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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: *Методи та програмно-апаратні засоби ідентифікації працівників для доступу до службового приміщення та контролю перебування в ньому.*

Виконав: студент(ка) 6 курсу, групи СІм-62
спеціальності 123 «Комп'ютерна інженерія»
123 Комп'ютерна інженерія
(шифр і назва спеціальності)

(підпис) Рожик А.М. (прізвище та ініціали)

Керівник (підпис) Жаровський Р.О. (прізвище та ініціали)

Нормоконтроль (підпис) Тиш Є.В. (прізвище та ініціали)

Завідувач кафедри (підпис) Осухівська Г.М. (прізвище та ініціали)

Рецензент (підпис) Дуда О.М. (прізвище та ініціали)

Тернопіль
2025

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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
«17» листопада 2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Рожик Анастасії Миколаївні*
(прізвище, ім'я, по батькові)

1. Тема роботи *Методи та програмно-апаратні засоби ідентифікації працівників для доступу до службового приміщення та контролю перебування в ньому*

Керівник роботи *Жаровський Руслан Олегович, к.т.н.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « *14* » *листопада 2025* року № 4/7-987
2. Термін подання студентом завершеної роботи *16 грудня 2025 р.*
3. Вихідні дані до роботи *Наукові літературні джерела.*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1 Аналіз методів та засобів побудови адаптивних систем контролю доступу
2 Теоретичні основи побудови адаптивної системи контролю доступу з використанням нечіткої логіки
3 Практична реалізація та імітаційне моделювання адаптивної системи контролю доступу
4 Охорона праці та безпека в надзвичайних ситуаціях
Висновки
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Актуальність і мета дослідження.
2. Завдання, об'єкт і предмет, наукова новизна і практична цінність дослідження.
3. Порівняльний аналіз методів ідентифікації
4. Блок-схема головного алгоритму роботи системи контролю доступу
5. Структурна схема адаптивної системи контролю доступу
6. Ієрархічна структура модулів та даних програмного комплексу
7. Результати експериментального дослідження
8. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	*Осухівська Г.М., зав.каф. КС*	*04.12.2025*	
Безпека в надзвичайних ситуаціях	*Стручок В.С., ст.викл.каф. ОХ*		

7. Дата видачі завдання *17.11.2025р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Огляд літературних джерел. Постановка завдання на кваліфікаційну роботу.*	*17.11.2025р. – 23.11.2025р.*	*Викон.*
2.	*Проєктування системи та розробка алгоритмічного забезпечення апаратно-програмного комплексу*	*24.11.2025р. – 02.12.2025р.*	*Викон.*
3.	*Програмна реалізація системи, аналіз результатів симуляції та оцінка адекватності роботи алгоритму вибору методу ідентифікації*	*03.12.2025р. – 10.12.2025р.*	*Викон.*
4.	*Охорона праці та безпека в надзвичайних ситуаціях*	*04.12.2025р. – 10.12.2025р.*	*Викон.*
5.	*Оформлення пояснювальної записки і графічного матеріалу*	*11.12.2025р. – 19.12.2025р.*	*Викон.*
6.	*Попередній захист кваліфікаційної роботи магістра*	*16.12.2025р.*	*Викон.*
7.	*Захист кваліфікаційної роботи магістра*	*23.12.2025р.*	*Викон.*

Студент _____ *Рожик А.М.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Жаровський Р.О.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Рожик А.М. Методи та програмно-апаратні засоби ідентифікації працівників для доступу до службового приміщення та контролю перебування в ньому: робота на здобуття кваліфікаційного ступеня магістра: спец. 123 — комп'ютерна інженерія / наук.кер. Жаровський Р.О. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2025.

Ключові слова: система контролю доступу, нечітка логіка, біометрична ідентифікація, адаптивне керування, MATLAB, алгоритм Мамдані, безпека.

Кваліфікаційна робота присвячена розробці та дослідженню адаптивної системи контролю доступу, здатної функціонувати в умовах динамічних змін параметрів навколишнього середовища. Робота включає аналіз впливу дестабілізуючих факторів, таких як освітленість, акустичний шум та температура, на надійність біометричних методів ідентифікації. Обґрунтовано доцільність використання математичного апарату нечіткої логіки для автоматичного вибору оптимального засобу автентифікації в режимі реального часу.

Для верифікації запропонованих рішень використано середовище імітаційного моделювання MATLAB, в якому реалізовано модель нечіткого контролера на базі алгоритму Мамдані. Отримані результати моделювання підтверджують ефективність адаптивного підходу, демонструючи здатність системи мінімізувати помилки першого та другого роду шляхом плавного перемикання пріоритетів методів ідентифікації залежно від зовнішніх умов.

ANNOTATION

Rozhyk A.M. Methods and hardware–software tools for employee identification for access to a service room and presence control within it. Master's Graduation Thesis: speciality 123 — Computer engineering / supervisor Zharovskyi R.O. Ternopil: Ternopil Ivan Puluj National Technical University, 2025.

Keywords: access control system, fuzzy logic, biometric identification, adaptive control, MATLAB, Mamdani algorithm, security.

The Master's graduation thesis is dedicated to the development and research of an adaptive access control system capable of functioning under dynamic changes in environmental parameters. The work includes an analysis of the influence of destabilizing factors, such as illumination, acoustic noise, and temperature, on the reliability of biometric identification methods. The feasibility of using fuzzy logic tools for the automatic selection of the optimal authentication means in real-time is justified.

To verify the proposed solutions, the MATLAB simulation environment was used, in which a model of a fuzzy controller based on the Mamdani algorithm was implemented. The obtained simulation results confirm the effectiveness of the adaptive approach, demonstrating the system's ability to minimize type I and type II errors by smoothly switching the priorities of identification methods depending on external conditions.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CSI – послідовний інтерфейс камери

CSV – текстовий формат даних, розділених комами

GPIO – інтерфейс введення-виведення загального призначення

ДСН – державні санітарні норми

ЗІЗ – засоби індивідуального захисту

ЗС – захисні споруди

НПАОП – нормативно-правовий акт з охорони праці

НС – надзвичайна ситуація

СКУД – система контролю та управління доступом

ВСТУП

Актуальність роботи. Забезпечення надійної ідентифікації особи в системах контролю доступу є критично важливим аспектом функціонування сучасних систем безпеки на об’єктах різного призначення. Традиційні підходи до побудови систем контролю та управління доступом зазвичай спираються на статичні методи автентифікації, які не враховують зміни умов навколишнього середовища. Існуючі рішення часто демонструють зниження ефективності роботи за несприятливих обставин, якими можуть бути недостатнє освітлення для розпізнавання обличчя, високий рівень акустичного шуму для розпізнавання голосових команд або екстремальні температури для сканерів відбитків пальців. Така вразливість створює передумови для помилок доступу або повного блокування пропускних пунктів, що негативно впливає на загальний рівень безпеки та комфорт користувачів.

У цьому контексті актуальним науково-технічним завданням виступає розробка адаптивних апаратно-програмних комплексів, здатних аналізувати стан навколишнього середовища та динамічно обирати оптимальний метод ідентифікації осіб в системах контролю доступу. Використання апарату нечіткої логіки дозволяє формалізувати процес прийняття рішень в умовах невизначеності та забезпечити безперебійну роботу системи. Впровадження таких інтелектуальних контролерів сприятиме підвищенню надійності систем безпеки та мінімізації впливу зовнішніх факторів на процес автентифікації.

Метою кваліфікаційної роботи виступає підвищення надійності та ефективності процесів ідентифікації в системах контролю доступу шляхом розробки адаптивного апаратно-програмного комплексу з використанням нечіткої логіки для вибору оптимального методу автентифікації залежно від умов навколишнього середовища.

Завдання кваліфікаційної роботи:

– провести аналіз існуючих рішень у галузі систем контролю доступу з метою виявлення недоліків функціонування біометричних сканерів у нестабільних умовах середовища;

– розробити математичну модель на базі нечіткої логіки типу Мамдані для прийняття рішень щодо вибору пріоритетного методу ідентифікації осіб в системах контролю доступу на основі показників освітленості, шуму та температури;

– спроєктувати архітектуру апаратно-програмного комплексу та обґрунтувати вибір компонентної бази для реалізації системи адаптивного контролю доступу;

– реалізувати програмне забезпечення для системи контролю доступу з функціями моніторингу сенсорів, нечіткого виводу та управління виконавчими механізмами;

– провести тестування розробленого прототипу та оцінити ефективність запропонованих алгоритмів у різних сценаріях експлуатації.

Відповідно до мети та завдань кваліфікаційної роботи визначено її об’єкт та предмет.

Об’єкт дослідження: процеси ідентифікації та управління доступом у комп'ютеризованих системах контролю доступу.

Предмет дослідження: методи та засоби адаптивного вибору способу автентифікації користувача в системах контролю доступу на основі аналізу параметрів навколишнього середовища з використанням нечіткої логіки.

Методи дослідження. У роботі використано комплексний підхід із застосуванням теоретичних та емпіричних методів. Побудова моделі прийняття рішень базується на теорії нечітких множин та нечіткої логіки. Проєктування апаратної частини виконано з використанням методів схемотехніки та модульного конструювання. Розробка програмного забезпечення здійснена з використанням об'єктно-орієнтованого підходу та мови програмування Python. Перевірка працездатності системи проведена експериментальним методом на фізичному прототипі.

Наукова новизна дослідження.

Запропоновано новий метод динамічного вибору засобу ідентифікації в системах контролю доступу, який базується на використанні нечіткого виводу

для комплексної оцінки придатності біометричних методів залежно від поточних показників освітленості, акустичного шуму та температури, що дозволило підвищити ймовірність успішної ідентифікації в умовах нестабільного зовнішнього середовища та зменшити кількість помилок першого і другого роду.

Удосконалено алгоритм роботи системи контролю доступу шляхом введення циклічного моніторингу безпеки та автоматичного переходу на резервні методи автентифікації у критичних умовах, що забезпечило безперервність функціонування системи та збереження пропускної здатності точки проходу при виникненні дестабілізуючих факторів або відмові основних сенсорів.

Практичне значення результатів кваліфікаційної роботи. Розроблено та реалізовано діючий прототип адаптивної системи контролю доступу на базі одноплатного комп'ютера Raspberry Pi. Створене програмне забезпечення дозволяє інтегрувати систему в існуючу інфраструктуру підприємств та забезпечує облік робочого часу персоналу. Запропоноване рішення може бути використане для обладнання пропускних пунктів на об'єктах зі складними умовами експлуатації, такими як виробничі цехи, відкриті майданчики або неопалювані приміщення.

Публікації. Результати дослідження апробовано на XIV міжнародній науково-технічній конференції молодих учнів та студентів «Актуальні задачі сучасних технологій», XIII науково-технічній конференції «Інформаційні моделі, системи та технології» у вигляді тез конференцій.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається із вступу, 4 розділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1
АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ПОБУДОВИ АДАПТИВНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

1.1. Огляд сучасних систем контролю доступу та технологій ідентифікації особи

1.1.1. Класифікація та принципи побудови сучасних систем безпеки.

Сучасний етап розвитку інфраструктури безпеки характеризується стрімким переходом від механічних засобів обмеження доступу до високотехнологічних автоматизованих комплексів. Системи контролю та управління доступом є невід'ємною частиною забезпечення безпеки функціонування підприємств, офісних центрів, державних установ та об'єктів критичної інфраструктури. Основне призначення таких систем, як зазначено в [27], полягає у автоматизованому розмежуванні прав доступу співробітників та відвідувачів до фізичних зон об'єкта, охороні майна та інтелектуальної власності, а також в автоматизації обліку робочого часу персоналу.

Функціонування будь-якої системи контролю доступу базується на процесі порівняння пред'явленого ідентифікатора з інформацією, що зберігається в базі даних системи. Цей процес складається з трьох послідовних етапів [30]:

– Ідентифікації, що являє собою процес розпізнавання суб'єкта за його унікальним ідентифікатором.

– Автентифікації, яка є процедурою перевірки справжності пред'явленого ідентифікатора та підтвердження того, що суб'єкт є саме тим, за кого себе видає.

– Авторизації, що полягає у перевірці наявності у суб'єкта прав на виконання певних дій, наприклад, проходу в конкретне приміщення у визначений час.

За способом управління системи контролю доступу поділяються на автономні, централізовані та розподілені [25].

Автономні системи є найпростішими та економічно вигідними рішеннями для контролю однієї або кількох точок проходу без необхідності передачі інформації на центральний пульт. Уся база даних користувачів та логіка прийняття рішень зберігаються безпосередньо у пам'яті контролера. Головним недоліком таких систем виступає складність адміністрування та відсутність можливості оперативного отримання звітів про події.

Централізовані або мережеві системи об'єднують велику кількість контролерів під управлінням одного або кількох серверів. Це дозволяє реалізувати складні алгоритми доступу, вести глобальний облік робочого часу та інтегруватися з іншими системами безпеки, такими як відеоспостереження або пожежна сигналізація.

Загальна схема взаємодії компонентів типової системи контролю доступу зображена на рис. 1.1.

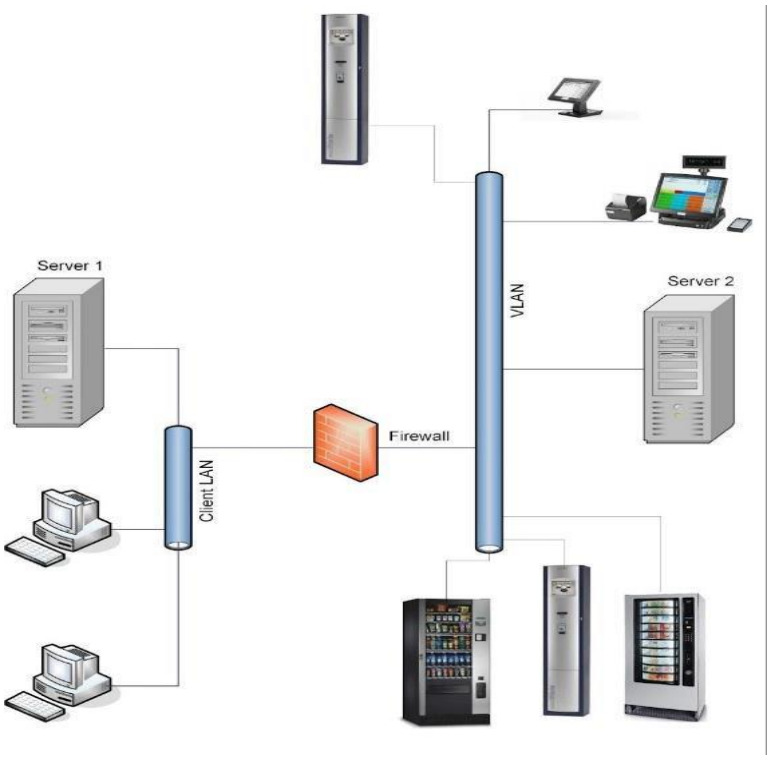

Рис. 1.1. Узагальнена структурна схема типової системи контролю доступу

Архітектура сучасної системи контролю доступу зазвичай включає наступні компоненти [38]:

– ідентифікатори, які служать носіями унікальної інформації про користувача;

– зчитувачі, що забезпечують отримання коду з ідентифікатора та передачу його на контролер;

– контролери, які обробляють отриману інформацію, приймають рішення про допуск та керують виконавчими пристроями;

– виконавчі механізми, до яких належать електромагнітні або електромеханічні замки, турнікети, шлагбауми.

Розвиток обчислювальних потужностей та алгоритмів штучного інтелекту сприяв появі нового класу адаптивних систем [1]. Такі системи здатні аналізувати не лише статичні права доступу, але й динамічні параметри навколишнього середовища та поведінкові фактори. Це дозволяє підвищити надійність ідентифікації та мінімізувати кількість помилок першого та другого роду. Інтелектуальні контролери, побудовані на базі сучасних мікрокомп'ютерів, здатні виконувати складну обробку біометричних даних безпосередньо на точці проходу, що підвищує швидкість реакції системи та її автономність.

1.1.2. Технології радіочастотної ідентифікації. Технологія радіочастотної ідентифікації (RFID) тривалий час залишається стандартом де-факто в індустрії систем безпеки [14]. Вона базується на використанні радіочастотного електромагнітного випромінювання для безконтактного обміну даними між зчитувачем та ідентифікатором. У системах контролю доступу найбільш поширеними є пасивні мітки, які не мають власного джерела живлення. Енергію, необхідну для роботи мікрочіпа та передачі відповідного сигналу, мітка отримує з електромагнітного поля, що генерується антеною зчитувача. Це забезпечує високу надійність, довговічність ідентифікаторів та їх низьку вартість.

У системах контролю доступу найбільш поширеними є пасивні мітки, які не мають власного джерела живлення. Енергію, необхідну для роботи мікрочіпа та передачі відповідного сигналу, мітка отримує з електромагнітного поля, що генерується антеною зчитувача. Це забезпечує високу надійність, довговічність ідентифікаторів та їх низьку вартість.

За частотним діапазоном системи радіочастотної ідентифікації класифікують на низькочастотні та високочастотні. Низькочастотні системи працюють у діапазоні 125 кГц та характеризуються невеликою дальністю зчитування і низькою швидкістю передачі даних. Високочастотні системи використовують частоту 13,56 МГц і забезпечують кращий захист даних завдяки використанню криптографічних алгоритмів. Саме цей стандарт часто використовується як надійний резервний метод доступу в адаптивних системах, коли біометричні методи не можуть бути застосовані через критичні умови середовища.

Принцип дії зчитувача на частоті 13,56 МГц базується на явищі електромагнітної індукції. Зчитувач генерує високочастотне магнітне поле. Коли мітка потрапляє в зону дії цього поля, в її антені наводиться електричний струм, який заряджає конденсатор контуру живлення. Після накопичення достатньої енергії мікрочіп мітки активується та модулює магнітне поле зчитувача своїм унікальним кодом. Зчитувач демодулює цей сигнал та передає отриманий ідентифікатор контролеру.

Популярність даного методу обумовлена високою стабільністю роботи незалежно від освітлення, температури чи вологості повітря. Проте суттєвим недоліком залишається можливість передачі картки іншій особі або її клонування, що стимулює перехід до біометричних методів ідентифікації.

1.1.3. Особливості застосування методів розпізнавання обличчя у системах контролю доступу. Широке розповсюдження набули технології розпізнавання обличчя наприклад в роботах [21] описані системи які забезпечують високу пропускну здатність і достовірність розпізнавання завдяки використанню сучасних алгоритмів.

Сучасні алгоритми комп'ютерного зору дозволяють виконувати детекцію та розпізнавання обличчя у відеопотоці в реальному часі. Цей процес включає кілька етапів:

- детекція обличчя, яка полягає у виділенні області обличчя на зображенні та відсіюванні фону;

– вирівнювання та нормалізація, що передбачає геометричну трансформацію зображення для компенсації кута нахилу голови, масштабування та корекцію яскравості;

– екстракція ознак, під час якої формується унікальний числовий вектор, що описує біометричні параметри обличчя;

– порівняння, яке полягає у розрахунку метричної відстані між отриманим вектором та еталонами з бази даних.

В роботі [8] для реалізації цих етапів використовуються мережі, які демонструють високу точність за умов достатнього освітлення та фронтального ракурсу зйомки. Застосування спеціалізованих камер, наприклад модуля Pi Camera, дозволяє інтегрувати функцію розпізнавання обличчя у компактні вбудовані системи.

Проте ефективність даного методу суттєво залежить від умов освітлення як це показано в роботі [6]. Недостатня освітленість, наявність глибоких тіней або засвічення камери прямими променями світла можуть унеможливити коректну детекцію обличчя. Крім того, на точність розпізнавання впливають такі фактори, як наявність масок, окулярів, зміни у зачісці або вікові зміни. Для подолання цих обмежень в адаптивних системах застосовується логіка перемикання на альтернативні методи ідентифікації при виявленні низького рівня освітленості.

1.1.4. Аналіз методів голосової ідентифікації та їх застосування в охоронних системах. В роботі [4] розглянуто метод голосової ідентифікації, який базується на аналізі унікальних акустичних характеристик голосу людини, які обумовлені анатомічною будовою її мовного апарату. Цей метод є зручним для користувача та не вимагає фізичного контакту зі зчитувальним пристроєм.

Системи голосової автентифікації поділяються на текстозалежні та текстонезалежні. У системах контролю доступу частіше використовуються текстозалежні методи, які вимагають від користувача вимовити заздалегідь визначену кодову фразу. Це додає рівень захисту від відтворення записаного голосу, оскільки система може запросити вимову випадкової комбінації слів.

Процес обробки голосового сигналу зазвичай включає попередню фільтрацію шумів, виділення активних ділянок мовлення та спектральний аналіз. Ключовим етапом є виділення мел-кепстральних коефіцієнтів, які формують так званий "голосовий відбиток" користувача. Порівняння отриманого зразка з еталоном здійснюється методами динамічної трансформації часової шкали або за допомогою імовірнісних моделей, таких як приховані марковські моделі або моделі сумішей Гауса.

Апаратна реалізація таких систем передбачає використання чутливих мікрофонів та цифрових сигнальних процесорів або мікрокомп'ютерів для обробки аудіопотоку як це описано в роботах [37]. Основною проблемою голосової ідентифікації є висока чутливість до акустичного шуму. Сторонні звуки, розмови інших людей або виробничий шум можуть спотворити корисний сигнал який не завжди може бути відфільтрований з використанням сучасних алгоритмів [10] та призвести до помилки ідентифікації. Тому аналіз рівня фонового шуму є необхідною умовою для прийняття рішення про доцільність використання цього методу в конкретний момент часу.

1.1.5. Дактилоскопічні методи ідентифікації та типи сканерів відбитків пальців. Ідентифікація за відбитками пальців є одним із найстаріших та найбільш поширених біометричних методів. Результати досліджень такого методу наведено в роботах [16]. Унікальність папілярного візерунка пальця людини забезпечує високу достовірність ідентифікації. Метод базується на аналізі розташування характерних точок, таких як закінчення ліній, розгалуження, центри петель та дельти.

Для отримання цифрового образу відбитка пальця використовуються різні типи сканерів, серед яких найбільш поширеними є оптичні, ємнісні та ультразвукові. Оптичні сенсори працюють за принципом порушеного повного внутрішнього відбиття. Палець освітлюється джерелом світла, і відбите від поверхні пальця світло фіксується матрицею. Гребені папілярного візерунка, що торкаються поверхні призми, поглинають або розсіюють світло інакше, ніж западини, що дозволяє сформувати контрастне зображення.

Оптичні сканери, такі як моделі серії R307/AS608, набули значного поширення завдяки своїй надійності, довговічності та відносно низькій вартості[4]. Вони забезпечують достатню роздільну здатність для виділення дрібних деталей візерунка та мають стандартні інтерфейси для підключення до контролерів.

Однак, як показано в [21] робота оптичних сканерів суттєво залежить від стану поверхні шкіри пальця та умов навколишнього середовища. Низька температура повітря може спричинити звуження капілярів та сухість шкіри, що погіршує контакт із поверхнею сканера та знижує якість зображення. Забруднення поверхні сканера або надмірна вологість також негативно впливають на результат зчитування. Саме тому в адаптивних системах контролю доступу необхідно враховувати температурні показники при виборі дактилоскопічного методу як основного засобу ідентифікації.

Узагальнюючи огляд технологій, можна стверджувати, що жоден із розглянутих методів не є універсальним та ідеальним для будь-яких умов експлуатації. Кожна технологія має свої сильні та слабкі сторони, які проявляються залежно від зовнішніх факторів. Це підтверджує доцільність створення мультимодальних систем, які здатні динамічно адаптуватися до поточної ситуації, обираючи найбільш надійний у даний момент метод автентифікації.

1.2. Дослідження впливу дестабілізуючих факторів на надійність біометричних систем

1.2.1. Аналіз впливу рівня освітленості на ефективність роботи оптичних сенсорів та камер.

Ефективність функціонування будь-якої біометричної системи контролю доступу безпосередньо залежить від якості вхідних даних, що надходять від сенсорів та зчитувачів.

У лабораторних умовах, де параметри навколишнього середовища є стабільними та контрольованими, сучасні алгоритми розпізнавання демонструють високі показники точності. Проте в умовах реальної експлуатації на прохідних промислових підприємств, офісних центрів або відкритих

майданчиках на процес ідентифікації впливає низка дестабілізуючих факторів. До найбільш критичних з них належать рівень освітленості, акустичний шум та температурний режим, які здатні суттєво спотворити біометричні ознаки та призвести до помилок першого та другого роду.

Освітленість є ключовим фактором, що визначає якість роботи систем розпізнавання обличчя та, меншою мірою, оптичних сканерів відбитків пальців. Алгоритми комп'ютерного зору базуються на аналізі піксельних даних цифрового зображення, тому недостатня або надмірна кількість світла призводить до втрати інформативності кадру.

При низькому рівні освітленості, що становить менше 50 люкс, матриця камери генерує значну кількість цифрового шуму. Цей шум спотворює контури обличчя та дрібні деталі, такі як форма очей, носа або губ, які є критично важливими для формування біометричного шаблону. Алгоритми детекції обличчя, наприклад каскади Хаара або згорткові нейронні мережі, можуть не розпізнати наявність обличчя в кадрі, що унеможливлює подальшу ідентифікацію. Крім того, в умовах темряви збільшується час експозиції камери, що при русі об'єкта призводить до ефекту розмиття зображення.

Проблема надмірної освітленості або контрастного освітлення є не менш серйозною. Пряме сонячне світло або яскраве штучне освітлення, спрямоване в об'єктив камери, викликає засвічення частини кадру та втрату деталей у світлих ділянках. Бокове освітлення створює глибокі тіні на обличчі, що змінює його геометричне сприйняття алгоритмом. Наприклад, тінь від носа може бути інтерпретована як зміна форми обличчя, що призводить до зниження коефіцієнта збігу з еталоном.

Графік залежності ймовірності успішного розпізнавання обличчя від рівня освітленості наведено на рис. 1.3.

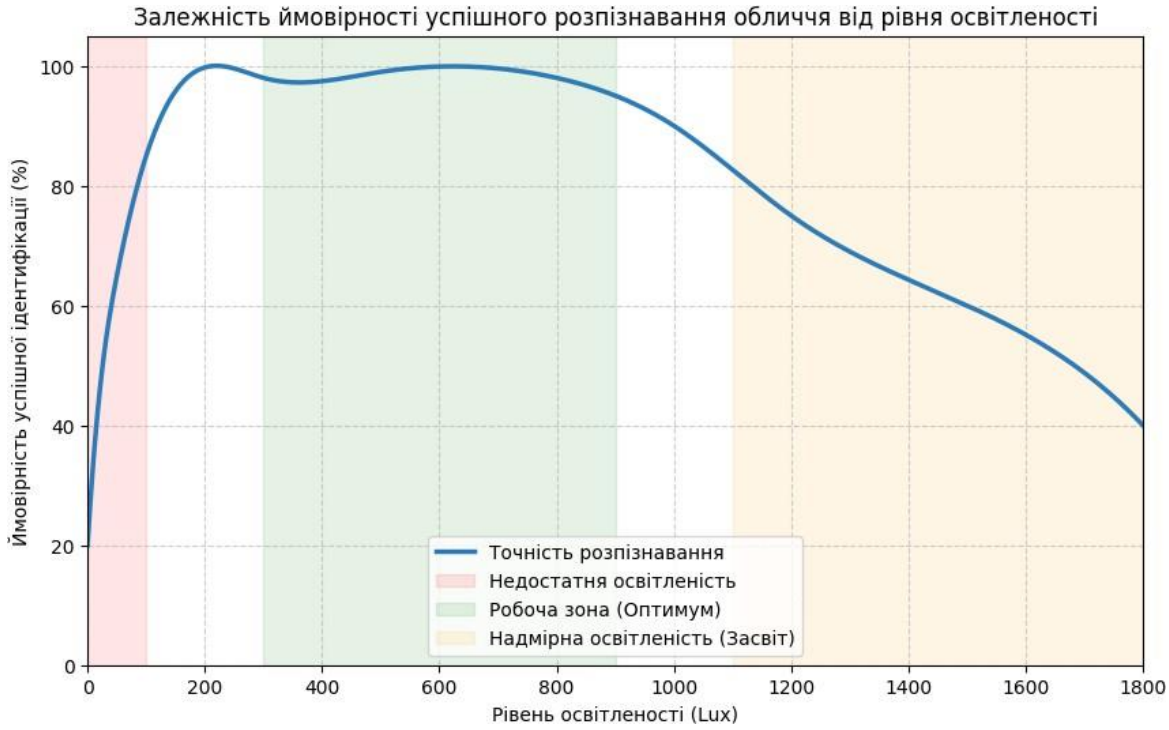

Рис. 1.3. Залежність точності розпізнавання обличчя від рівня освітленості

Як видно з графіка, існує певний діапазон оптимальної освітленості, зазвичай від 300 до 800 люкс, в межах якого система працює з максимальною ефективністю. Вихід за межі цього діапазону вимагає або застосування додаткового апаратного забезпечення, такого як інфрачервона підсвітка, або перемикання на альтернативний метод ідентифікації.

1.2.2. Оцінка впливу акустичного шуму на точність систем голосової автентифікації. Системи голосової ідентифікації базуються на обробці акустичного сигналу та виділенні з нього унікальних характеристик голосу користувача.

Основним показником якості вхідного аудіосигналу виступає співвідношення сигнал-шум SNR [7] яке визначає перевищення рівня корисного сигналу над рівнем фонового шуму.

У реальних умовах експлуатації джерела акустичного шуму мають різну природу та спектральний склад. Це може бути стаціонарний шум від роботи вентиляційних систем або серверного обладнання, нестаціонарний шум від проїжджаючого транспорту, або так званий "мовний шум", що утворюється

розмовами інших людей. Останній тип шуму є найбільш складним для фільтрації, оскільки його частотні характеристики збігаються з корисним сигналом.

Вплив шуму на процес ідентифікації проявляється у спотворенні спектральних ознак мови, зокрема мел-кепстральних коефіцієнтів. Високий рівень фонового шуму маскує форманти голосу, що ускладнює роботу алгоритмів порівняння з еталоном. При рівні шуму понад 80 дБ, що відповідає гучній розмові або шуму вулиці, ймовірність помилкової відмови у доступі стрімко зростає.

Крім прямого впливу на сигнал, шум впливає і на поведінку самого користувача. В умовах підвищеного шуму людина рефлекторно підвищує голос, змінюючи його інтонацію, тембр та артикуляцію. Це явище відоме як ефект Ломбарда [3]. Оскільки еталонний запис голосу зазвичай створюється в тихих умовах, зміна характеристик голосу під впливом ефекту Ломбарда призводить до розбіжності між поточним зразком та шаблоном у базі даних.

Ілюстрація впливу шуму на спектрограму мовного сигналу наведена на рис. 1.4.

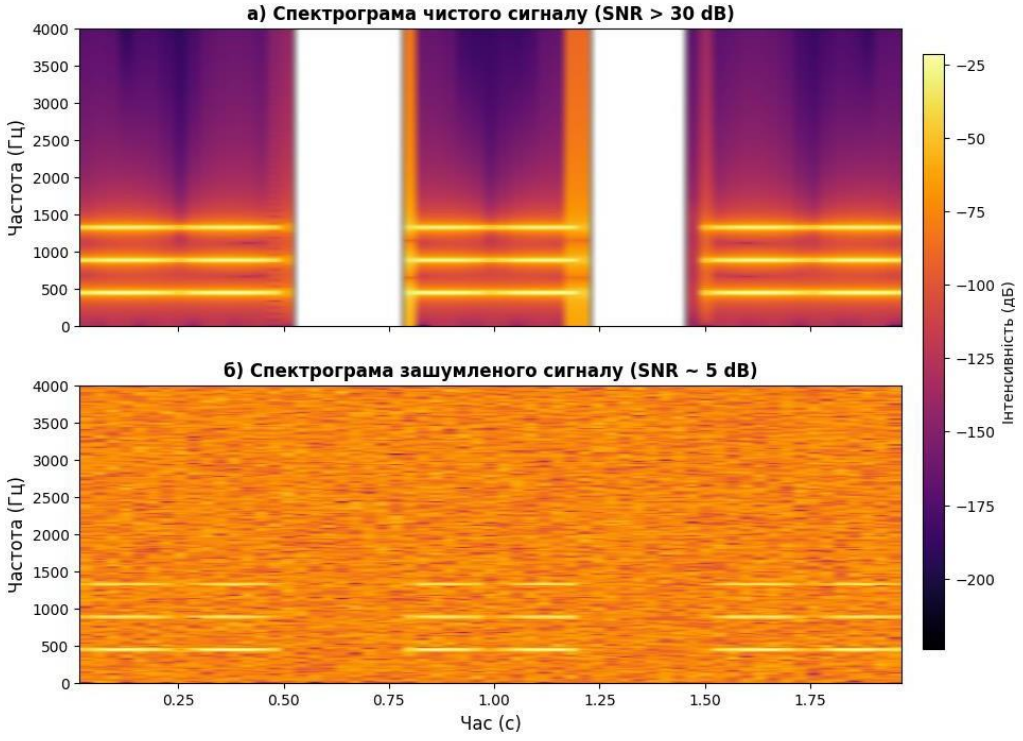

Рис. 1.4. Порівняння спектрограм чистого та зашумленого мовного сигналу

Для забезпечення надійної роботи системи голосової ідентифікації необхідно здійснювати постійний моніторинг рівня акустичного шуму та блокувати спроби автентифікації в моменти пікових шумових навантажень.

1.2.3. Залежність роботи контактних сканерів від температурних режимів.

Температура навколишнього середовища має опосередкований, але суттєвий вплив на роботу контактних біометричних сканерів, зокрема дактилоскопічних сенсорів. В роботі [11] показано що цей вплив призводить до зміни фізіологічного стану шкіри пальця користувача. Низькі температури повітря, особливо в діапазоні нижче нуля градусів Цельсія, викликають звуження капілярів та зменшення вологості шкірних покривів. Суха шкіра має низьку еластичність та поганий контакт з поверхнею призми оптичного сканера. Це призводить до того, що на отриманому зображенні папілярні лінії виглядають переривчастими, а контрастність зображення знижується. У критичних випадках сухий палець може взагалі не ініціювати процес сканування, оскільки сенсор не зможе детестувати дотик.

Високі температури, навпаки, стимулюють потовиділення. Надмірна волога на поверхні пальця заповнює проміжки між папілярними лініями, що на зображенні виглядає як злиття ліній в суцільні плями. Це унеможливлює виділення характерних точок візерунка та призводить до помилок розпізнавання.

Окрім впливу на біологічний об'єкт, температура впливає і на електронні компоненти самого сканера. Екстремальні температури можуть змінювати чутливість матриці сенсора або викликати появу конденсату на оптичних поверхнях при різкій зміні температурного режиму. Тому при розробці адаптивних систем контролю доступу показник температури повітря виступає важливим критерієм для визначення доцільності використання контактних методів ідентифікації.

1.2.4. Проблематика використання статичних алгоритмів ідентифікації в динамічному середовищі. Аналіз принципів функціонування класичних систем контролю доступу в роботах [19] свідчить про широке застосування статичних алгоритмів прийняття рішень. Даний підхід передбачає використання фіксованих порогових значень коефіцієнтів подібності, які встановлюються на етапі інсталяції та налаштування обладнання. Ефективність таких систем гарантується лише за умови стабільності зовнішніх факторів, що рідко досягається в реальних умовах експлуатації.

В умовах динамічного середовища, що характеризується стохастичними змінами освітленості, акустичного фону та температури, використання фіксованих порогів призводить до порушення балансу між захищеністю об'єкта та зручністю користування системою. Встановлення завищеного порогу прийняття рішення з метою підвищення безпеки при погіршенні зовнішніх умов неминуче призводить до зростання ймовірності помилкової відмови у доступі. Це спричиняє необхідність повторних спроб ідентифікації, зниження пропускної здатності точки проходу та викликає дискомфорт у легітимних користувачів. Натомість зниження порогового значення для покращення ергономічних показників підвищує ймовірність помилкового допуску, роблячи систему вразливою до атак підробки біометричних даних (Presentation Attack).

Критичним недоліком статичних архітектур є відсутність механізмів попередньої валідації умов середовища. Система ініціює ресурсомісткі процедури захоплення та обробки біометричних даних навіть у тих випадках, коли фізичні умови роблять успішну ідентифікацію апріорі неможливою. Такий алгоритм роботи призводить до нераціонального використання обчислювальних ресурсів контролера та збільшення часу реакції системи.

Вирішенням цієї проблеми виступає впровадження адаптивних алгоритмів, здатних оцінювати поточний стан середовища та гнучко змінювати стратегію автентифікації. Такі алгоритми повинні:

– здійснювати попередній аналіз умов за допомогою сенсорів освітленості, шуму та температури;

- розраховувати коефіцієнт придатності для кожного доступного методу ідентифікації в реальному часі;
- автоматично обирати метод, який забезпечує найвищу ймовірність успішної та безпечної ідентифікації в даних умовах;
- ініціювати перехід на резервні методи, такі як RFID-картки, у випадку критичних значень параметрів середовища.

Реалізація такого підходу вимагає застосування математичного апарату, здатного працювати з нечіткими та неповними даними, оскільки межі між "хорошими" та "поганими" умовами часто є розмитими. Саме тому використання нечіткої логіки є перспективним напрямком у розробці інтелектуальних контролерів доступу нового покоління.

1.3 Обґрунтування вибору методів та засобів реалізації адаптивної системи

1.3.1. Аналіз методів адаптивного управління та прийняття рішень в умовах невизначеності. Створення ефективної системи адаптивного контролю доступу вимагає комплексного підходу до вибору як математичного апарату для прийняття рішень [42]

Головним критерієм вибору виступає здатність системи функціонувати в реальному часі та забезпечувати високу надійність в умовах невизначеності вхідних даних.

Традиційні алгоритми управління в системах безпеки базуються на чіткій булевій логіці, де параметри середовища порівнюються з фіксованими пороговими значеннями [29]. Такий підхід є ефективним лише у стабільних умовах, проте він втрачає гнучкість при роботі з нечіткими або зашумленими даними. Наприклад, незначне перевищення порогового значення рівня шуму може призвести до повного відключення голосової ідентифікації, хоча фактичні умови ще дозволяли б її використання.

Для вирішення задач управління в умовах невизначеності доцільно використовувати методи обчислювального інтелекту, до яких належать нейронні мережі та нечітка логіка. Нейронні мережі забезпечують високу точність

класифікації ситуацій, але потребують значних обчислювальних ресурсів для навчання та великих наборів навчальних даних, що ускладнює їх реалізацію на вбудованих пристроях з обмеженою продуктивністю.

Натомість нечітка логіка дозволяє формалізувати експертні знання про предметну область у вигляді лінгвістичних правил. Вона оперує поняттями природної мови, що спрощує процес налаштування системи та інтерпретації результатів прийняття рішень. Використання нечітких множин дозволяє уникнути різких перемикань режимів роботи системи на межах діапазонів, забезпечуючи плавну адаптацію до змін навколишнього середовища. Враховуючи необхідність обробки різнорідних даних від сенсорів та обмежені ресурси контролера, метод нечіткого виводу є найбільш оптимальним для реалізації ядра прийняття рішень в адаптивній системі контролю доступу.

1.3.2. Застосування апарату нечіткої логіки для мультифакторної автентифікації. Для реалізації алгоритму адаптивного вибору методу ідентифікації доцільно використати систему нечіткого виводу типу Мамдані, яка описана в роботах [28]. Цей тип систем характеризується використанням функцій належності для вхідних та вихідних змінних, а також логічних правил у формі «ЯКЩО-ТО», що дозволяє точно описати нелінійні залежності між станом середовища та ефективністю біометричних сканерів.

Процес функціонування нечіткого контролера включає етапи фазифікації, агрегації, активізації та дефазифікації. На етапі фазифікації чіткі значення від сенсорів перетворюються у лінгвістичні змінні. Вхідними змінними моделі виступають рівень освітленості, рівень акустичного шуму та температура повітря. База правил формується на основі аналізу фізичних обмежень кожного методу ідентифікації. Наприклад, правило може визначати, що при низькому рівні освітленості придатність методу розпізнавання обличчя є низькою.

Результатом роботи алгоритму є коефіцієнт придатності для кожного доступного методу автентифікації, який визначається на етапі дефазифікації методом центру тяжіння. Це дозволяє системі динамічно ранжувати методи від найбільш до найменш пріоритетного та пропонувати користувачеві оптимальний

варіант проходу. Такий підхід забезпечує компроміс між безпекою та зручністю користування системою.

1.3.3. Порівняльний аналіз одноплатних мікрокомп’ютерів для обробки біометричних даних. Реалізація функцій комп'ютерного зору та нечіткого виводу висуває підвищені вимоги до обчислювальної потужності контролера. Класичні мікроконтролери, такі як Arduino або STM32, мають обмежену тактову частоту та обсяг оперативної пам'яті, що унеможливлює обробку відеопотоку в реальному часі.

Тому для побудови інтелектуального контролера необхідно використовувати одноплатні мікрокомп'ютери, що працюють під управлінням повноцінної операційної системи.

Серед доступних на ринку рішень найбільш поширеними є платформи Raspberry Pi, Orange Pi та NVIDIA Jetson. Платформа NVIDIA Jetson орієнтована на задачі штучного інтелекту та має потужний графічний процесор, але її вартість є значно вищою, що знижує економічну доцільність для масового впровадження. Плати Orange Pi пропонують хороше співвідношення ціни та продуктивності, проте часто мають проблеми з програмною підтримкою та стабільністю драйверів.

Оптимальним вибором для реалізації системи є мікрокомп'ютер Raspberry Pi 3 B+. Він оснащений чотириядерним процесором з архітектурою ARM Cortex-A53, має 1 ГБ оперативної пам'яті та розвинену периферію. Наявність інтерфейсу CSI дозволяє підключати камеру безпосередньо до процесора, що зменшує затримки при передачі зображення. Підтримка операційної системи Linux дає змогу використовувати потужні бібліотеки для комп'ютерного зору OpenCV та обчислень scikit-fuzzy, а наявність портів GPIO забезпечує легку інтеграцію з сенсорами та виконавчими механізмами.

1.3.4. Вибір сенсорного забезпечення для моніторингу параметрів навколишнього середовища. Для отримання достовірних даних про стан навколишнього середовища система повинна бути оснащена набором спеціалізованих сенсорів. Вибір конкретних моделей датчиків здійснювався з урахуванням критеріїв точності, інтерфейсів підключення та сумісності з обраною обчислювальною платформою.

Вимірювання рівня освітленості покладено на цифровий сенсор BH1750. Цей модуль має широкий діапазон вимірювання від 1 до 65535 люкс та використовує інтерфейс I2C, що спрощує його підключення до мікрокомп'ютера. Висока спектральна чутливість сенсора, наближена до чутливості людського ока, дозволяє отримувати коректні дані незалежно від типу джерела світла.

Для контролю кліматичних параметрів обрано датчик DHT22, також відомий як AM2302. Він забезпечує вимірювання температури в діапазоні від - 40 до + 80 градусів Цельсія з похибкою не більше 0,5 градуса. Цей сенсор використовує цифровий протокол передачі даних, що забезпечує високу завадостійкість сигналу при передачі на значні відстані.

Аналіз акустичного фону реалізується за допомогою USB-мікрофона, підключеного безпосередньо до порту мікрокомп'ютера. Це дозволяє використовувати стандартні драйвери операційної системи для захоплення аудіопотоку та його подальшої цифрової обробки для визначення рівня шуму в децибелах. Додатково до складу системи включено датчик газу MQ-2 для виявлення задимлення, що дозволяє реалізувати функцію аварійного розблокування дверей у випадку пожежі.

1.4. Висновки до розділу

У першому розділі кваліфікаційної роботи проведено детальний аналіз сучасного стану та проблематики систем контролю та управління доступом. Встановлено, що існуючі біометричні методи ідентифікації мають суттєву залежність від умов навколишнього середовища. Недостатня освітленість, високий рівень шуму або екстремальні температури призводять до різкого

зниження надійності розпізнавання, що створює загрози безпеці об'єкта або спричиняє незручності для користувачів.

Аналіз методів управління показав, що статичні алгоритми не здатні ефективно працювати в динамічному середовищі. Обґрунтовано доцільність використання адаптивного підходу, який базується на теорії нечіткої логіки. Це дозволить системі автоматично оцінювати придатність кожного методу ідентифікації та обирати оптимальний варіант у режимі реального часу. Аналіз методів ідентифікації зображений на табл. 1.1

Таблиця 1.1

Порівняльний аналіз методів ідентифікації

Функціональна характеристика	RFID	Face ID	Voice ID	Touch ID	СКУД
Незалежність від рівня освітленості	+	-	+	+	+
Незалежність від акустичного шуму	+	+	-	+	+
Незалежність від температури середовища	+	+	+	-	+
Захист від передачі ідентифікатора іншій особі	-	+	+	+	+
Безконтактний спосіб зчитування	+	+	+	-	+
Автоматична адаптація до зміни зовнішніх умов	-	-	-	-	+
Забезпечення доступу при відмові одного з сенсорів	-	-	-	-	+

Дані таблиці демонструють, що кожен з окремих методів має критичні вразливості до певних факторів середовища. Водночас запропонована адаптивна система, завдяки інтеграції цих технологій та використанню логіки динамічного вибору, дозволяє нівелювати недоліки окремих сенсорів та забезпечити відповідність усім критеріям надійності незалежно від зовнішніх умов.

Для реалізації системи обрано апаратну платформу на базі одноплатного комп'ютера Raspberry Pi 3 B+, яка забезпечує необхідну обчислювальну потужність для роботи алгоритмів комп'ютерного зору та нечіткого виводу. Визначено набір сенсорів для моніторингу параметрів середовища, який включає датчики освітленості BH1750, температури DHT22 та мікрофон для аналізу шуму. Запропонована архітектура та алгоритмічне забезпечення створюють основу для розробки надійної адаптивної системи контролю доступу.

РОЗДІЛ 2
ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ АДАПТИВНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ З ВИКОРИСТАННЯМ НЕЧІТКОЇ ЛОГІКИ

2.1. Математичне моделювання процесу прийняття рішень у системі контролю доступу

2.1.1. Формалізація задачі вибору методу ідентифікації в умовах невизначеності.

Розробка адаптивної системи контролю доступу вимагає створення формальної математичної моделі, яка здатна описувати залежність ефективності методів біометричної ідентифікації від дестабілізуючих факторів навколишнього середовища. Оскільки параметри середовища мають безперервний та часто непередбачуваний характер, використання класичної булевої логіки є недостатнім для забезпечення плавної адаптації системи. Тому в основу моделювання покладено теорію нечітких множин, яка дозволяє оперувати лінгвістичними змінними та експертними знаннями для прийняття рішень в умовах невизначеності.

Задачу вибору оптимального методу ідентифікації можна сформулювати як пошук відображення вектора вхідних параметрів стану навколишнього середовища у вектор вихідних оцінок придатності доступних методів автентифікації.

Нехай E є множиною вхідних параметрів, що характеризують поточний стан середовища у зоні проходу. Згідно з технічною документацією система здійснює моніторинг трьох ключових параметрів, тому вхідний вектор можна представити формулою:

$$E = \{L, N, T\}, \tag{2.1}$$

де E – множина вхідних лінгвістичних змінних;

L – рівень освітленості, виміряний у люксах;

N – рівень акустичного шуму в децибелах;

T – температура навколишнього середовища у градусах Цельсія.

Кожен з параметрів визначений у своєму діапазоні допустимих значень. Для освітленості L область визначення становить інтервал від 0 до 1000 Люкс. Рівень шуму N визначено на проміжку від 0 до 100 дБ. Температурний показник T змінюється в межах від -20 до +50 градусів Цельсія.

Вихідною множиною S виступає вектор оцінок придатності для кожного з наявних у системі біометричних методів ідентифікації. Оскільки система підтримує розпізнавання за обличчям, голосом та відбитком пальця, вихідний вектор описується виразом:

$$S = \{S_{face}, S_{voice}, S_{finger}\}, \tag{2.2}$$

де S – множина вихідних лінгвістичних змінних;

S_{face} – коефіцієнт придатності методу розпізнавання обличчя;

S_{voice} – коефіцієнт придатності методу голосової ідентифікації;

S_{finger} – коефіцієнт придатності методу сканування відбитків пальців.

Значення кожного коефіцієнта належить безперервному інтервалу від 0 до 10, де 0 означає повну неможливість використання методу, а 10 свідчить про ідеальні умови для його застосування.

Основною задачею математичного моделювання є побудова функціонального відображення F, яке ставить у відповідність вектору вхідних умов E вектор вихідних пріоритетів S, що наведено у формулі:

$$S = F(E). \tag{2.3}$$

Враховуючи нелінійний характер залежностей та наявність перехресного впливу параметрів, аналітичний опис функції F у вигляді системи диференціальних або алгебраїчних рівнянь є надмірно складним та неефективним для реалізації на вбудованих системах. Тому для апроксимації цієї

функції доцільно використати систему нечіткого виводу, яка дозволяє описати поведінку системи набором евристичних правил.

Процес прийняття рішення системою можна представити як послідовність етапів, що включають вимірювання фізичних величин сенсорами, фазифікацію отриманих чітких значень, агрегацію та активізацію правил бази знань. Завершальними етапами є акумуляція результатів виводу та дефазифікація отриманих нечітких множин для знаходження чітких значень вихідного вектора S. Отримані результати дозволяють ранжувати методи за значенням коефіцієнта та обирати метод з максимальним показником.

2.1.2. Обґрунтування вибору алгоритму Мамдані для реалізації інтелектуального ядра системи. Серед існуючих алгоритмів нечіткого виводу найбільш поширеними є алгоритми Мамдані та Сугено [44]. Вибір конкретного алгоритму визначається специфікою задачі, вимогами до точності моделювання та обчислювальною складністю. Для розроблюваної адаптивної системи контролю доступу обрано алгоритм Мамдані, що зумовлено їх здатністю описувати базу знань зрозумілою природною мовою через правила «ЯКЩО-ТО», високою гнучкістю моделювання нелінійних залежностей та прозорістю процесу прийняття рішень, що спрощує налаштування системи.

Головною перевагою алгоритму Мамдані виступає його інтуїтивна зрозумілість та здатність працювати з лінгвістичними змінними як у вхідних, так і у вихідних параметрах. База правил у такій системі формується природною мовою, що дозволяє безпосередньо імплементувати експертні знання про фізичні обмеження біометрії. Наприклад, залежність може бути описана правилом, згідно з яким низька освітленість призводить до неприйнятної придатності розпізнавання обличчя. Така структура правила повністю відповідає логіці виводу Мамдані.

На відміну від алгоритму Сугено, де вихідні змінні задаються лінійною функцією або константою, алгоритм Мамдані використовує нечіткі множини для вихідних змінних. Це забезпечує більш плавний перехід між станами системи та дозволяє точніше моделювати нелінійні процеси прийняття рішень. У контексті

системи безпеки це дозволяє уникнути ситуацій, коли незначна зміна вхідного параметра призводить до різкої та необґрунтованої зміни пріоритетного методу доступу.

Процес отримання чіткого значення на виході системи, який називається дефазифікацією, у моделі Мамдані реалізується методом центру тяжіння який описаний в [44].

Цей метод розраховує абсцису центру ваги площі, обмеженої функцією належності результуючої нечіткої множини. Математично це виражається формулою:

$$y = \frac{\int x \cdot \mu(x) dx}{\int \mu(x) dx}, \tag{2.4}$$

де y – результуюче чітке значення вихідної змінної;

x – змінна області міркувань;

$\mu(x)$ – функція належності агрегованої вихідної нечіткої множини;

Використання методу центру тяжіння дозволяє врахувати внесок усіх активних правил бази знань, що підвищує робастність системи до шумів у вхідних даних. Хоча цей метод є більш обчислювально складним порівняно з методами визначення максимуму, обрана апаратна платформа Raspberry Pi 3 B+ володіє достатньою потужністю для виконання необхідних математичних операцій у реальному часі за допомогою спеціалізованих бібліотек, таких як scikit-fuzzy.

Таким чином, використання системи нечіткого виводу типу Мамдані дозволяє створити гнучку та інтерпретовану модель управління доступом, яка здатна ефективно функціонувати в умовах невизначеності та забезпечувати адекватну реакцію системи на зміни параметрів навколишнього середовища.

2.2. Проєктування системи нечіткого виводу для оцінки умов навколишнього середовища

2.2.1. Фазифікація вхідних параметрів освітленості, акустичного шуму та температури.

Ефективність функціонування адаптивної системи контролю доступу безпосередньо залежить від якості налаштування параметрів нечіткого контролера. Процес проєктування системи нечіткого виводу включає етапи визначення лінгвістичних змінних, вибору типів та параметрів функцій належності, а також формування бази продукційних правил, які пов'язують вхідні умови з вихідними рішеннями. Коректна реалізація цих етапів дозволяє забезпечити адекватну реакцію системи на зміни параметрів освітленості, шуму та температури.

Етап фазифікації полягає у перетворенні чітких числових значень, отриманих від сенсорів, у ступені належності до нечітких множин відповідних лінгвістичних змінних. Для кожної вхідної змінної необхідно визначити терм-множину та відповідні функції належності. Аналіз технічної документації та специфіки предметної області дозволив сформувати наступну структуру лінгвістичних змінних.

Лінгвістична змінна «Освітленість» (позначається як L) визначена на універсумі від 0 до 1000 Люкс. Для опису цієї змінної обрано терм-множину, яка описуєтсья виразом:

$$T_L = \{Dark, Dim, Normal, Bright\}, \quad (2.5)$$

Терм Dark відповідає умовам повної темряви або недостатнього освітлення, Dim описує сутінки або тьмяне світло, Normal характеризує нормальне робоче освітлення, а Bright відповідає яскравому або надмірному освітленню. Для математичного опису термів використано трикутні та трапецієподібні функції належності [5].

Аналітичний вираз для трикутної функції належності $(x;\ a,\ b,\ c)$ має вигляд (2.5).

$$\mu(x;a,b,c) = \begin{cases} 0, & x \le a \\ \frac{x-a}{b-a}, & a < x \le b \\ \frac{c-x}{c-b}, & b < x < c \\ 0, & x \ge c \end{cases}, \tag{2.6}$$

де *a, b, c* є числовими параметрами, що визначають координати вершин трикутника;

x — вхідне значення змінної.

Для терма *Dark* використано трикутну функцію з параметрами [0, 0, 150], що означає максимальний ступінь належності при 0 Люкс та його лінійне спадання до 0 при 150 Люкс. Терм *Dim* описується трикутною функцією з координатами [100, 300, 500], а Normal відповідає параметрам [400, 600, 800]. Для терма *Bright* доцільно використати трапецієподібну функцію, оскільки висока надійність розпізнавання зберігається у широкому діапазоні високої освітленості. Трапецієподібна функція (x; a, b, c, d) описується виразом (2.6):

$$\mu(x;a,b,c,d) = \begin{cases} 0, & x \le a \\ \frac{x-a}{b-a}, & a < x \le b \\ 1, & b < x < c \\ \frac{d-x}{d-c}, & c < x < d \\ 0, & x \ge d \end{cases}, \tag{2.7}$$

Для терма Bright встановлено параметри [700, 900, 1000, 1000]. Графічне представлення функцій належності для змінної «Освітленість» наведено на рис. 2.1.

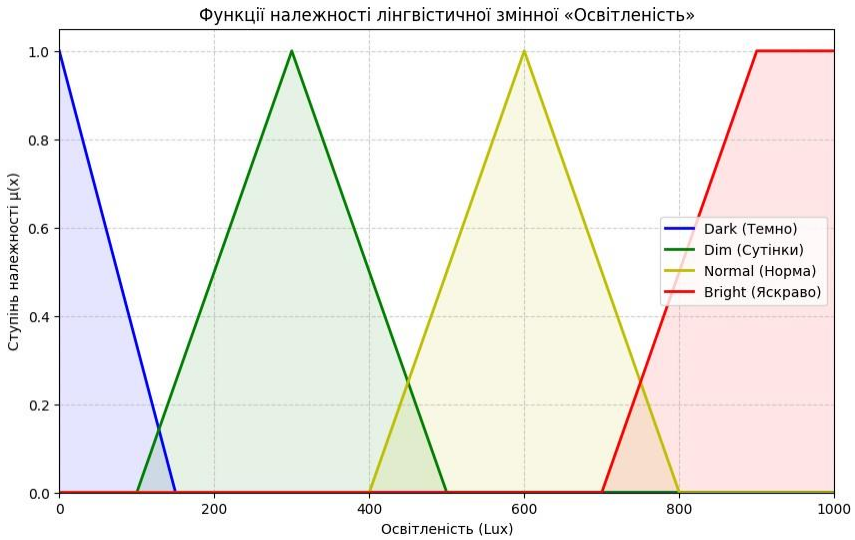

Рис. 2.1. Графік функцій належності лінгвістичної змінної «Освітленість»

Лінгвістична змінна «Акустичний шум» (N) визначена на інтервалі від 0 до 100 дБ. Терм-множина включає значення:

$$T_N = \{Silent, Moderate, Loud, VeryHigh\}. \quad (2.8)$$

Терм Silent задано трикутною функцією на інтервалі [0, 0, 30], що відповідає тиші. Moderate описує помірний шум у діапазоні [20, 50, 70]. Loud характеризує гучний шум з параметрами [60, 80, 90]. Для критичного рівня шуму VeryHigh використано трапецієподібну функцію [85, 95, 100, 100], що дозволяє врахувати насичення сенсора.

Змінна «Температура» (T) розглядається в діапазоні від -20 до +50 градусів Цельсія. Вона описується трьома термами:

$$T_T = \{Freezing, Comfortable, Hot\}. \quad (2.9)$$

Терм Freezing відповідає низьким температурам і описується трапецієподібною функцією [-20, -20, 0, 10]. Comfortable визначає комфортний діапазон для роботи сканерів відбитків пальців і задається трикутною функцією [5, 22, 35]. Терм Hot відповідає високим температурам і описується функцією [30, 40, 50, 50].

2.2.2. Формування бази знань та нечітких продукційних правил. Ядром системи нечіткого виводу виступає база знань, яка містить набір правил, що формалізують експертні знання про залежність якості біометричної ідентифікації від умов середовища. Правила мають структуру «ЯКЩО <умова>, ТО <висновок>», де умова може бути складеним логічним виразом із використанням операторів AND (і), OR (або) та NOT (ні).

Для розроблюваної системи сформовано набір правил, які поділяються на обмежувальні та дозвільні. Обмежувальні правила описують ситуації, коли використання певного методу є неможливим або небажаним через фізичні обмеження технології. Дозвільні правила визначають умови, сприятливі для застосування методів.

Матриця правил бази знань для системи адаптивного контролю доступу наведена в табл. 2.1.

Таблиця 2.1

База правил системи нечіткого виводу

№	Умова (IF)	Оператор	Висновок (THEN)
1	Light is Dark	-	Face Suitability is Unusable
2	Noise is Loud	OR	Voice Suitability is Low
3	Noise is VeryHigh	OR	Voice Suitability is Low
4	Temp is Freezing	OR	Fingerprint Suitability is Low
5	Temp is Hot	OR	Fingerprint Suitability is Low
6	Light is Normal	OR	Face Suitability is High
7	Light is Bright	OR	Face Suitability is High
8	Noise is Silent	OR	Voice Suitability is High
9	Noise is Moderate	OR	Voice Suitability is High
10	Temp is Comfortable	-	Fingerprint Suitability is High

При реалізації механізму логічного виводу для операції OR (диз'юнкція) використано метод максимуму, а для операції AND (кон'юнкція), метод мінімуму. Це означає, що ступінь істинності висновку правила визначається максимальним або мінімальним значенням ступенів належності вхідних змінних відповідно. Отримані в результаті активізації правил усічені нечіткі множини агрегуються в єдину результуючу множину для кожної вихідної змінної.

2.2.3. Методи дефазифікації та інтерпретація вихідних коефіцієнтів придатності. Останнім етапом роботи нечіткого контролера є дефазифікація, метою якої виступає отримання чіткого числового значення вихідної змінної на основі агрегованої нечіткої множини. Для кожної з трьох вихідних змінних (Suitability_face, Suitability_voice, Suitability_finger) визначено універсум від 0 до 10.

Вихідні змінні описуються трьома термами:

– Unusable (непридатний),
– Low (низька придатність),
– High (висока придатність).

Терм Unusable задано функцією належності [0, 0, 3], Low [2, 4, 6], a High [6, 8, 10, 10]. Така структура дозволяє чітко розділити методи на категорії за пріоритетністю.

Для дефазифікації у розробленій системі застосовано метод центру тяжіння (Centroid). Цей метод забезпечує найбільш точне врахування внеску всіх активних правил і дозволяє отримати плавні зміни вихідного сигналу при незначних коливаннях вхідних даних. Розрахунок проводиться шляхом числового інтегрування площі фігури, утвореної агрегацією вихідних термів.

Результатом роботи модуля нечіткої логіки є набір із трьох дійсних чисел у діапазоні [0..10]. Інтерпретація цих значень здійснюється наступним чином:

– значення в діапазоні 0..3 свідчать про критичні умови, за яких використання методу є неможливим або небезпечним;

– значення в діапазоні 3..6 вказують на можливість використання методу, але з високою ймовірністю помилок або затримок;

– значення в діапазоні 6..10 характеризують оптимальні умови для роботи біометричного сканера.

На основі отриманих оцінок система формує пріоритетний список методів. Метод із найвищим балом обирається як основний для поточної спроби ідентифікації. У випадку, якщо всі методи отримали оцінку нижче критичного порогу (наприклад, менше 3.0), система активує резервний алгоритм доступу за допомогою RFID-картки, ігноруючи біометричні дані.

2.3. Розробка алгоритмічного забезпечення апаратно-програмного комплексу

2.3.1. Обгрунтування алгоритму функціонування системи та взаємодії модулів. Надійність та ефективність функціонування розробленої системи адаптивного контролю доступу визначаються не лише обраною математичною моделлю, але й якістю реалізації керуючих алгоритмів. Програмне забезпечення комплексу базується на принципах модульної архітектури, що дозволяє забезпечити незалежну обробку даних від сенсорів, виконання процедур нечіткого виводу та керування виконавчими механізмами у реальному часі. Алгоритмічна структура системи спроєктована таким чином, щоб гарантувати пріоритетність завдань безпеки над сервісними функціями та забезпечити стабільну роботу пристрою в умовах безперервного циклу експлуатації.

Головний цикл роботи контролера реалізує послідовну обробку подій згідно з визначеними пріоритетами безпеки та логікою обслуговування користувачів.

Схематичне зображення загального алгоритму роботи системи наведено на рис. 2.3. Процес функціонування системи розпочинається з етапу ініціалізації, який відбувається автоматично при подачі живлення на обчислювальний модуль. На цьому етапі відбувається завантаження драйверів периферійних пристроїв,

перевірка працездатності шин передачі даних та встановлення з'єднання з локальною базою даних. Окремим важливим кроком є компіляція ядра нечіткої логіки, під час якої формуються об’єкти лінгвістичних змінних та будується база продукційних правил. У разі успішного завершення всіх діагностичних процедур система переходить у режим очікування та циклічного виконання основного алгоритму.

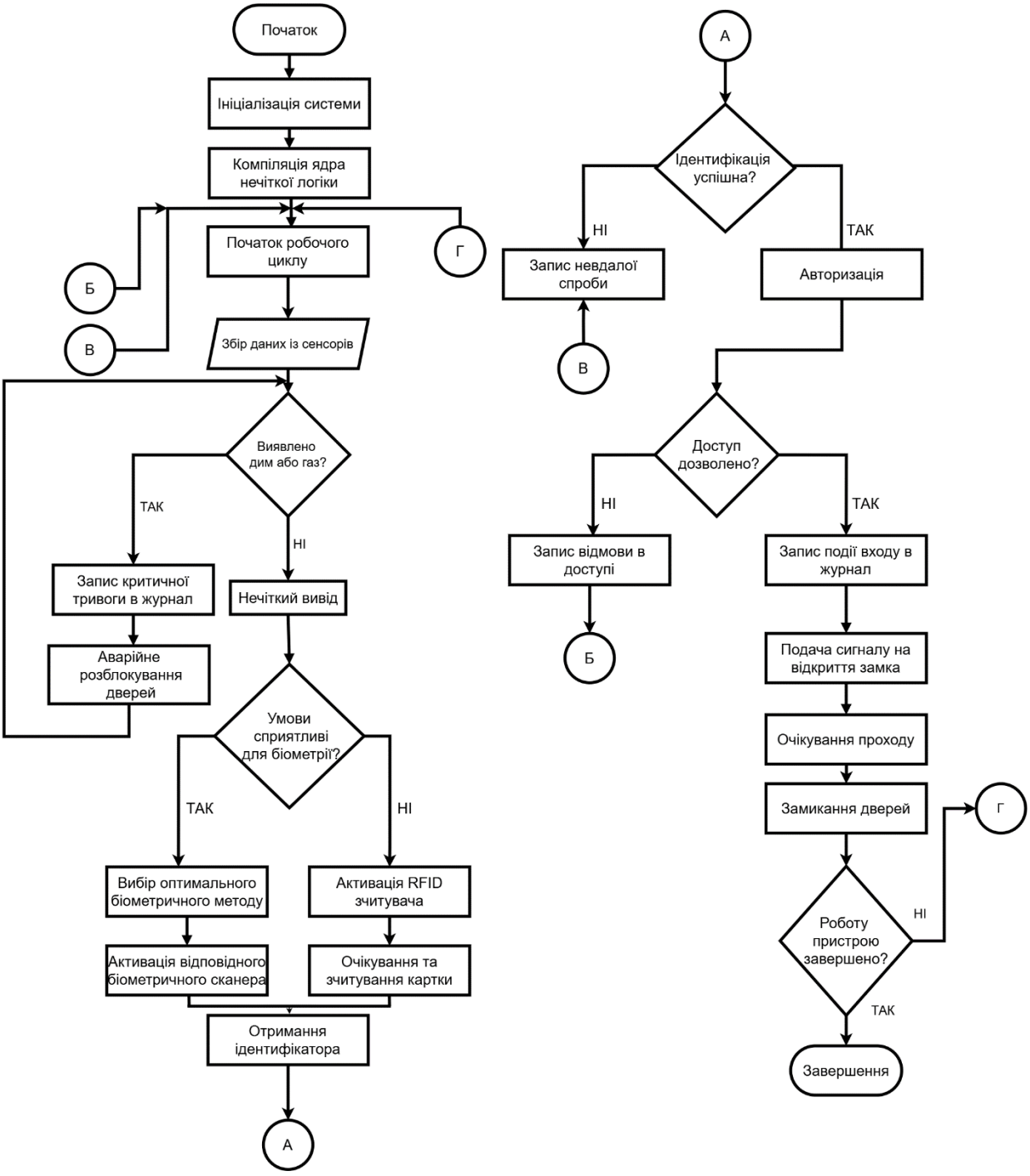

Рис. 2.3. Блок-схема головного алгоритму роботи системи контролю доступу

Робочий цикл системи побудований за ітераційним принципом і на кожній ітерації виконує чітко визначену послідовність дій. На початку кожного циклу відбувається збір даних про стан навколишнього середовища. Система послідовно опитує цифрові сенсори освітленості та температури, а також здійснює захоплення аудіопотоку для оцінки рівня акустичного шуму. Отримані дані проходять попередню обробку та нормалізацію для приведення їх до форматів, придатних для подальшого аналізу.

Наступним кроком виконується процедура нечіткого виводу, де нормалізовані показники середовища передаються на вхід контролера нечіткої логіки. Математичне ядро системи розраховує коефіцієнти придатності для кожного доступного методу ідентифікації, базуючись на закладеній базі знань.

На основі розрахованих коефіцієнтів блок прийняття рішень формує пріоритетний список методів автентифікації. Алгоритм порівнює отримані оцінки з пороговим значенням критичності. Якщо умови середовища визнаються сприятливими хоча б для одного біометричного методу, система активує відповідний сканер та ініціює процедуру розпізнавання користувача. У випадку, коли всі розраховані коефіцієнти виявляються нижчими за допустимий поріг, система автоматично переходить у режим роботи з резервним методом ідентифікації та активує зчитувач безконтактних карток.

Завершальним етапом циклу є виконання процедури авторизації, яка передбачає перевірку прав доступу ідентифікованої особи в базі даних та генерацію керуючого сигналу для електрозамка.

2.3.2. Логіка роботи підсистеми моніторингу безпеки та реагування на аварійні ситуації. Забезпечення фізичної безпеки персоналу є пріоритетним завданням будь-якої системи контролю доступу, тому підсистема моніторингу аварійних ситуацій функціонує паралельно з основним процесом ідентифікації.

Для реалізації миттєвої реакції на критичні події використано механізм апаратних переривань, що дозволяє обробляти сигнали тривоги незалежно від поточного стану виконання основної програми чи завантаженості центрального процесора.

Основним чутливим елементом підсистеми безпеки виступає комбінований датчик газу та диму. Алгоритм роботи підсистеми базується на постійному моніторингу стану вихідного сигналу цього сенсора. У штатному режимі роботи на виході датчика утримується низький логічний рівень. При детекції перевищення допустимої концентрації диму або продуктів горіння драйвер портів введення-виведення мікрокомп'ютера фіксує зміну логічного рівня та генерує сигнал переривання по передньому фронту імпульсу. Ця подія призводить до негайного призупинення всіх поточних процесів ідентифікації та передачі керування спеціалізованій функції обробки аварії.

Функція обробки аварійної ситуації виконує ряд критично важливих дій для забезпечення вільної евакуації персоналу. Першочергово контролер змінює стан керуючого виходу реле електрозамка на низький логічний рівень. Це призводить до знеструмлення електромагніту або соленоїда замка, внаслідок чого двері переходять у відчинений стан. Таке технічне рішення відповідає принципу безпеки при відмові, який є обов'язковою вимогою міжнародних стандартів для систем контролю доступу на шляхах евакуації. Паралельно з розблокуванням дверей подія фіксується у системному журналі з відповідним статусом критичної тривоги та точною часовою міткою. Після цього система переходить у режим блокування, в якому всі спроби ідентифікації ігноруються до моменту ручного скидання тривоги адміністратором системи безпеки.

2.3.3. Алгоритмічна реалізація перевірки прав доступу та обліку робочого часу. Модуль авторизації та обліку робочого часу активується виключно після успішного проходження користувачем процедури біометричної ідентифікації або валідації безконтактної картки. Цей програмний компонент відповідає за прийняття остаточного рішення про надання доступу на основі співставлення ідентифікатора особи з її робочим графіком та правами доступу. Логіка роботи модуля реалізована на основі взаємодії з реляційною базою даних, що забезпечує надійне зберігання інформації про користувачів та історію подій.

Процедура перевірки розпочинається із синхронізації часу, під час якої система отримує поточне значення часу та дня тижня від системного годинника.

Для забезпечення точності обліку робочого часу системний годинник періодично синхронізується з еталонними серверами часу через мережевий протокол. Наступним кроком виконується формування та виконання запиту до таблиці розкладів бази даних. Метою запиту є пошук актуального правила доступу для ідентифікованого користувача на поточний день тижня.

Ключовим етапом алгоритму виступає перевірка часового інтервалу. Система порівнює поточний час спроби входу з дозволеним часовим вікном, визначеним у робочому графіку співробітника. Математична умова надання доступу описується логічним виразом:

$$Access = (T_{start} \leq T_{cur} \leq T_{end}), \quad (2.7)$$

де *Access* – логічна змінна, що визначає дозвіл на доступ;

Tstart – час початку робочої зміни згідно з графіком;

Tcur – поточний час спроби проходу;

Tend – час завершення робочої зміни.

Результат перевірки умови фіксується у таблиці журналу подій. Якщо поточний час знаходиться в межах дозволеного інтервалу, система генерує подію успішного входу та подає команду на відкриття виконавчого механізму. Запис про цю подію надалі використовується підсистемою звітності для автоматичного розрахунку відпрацьованих годин. У випадку, якщо спроба входу відбувається у позаробочий час, доступ блокується, а у журналі створюється запис про порушення трудового розпорядку. Реалізований алгоритм забезпечує гнучку настройку політик доступу та дозволяє автоматизувати табельний облік на підприємстві.

2.4. Висновки до розділу

У другому розділі кваліфікаційної роботи здійснено теоретичне обґрунтування та математичне моделювання процесу адаптивного управління доступом на об’єктах зі змінними умовами експлуатації. Встановлено, що

використання апарату нечіткої логіки є найбільш ефективним підходом для формалізації процесу прийняття рішень в умовах невизначеності та неповноти вхідних даних. Розроблена математична модель на базі алгоритму Мамдані дозволяє встановити нелінійні залежності між фізичними параметрами навколишнього середовища та показниками надійності біометричних методів ідентифікації.

В ході проєктування системи нечіткого виводу виконано фазифікацію вхідних змінних, якими виступають рівень освітленості, акустичний шум та температура повітря. Для кожної змінної побудовано відповідні функції належності та сформовано базу продукційних правил, яка відображає експертні знання про фізичні обмеження сенсорів. Вибір методу центру тяжіння для етапу дефазифікації забезпечує високу точність розрахунків та плавність адаптації системи до змін зовнішніх факторів, що мінімізує ймовірність помилкових перемикань режимів роботи.

Розроблене алгоритмічне забезпечення комплексу охоплює повний цикл функціонування системи, починаючи від ініціалізації апаратних засобів і завершуючи керуванням виконавчими механізмами. Реалізований алгоритм моніторингу безпеки з використанням механізму апаратних переривань гарантує пріоритетне виконання функцій аварійного розблокування дверей, що відповідає вимогам стандартів безпеки.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ АДАПТИВНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1. Обґрунтування структурної організації апаратно-програмного комплексу

Проєктування апаратної частини адаптивної системи контролю доступу базується на принципах модульності та функціональної декомпозиції. Такий підхід дозволяє забезпечити гнучкість конфігурації, зручність обслуговування та можливість подальшої модернізації окремих вузлів без зміни загальної архітектури пристрою [28]. Головною вимогою до структурної організації комплексу виступає забезпечення надійної взаємодії між підсистемою збору даних про стан навколишнього середовища, модулями біометричної ідентифікації та центральним обчислювальним ядром, яке реалізує логіку нечіткого виводу [37].

Побудова архітектури апаратно-програмного комплексу базується на використанні модульного принципу, де центральне обчислювальне ядро координує роботу периферійних підсистем через спеціалізовані цифрові інтерфейси. Структурна схема системи наведена на рис. 3.1.

Розглянемо більш детально модулі системи, а також зв'язки та інтерфейси. Головним керуючим елементом системи виступає одноплатний мікрокомп’ютер Raspberry Pi 3 B+, який забезпечує виконання алгоритмів комп’ютерного зору та функціонування ядра нечіткої логіки [13]. Взаємодія між центральним процесором та функціональними блоками реалізована з використанням шин передачі даних I2C, SPI, UART та ліній GPIO, що дозволяє досягти необхідної швидкодії та завадостійкості.

.

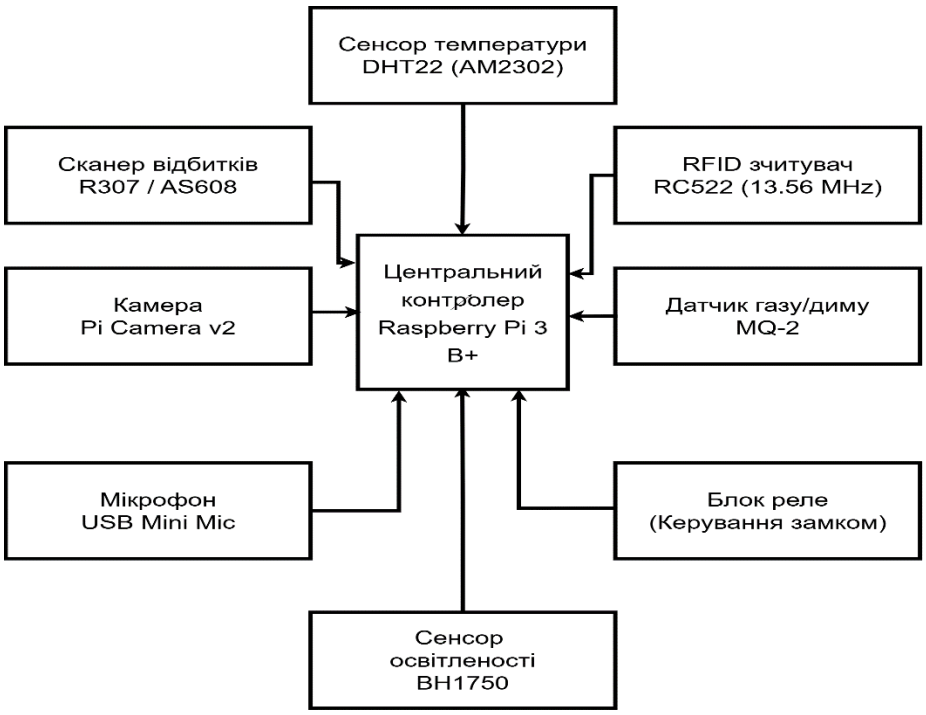

Рис. 3.1. Структурна схема адаптивної системи контролю доступу

Підсистема візуальної ідентифікації реалізована на базі модуля камери Pi Camera. Підключення цього компонента здійснюється через спеціалізований інтерфейс CSI, який забезпечує прямий високошвидкісний доступ до графічного підсистеми процесора для передачі відеопотоку без затримок. Така організація зв'язку є критично важливою для ефективної роботи алгоритмів розпізнавання обличчя у реальному часі.

Акустичний моніторинг та голосова ідентифікація забезпечуються підсистемою на основі мікрофона USB Mini Microphone. Цей пристрій підключається до універсальної послідовної шини USB центрального контролера, що дозволяє використовувати стандартні драйвери операційної системи для оцифровки та обробки звукового сигналу.

Блок дактилоскопічної ідентифікації побудовано з використанням оптичного сканера R307 або його аналога AS608. Обмін керуючими командами та даними про відбитки пальців між сканером та мікрокомп'ютером відбувається

через асинхронний послідовний інтерфейс UART. Це дозволяє розвантажити центральний процесор, оскільки операції порівняння шаблонів частково виконуються внутрішнім контролером сканера.

Підсистема моніторингу параметрів навколишнього середовища об'єднує різнорідні сенсори, які підключаються через відповідні цифрові протоколи. Високоточний сенсор освітленості BH1750 взаємодіє з контролером через двопровідну шину I2C, що забезпечує адресну передачу даних про рівень освітленості у люксах. Датчик температури та вологості DHT22 використовує для комунікації дискретну лінію GPIO зі специфічним однопровідним протоколом обміну.

Резервний контур доступу реалізовано на базі модуля зчитування безконтактних карток RC522 [14]. Для забезпечення високої швидкості зчитування даних з RFID-міток на частоті 13,56 МГц використовується послідовний периферійний інтерфейс SPI. Цей канал зв'язку характеризується високою пропускною здатністю та дозволяє миттєво передавати ідентифікатор картки до системи прийняття рішень.

Блок безпеки та виконавчих механізмів підключається безпосередньо до портів введення-виведення загального призначення GPIO. Датчик газу та диму MQ-2 використовує цифрову лінію для генерації сигналу переривання при виявленні небезпеки, а керування реле електрозамка здійснюється шляхом зміни логічного рівня на відповідному вихідному піні контролера. Така схема підключення гарантує мінімальний час реакції системи на аварійні події.

3.2. Програмна реалізація системи управління та прийняття рішень

3.2.1. Обґрунтування вибору середовища розробки та програмних бібліотек. Розробка програмного забезпечення для адаптивної системи контролю доступу вимагає використання інструментів, які забезпечують гнучкість, швидкодію та простоту інтеграції з апаратним забезпеченням.

Програмна архітектура побудована за об'єктно-орієнтованим принципом, де кожен функціональний модуль інкапсульований в окремий клас. Такий підхід

дозволяє локалізувати зміни коду та спрощує процес налагодження окремих підсистем.

В якості основної мови програмування обрано Python версії 3.9. Цей вибір зумовлений наявністю широкого спектру спеціалізованих бібліотек для роботи з периферією мікрокомп'ютерів Raspberry Pi, а також потужних інструментів для математичного моделювання. Середовищем розробки виступає Visual Studio Code, яке забезпечує зручні засоби для написання коду, віддаленого налагодження через SSH та контролю версій.

Для реалізації функціоналу системи використано ряд спеціалізованих бібліотек. Взаємодія з портами введення-виведення здійснюється за допомогою бібліотеки RPi. GPIO [15], яка надає низькорівневий доступ до керування реле та зчитування сигналів переривання. Робота з шиною I2C реалізована через модуль smbus2, що є стандартом для Linux-систем.

Ключовим компонентом програмного комплексу виступає бібліотека scikit-fuzzy. Вона містить реалізацію алгоритмів нечіткої логіки, включаючи функції для створення лінгвістичних змінних, визначення функцій належності та виконання процедур фазифікації і дефазифікації. Для роботи з базою даних використано вбудований модуль sqlite, який забезпечує надійне зберігання інформації про користувачів та події у локальному файлі без необхідності розгортання важкого сервера баз даних.

Структура файлів проекту організована за модульним принципом, де кожен логічний компонент системи винесено в окремий файл. Це дозволяє спростити навігацію по коду та полегшити процес супроводу програмного забезпечення. Ієрархія файлів та каталогів розробленого програмного забезпечення представлена на рис. 3.2.

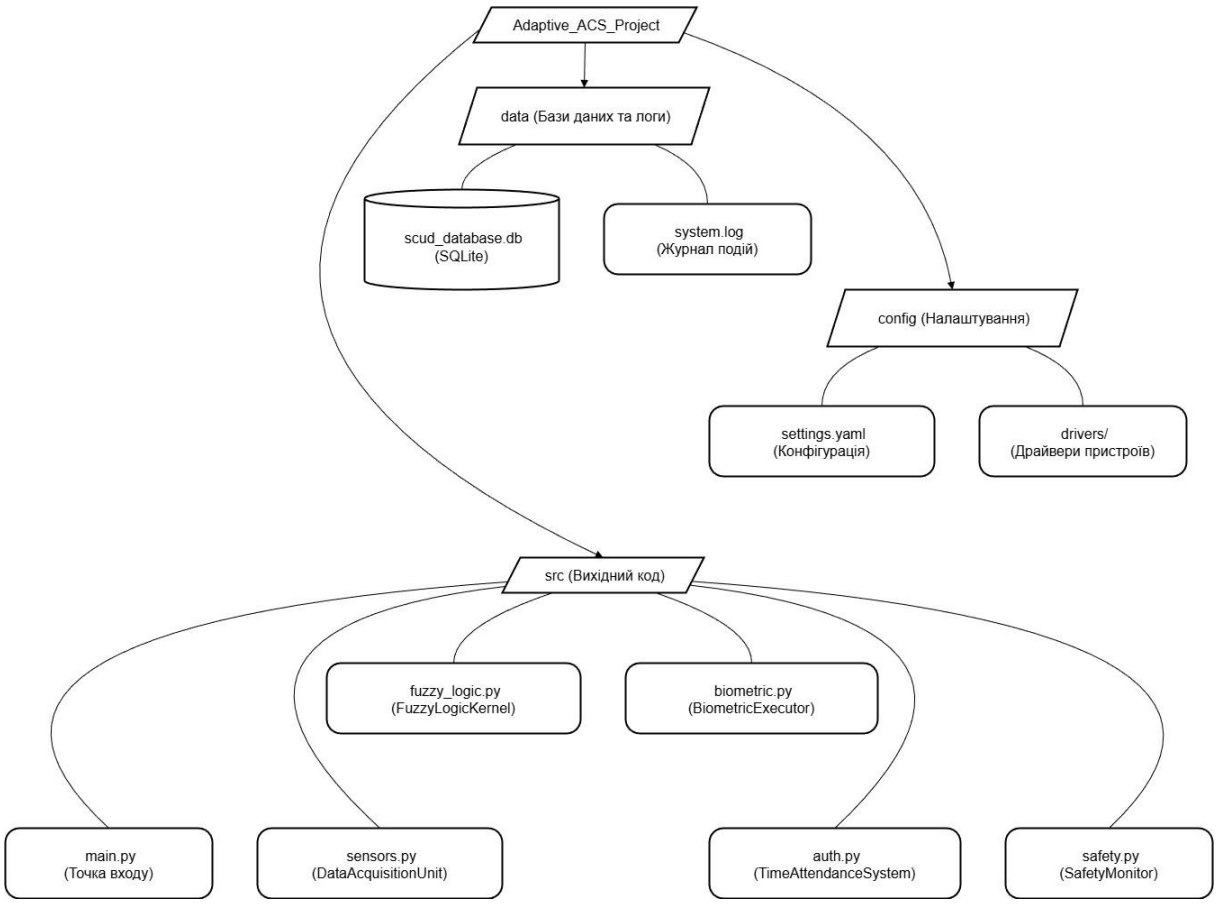

Рис. 3.2. Структура файлів проекту програмного забезпечення

У кореневій директорії розміщено головний виконуваний файл main.py, який ініціалізує всі підсистеми [12]. Модулі, що відповідають за роботу з сенсорами, нечіткою логікою та базою даних, винесені у відповідні класи, що забезпечує високий рівень абстракції та інкапсуляції даних.

3.2.2. Реалізація підсистем збору даних, логіки нечіткого виводу та роботи з базою даних. Програмна реалізація функціональних вузлів системи базується на принципах об'єктно-орієнтованого програмування, що дозволяє інкапсулювати логіку роботи окремих компонентів у відповідні класи. Такий підхід забезпечує модульність коду та спрощує його подальшу підтримку і масштабування.

Першим рівнем обробки інформації виступає підсистема збору даних, реалізована у класі DataAcquisitionUnit. Цей модуль відповідає за ініціалізацію апаратних інтерфейсів та зчитування первинних показників із сенсорів. Основна

складність реалізації полягає у необхідності одночасної роботи з різними протоколами передачі даних, такими як I2C для сенсора освітленості та специфічний однопровідний протокол для датчика температури. Для підвищення відмовостійкості системи у коді передбачено механізми обробки виключних ситуацій, які виникають при помилках на шині даних або тимчасовій недоступності сенсорів. У випадку збою зчитування програма виконує серію повторних запитів перед тим, як повернути значення помилки або перемкнутися на режим симуляції.

Алгоритм зчитування даних із цифрового сенсора освітленості BH1750 [2] передбачає звернення до регістрів пристрою через шину I2C та подальшу конвертацію отриманих байтів у фізичну величину. Лістинг методу, що реалізує цей процес, наведено на рис. 3.4.

```
  def _read_bh1750(self):
        """Зчитування освітленості (Lux) через шину I2C."""
        try:
                        data =
self.bus.read_i2c_block_data(self.BH1750_ADDR,
                                                self.BH1750_MODE, 2)

            raw_lux = (data[0] * 256 + data[1]) / 1.2
                        return min(max(raw_lux, 0), 1000)
        except Exception:
            return 0.0
```

Рис. 3.4. Лістинг методу зчитування даних із сенсора освітленості

Центральним елементом системи прийняття рішень виступає модуль нечіткої логіки, інкапсульований у класі FuzzyLogicKernel. Програмна реалізація цього модуля базується на використанні бібліотеки scikit-fuzzy, яка надає інструментарій для створення лінгвістичних змінних та операцій над нечіткими множинами. Процес ініціалізації контролера включає визначення вхідних змінних антецедентів та вихідних змінних консеквентів, а також формування бази продукційних правил.

Кожне правило описується програмним об'єктом, що зв'язує умови спрацювання з відповідним висновком. Це дозволяє гнучко налаштовувати

поведінку системи шляхом додавання або модифікації правил без зміни основного алгоритму виводу. Реалізація ініціалізації змінних та формування бази знань представлена на рис. 3.5.

```
       def _compile_fis_controller(self):
                    light = ctrl.Antecedent(np.arange(0, 1001, 1),
'light')
             noise = ctrl.Antecedent(np.arange(0, 101, 1), 'noise')

                   suit_face = ctrl.Consequent(np.arange(0, 11,
0.1), 'face_suit')

             rules = []
             rules.append(ctrl.Rule(light['Dark'],
suit_face['Unusable']))

             rules.append(ctrl.Rule(noise['Loud'] | noise['Very
High'],
                                    suit_voice['Low']))

             access_ctrl = ctrl.ControlSystem(rules)
             return ctrl.ControlSystemSimulation(access_ctrl)
```

Рис. 3.5. Лістинг програмної реалізації ядра нечіткої логіки

Збереження та обробка даних про користувачів, їхні графіки роботи та історію подій доступу покладено на підсистему бази даних, реалізовану в класі TimeAttendanceSystem. Для забезпечення автономності та надійності зберігання даних використано вбудовану бібліотеку sqlite [17], яка дозволяє працювати з локальною реляційною базою даних без необхідності розгортання окремого серверного програмного забезпечення.

Взаємодія з базою даних здійснюється через параметризовані SQL-запити, що підвищує безпеку системи та захищає від ін'єкцій шкідливого коду. У класі реалізовано методи для створення структури таблиць при першому запуску, перевірки прав доступу користувача на основі поточного часу та запису подій у журнал. Такий підхід забезпечує цілісність даних та дозволяє формувати звіти для обліку робочого часу. Лістинг методу реєстрації подій у базі даних наведено на рис. 3.6.

```
        def _log_transaction(self, timestamp, user_id, event_type,
method):
            """Запис події у журнал бази даних."""
            cursor = self.conn.cursor()
            query = """
                INSERT INTO AccessLog (timestamp, user_id,
event_type, method)
                VALUES (?, ?, ?, ?)
            """
            try:
                cursor.execute(query, (timestamp, user_id,
event_type, method))
                self.conn.commit()
                print(f"[LOG] Event '{event_type}' saved to
database.")
            except sqlite3.Error as e:
                print(f"[DB ERROR] Failed to log transaction:
{e}")
```

Рис. 3.6. Лістинг методу реєстрації подій у базі даних

Комплексна взаємодія описаних підсистем забезпечує повний цикл обробки інформації від моменту отримання фізичного сигналу сенсором до прийняття рішення про допуск та фіксації цієї події в енергонезалежній пам'яті. Використання модульної архітектури та спеціалізованих бібліотек дозволило створити надійне та ефективне програмне забезпечення, адаптоване до обмежених ресурсів вбудованої системи.

3.2.3. Організація інтерфейсу користувача та підсистеми звітності. Взаємодія людини з автоматизованою системою контролю доступу відбувається на двох рівнях, а саме на рівні пересічного користувача та на рівні адміністратора системи безпеки. Оскільки розроблюваний пристрій належить до класу вбудованих систем, організація інтерфейсу має специфічні особливості, спрямовані на забезпечення автономності та мінімізацію апаратних ресурсів.

Для кінцевого користувача інтерфейс реалізовано через фізичні методи взаємодії. Індикація стану системи здійснюється за допомогою світлодіодних індикаторів або невеликого символьного дисплея, підключеного до портів введення-виведення контролера. Успішна ідентифікація супроводжується візуальним сигналом та звуковим оповіщенням, після чого відбувається

розблокування виконавчого механізму. Такий підхід забезпечує інтуїтивно зрозумілу взаємодію та високу пропускну здатність точки проходу.

Для адміністратора системи реалізовано програмний інтерфейс командного рядка, який дозволяє переглядати потік подій у реальному часі та керувати налаштуваннями бази даних. Ключовим елементом адміністративного інтерфейсу виступає підсистема звітності, програмно реалізована у класі AccessLogger. Цей модуль відповідає за фіксацію всіх транзакцій системи, включаючи успішні входи, відмови у доступі через порушення графіка, спроби несанкціонованого доступу та аварійні ситуації.

Важливою функцією підсистеми звітності є забезпечення інтеграції з зовнішніми системами обліку робочого часу та бухгалтерії. Для цього розроблено механізм експорту накопичених даних у універсальний текстовий формат CSV. Вибір цього формату обумовлений його широкою підтримкою більшістю табличних процесорів та баз даних. Алгоритм експорту виконує вибірку всіх записів із таблиці історії, формує заголовки стовпців та записує дані у файл з відповідним кодуванням. Програмна реалізація методу експорту наведена на рис. 3.7.

```
        def export_logs_to_csv(self, filename="daily_report.csv"):
            """Експорт журналу подій у формат CSV."""
            try:
                with sqlite3.connect(self.db_file) as conn:
                    cursor = conn.cursor()
                    cursor.execute("SELECT * FROM AccessHistory
ORDER BY timestamp DESC")
                    rows = cursor.fetchall()
                                headers = [description[0] for
description in cursor.description]


                    with open(filename, 'w', newline='',
encoding='utf-8') as f:
                        writer = csv.writer(f)
                        writer.writerow(headers)
                        writer.writerows(rows)
                print(f"[REPORT] Logs exported successfully to
{filename}")
            except Exception as e:
                print(f"[REPORT ERROR] Export failed: {e}")
```

Рис. 3.7. Лістинг методу експорту звітності у формат CSV

Для оперативного моніторингу ситуації на об'єкті адміністратору необхідно мати доступ до останніх зафіксованих подій без необхідності повного вивантаження бази даних. Для цього в системі реалізовано функцію вибірки останніх записів, яка може використовуватися для виведення інформації на локальний дисплей контролера або у консоль віддаленого термінала.

Ця функція виконує оптимізований SQL-запит до бази даних, обмежуючи кількість результатів заданим параметром. Такий підхід дозволяє миттєво отримувати інформацію про те, хто саме пройшов через турнікет або кому було відмовлено у доступі, що підвищує ситуаційну обізнаність служби охорони. Лістинг методу отримання останніх записів журналу представлено на рис. 3.8.

```
    def get_last_n_logs(self, n=5):
            """Отримання останніх n записів для відображення на
дисплеї."""
            with sqlite3.connect(self.db_file) as conn:
                cursor = conn.cursor()
                query = """
                    SELECT timestamp, user_id, status, method_used
                    FROM AccessHistory
                    ORDER BY id DESC LIMIT ?
                """
                cursor.execute(query, (n,))
                return cursor.fetchall()
```

Рис. 3.8. Лістинг методу отримання оперативної інформації про події

Реалізована підсистема звітності забезпечує надійне збереження даних завдяки транзакційному механізму бази даних SQLite. Усі операції запису виконуються з автоматичною фіксацією змін, що мінімізує ризик втрати інформації при раптовому вимкненні живлення. Структура таблиці журналу подій спроєктована таким чином, щоб зберігати не лише факт проходу, але й контекстну інформацію, таку як використаний метод ідентифікації та значення параметрів навколишнього середовища в момент події, що є важливим для подальшого аналізу ефективності роботи адаптивних алгоритмів.

3.3. Моделювання та аналіз ефективності системи в середовищі MATLAB

3.3.1. Побудова моделі нечіткого контролера шляхом програмної реалізації алгоритму Мамдані. Для перевірки коректності функціонування розроблених алгоритмів адаптивного керування проведено серію експериментів у середовищі імітаційного моделювання MATLAB [5].

Цей інструмент дозволяє візуалізувати внутрішні процеси нечіткого виводу та оцінити реакцію системи на зміну вхідних параметрів без необхідності фізичного відтворення екстремальних умов експлуатації. Результати моделювання представлені у вигляді графічних залежностей, що демонструють роботу механізму прийняття рішень.

Першим етапом моделювання виступає верифікація налаштування вхідних лінгвістичних змінних. Програмна реалізація моделі виконує розрахунок функцій належності для кожного терму на заданому універсумі значень. На рис. 3.9 представлено графік функцій належності для змінної рівня освітленості. Графік демонструє поділ робочого діапазону сенсора на чотири перекривні зони, що відповідають станам темряви, сутінків, нормального та яскравого освітлення. Використання трикутних та трапецієподібних функцій дозволяє забезпечити плавність переходу між станами системи при зміні освітленості від 0 до 1000 Люкс.

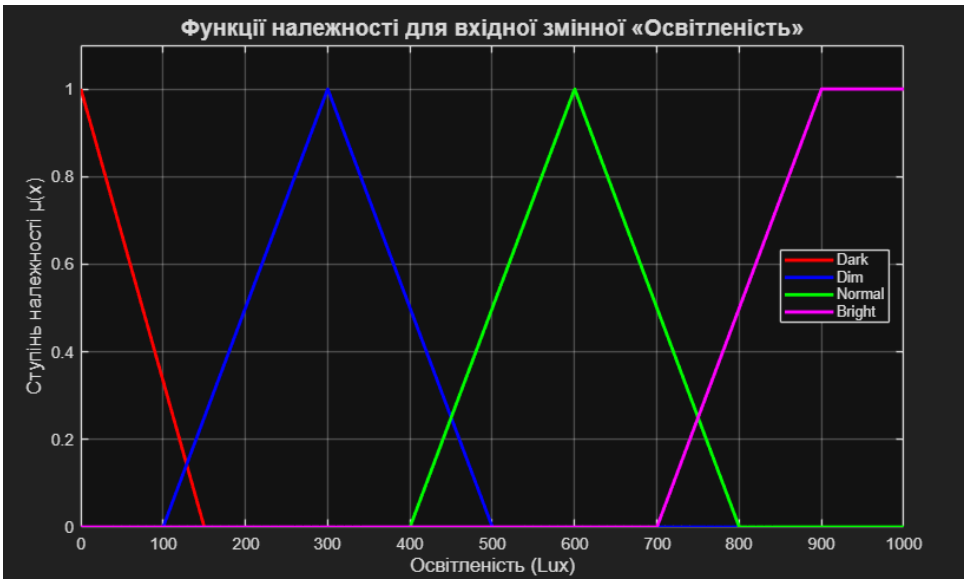

Рис. 3.9. Функції належності для вхідної змінної «Освітленість»

Ключовим етапом роботи алгоритму є процес дефазифікації, під час якого розмиті логічні висновки перетворюються на чіткі числові оцінки придатності методів. Центроїд, або центр тяжіння, у даному контексті виступає точкою рівноваги агрегованої фігури, що дозволяє отримати єдине скалярне значення, яке враховує внесок усіх активних правил бази знань. На рис. 3.10 наведено результати роботи алгоритму для тестового сценарію зі складними умовами, де освітленість є недостатньою, але рівень шуму та температура знаходяться в межах норми.

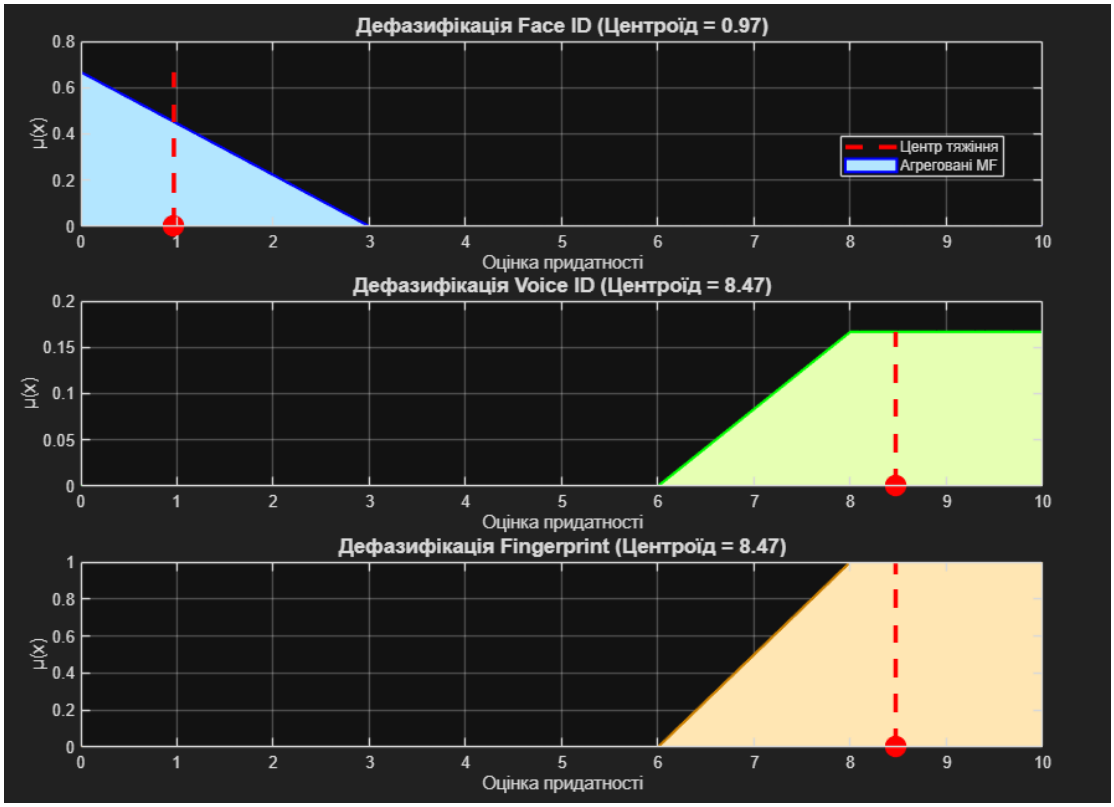

Рис. 3.10. Результати дефазифікації для трьох біометричних методів

Графік містить три панелі, що відображають результат для кожного методу ідентифікації. Для розпізнавання обличчя (верхня панель) центр тяжіння знаходиться в зоні низьких значень (0.97), що свідчить про непридатність методу. Водночас для голосової та дактилоскопічної ідентифікації (середня та нижня панелі) розраховані оцінки становлять 8.47 балів, що підтверджує високу надійність цих методів у заданих умовах.

3.3.2. Моделювання сценаріїв роботи системи при динамічній зміні параметрів навколишнього середовища. Для оцінки динамічних характеристик системи проведено моделювання реакції контролера на зміну окремих параметрів середовища.

Перший сценарій імітує зміну освітленості від повної темряви до яскравого світла. Результати, наведені на рис. 3.11, демонструють чітку залежність оцінки придатності розпізнавання обличчя від рівня освітленості. У зоні темряви до 150 Люкс оцінка залишається мінімальною, що унеможливлює використання камери. При зростанні освітленості спостерігається різке підвищення пріоритету методу, який стабілізується на максимальному рівні при досягненні значення 400 Люкс.

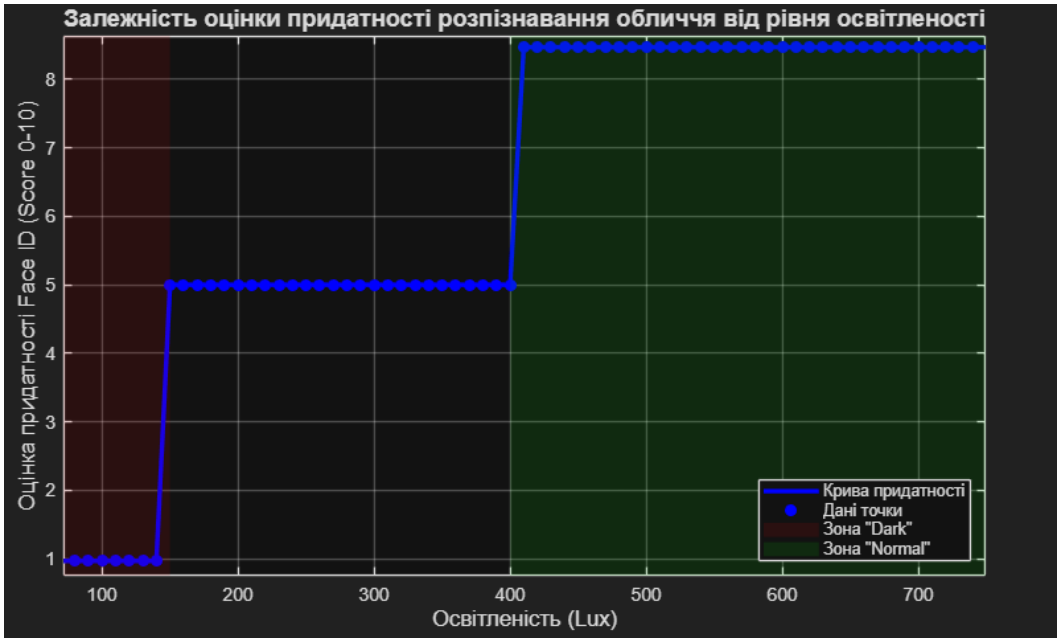

Рис. 3.11. Залежність оцінки придатності розпізнавання обличчя від рівня освітленості

Другий сценарій присвячено дослідженню впливу температури на роботу сканера відбитків пальців. Графік на рис. 3.12 має характерну трапецієподібну форму, що відображає наявність чітко окресленої зони комфорту. У діапазоні температур від 10 до 30 градусів Цельсія система присвоює дактилоскопічному методу високий пріоритет з оцінкою 8.5 балів. При виході температури за межі

цього діапазону, як у бік морозів, так і у бік спеки, спостерігається лінійне зниження оцінки до рівня 4.0 балів, що запобігає помилкам зчитування.

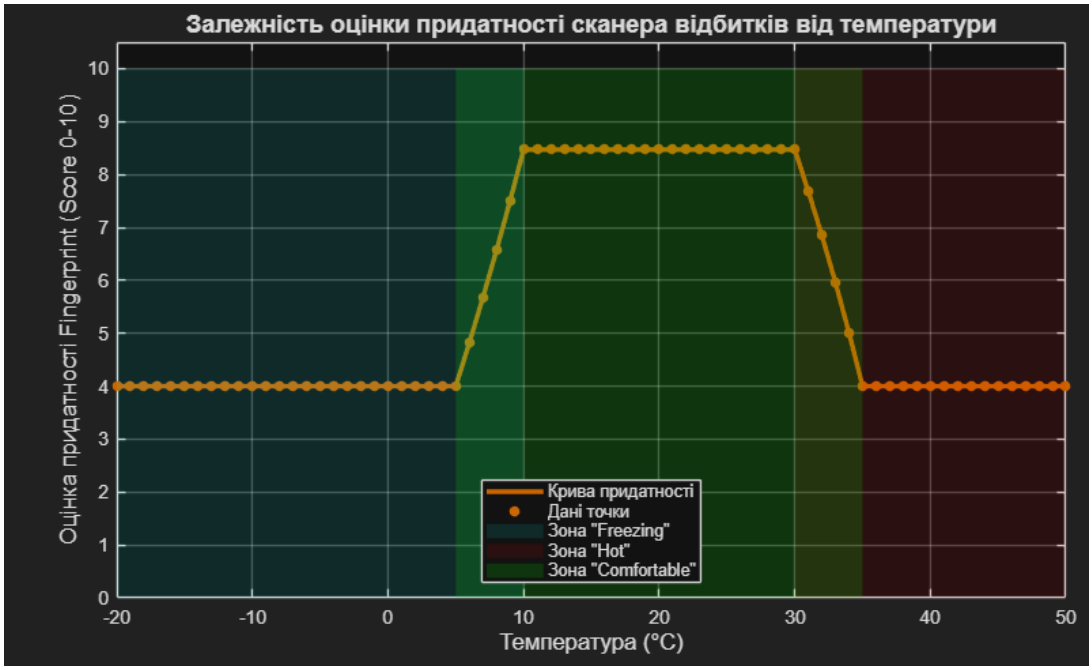

Рис. 3.12. Залежність оцінки придатності сканера відбитків від температури

3.3.3. Аналіз результатів симуляції та оцінка адекватності роботи алгоритму вибору методу ідентифікації. Для перевірки відсутності взаємного негативного впливу параметрів побудовано поверхню нечіткого виводу, представлену на рис. 3.13. Тривимірний графік ілюструє залежність оцінки придатності розпізнавання обличчя одночасно від рівня освітленості та акустичного шуму. Поверхня демонструє, що зміна рівня шуму не впливає на пріоритет відеоканалу, оскільки профіль поверхні залишається незмінним уздовж відповідної осі. Водночас зростання освітленості призводить до прогнозованого підвищення оцінки, формуючи характерний схил поверхні. Це підтверджує коректність сформованої бази правил та незалежність каналів ідентифікації.

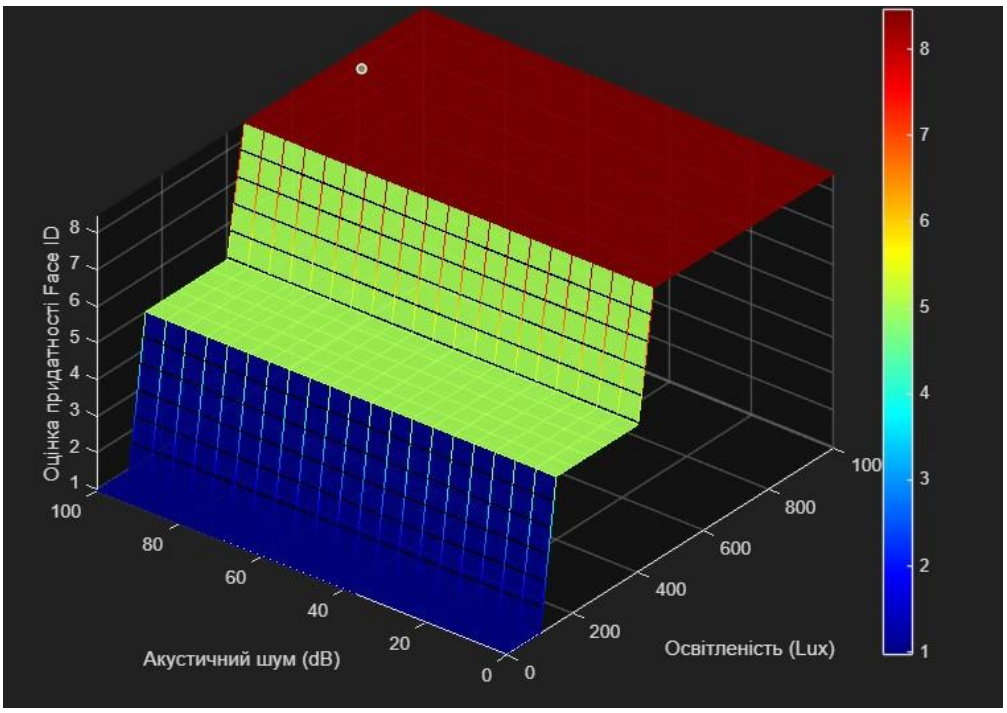

Рис. 3.13. Поверхня нечіткого виводу для оцінки придатності розпізнавання обличчя

Отримані результати моделювання підтверджують здатність розробленої системи адекватно реагувати на зміни зовнішніх умов. Алгоритм забезпечує коректне блокування ненадійних методів ідентифікації та автоматичний вибір оптимального засобу автентифікації, що гарантує стабільну роботу системи контролю доступу в реальних умовах експлуатації.

3.4. Висновки до розділу

У третьому розділі кваліфікаційної роботи здійснено практичну реалізацію та верифікацію розробленої адаптивної системи контролю доступу. На основі проведеного аналізу вимог обґрунтовано вибір апаратної платформи, якою виступає одноплатний мікрокомп’ютер Raspberry Pi 3 B+. Цей пристрій забезпечує необхідну обчислювальну потужність для функціонування алгоритмів комп’ютерного зору та ядра нечіткої логіки. Розроблена структурна схема комплексу відображає організацію взаємодії центрального процесора з

периферійними модулями через стандартизовані інтерфейси передачі даних, що гарантує сумісність компонентів та надійність обміну інформацією.

Програмна реалізація системи виконана мовою Python з використанням принципів об’єктно-орієнтованого програмування. Створена архітектура програмного забезпечення забезпечує модульність та гнучкість, дозволяючи незалежно розвивати підсистеми збору даних, прийняття рішень та роботи з базою даних. Реалізовані алгоритми обробки виключних ситуацій та механізм апаратних переривань гарантують стабільність роботи комплексу та пріоритетне виконання функцій безпеки.

Ефективність запропонованих алгоритмів адаптації підтверджено шляхом імітаційного моделювання у середовищі MATLAB. Розроблена програмна модель контролера дозволила детально дослідити динаміку процесів прийняття рішень в умовах невизначеності.

Результати експериментів доводять, що розроблений апаратно-програмний комплекс здатен забезпечити високий рівень надійності ідентифікації в реальних умовах експлуатації, мінімізуючи вплив дестабілізуючих факторів на роботу біометричних сканерів.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Розробка та тестування адаптивного апаратно-програмного комплексу системи контролю доступу пов’язана з тривалою роботою за комп’ютером, а також із монтажем та налаштуванням електронних компонентів, зокрема одноплатного комп’ютера Raspberry Pi, сенсорів та виконавчих механізмів. Відповідно до Закону України «Про охорону праці», роботодавець зобов'язаний створити на робочому місці безпечні умови праці.

Основним нормативним документом, що регулює безпеку під час роботи з комп’ютерною технікою, є НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [34]. Згідно з цим документом, робоче місце повинно бути спроектоване таким чином, щоб працівник мав достатньо простору для зміни робочого положення та рухів.

Приміщення для розробки відповідає вимогам ДБН В.2.2-28:2010 «Будинки адміністративного та побутового призначення». Площа на одне робоче місце складає не менше 6,0 м², що дозволяє вільно розмістити необхідне обладнання та забезпечити вільний доступ до нього для технічного обслуговування.

Параметри мікроклімату в приміщенні підтримуються відповідно до ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Оскільки робота розробника належить до категорії легких фізичних робіт, оптимальними параметрами є температура повітря 22–24°C в холодний період року та 23–25°C у теплий. Відносна вологість повітря має становити 40–60%, а швидкість руху повітря не повинна перевищувати 0,1 м/с.

Освітлення робочого місця організовано згідно з ДБН В.2.5-28:2018 «Природне і штучне освітлення». У приміщенні використовується суміщене освітлення. Природне світло потрапляє через вікна, орієнтовані так, щоб уникнути засліплення [22]. Штучне загальне освітлення забезпечується

світлодіодними світильниками, що гарантують відсутність пульсацій та сліпучої дії. Рівень освітленості на поверхні робочого столу становить не менше 300–500 лк, що відповідає нормам для зорових робіт високої точності.

Організація робочого місця відповідає ергономічним вимогам ДСТУ EN 894-1:2019 та загальним принципам НПАОП 0.00-7.15-18. Робочий стіл має достатню поверхню для розміщення периферії, екрана та документів. Монітор розташовано на відстані витягнутої руки, приблизно 600–700 мм, а верхній край екрана знаходиться на рівні очей, що запобігає перенапруженню шийного відділу хребта.

Забезпечення електробезпеки здійснюється відповідно до НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів». Живлення обладнання виконується від мережі 220 В із обов'язковим захисним заземленням. Усі підключення макетної плати та сенсорів до Raspberry Pi проводилися при вимкненому живленні для запобігання короткому замиканню та ураженню електричним струмом [35].

Пожежна безпека об’єкта відповідає вимогам Кодексу цивільного захисту України та НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні». Приміщення оснащене автоматичними пожежними сповіщувачами. Як первинний засіб пожежогасіння використовується вуглекислотний вогнегасник типу ВВК, який дозволяє гасити електроустановки під напругою без ризику пошкодження електронного обладнання [33].

Вжиті заходи з охорони праці дозволили мінімізувати вплив небезпечних та шкідливих виробничих факторів, забезпечити працездатність та зберегти здоров’я під час роботи апаратно-програмного комплексу системи контролю доступу.

4.2 Безпека в надзвичайних ситуаціях

4.2.1 Оцінка надійності захисту виробничого персоналу і її послідовність.

Під час оцінювання надійності захисту виробничого персоналу слід враховувати, що практично будь-які наслідки надзвичайних ситуацій можуть спричинити ураження людей, стати причиною їхньої загибелі або призвести до тривалої втрати працездатності.

Надійний захист персоналу є одним із ключових чинників, що визначають стійкість функціонування підприємства в умовах надзвичайних ситуацій як мирного, так і воєнного часу.

Найрезультативнішим способом захисту вважається укриття персоналу в захисних спорудах (ЗС) за умови дотримання таких вимог:

- місткість захисних споруд повинна забезпечувати укриття всіх працівників підприємства;
- конструкція та стан ЗС мають відповідати нормам захисту від усіх небезпечних факторів надзвичайних ситуацій;
- споруди повинні бути обладнані системами життєзабезпечення на час, необхідний для перебування людей всередині;
- розташування укриттів повинно дозволяти всім працівникам вчасно дістатися до них після сигналів оповіщення;
- персонал має бути завчасно проінформований та навчений діям за сигналами оповіщення й правилам поведінки в НС.

Показником надійності захисту працівників за використання ЗС може слугувати коефіцієнт надійності захисту КН.З., який відображає частку працівників, забезпечених гарантованим захистом від усіх небезпечних наслідків надзвичайної ситуації.

Цей коефіцієнт визначають на основі сукупності окремих показників, що характеризують рівень підготовленості підприємства до виконання завдань із захисту персоналу за основними напрямами роботи.

Оцінка надійності захисту виробничого персоналу проводиться поетапно. Насамперед аналізується інженерний захист робітників та службовців об’єкта.

Показником цього виду захисту є коефіцієнт $K_{\text{інж. зах.}}$, який визначає, яка частина виробничого персоналу працюючої зміни може своєчасно укритися в захисних спорудах із достатніми захисними властивостями та системами життєзабезпечення, що забезпечують перебування людей протягом установленого терміну:

$$\text{K}_{\text{інж. зах.}} = \frac{N_{\text{інж. зах.}}}{N}, \tag{4.1}$$

де (N) – це чисельність найбільшої працюючої зміни.

Далі вивчається система сповіщення та оцінюється здатність забезпечити своєчасне доведення сигналу до всіх робітників і службовців. Показником надійності з урахуванням сповіщення є коефіцієнт $K_{\text{сп}}$:

$$K_{\text{сп}} = \frac{N_{\text{сп}}}{N}, \tag{4.2}$$

Після цього оцінюється навченість виробничого персоналу способам захисту та діям за сигналами сповіщення. Відповідним показником є коефіцієнт навченості $K_{\text{навч.}}$:

$$K_{\text{навч.}} = \frac{N_{\text{навч}}}{N}, \tag{4.3}$$

Додатково визначається готовність сховищ до прийому людей. Для цього враховується фактичний час підготовки сховищ подвійного призначення, які перед укриттям звільняються від сторонніх речей, поповнюються запасами їжі та води, а також перевіряється герметичність і працездатність систем життєзабезпечення. Порівнюючи фактичний час підготовки сховища $T_{\text{г. факт}}$ з потрібним $T_{\text{г. потр.}}$, визначається готовність сховища до прийому людей. Для оцінки надійності захисту враховуються лише ті сховища, для яких:

$$\frac{T_{\text{г. факт}}}{T_{\text{г. потр.}}} \leq 1, \tag{4.4}$$

Показником надійності захисту з урахуванням готовності є коефіцієнт готовності $K_{\text{гот}}$:

$$K_{\text{гот}} = \frac{N_{\text{гот}}}{N}, \tag{4.5}$$

На основі окремих показників визначається коефіцієнт надійності захисту робітників та службовців $K_{\text{Н.З.}}$ за мінімальним значенням окремих показників: $K_{\text{інж.зах.}}, K_{\text{сп.}}, K_{\text{навч.}}, K_{\text{гот.}}$.

Визначаються слабкі місця в підготовці об’єкту до успішного вирішення задачі захисту виробничого персоналу у надзвичайних ситуаціях та передбачаються можливі шляхи підвищення показників надійності захисту.

У висновках вказується:

- надійність захисту робітників та службовців;
- необхідність підвищення захисних властивостей наявних захисних споруд та заходи для підвищення надійності;
- приміщення, які доцільно пристосувати під ЗС;
- кількість та тип ЗС, що швидко зводяться;
- заходи надійного захисту чергового персоналу;
- заходи з повного забезпечення персоналу ЗІЗ;
- заходи покращення умов зберігання, профілактики та ремонту ЗІЗ;
- заходи забезпечення об’єкту в умовах Р. Х. Б. З. [41].

4.2.2 Кримінологічна безпека. Джерела загроз об’єкту економіки та система безпеки. Кримінологічна безпека є ключовою складовою загальної системи економічної безпеки підприємства, оскільки вона спрямована на виявлення, попередження та нейтралізацію кримінальних загроз, здатних завдати шкоди діяльності об’єкта економіки.

У сучасних умовах нестабільності, зростання кіберзлочинності, корупційних проявів і зовнішніх ризиків ефективне забезпечення кримінологічної безпеки стає необхідним елементом функціонування будь-якої організації, незалежно від форми власності чи масштабу діяльності.

Джерела загроз для економічних об’єктів можуть бути як зовнішніми, так і внутрішніми. До зовнішніх загроз належать такі криміногенні фактори, як діяльність організованих злочинних груп, шахрайські схеми, рейдерські атаки, корупційний тиск, кіберзлочинність та незаконні дії контрагентів. Ці загрози формуються внаслідок недосконалості правозастосовчої практики, високого рівня тіньової економіки та глобальних ризиків, що супроводжують цифровізацію. Внутрішніми джерелами кримінальних загроз є зловживання персоналу, крадіжки матеріальних ресурсів, витік інформації, службові підроблення, неналежний контроль доступу та низький рівень корпоративної культури. Значну частку внутрішніх ризиків створює людський фактор, як через умисні дії, так і через недбалість або недостатню кваліфікацію працівників.

Система забезпечення кримінологічної безпеки підприємства включає комплекс організаційних, правових, технічних та профілактичних заходів. Її основою є кримінологічний моніторинг, який дозволяє виявляти потенційні загрози на ранніх етапах. Важливими елементами системи є: перевірка контрагентів, аудит безпеки, впровадження внутрішніх регламентів доступу, технічний захист інформації, системи спостереження, контроль фінансових операцій, перевірка персоналу та його навчання. На додаток, ефективне реагування на кримінальні ризики передбачає взаємодію з правоохоронними органами, страхування ризиків, а також створення спеціалізованих внутрішніх служб безпеки [40].

ВИСНОВКИ

У магістерській кваліфікаційній роботі вирішено актуальне науково-прикладне завдання підвищення надійності та ефективності систем контролю та управління доступом шляхом розробки адаптивних алгоритмів, що функціонують на основі методів нечіткої логіки.

Аналіз сучасних методів біометричної ідентифікації показав їх критичну залежність від дестабілізуючих факторів навколишнього середовища. Встановлено, що використання статичних порогових алгоритмів у динамічних умовах, таких як зміна освітленості, акустичний шум та температурні коливання, призводить до суттєвого зростання помилок першого та другого роду, порушуючи баланс між безпекою об’єкта та зручністю для користувачів.

Теоретичним підґрунтям роботи стала обґрунтована математична модель системи прийняття рішень на базі апарату нечіткої логіки з використанням алгоритму Мамдані. Сформована база лінгвістичних правил дозволила формалізувати експертні знання про фізичні обмеження біометричних методів та реалізувати механізм динамічного оцінювання коефіцієнта придатності для кожного способу ідентифікації у режимі реального часу.

Ефективність запропонованого підходу підтверджено результатами імітаційного моделювання, які засвідчили здатність системи плавно перемикати пріоритети методів ідентифікації. Зокрема, підтверджено коректність роботи логіки блокування каналу розпізнавання обличчя в умовах недостатньої освітленості та обмеження використання контактних сканерів при виході температури за межі допустимого діапазону.

Наукова новизна отриманих результатів полягає у вдосконаленні методу вибору засобу автентифікації, який, на відміну від існуючих рішень, враховує комплексний вплив зовнішніх факторів. Доведено доцільність використання дефазифікації методом центру тяжіння для отримання чітких керуючих сигналів, що дозволило уникнути часового «брязкоту» при перемиканні режимів та забезпечити стабільну роботу системи в перехідних процесах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. AM2302 (wired type) Humidity and Temperature Sensor. URL: https://cdn-shop.adafruit.com/datasheets/Digital+humidity+and+temperature+sensor+AM2302.pdf (дата звернення: 05.12.2025).

2. BH1750FVI Digital Light Intensity Sensor Datasheet. URL: https://www.mouser.com/datasheet/2/348/bh1750fvi-e-186247.pdf (дата звернення: 05.12.2025).

3. Breaking the Vicious Cycle of the Lombard Effect. URL: https://en.rockfon.international/about-us/blogs/2023/lombard-effect/ (дата звернення: 06.12.2025).

4. Biometric Authentication Methods: A Review. URL: https://www.researchgate.net/publication/338522765_Biometric_Authentication_Methods_A_Review (дата звернення: 05.12.2025).

5. Fuzzy Logic Toolbox User's Guide. URL: https://www.mathworks.com/help/pdf_doc/fuzzy/fuzzy.pdf (дата звернення: 06.12.2025).

6. ISO/IEC 19794-5:2011. Information technology — Biometric data interchange formats — Part 5: Face image data. URL: https://www.iso.org/standard/50867.html (дата звернення: 04.12.2025).

7. Kozlovskyi V., Scherbak L., Martyniuk H., Zharovskyi R., Balanyuk Y., Boiko Y. Applying an adaptive method of the orthogonal laguerre filtration of noise interference to increase the signal/noise ratio. Eastern-European Journal of Enterprise Technologies. 2020. Vol. 2/9 (104). P. 14–21.

8. OpenCV-Python Tutorials. URL: https://docs.opencv.org/4.x/d6/d00/tutorial_py_root.html (дата звернення: 05.12.2025).

9. Palamar A. Research and design of computer systems and networks for critical infrastructure. *Scientific Journal of TNTU*. 2023. Vol. 109, No 1. P. 45–54.

10. Palamar A., Karpinski M., Palamar M., Osukhivska H., Mytnyk M. Remote Air Pollution Monitoring System Based on Internet of Things. *CEUR Workshop Proceedings*. 2022. Vol. 3309. P. 194–204.

11. Palamar A., Palamar M., Osukhivska H. Real-time Health Monitoring Computer System Based on Internet of Medical Things. *CEUR Workshop Proceedings*. 2023. Vol. 3628. P. 106–115.

12. Python 3.9.13 Documentation. URL: https://docs.python.org/3.9/ (дата звернення: 06.12.2025).

13. Raspberry Pi 3 Model B+ Product Brief. URL: https://datasheets.raspberrypi.com/rpi3/raspberry-pi-3-b-plus-product-brief.pdf (дата звернення: 05.12.2025).

14. RC522 RFID Module Datasheet. URL: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf (дата звернення: 06.12.2025).

15. RPi.GPIO module basics. URL: https://sourceforge.net/p/raspberry-gpio-python/wiki/BasicUsage/ (дата звернення: 06.12.2025).

16. Scikit-fuzzy: Fuzzy Logic SciKit (Toolkit for SciPy). URL: https://pythonhosted.org/scikit-fuzzy/ (дата звернення: 05.12.2025).

17. SQLite Documentation. URL: https://www.sqlite.org/docs.html (дата звернення: 05.12.2025).

18. Velychko D., Osukhivska H., Palaniza Y., Lutsyk N., Sobaszek L. Artificial Intelligence Based Emergency Identification Computer System. *Advances in Science and Technology Research Journal*. 2024. Vol. 18, no. 2. P. 296–304.

19. Voloshchuk A., Velychko D., Osukhivska H., Palamar A. Computer system for energy distribution in conditions of electricity shortage using artificial intelligence. *CEUR Workshop Proceedings*. 2024. Vol. 3742. P. 66–75.

20. Voloskyi V., Leshchyshyn Y., Romanyshyn N., Palamar A., Tarasenko L. Method and algorithm for efficient cell balancing in the lithium-ion battery control system. *CEUR Workshop Proceedings*. 2024. Vol. 3842. P. 258–267.

21. What is Face Recognition? URL: https://aws.amazon.com/what-is/facial-recognition/ (дата звернення: 04.12.2025).

22. ДБН В.2.2-28:2010. Будинки і споруди. Будинки адміністративного та побутового призначення / Мінрегіонбуд України. Київ : Мінрегіонбуд України, 2010. 36 с.

23. Жаровський Р.О., Іваницький В.А. GSM-сигналізації як спосіб розширення функціональності розумних будинків та підвищення безпеки об’єктів нерухомості. Матеріали XIII міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій» Тернопіль: ТНТУ. 2024

24. Жаровський Р.О., Іваницький В.А. Організація захисту стаціонарного об’єкту нерухомості на основі GSM-сигналізації та мікроконтролера Raspberry PI. Матеріали XII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі системи та технології». Тернопіль: ТНТУ. 2024

25. Жаровський Р. О. Конспект лекцій з дисципліни Захист інформації у комп’ютерних системах для студентів денної та заочної форми навчання спеціальності 123 "Комп'ютерна інженерія". Тернопіль, 2019. 268 с.

26. Жаровський Р. О. Методичні вказівки до виконання лабораторних робіт з дисципліни "Захист інформації у комп’ютерних системах" для студентів денної та заочної форми навчання спеціальності 123 "Комп'ютерна інженерія". Тернопіль, 2019. 68 с.

27. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 04.12.2025).

28. Зінов'єва О. Г., Лубко Д. В. Алгоритм Мамдані в системах нечіткого виведення. *Сучасні комп'ютерні та інформаційні системи і технології: матеріали III Всеукраїнської наук.-практ. інтернет-конф.* (Запоріжжя, 12-19 грудня 2022 р.). URL: http://elar.tsatu.edu.ua/handle/123456789/16952 (дата звернення: 05.12.2025).

29. Лупенко С.А., Пасічник В.В., Тиш Є.В. Комп’ютерна логіка. Навчальний посібник. Львів: Видавництво «Магнолія 2006», 2024. 354 с.

30. Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Програма та методичні рекомендації з проходження практики за тематикою кваліфікаційної роботи для студентів спеціальності 123 «Комп'ютерна інженерія». Тернопіль: ТНТУ. 2024. 45 с.

31. Луцків А., Лупенко С., Пасічник В. Паралельні та розподільнені обчислення. Навчальний посібник. Львів: Видавництво «Магнолія 2006», 2024. 566 с.

32. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі. Книга 1. Львів: «Магнолія 2006», 2024. 256 с.

33. НАПБ А.01.001-2014. Правила пожежної безпеки в Україні : затв. наказом М-ва внутр. справ України від 30.12.2014 № 1417 / Верховна Рада України. Київ, 2014.

34. НПАОП 0.00-7.15-18. Вимоги до роботодавців стосовно забезпечення безпечного виконання робіт у потенційно вибухонебезпечних середовищах : затв. наказом М-ва енергетики та вугільної пром-сті України від 05.06.2018 № 317 / Верховна Рада України. Київ, 2018.

35. НПАОП 40.1-1.21-98. Правила безпечної експлуатації електроустановок споживачів : затв. наказом Держнаглядохоронпраці України від 09.01.1998 № 4 / Верховна Рада України. Київ, 1998.

36. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі. Книга 2. Львів: «Магнолія 2006», 2024. 328 с.

37. Оконський М.В., Лупенко С.А., Паламар А.М. Комп'ютерна система для моніторингу метеорологічних параметрів на основі IoT. *Актуальні задачі сучасних технологій: збірник тез доповідей*. Тернопіль: ТНТУ, 2021. С. 112.

38. Рожик А. М., Жаровський Р.О. Аналіз ефективності роботи адаптивної системи контролю доступу на основі нечіткої логіки. *Матеріали наукової конференції ТНТУ*. Тернопіль: ТНТУ, 2025. С. 12–13.

39. Рожик А. М., Жаровський Р.О. Методи та програмно-апаратні засоби ідентифікації працівників з метою визначення робочого часу та доступу до приміщення. *Збірник тез доповідей науково-технічної конференції*. Тернопіль: ТНТУ, 2025. С. 45.

40. Стручок В.С. Безпека в надзвичайних ситуаціях: метод. посіб. для здобувачів освітнього ступеня «магістр». Тернопіль: ФОП Паляниця В. А., 2024. 156 с.

41. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека»: навч. посіб. Тернопіль: ФОП Паляниця В. А., 2024. 156 с.

42. Чайковський А.В., Жаровський Р.О., Лещишин Ю.З. Методичні вказівки до виконання лабораторних робіт з дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» для здобувачів другого (магістерського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання , Тернопіль: ТНТУ, 2021. 94 с.

43. Чайковський А.В., Жаровський Р.О., Лещишин Ю.З. Конспект лекцій з дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» для студентів спеціальності 123 – Комп'ютерна інженерія. Тернопіль, 2021. 148 с.

44. Штовба С., Резнік Р. Покращення точності нечіткої бази Мамдані за допомогою суперечливих правил. *Ukrainian Journal of Information Systems and Data Science*. 2023. Т. 1, № 1. URL: https://jujisds.donnu.edu.ua/article/view/14740 (дата звернення: 05.12.2025).

Додаток А

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя
Маріборский університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Краківський економічний університет (Польща)
Вроцлавський економічний університет (Польща)
Університет «Опольська Політехніка» (Польща)
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Вінницький національний аграрний університет
Львівський національний університет ім. І. Франка
Головне управління Пенсійного фонду в Тернопільській області
Наукове товариство ім. Шевченка
Тернопільський обласний комунальний інститут післядипломної педагогічної освіти
Сумський державний педагогічний університет
Запорізький національний університет

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

XIV Міжнародної науково-технічної конференції молодих учених та студентів

11-12 грудня 2025 року

УКРАЇНА
ТЕРНОПІЛЬ – 2025

УДК 004.5:004.93
Рожик А. М., здобувач вищої освіти
Жаровський Р.О. канд. техн. наук, доц
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОДИ ТА ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ІДЕНТИФІКАЦІЇ ПРАЦІВНИКІВ З МЕТОЮ ВИЗНАЧЕННЯ РОБОЧОГО ЧАСУ ТА ДОСТУПУ ДО ПРИМІЩЕННЯ

Rozhyk A. M.
R.O. Zharovskyi PhD., Associate Prof.

METHODS AND SOFTWARE-HARDWARE MEANS OF EMPLOYEE IDENTIFICATION FOR DETERMINING WORKING TIME AND ACCESS TO PREMISES

Стрімкий розвиток цифрових технологій та підвищення вимог до корпоративної безпеки зумовили широке впровадження біометричних систем контролю та управління доступом. Такі системи забезпечують високий рівень захисту об'єктів та дозволяють автоматизувати облік робочого часу персоналу, використовуючи унікальні фізіологічні характеристики людини, такі як відбиток пальця, геометрія обличчя або голос. Проте практика експлуатації показує, що статичні біометричні системи, які покладаються на один фіксований метод ідентифікації, є вразливими до змін умов навколишнього середовища. Недостатнє або надмірне освітлення критично впливає на точність роботи алгоритмів розпізнавання обличчя, високий рівень акустичного шуму унеможливлює коректну ідентифікацію за голосом, а низькі температури або забруднення поверхонь знижують ефективність ємнісних та оптичних дактилоскопічних сканерів. Вказані фактори призводять до зростання кількості помилкових відмов у доступі, що знижує пропускну здатність контрольно-пропускних пунктів та створює незручності для користувачів [1].

Метою даного дослідження є підвищення надійності та відмовостійкості систем контролю доступу шляхом розробки концепції та програмної реалізації адаптивного інтелектуального ядра. Це ядро повинно в реальному часі аналізувати параметри навколишнього середовища та динамічно обирати оптимальний метод ідентифікації, який забезпечить найкращий результат у поточних умовах.

Для вирішення проблеми чутливості біометричних методів до зовнішніх факторів у роботі запропоновано використання математичного апарату нечіткої логіки. На відміну від жорстких алгоритмів або дерев рішень, які оперують бінарною логікою та чіткими пороговими значеннями, нечітка логіка дозволяє оперувати лінгвістичними змінними та ступенями належності. Це забезпечує плавну адаптацію системи до змін у середовищі та дозволяє уникнути помилок на межі діапазонів, коли незначна зміна фізичного параметра може призвести до кардинальної зміни рішення системи [4].

Розроблена математична модель системи нечіткого виводу базується на аналізі трьох вхідних лінгвістичних змінних, дані для яких надходять із відповідних апаратних сенсорів. Першою змінною виступає рівень шуму, який визначається через співвідношення сигнал до шуму в децибелах і дозволяє оцінити акустичну обстановку для коректної роботи голосових модулів [3]. Другою змінною є освітленність та динаміка сцени, що визначається відсотком рухомих пікселів у відеопотоці та дозволяє виявити рух об'єкта перед камерою. Третьою змінною є температура навколишнього середовища, яка впливає на фізичний стан шкіри пальців та роботу сканерів.

Вихідними змінними моделі є оцінки пріоритетності або придатності для трьох доступних методів ідентифікації, а саме розпізнавання обличчя, голосу та сканування відбитка пальця. Діапазон оцінювання для кожного методу становить від нуля до десяти балів, де вищий бал означає більшу рекомендацію до використання даного методу в поточних умовах.

Програмна реалізація ядра виконана мовою програмування Python із використанням спеціалізованої бібліотеки scikit-fuzzy [2]. Ця бібліотека забезпечує необхідний інструментарій для створення функцій належності, реалізації етапу фазифікації вхідних даних, обробки бази правил та дефазифікації результатів. Для емуляції вхідних сигналів та попередньої обробки медіаданих використано бібліотеки комп'ютерного зору OpenCV та обробки аудіо Librosa. OpenCV застосовується для аналізу відеопотоку та симуляції умов низького освітлення шляхом модифікації яскравості зображення. Librosa використовується для розрахунку співвідношення сигнал до шуму та накладання шумових ефектів на аудіозаписи для тестування стійкості алгоритму.

База знань системи сформована на основі експертних правил, які формалізують залежності між станом середовища та ефективністю біометричних методів. Логіка системи передбачає, що низька освітленість або висока динаміка руху в кадрі роблять метод розпізнавання обличчя непридатним. Аналогічно, високий рівень фонового шуму призводить до зниження пріоритету голосової ідентифікації, а екстремально низькі температури негативно впливають на придатність сканера відбитка пальця. Система агрегує виконання всіх активних правил для формування єдиного узгодженого рішення.

Валідація розробленої математичної моделі проведена шляхом комп'ютерної симуляції різних експлуатаційних сценаріїв. Під час тестування сценарію нічного режиму, який характеризується низьким рівнем освітлення та тишею, система коректно визначила критично низький пріоритет для розпізнавання обличчя та високий пріоритет для голосової ідентифікації. Це дозволяє системі автоматично переключитися на надійніший метод і уникнути помилок розпізнавання в темряві. У сценарії, що імітує шумний виробничий цех з високим рівнем акустичних перешкод та активним рухом персоналу, система деактивувала методи розпізнавання голосу та обличчя, надавши найвищий пріоритет контактному методу сканування відбитків пальців або використанню RFID-картки.

Окрім адаптивного ядра на базі нечіткої логіки, архітектура спроєктованої системи включає пріоритетний модуль безпеки. Цей модуль працює на основі апаратних переривань та має найвищий пріоритет виконання. У разі отримання сигналу тривоги від датчиків пожежної безпеки або задимлення робота інтелектуального ядра блокується. Система миттєво переходить у режим аварійного розблокування всіх точок доступу для забезпечення безперешкодної евакуації персоналу, що є критично важливою вимогою для забезпечення техногенної безпеки на підприємстві.

Література

1. Біометричні системи контролю доступу. UALock. URL: https://ualock.com.ua/ua/p6541327-biometricheskie-sistemy-kontrolya.html (дата звернення: 08.11.2025).

2. Getting started with scikit-fuzzy. Read the Docs. URL: https://scikit-fuzzy.readthedocs.io/en/latest/userguide/getting_started.html (дата звернення: 08.11.2025).

3. Understanding Speech-to-Noise Ratio and Its Impact on Your App. Symbl.ai. URL: https://symbl.ai/developers/blog/understanding-speech-to-noise-ratio-and-its-impact-on-your-app/ (дата звернення: 08.11.2025).

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

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

УДК 004.5:004.93
А. Рожик; Р. Жаровський, к. т. н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ЕФЕКТИВНОСТІ РОБОТИ АДАПТИВНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

UDC 004.5:004.93
A. Rozhyk; R. Zharovskyi, PhD.

ANALYSIS OF THE EFFICIENCY OF THE ADAPTIVE ACCESS CONTROL SYSTEM BASED ON FUZZY LOGIC

В умовах зростання вимог до систем безпеки критично важливим завданням є забезпечення надійної ідентифікації особи незалежно від зовнішніх факторів. Традиційні системи контролю доступу, що базуються на статичних алгоритмах, демонструють зниження ефективності при зміні умов експлуатації: недостатньому освітленні, акустичному шумі або екстремальних температурах. Метою роботи є оцінка ефективності розробленого програмно-апаратного комплексу, що використовує апарат нечіткої логіки для динамічного вибору оптимального методу аутентифікації [1].

Для верифікації розроблених алгоритмів було проведено серію імітаційних експериментів у середовищі MATLAB та реалізовано прототип на базі Raspberry Pi 3 B+. Вхідними даними слугували показники сенсорів: рівень освітленості (Lux), акустичний шум (dB) та температура (°C). Ядром прийняття рішень виступає контролер нечіткої логіки типу Мамдані, який розраховує коефіцієнт придатності для методів розпізнавання обличчя, голосу та відбитків пальців.

На першому етапі було проаналізовано адекватність реакції системи на динамічну зміну освітленості. Результати моделювання (рис. 1), дозволили визначити оцінку придатності методу Face ID в залежності від рівня освітленості.

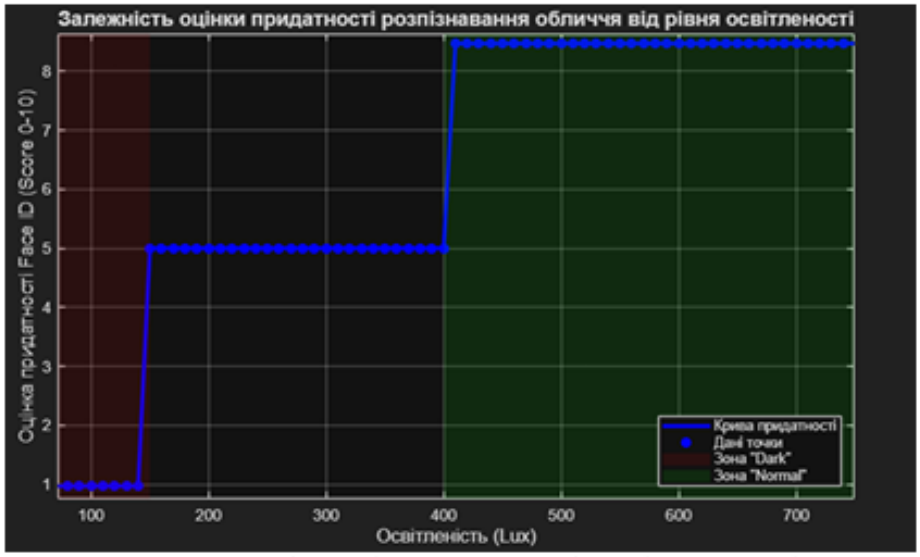

Рисунок 1. Залежність оцінки придатності розпізнавання обличчя від рівня освітленості

Графік показує, що у зоні «Dark» система присвоює методу мінімальний пріоритет, що блокує його використання. При зростанні освітленості понад 400 Люкс оцінка придатності різко зростає до максимуму, стабілізуючись у зоні нормального освітлення. Це підтверджує здатність системи адаптуватися до умов видимості з мінімальним рівнем помилкових спрацювань.

Другим етапом стала перевірка стабільності роботи дактилоскопічного сканера в залежності від температурних режимів. Моделювання динаміки, зображене на рисунку 2, підтверджує наявність чітко вираженої «зони комфорту».

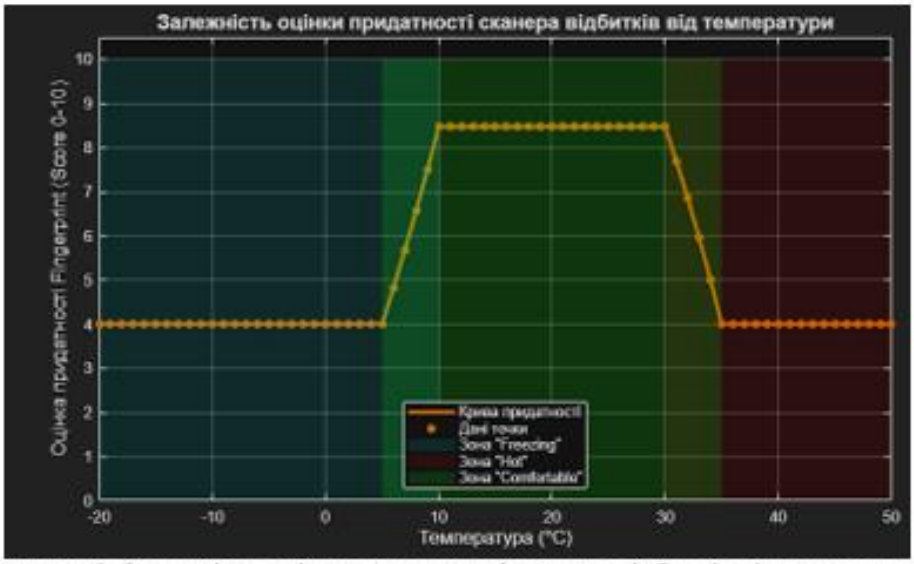

Рисунок 2. Залежність оцінки придатності сканера відбитків від температури

Як видно з графіка, система утримує високий пріоритет для сканера відбитків у діапазоні температур від +10°C до +30°C. При виході за ці межі оцінка лінійно знижується до 4 балів. Це дозволяє уникнути помилок зчитування, викликаних зміною фізіологічного стану шкіри [2].

Третім етапом став комплексний аналіз взаємного впливу факторів. Встановлено, що розроблена база правил коректно обробляє ситуації з декількома змінними. На рисунку 3 наведено поверхню нечіткого виводу для оцінки придатності відеоканалу.

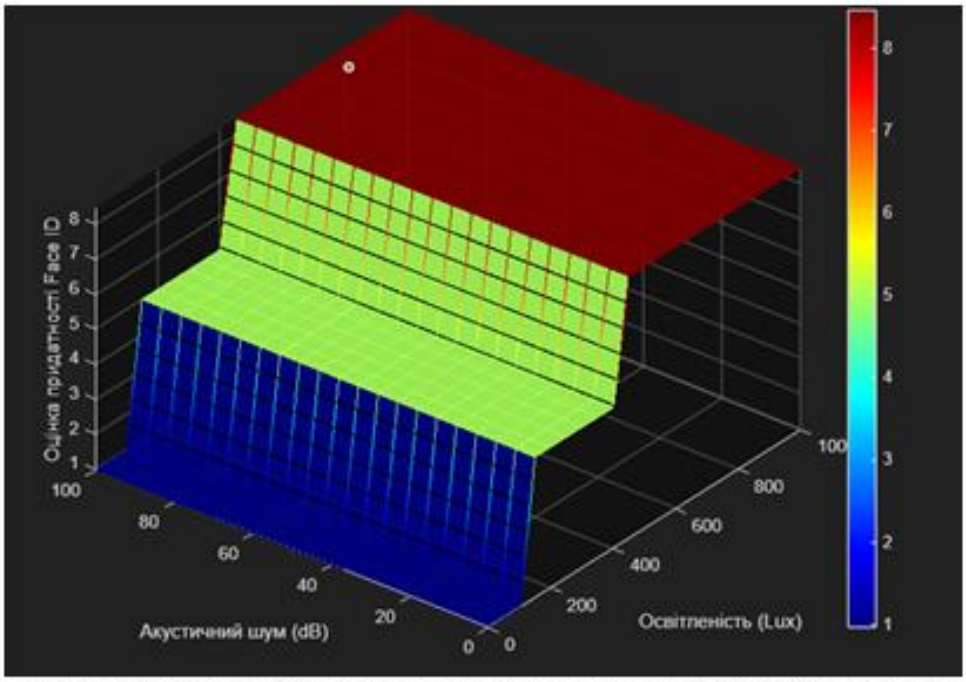

Рисунок 3. Поверхня нечіткого виводу для оцінки придатності розпізнавання обличчя

Наведений графік демонструє, що рівень акустичного шуму не впливає на пріоритет розпізнавання обличчя (профіль не змінюється вздовж осі шуму), тоді як освітленість є

визначальним фактором. Це свідчить про коректну ізоляцію каналів прийняття рішень та відсутність негативної інтерференції між правилами [3].

Результати досліджень свідчать, що впровадження розробленого адаптивного алгоритму дозволяє автоматизувати вибір надійного методу ідентифікації. Система забезпечує перемикання на альтернативні методи (голосовий або RFID) у критичних умовах, що підвищує загальну надійність комплексу та зменшує кількість помилок відмови у доступі.

Література

1. AI-Driven Adaptive Authentication for Multi-Modal Biometric Systems. *ResearchGate*. 2024. URL: https://www.researchgate.net/publication/385002869_AI-Driven_Adaptive_Authentication_for_Multi-Modal_Biometric_Systems (дата звернення: 09.12.2025).
2. Biometric Authentication System For Access Control. *CEUR Workshop Proceedings*. 2024. Vol. 3706. URL: https://ceur-ws.org/Vol-3706/Paper13.pdf (дата звернення: 09.12.2025).
3. Fuzzyfortify: a multi-attribute risk assessment for multi-factor authentication. *Frontiers in Computer Science*. 2025. URL: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp. 2025.1557918/full (дата звернення: 09.12.2025).

Додаток Б

Лістинг програми

```
import numpy as np
import skfuzzy as fuzz
from skfuzzy import control as ctrl

class FuzzyLogicKernel:
    def __init__(self):
        print("--- Initializing Fuzzy Logic Kernel (Mamdani) ---")

        #
================================================================
        # 1. Вхідні лінгвістичні змінні (Antecedents) [cite: 16-
20]
        #
================================================================

        # Освітленість ($L$): Діапазон [0...1000] Lux [cite: 17]
        self.L = ctrl.Antecedent(np.arange(0, 1001, 1), 'light')

        # Акустичний шум ($N$): Діапазон [0...100] dB [cite: 18]
        self.N = ctrl.Antecedent(np.arange(0, 101, 1), 'noise')

        # Температура ($T$): Діапазон [-20...+50] C [cite: 20]
        self.T = ctrl.Antecedent(np.arange(-20, 51, 1), 'temp')

        #
================================================================
        # 2. Вихідні лінгвістичні змінні (Consequents) [cite: 29]
        #
================================================================

        # Коефіцієнт придатності (Score) для кожного методу: 0-10
        # Методи: Обличчя, Голос, Відбиток [cite: 5]
        self.suit_face = ctrl.Consequent(np.arange(0, 11, 0.1),
'face_suit')
        self.suit_voice = ctrl.Consequent(np.arange(0, 11, 0.1),
'voice_suit')
        self.suit_finger = ctrl.Consequent(np.arange(0, 11, 0.1),
'finger_suit')

        # Налаштування методу дефазифікації: Центр тяжіння
(Centroid) [cite: 28]
        self.suit_face.defuzzify_method = 'centroid'
        self.suit_voice.defuzzify_method = 'centroid'
        self.suit_finger.defuzzify_method = 'centroid'

        #
================================================================
        # 3. Функції належності (Membership Functions) [cite: 17,
18, 20]
        #
```

```
================================================================

        # --- Light Terms: Dark, Dim, Normal, Bright ---
        self.L['Dark']   = fuzz.trimf(self.L.universe, [0, 0,
150])
        self.L['Dim']    = fuzz.trimf(self.L.universe, [100, 300,
500])
        self.L['Normal'] = fuzz.trimf(self.L.universe, [400, 600,
800])
        self.L['Bright'] = fuzz.trapmf(self.L.universe, [700, 900,
1000, 1000])

        # --- Noise Terms: Silent, Moderate, Loud, Very High ---
        self.N['Silent']   = fuzz.trimf(self.N.universe, [0, 0,
30])
        self.N['Moderate'] = fuzz.trimf(self.N.universe, [20, 50,
70])
        self.N['Loud']     = fuzz.trimf(self.N.universe, [60, 80,
90])
        self.N['VeryHigh'] = fuzz.trapmf(self.N.universe, [85, 95,
100, 100])

        # --- Temp Terms: Freezing, Comfortable, Hot ---
        self.T['Freezing']    = fuzz.trapmf(self.T.universe, [-20,
-20, 0, 10])
        self.T['Comfortable'] = fuzz.trimf(self.T.universe, [5,
22, 35])
        self.T['Hot']         = fuzz.trapmf(self.T.universe, [30,
40, 50, 50])

        # --- Output Terms: Unusable, Low, Medium, High ---
        # Універсальні терми для всіх вихідних змінних
        for method in [self.suit_face, self.suit_voice,
self.suit_finger]:
            method['Unusable'] = fuzz.trimf(method.universe, [0,
0, 3])
            method['Low']      = fuzz.trimf(method.universe, [2,
4, 6])
            method['High']     = fuzz.trapmf(method.universe, [6,
8, 10, 10])

        #
================================================================
        # 4. База правил (Rule Base) [cite: 21-26]
        #
================================================================

        rules = []

        # --- Негативні правила (Обмеження фізики сенсорів) ---

        # [cite: 24] IF (Light is Dark) THEN (Face_Suitability is
Unusable)
        rules.append(ctrl.Rule(self.L['Dark'],
self.suit_face['Unusable']))
```

```
        # [cite: 25] IF (Noise is Loud) THEN (Voice_Suitability is
Low)
        # Розширено логіку на VeryHigh
        rules.append(ctrl.Rule(self.N['Loud'] |
self.N['VeryHigh'],
self.suit_voice['Low']))

        # [cite: 26] IF (Temp is Freezing OR Hot) THEN
(Fingerprint_Suitability is Low)
        rules.append(ctrl.Rule(self.T['Freezing'] | self.T['Hot'],
self.suit_finger['Low']))

        # --- Позитивні правила (Евристика для нормальних умов) --
-

        # Хороше світло -> Високий пріоритет обличчя
        rules.append(ctrl.Rule(self.L['Normal'] |
self.L['Bright'], self.suit_face['High']))

        # Тиша -> Високий пріоритет голосу
        rules.append(ctrl.Rule(self.N['Silent'] |
self.N['Moderate'],
self.suit_voice['High']))

        # Комфортна температура -> Високий пріоритет відбитка
        rules.append(ctrl.Rule(self.T['Comfortable'],
self.suit_finger['High']))

        # Компіляція контролера
        self.access_ctrl = ctrl.ControlSystem(rules)
        self.simulation =
ctrl.ControlSystemSimulation(self.access_ctrl)
        print("[OK] Fuzzy Kernel Compiled.")

    def compute_priorities(self, lux_val, noise_val, temp_val):
        """
        Виконання розрахунку нечіткої моделі.
        Етап: 4. Computing

        Args:
            lux_val (float): Поточна освітленість.
            noise_val (float): Поточний шум.
            temp_val (float): Поточна температура.

        Returns:
            list: Список кортежів (method_name, score),
відсортований за
спаданням[cite: 29].
        """
        # 1. Передача чітких значень на вхід (Fuzzification)
        self.simulation.input['light'] = np.clip(lux_val, 0, 1000)
        self.simulation.input['noise'] = np.clip(noise_val, 0,
100)
```

```
        self.simulation.input['temp']  = np.clip(temp_val, -20,
50)

        # 2. Виконання нечіткого виводу (Inference)
        try:
            self.simulation.compute()
        except Exception as e:
            print(f"[ERROR] Fuzzy Compute Failed: {e}")
            # Fallback у випадку помилки розрахунку
            return [('rfid', 10.0)]

        # 3. Отримання результатів дефазифікації (Defuzzification)
        scores = {
            'face':        self.simulation.output['face_suit'],
            'voice':       self.simulation.output['voice_suit'],
            'fingerprint': self.simulation.output['finger_suit']
        }

        # Логування розрахованих балів
        print(f"[DEBUG] Calculated Scores -> Face:
{scores['face']:.2f}, "
              f"Voice: {scores['voice']:.2f}, Finger:
{scores['fingerprint']:.2f}")

        # 4. Формування пріоритетного списку [cite: 29]
        # Сортування: max -> min
        sorted_methods = sorted(scores.items(), key=lambda item:
item[1],
reverse=True)

        return sorted_methods

# Приклад виклику для тестування логіки
if __name__ == "__main__":
    fuzzy_brain = FuzzyLogicKernel()

    # Тест 1: Темна кімната, тихо, холодно
    # Очікуємо: Face -> Low, Voice -> High, Finger -> Low
    print("\n--- TEST CASE: Dark, Silent, Freezing ---")
    result = fuzzy_brain.compute_priorities(lux_val=10,
noise_val=20, temp_val=-10)
    print(f"Winner: {result[0][0].upper()} (Score:
{result[0][1]:.2f})")

    # Тест 2: Яскраво, шумно, комфортно
    # Очікуємо: Face -> High, Voice -> Low, Finger -> High
    print("\n--- TEST CASE: Bright, Loud, Comfortable ---")
    result = fuzzy_brain.compute_priorities(lux_val=800,
noise_val=85, temp_val=22)
    print(f"Winner: {result[0][0].upper()} (Score:
{result[0][1]:.2f})")
```