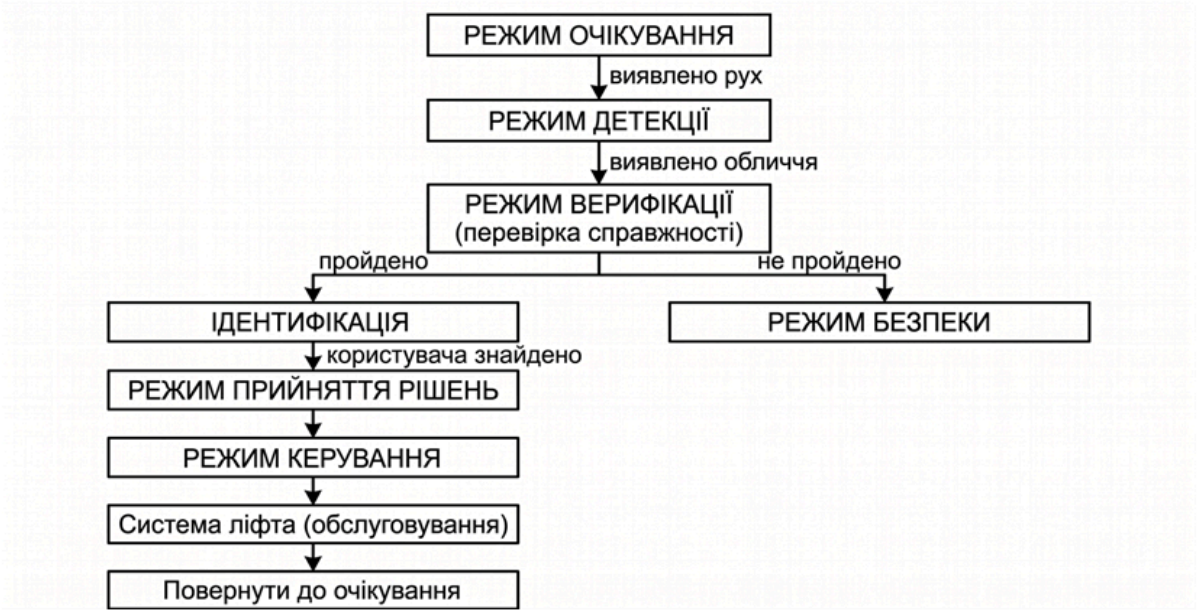
Структурна схема конвеєра обробки біометричних даних



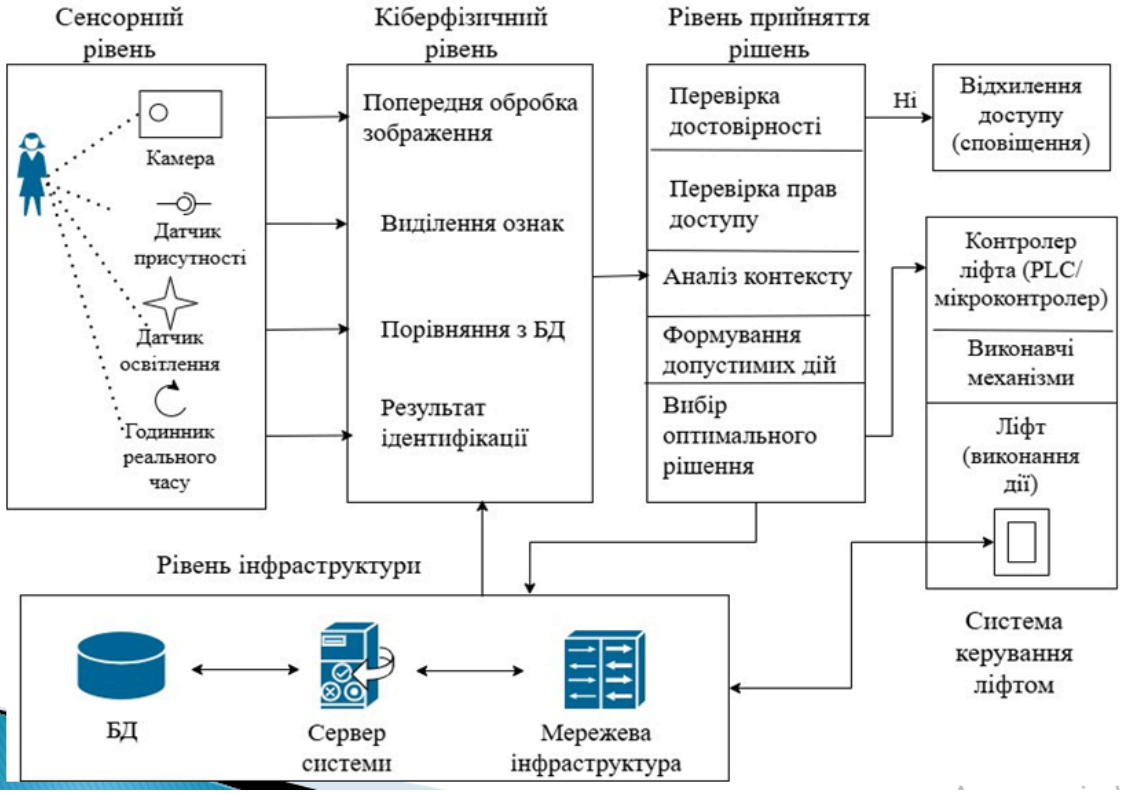
Метод адаптивного керування ліфтовим обладнанням

1. Оцінка достовірності та ідентифікація. Система отримує вектор ознак із AI-конвеєра, проводить зіставлення з еталонами та визначає ідентифікатор особи та показник впевненості Q.
2. Перевірка прав доступу. На основі ідентифікатора здійснюється звернення до бази прав доступу для формування первинної множини дозволених поверхів.
3. Аналіз контекстного вектора. Система зчитує поточний час t, стан ліфта s та історію h. Якщо користувач регулярно о 9:00 переміщується на 12-й поверх, цей поверх отримує найвищий пріоритет.
4. Селекція оптимальної дії. Відбувається остаточний вибір цільового поверху на основі перетину прав доступу та прогнозної моделі поведінки.
5. Генерація керуючого сигналу. Рішення транслюється у фізичну дію через інтерфейси GPIO або промислові протоколи (Modbus/RS-485), що замикає контур керування обчислювач – виконавчий механізм.

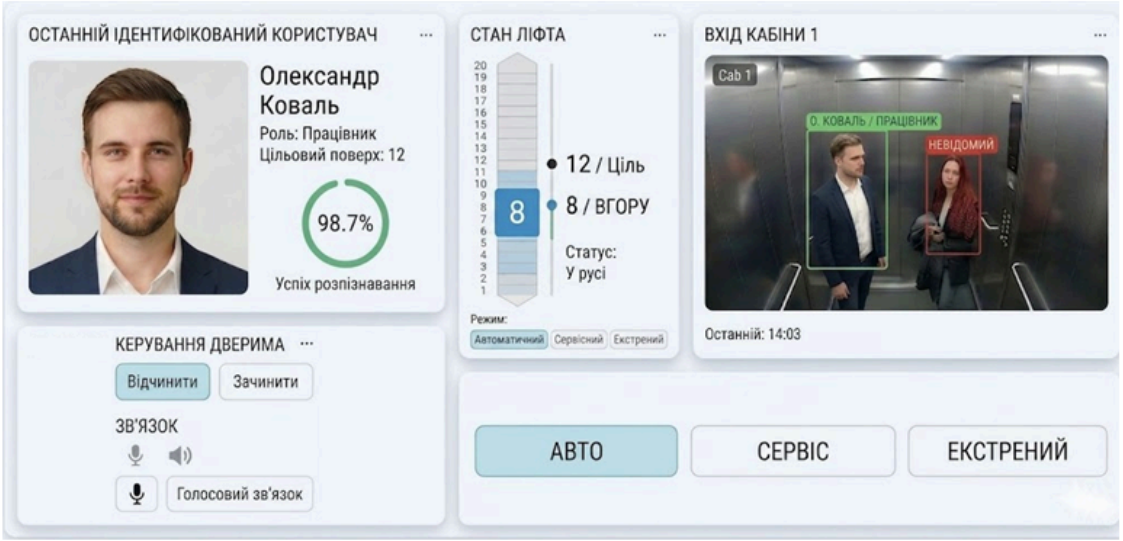
Схема перемикання станів кіберфізичної системи в процесі автоматизації роботи розумного ліфта на основі біометричної ідентифікації



Архітектурна схема кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта»



Інтерфейс користувача



Висновки

- проаналізувано архітектурні особливості сучасних комп'ютерних систем керування ліфтами та методи біометричної ідентифікації;
- розроблено структурну модель КФС як багаторівневу ієрархію фізичного, мережевого та обчислювального рівнів;
- обґрунтувано вибір апаратної платформи (Edge AI) та сенсорної підсистеми для забезпечення низької затримки обробки;
- спроектовано цифровий конвеєр обробки біометричних даних та інтерфейс взаємодії з ліфтовою автоматикою (GPIO, релейні модулі, промислові протоколи).

Дякую за увагу!

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Іван КРОТЕВИЧ

Тема: Кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта»

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень – ; кількість сторінок записки 92

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано кіберфізичну систему ідентифікації особи для автоматизації роботи «розумного ліфта»

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз предметної галузі де визначено, що «розумний ліфт» є складною кіберфізичною системою, де надійність функціонування залежить від швидкодії обчислювальних вузлів та стабільності каналів передачі даних. Обґрунтовано доцільність використання вбудованих систем для локальної ідентифікації особи, що дозволяє уникнути затримок хмарної інфраструктури та підвищити безпеку персональних даних. У другому розділі виконано моделювання кіберфізичної системи ідентифікації особи як багаторівневої інтегрованої структури, що поєднує фізичні процеси збору даних та їх інтелектуальну обробку. У третьому розділі розроблено та обґрунтовано методи і алгоритми ідентифікації особи, а також підходи до адаптивного керування ліфтовою системою. Проведений аналіз існуючих підходів показав, що класичні статистичні методи поступаються сучасним нейромережевим архітектурам за точністю та стійкістю до шумів. У четвертому розділі виконано проєктування кіберфізичної системи ідентифікації особи для автоматизації роботи «розумного ліфта» та реалізовано її архітектурні й програмно-апаратні рішення.

4. Позитивні сторони роботи: Запропонована кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта» дозволила представити процес ідентифікації як послідовність взаємопов'язаних перетворень, від отримання сирих біометричних даних до прийняття рішення. Це дало змогу формалізувати систему у вигляді математичних відображень, що є важливим для подальшого аналізу, оптимізації та програмної реалізації.

5. Негативні сторони роботи: Недостатнє обґрунтування вибору та порівняльного аналізу базових обчислювальних платформ, а також недостатня деталізація алгоритму виходу зі стану помилки у моделі скінченного автомата

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому нуково-професійному рівні.

8. Інші зауваження: –

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «задовільно» 70.00 (D)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) д.т.н., професор Марцишук В.В., завідувач кафедри автоматизації та робототехнічних інтегрованих технологій

"18" травня 2026р.

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Іван КРОТЕВИЧ
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-24-2

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1 травня 2026 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта»
Автор Іван КРОТЕВИЧ
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: к.т.н., доцент Володимир ГРИГА

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 3.89 % і адресується до 20 першоджерела; та системою Anti-Plagiarism складає 0%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

01.05.2026

Завідувач кафедри _____ Підпис Ольга ПАВЛОВА Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Підпис Олег САВЕНКО Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Підпис Володимир ГРИГА Ім'я, ПРІЗВИЩЕ

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Іван КРОТЕВИЧ

Співавтор:

Назва: Кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта»

Експерт: Володимир ГРИГА

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:3.89%

Коефіцієнт подібності 2:1.05%

Мікропробіли: 103

Заміна букв: 1

Інтервали: 0

Білі знаки: 6

Дата створення звіту: 2026-05-12 21:06:27.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-05-12 Доцент Андрій Нічепорук

Дата експерт

Tue May 12 21:15:04 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

ID: 271398 Назва: МКР Кіберфізична система ідентифікації особи для автоматизації роботи «розумного ліфта» Додано в БД: 2026-05-12 Автора: Іван КРОТЕВИЧ Керівники: Володимир ГРИГА Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	163739	1202	1016 (1%)	14 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми