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 наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження смарт систем біометричної ідентифікації на базі IoT-пристроїв

Виконав: студент VI курсу, групи СНнм-61
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Савчишин Я.С.
(підпис) (прізвище та ініціали)

Керівник _____ Дуда О.М.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Никитюк В.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (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 наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« 28 » _травня__ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Савчишину Ярославу Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження смарт систем біометричної ідентифікації на базі IoT-пристроїв

Керівник роботи Дуда Олексій Михайлович, кандидат технічних наук, доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 29 » листопада 2024 року № 4/7-1139

2. Термін подання студентом завершеної роботи 26 травня 2025р.

3. Вихідні дані до роботи Наукові публікації, присвячені дослідженню інтеграції біометричних технологій із хмарними платформами та штучним інтелектом у межах IoT та дослідженню смарт-систем біометричної ідентифікації на базі IoT.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналітичний огляд біометричних систем в контексті IoT: сучасні підходи, тренди та перспективи. 2 Дослідження смарт систем та технологій біометричної ідентифікації на основі IoT. 3 Розпізнавання облич у смарт-системі: аналіз, реалізація, доцільність. 4 Охорона праці та безпека в надзвичайних ситуаціях. Висновки. Додатки.

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

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин В.С., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач		

7. Дата видачі завдання 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.11.2024	
2.	Підбір та опрацювання наукових публікацій, збір	02.12.2024-10.01.2025	
	даних щодо смарт систем біометричної ідентифікації		
	на базі IoT-пристроїв		
3.	Виконання дослідження смарт систем біометричної	13.01.2025-14.03.2025	
	ідентифікації на базі IoT-пристроїв		
4.	Оформлення розділу «Аналітичний огляд	17.03.2025-28.03.2025	
	біометричних систем в контексті IoT: сучасні підходи,		
	тренди та перспективи»		
5.	Оформлення розділу «Дослідження смарт систем	31.03.2025-11.04.2025	
	та технологій біометричної ідентифікації на		
	основі IoT»		
6.	Оформлення розділу «Розпізнавання облич у	14.04.2025-25.04.2025	
	смарт-системі: аналіз, реалізація, доцільність»		
7.	Виконання завдання до підрозділу «Охорона праці»	28.04.2025-02.05.2025	
8.	Виконання завдання до підрозділу «Безпека в	28.04.2025-02.05.2025	
	надзвичайних ситуаціях»		
9.	Оформлення кваліфікаційної роботи	05.05.2025-09.05.2025	
10.	Нормоконтроль	12.05.2025-15.05.2025	
11.	Перевірка на плагіат	16.05.2025	
12.	Попередній захист кваліфікаційної роботи	19.05.2025	
13.	Захист кваліфікаційної роботи	29.05.2025	

Студент _____ Савчишин Я.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Дуда О.М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження смарт систем біометричної ідентифікації на базі IoT-пристроїв // Кваліфікаційна робота освітнього рівня «Магістр» // Савчишин Ярослав Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНнм-61 // Тернопіль, 2025 // С. 74, рис. – 6, табл. – 2, додат. – 2, бібліогр. – 74.

Ключові слова: штучний інтелект, розпізнавання облич, інтернет речей, біометрична ідентифікація, нейронні мережі, смарт системи, контроль доступу.

Кваліфікаційна робота присвячена дослідженню смарт систем біометричної ідентифікації на базі IoT-пристроїв.

В першому розділі кваліфікаційної роботи розглянуто сучасні підходи до побудови біометричних систем ідентифікації в контексті IoT. Проаналізовано технологічну еволюцію, архітектури, алгоритми та етичні виклики, що виникають під час впровадження біометрії у смарт середовища.

У другому розділі досліджено концепцію смарт систем, методи біометричного розпізнавання та технічну інтеграцію з IoT-пристроями. Описано архітектури, типи сенсорів, протоколи обміну та платформне забезпечення, зокрема на базі Raspberry Pi.

У третьому розділі представлено реалізацію системи розпізнавання обличчя для обліку присутності, охарактеризовано технічні обмеження, переваги використання, виклики впровадження та етапи практичного тестування.

Об'єкт дослідження: біометрична ідентифікація особи в реальному часі. Предмет дослідження: смарт система на базі IoT для розпізнавання облич та контролю присутності.

ANNOTATION

Study of Smart Biometric Identification Systems Based on IoT Devices // The educational level "Master" qualification work // Savchyshyn Yaroslav // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SNnm-61 group // Ternopil, 2025 // P. 74, fig. – 6, tables – 2, annexes – 2, ref. – 74.

Keywords: artificial intelligence, facial recognition, Internet of Things, biometric identification, neural networks, smart systems, access control.

The qualification thesis is devoted to the study of smart biometric identification systems based on IoT devices.

The first chapter explores modern approaches to building biometric identification systems in the context of IoT. It analyzes technological evolution, system architectures, recognition algorithms, and ethical challenges arising from implementing biometrics in smart environments.

The second chapter examines the concept of smart systems, biometric recognition methods, and technical integration with IoT devices. It describes system architectures, sensor types, communication protocols, and platform-level implementation, particularly on Raspberry Pi.

The third chapter presents the implementation of a facial recognition system for attendance tracking, outlines technical limitations, usage advantages, deployment challenges, and the stages of practical testing.

Object of research: real-time biometric identification of individuals. Subject of research: IoT-based smart system for facial recognition and presence monitoring.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ШІ – Штучний інтелект.

IoT (Internet of Things) – Інтернет речей.

RFID (Radio Frequency Identification) – радіочастотна ідентифікація.

CNN (Convolutional Neural Network) – згорткова нейронна мережа.

LFW (Labeled Faces in the Wild) – база зображень облич, маркованих для задач розпізнавання.

VGGFace – набір даних зображень облич, зібраний для тренування моделей розпізнавання (створений Visual Geometry Group, Oxford).

MQTT (Message Queuing Telemetry Transport) – телеметричний транспорт протоколу обміну повідомленнями.

BLE (Bluetooth Low Energy) – енергоефективний Bluetooth.

TPM (Trusted Platform Module) – модуль довіреної платформи.

HSM (Hardware Security Module) – апаратний модуль безпеки.

HOG (Histogram of Oriented Gradients) – гістограма орієнтованих градієнтів.

LBP (Local Binary Patterns) – локальні бінарні шаблони.

PCA (Principal Component Analysis) – метод головних компонент.

GPRS (General Packet Radio Service) – загальна пакетна радіослужба.

TCP (Transmission Control Protocol) – протокол керування передаванням.

IP (Internet Protocol) – інтернет-протокол.

AI (Artificial Intelligence) – штучний інтелект.

SSL (Secure Sockets Layer) – рівень захищених сокетів.

TLS (Transport Layer Security) – захист транспортного рівня.

FRT (Face Recognition Technology) – технологія розпізнавання облич.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному цифровому середовищі стрімке поширення Інтернету речей (IoT) та зростання вимог до безпеки персональних даних зумовлюють потребу у впровадженні новітніх методів автентифікації. Особливої уваги в цьому контексті набувають смарт системи біометричної ідентифікації, які поєднують інтелектуальні алгоритми розпізнавання з можливостями розподілених обчислень. Такі системи дозволяють не лише підвищити точність розпізнавання особи, а й забезпечити безконтактність, адаптивність і оперативність обробки, що критично важливо у сферах безпеки, логістики, охорони здоров'я та міської інфраструктури.

Актуальність теми полягає у необхідності комплексного аналізу та практичної реалізації смарт систем біометричної ідентифікації на базі IoT-платформ з урахуванням технічних, програмних, етичних та нормативно-правових аспектів.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є вивчення алгоритмів та технологій створення смарт систем біометричної ідентифікації на базі IoT-пристроїв, а також розробка прототипу такої системи з використанням технології розпізнавання облич. Для досягнення цієї мети визначено наступні завдання:

– Проаналізувати ключові терміни, підходи та алгоритмічні моделі, які використовуються у смарт-системах біометричної ідентифікації на базі IoT-пристроїв.

– Дослідити технологічні засоби та інфраструктуру для реалізації розпізнавання обличчя в смарт системах.

– Проаналізувати, яким чином вибір архітектури, протоколів безпеки та ресурсних обмежень IoT-пристроїв позначається на точності, швидкодії та стійкості процесу ідентифікації користувача.

– Виокремити виклики та перспективи подальшого розвитку смарт систем біометричної ідентифікації.

– Розробити прототип системи розпізнавання облич на платформі Raspberry Pi.

Об’єкт дослідження: алгоритми обробки біометричних даних, технічні засоби реалізації систем розпізнавання облич у розподіленому середовищі IoT.

Предмет дослідження: процес біометричної ідентифікації у смарт системах, інтегрованих із IoT-пристроями.

Наукова новизна полягає у подальшому розвитку біометричної ідентифікації, що поєднує локальне (edge) обчислення ознак із апаратною реакцією на результат розпізнавання та інтегрує мінімальні IoT-компоненти у повнофункціональне рішення.

Практичне значення одержаних результатів. Спроєктовано й випробувано смарт-систему, придатну для контролю доступу, автоматизованого обліку та персональної безпеки без залучення ресурсоємного серверного обладнання.

Апробація результатів магістерської роботи здійснена під час створення прототипу системи, яка була протестована у реальних умовах. Основні результати обговорено на конференції «Міжнародні наукові дослідження: інтеграція науки та практики як механізм ефективного розвитку» в Інституті інноваційної освіти, науково-навчальному центрі прикладної інформатики НАН України.

Структура роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Основний обсяг становить 74 сторінок, включаючи 6 рисунків та 2 таблиці.

1 АНАЛІТИЧНИЙ ОГЛЯД БІОМЕТРИЧНИХ СИСТЕМ В КОНТЕКСТІ IOT: СУЧАСНІ ПІДХОДИ, ТРЕНДИ ТА ПЕРСПЕКТИВИ

1.1 Основні поняття біометричної ідентифікації та IoT-технологій

В умовах зростаючої залежності суспільства від цифрових технологій питання безпеки особистих даних та захисту від несанкціонованого доступу набувають актуальності, що зумовлює потребу у впровадженні більш надійних методів ідентифікації особи – саме тому біометричну ідентифікацію дедалі частіше застосовують як зручний та ефективний засіб підтвердження особи. Біометрія людини дозволяє використання її унікальних фізичних або поведінкових характеристик, їх важко підробити чи передати іншій особі. У контексті інформаційних технологій це дозволяє ідентифікацію користувача не за допомогою традиційного логіна і пароля, інформацію яка може передаватись, а через те, чим він є.

З найбільш розповсюджених фізіологічних ознак, які використовуються для ідентифікації особи, можна виділити відбитки пальців, геометрію долоні, структуру райдужної оболонки ока, голос, а також обличчя. Саме розпізнавання обличчя є прикладом фізіологічної біометрії, що не потребує безпосереднього контакту, а отже, має вищу зручність у повсякденному застосуванні [1].

З іншого боку, технологія IoT (Internet of Things) передбачає об’єднання фізичних пристроїв: сенсорів, контролерів, виконавчих механізмів в єдину мережу, здатну до автоматичного збору, передачі та обробки даних. Інтернет речей дає змогу розширити функціональні можливості цифрових систем, дозволяючи їм працювати у фізичному світі: реагувати на події, змінювати середовище, вести облік тощо.

Поєднання біометричної ідентифікації з інфраструктурою IoT створює передумови для формування нових типів «розумних» систем. Наприклад, двері, які автоматично відкриваються лише при розпізнаванні авторизованого обличчя, або система відвідування, що фіксує присутність працівників без потреби у паперовому обліку чи використанні RFID-карт [2]. Завдяки інтеграції IoT, такі

системи можуть не лише фіксувати факт ідентифікації, але й зберігати дані у хмарних сервісах, відправляти звіти адміністрації або автоматично запускати додаткові сценарії такі, як включення світла чи запуск вентиляції.

Слід зазначити, що поняття «смарт-система біометричної ідентифікації» не обмежується лише апаратною частиною. Вона включає програмні алгоритми машинного навчання, мережеві протоколи, системи управління базами даних, елементи інтерфейсу користувача та засоби кібербезпеки. Таким чином, вона перетворюється на багаторівневу інформаційно-технічну систему, здатну до адаптування, масштабування та інтеграції у різні цифрові платформи [3].

Варто наголосити, що біометрична ідентифікація та IoT-технології – це не окремі напрямки, а взаємопов’язані складові одного цілого, це не лише покращує якість цифрової взаємодії, а й дозволяє побудову безпечних, автономних і зручних середовищ у сфері освіти, охорони здоров’я, промисловості та міського управління.

1.2 Технологічна еволюція біометричних систем і інтеграція з IoT

Біометричні технології не є новим явищем: наприкінці XIX століття антропометрія почала застосовуватися в криміналістиці для фіксації індивідуальних ознак людини [4]. Однак, тільки з розвитком цифрових обчислювальних потужностей та нейромережевого моделювання стало можливим створення систем, здатних до автоматичного, безконтактного та масштабованого розпізнавання користувачів. Біометрія в сучасному розумінні – це не лише про відбитки пальців або сканування обличчя, а технічна екосистема, у якій зчитування, обробка, передача та аналіз даних тісно пов’язані з інтелектуальними обчисленнями.

Якщо подивитися на те, що саме дало поштовх розвитку таких систем, то варто згадати кілька ключових речей. По-перше, стрімке зменшення розмірів апаратних засобів: камери з високою роздільною здатністю, мультиспектральні сенсори, мініатюрні процесори, усе це дозволило вбудовувати біометричні модулі навіть у звичайні смартфони чи маленькі плати на зразок Raspberry Pi.

По-друге, із переходом до концепцій edge computing і fog computing з’явилася можливість обробляти дані прямо на пристрої, без необхідності надсилати їх у "хмару". Це не тільки пришвидшує процес, а й зменшує ризики витоку чутливої інформації.

Третім вагомим кроком стало поступове впровадження алгоритмів глибокого навчання для ідентифікації осіб, насамперед на базі згорткових нейронних мереж (Convolutional neural network, CNN) [5]. Дані моделі дозволили значно підвищити точність та стійкість до факторів, що раніше знижували ефективність розпізнавання зміни освітлення, кути огляду, наявність часткових перешкод або аксесуарів. Зрештою, поява відкритих датасетів (LFW, VGGFace, MS-Celeb-1M) сприяла стандартизації підходів до тренування моделей та зростанню академічної і промислової уваги до тематики [6].

Еволюція біометрії не відбулася б без розвитку цифрової взаємодії. Саме IoT-інфраструктура стала середовищем, що дозволила біометричним системам вийти у широкий доступ. З'єднання ідентифікаційних сенсорів із мережами передачі даних (Wi-Fi, Bluetooth, Zigbee, LoRaWAN) забезпечило можливість масштабованого розгортання в умовах обмеженого середовища. Особливо це помітно в контексті «розумних міст», де розпізнавання облич у транспорті, безпекових системах або сервісах доступу стало реальністю, а не концепцією.

Проте не всі науковці погоджуються з масовою інтеграцією біометрії з IoT. Ці дослідники повідомляють про ризики надмірної автоматизації контролю, втрату приватності та вразливість систем до атак типу spoofing або підміни даних. Це спричиняє потребу у додаткових протоколах захисту: багатофакторній автентифікації, шифруванні на рівні edge-пристрою, а також у запровадженні політик прозорого керування біометричними записами.

У широкому контексті, еволюція біометричних систем демонструє відступ від лінійних технологічних рішень до адаптивних, інтелектуально-контекстуалізованих екосистем. Завдяки взаємодії з IoT, вони отримують здатність до самонавчання, прогнозування поведінки користувача та реакції у реальному часі на зміни середовища. Водночас така складність викликає нові

виклики, пов’язані з етичним впровадженням, юридичним регулюванням і технічною відповідальністю систем.

Тому, сучасна біометрична ідентифікація – це вже не окрема технологія, а частина великої екосистеми IoT, яка поступово трансформує способи ідентифікації, безпеки й персоналізації в цифровому світі.

1.3 Огляд сучасних архітектур IoT-біометричних систем

Архітектура відіграє ключову роль у проектуванні смарт систем біометричної ідентифікації, оскільки вона визначає спосіб взаємодії між фізичними пристроями, обчислювальними модулями та програмною логікою. Вона впливає не лише на продуктивність, але й на масштабованість, захищеність та стійкість системи до збоїв. У випадку з IoT-рішеннями, що використовують біометричні дані, зокрема зображення обличчя, важливо враховувати специфіку розподіленого середовища, обмеженість ресурсів кінцевих пристроїв та вимоги до реального часу.

Типова архітектура таких систем зазвичай має три або більше рівнів, у спрощеному варіанті її можна представити у вигляді тришарової моделі [7]. Дану архітектуру зображено у таблиці 1.1

Таблиця 1.1 – Архітектура IoT-біометричних систем

Рівень	**Назва рівня**	**Основні функції**
1	Фізичний (сенсорний) рівень	Збір біометричних даних за допомогою сенсорів, камер або мікрофонів
2	Мережевий рівень	Передача даних через мережеві протоколи (Wi-Fi, BLE, MQTT, LoRa)
3	Прикладний рівень	Обробка, зберігання, ідентифікація, авторизація, візуалізація результатів

Іноді в архітектурі біометричних систем між сенсором і центральним сервером додається проміжний рівень обробки, так зване edge або fog computing. Цей проміжний рівень дозволяє виконувати частину обчислень прямо «на місці», вилучати ключові ознаки, фільтрувати шум або навіть частково ідентифікувати користувача ще до передачі даних далі. Це помітно розвантажує центральну систему та скорочує затримки, що особливо критично в умовах нестабільного інтернет-з'єднання або обмежених ресурсів, наприклад у польових умовах чи в розумних пристроях із низькою пропускною здатністю.

У літературі, як академічній, так і прикладній можна знайти кілька типових архітектурних підходів до побудови IoT-систем із біометрією [8]:

– Централізована модель. Біометричні дані надходять на центральний сервер, де й відбувається обробка. Такий варіант зручний для невеликих інсталяцій, де мережеві умови контрольовані. Але з масштабуванням виникають проблеми: зростають затримки, зростає вразливість до обриву з'єднання.

– Розподілена модель з локальною обробкою (edge-based). Частина роботи виконується прямо на пристрої, наприклад, первинне виявлення обличчя, його кодування. Це дозволяє мінімізувати обсяг трафіку й підвищує незалежність системи від зовнішніх каналів зв'язку.

– Гібридна модель (fog + cloud). Найгнучкіший варіант, де обчислення розподілені між локальними вузлами та хмарними сервісами. Вона дає більше можливостей для адаптації, але і складна в реалізації, особливо коли йдеться про узгодженість даних і безпеку.

У специфічних випадках, наприклад, для військових або банківських системах – безпека в приорітеті. Тут можуть шифрувати дані вже на сенсорному рівні, а для обробки та зберігання ключів використовуються спеціалізовані модулі: TPM, HSM або інші апаратні рішення з високим рівнем довіри. Досить популярним підходом останніх років стало також використання так званої serverless-архітектури чи мікросервісного підходу, де кожна функція є незалежним компонентом [9]. Це забезпечує гнучкість і масштабованість, але ускладнює контроль за цілісністю процесу обробки даних.

Зрештою, жодну з цих моделей не можна назвати універсальною або «найкращою». Кожна має свої переваги та недоліки, і вибір завжди залежить від конкретних обставин.

1.4 Методи та алгоритми біометричної ідентифікації на IoT-платформах

Використання алгоритмічних методів у біометричних системах, що функціонують у межах IoT-інфраструктури, передбачає поєднання двох принципово різних вимог: високої точності розпізнавання та обмеженості ресурсів. Цей баланс вимагає адаптації або навіть спрощення традиційних алгоритмів комп'ютерного зору, не жертвуючи при цьому базовими показниками надійності. Розуміння, які саме методи доцільні в умовах IoT, потребує критичного переосмислення класичних підходів до біометрії.

На сьогодні більшість рішень, що працюють з розпізнаванням облич, ґрунтуються на багатоступеневому процесі, який включає: виявлення обличчя у зображенні, вилучення унікальних ознак, побудову векторного представлення (ембедінгу) та порівняння з існуючими шаблонами у базі.

У кожному з цих кроків можливе застосування різних алгоритмів, вибір яких значною мірою залежить від обчислювальних можливостей пристрою. Умовно, всі методи можна поділити на традиційні, на основі ознак, та сучасні, на основі глибинного навчання. Таблиця 1.2 подає узагальнення цих підходів.

Таблиця 1.2 – Поширені методи біометричної ідентифікації для IoT-систем

Етап	Алгоритм	Особливості застосування в IoT
Виявлення обличчя	Haar Cascades, HOG (Histogram of Oriented Gradients), MTCNN	Haar – швидкий, але менш точний; HOG добре працює на малих пристроях; MTCNN – глибока мережа для точного виявлення

Продовження таблиці 1.2

Вилучення ознак	LBP (Local Binary Patterns), PCA, Gabor Filters	Створюють 128 або 512-розмірні вектори; потребують GPU для тренування, але inference можливий на CPU
Побудова ембедінгу	FaceNet, Dlib ResNet, ArcFace	Створюють 128 або 512-розмірні вектори; потребують GPU для тренування, але inference можливий на CPU
Порівняння	cosine similarity, Euclidean distance, k-NN	Простота реалізації, можливість оптимізації під обмеження IoT

Застосування CNN та їх варіантів (наприклад, MobileNet, SqueezeNet) дозволяє ефективно вилучати ознаки зображень навіть у випадках, коли вхідні дані мають низьку роздільну здатність. Саме такі архітектури часто використовують у пристроях з обмеженим обсягом оперативної пам’яті.

Водночас деякі IoT-сценарії не дозволяють зберігати велику кількість шаблонів або постійно звертатись до центрального серверу. У таких випадках популярним є підхід до «on-device inference», коли вся обробка, включно з порівнянням ембедінгів, виконується локально. Це забезпечує кращу латентність, але вимагає додаткової оптимізації моделі (наприклад, квантування ваг, pruning) [10].

Значна частина академічних публікацій також звертає увагу на проблему енергоспоживання. Алгоритми, що потребують тривалого часу обробки, спричиняють швидке виснаження живлення пристрою, що критично для автономних IoT-розгортань. Одним із напрямів вирішення цієї проблеми є використання т.зв. «lightweight models», спрощених нейронних мереж із меншою кількістю параметрів, спеціально призначених для мікроконтролерів.

У певних сценаріях, зокрема в біометричному контролі доступу, доречним є застосування комбінованих моделей, наприклад, об'єднання детектора обличчя

на основі HOG з класифікатором, що працює на CNN. Це дозволяє досягти прийнятного компромісу між продуктивністю і точністю. Сучасні фреймворки, як-от TensorFlow Lite, OpenVINO чи MediaPipe, дають змогу запускати такі моделі навіть на пристроях із мінімальними ресурсами (Raspberry Pi, Jetson Nano) [10].

Однак, попри досягнутий прогрес, залишається відкритим питання захисту від атак типу spoofing – підміни справжнього обличчя фотографією або відео. Частина дослідників вважає, що лише поєднання кількох біометричних факторів (мультимодальність) або виявлення живості (liveness detection) може суттєво зменшити ризики таких атак.

Таким чином, вибір алгоритмів для IoT-біометрії не можна розглядати ізольовано. Він формується в умовах компромісів між точністю, швидкістю, обсягом пам’яті, енергоспоживанням та надійністю, а тому вимагає як технічного аналізу, так і врахування контексту впровадження.

1.5 Порівняльний аналіз сучасних рішень та комерційних платформ

1.5.1 Біометричнний термінал SpeedFace-V5L

Компанія ZKTeco відома як один з провідних виробників рішень у сфері біометричної безпеки та RFID-технологій. Її діяльність сконцентрована, передусім, на технологіях розпізнавання обличчя, вен долоні, відбитків пальців і райдужної оболонки ока. Ці рішення широко впроваджуються у системи контролю доступу, автоматизованого обліку робочого часу, а також використовуються у системах відеоспостереження. Важливо підкреслити, що ці технології не є винятково технічними новаціями, а радше відповіддю на потреби у підвищеній ідентифікаційній надійності.

SpeedFace-V5L – це високошвидкісний біометричний термінал контролю доступу з розпізнаванням осіб (рисунок 1.1).

Рисунок 1.1 – Біометричний термінал ZKTeco SpeedFace-V5L

Серед останніх розробок компанії виділяється серія терміналів SpeedFace-V5L – оновлена лінійка пристроїв, що працюють на основі алгоритмів комп'ютерного зору та підтримують мультифакторну ідентифікацію. Вони можуть ідентифікувати користувача як за обличчям, так і за відбитком пальця чи долонею, демонструючи при цьому високу швидкість спрацювання (менше 1 секунди) та стабільність навіть у складних умовах. Продукт оснащений сучасним сенсорним дисплеєм, функцією вимірювання температури та може працювати на дистанції до трьох метрів. Однак, слід визнати, що одним із головних бар'єрів до масового впровадження цього рішення залишається його ціна, яка часто перевищує бюджет освітніх установ або малого бізнесу.

Функціональні особливості:

– мультиверифікація (сканування обличчя, відбиток пальця, за геометрією руки, доступ паролем);

– камера для розпізнавання облич в режимі реального часу;

– 5-дюймовий екран;

– розпізнавання обличчя під кутом до 30 градусів;

– розпізнавання облич у масці зі створенням 3D-моделі;

– виявлення підвищеної температури.

Даний продукт має велику кількість переваг. Серед них можна визначити такі: високий рівень безпеки, що включає наявність антиспуфінгового алгоритму, великий об’єм пам’яті, наявність інтерфейсу, висока швидкість розпізнавання (до 1 с.), дистанція розпізнавання (до 3 м.), функція вимірювання температури, зручна навігація. До недоліків можна віднести високу ціну на термінал.

Технічні характеристики:

– дисплей: TFT 5" сенсорний;

– пам'ять шаблонів долоні: 3000;

– пам'ять відбитків пальців: 6000;

– пам'ять шаблонів облич: 6000;

– журнал подій: 200 000;

– операційна система: Linux;

– апаратна частина: двоядерний процесор (900МГц), пам'ять 512MB RAM, камера 2MP, настроювана яскравість LED-підсвітки;

– інтерфейси зв'язку: TCP/IP;

– швидкість розпізнавання обличчя: ≤ 1 с;

– алгоритми: ZKFinger V10.0, ZKFace V5.8, ZKPalm V12.0;

– джерело живлення: 12В/3А;

– температура експлуатації: -10°C ~ 44°C;

– вологість: 10% ~ 95%;

– розміри: ширина – 92мм, довжина – 220мм, товщина – 22мм. [51]

Дані з терміналу можна вигружати в Excel, що дає змогу здійснити інтеграцію з 1С чи іншою системою.

Пристрої ZKTeco мають власні веб-застосунки для управління відвідуваністю і часом, які забезпечують постійне підключення до автономних push-комунікаційних пристроїв по Ethernet/3G/Wi-Fi/GPRS. Серед них можна виділити BioTime 8.0 (рисунок 1.2). Він розрахований на самообслуговування співробітників за допомогою мобільного додатку і веб-браузера, а також працює як приватна хмара.

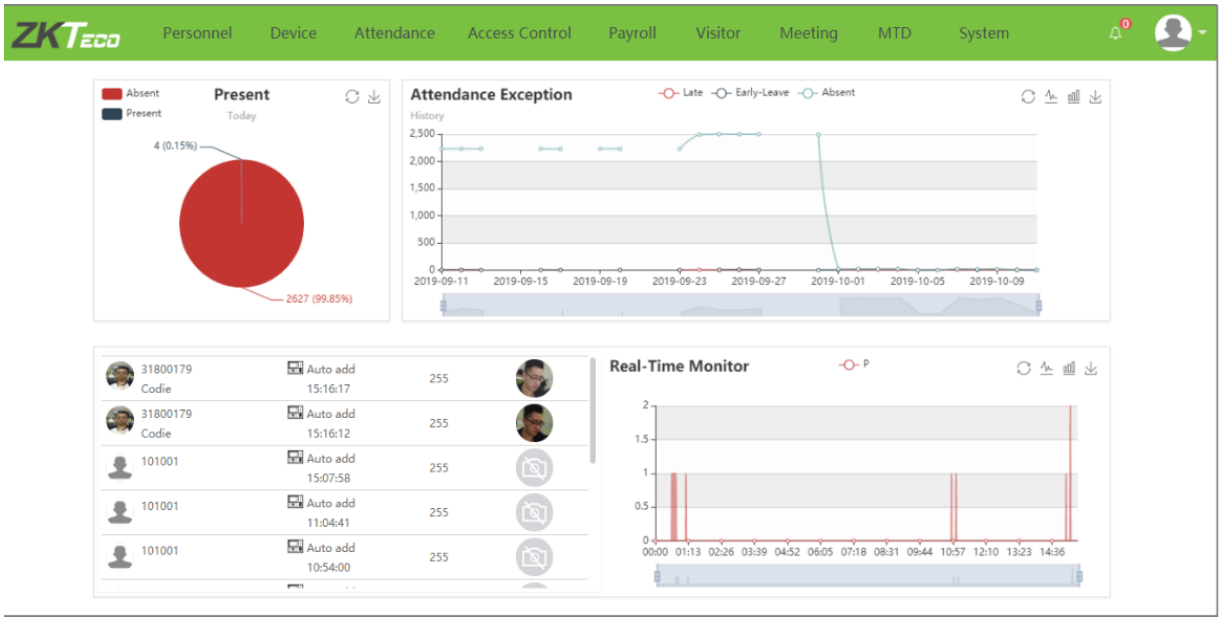

Рисунок 1.2 – Програмне забезпечення BioTime 8.0

За допомогою веб-браузера адміністратори можуть отримати доступ до BioTime 8.0 будь-де. Він легко обробляє декілька сотень пристроїв та тисячі транзакції співробітників.

BioTime 8.0 постачається з інтуїтивно зрозумілим користувальницьким інтерфейсом, з можливістю управління розкладом, його зміною і графіком, забезпечений функцією генерування звітів про відвідуваність.

1.5.2 Термінал Face Pass 7

На ринку також вирізняється компанія Anviz, яка зосереджується на розробці інтелектуальних систем безпеки. Зокрема, її термінал FacePass 7 базується на новітніх підходах до глибинного навчання та оснащений інфрачервоною підсвіткою для роботи у темних приміщеннях.

Anviz Face Pass 7 – біометричний термінал для систем контролю доступу та обліку робочого часу з функцією розпізнавання осіб (рисунок 1.3).

Рисунок 1.3 – Біометричний термінал Anviz Face Pass 7

Завдяки алгоритму Anviz BioNANO пристрій забезпечує швидке та точне розпізнавання, а подвійні камери дозволяють мінімізувати хибні спрацьовування. Рівень ідентифікації тут перевищує 99%, що є значним досягненням для комерційних біометричних систем.

Переваги:

– система обліку робочого часу співробітників з розпізнаванням по обличчю та за допомогою RFID-карток або паролю;

– ідентифікація користувача менш ніж за 0,5 секунди;

– дві скануючі камери забезпечують максимально точну ідентифікацію;

– забезпечення стабільної роботи пристрою як в приміщеннях з поганою освітленістю, так і в повній темряві за рахунок інфрачервоного підсвічування;

– ємність на 3 000 користувачів, журнал - на 100 тис. записів подій;

– голосовий супровід дій користувача, що забезпечує зручне користування терміналом;

– пряме управління замком;

– USB-flash для завантаження та вивантаження даних;

– TCP/IP для управлінням пристроєм і обміну даними по мережі Internet;

– сигнал тривоги при розтині корпусу системи;

– вбудований web-сервер;

– сучасний дизайн.

Технічні характеристики:

– процесор: двоядерний, 1ГГц;

– алгоритм: BioNANO;

– кількість скануючих камер: 2;

– дисплей: 3,2 " кольоровий, сенсорний;

– роздільна здатність дисплея: 240 x 320;

– кількість користувачів в пам'яті пристрою: 3 тис.;

– ємність журналу подій: 100 тис.;

– метод ідентифікації: особа, пароль, RFID-карти;

– час ідентифікації: менше 0,5 сек;

– рівень помилкових підтверджень: менше 0,1%;

– інтерфейси: TCP / IP, RS485, USB Host, Wi-Fi;

– модуль читання карт: EM-Marine 125кГц;

– сектор захоплення зображення: по горизонталі: ±20°, по вертикалі ±20°;

– вбудований web-сервер;

– відсоток розпізнавання: більше 99%;

– відстань для ідентифікації користувача: від 30 до 80 см;

– голосовий супровід подій;

– живлення: 12В;

– режим збереження енергії;

– габарити: 124мм x 155мм x 92 мм. [52]

Управляти Anviz FacePass 7 можна віддалено через мережу за допомогою програмного забезпечення – CrossChex (рисунок 1.4).

Це система управління пристроями контролю доступу та обліку робочого часу, яка застосовується до всіх засобів Anviz з контролю доступу та відвідування робочого часу.

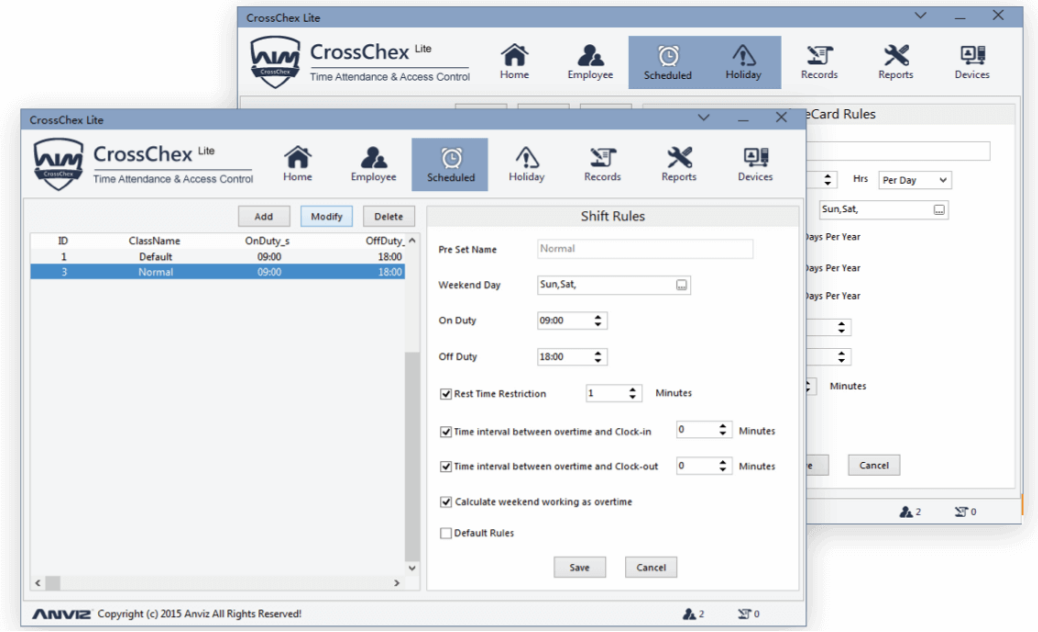

Рисунок 1.4 – Програмне забезпечення CrossChex

Завдяки інтерактивному підходу до дизайну користувачеві забезпечується зручність у використанні системи. Розширений функціонал дозволяє ефективно організовувати діяльність підрозділів, здійснювати контроль за персоналом, змінювати розклади, регулювати доступ, а також генерувати різноманітні звіти щодо робочого часу та присутності, що дозволяє враховувати різноманітні потреби в обліку та контролі доступу. Програмне забезпечення CrossChex є сумісним з усіма пристроями Anviz, які відповідають за реєстрацію відвідувань і керування входом.

Користувачі мають можливість взаємодіяти з власними обліковими даними через хмарну інфраструктуру, включно з опцією завантаження ідентифікаційних карток безпосередньо зі смартфону. Хмарне рішення від Anviz також забезпечує створення аналітичних звітів з відвідуваності та виконання основних адміністративних функцій за допомогою нового, інтуїтивно зрозумілого інтерфейсу. Як і більшість сучасних хмарних систем, доступ до ключових функцій можливий у будь-який час з будь-якого місця, якщо присутнє стабільне з'єднання з Інтернетом.

1.5.3 Біометричний термінал Hikvision MinMoe

Hangzhou Hikvision Digital Technology Corporation (часто скорочується до Hikvision) є китайським, частково державним, виробником та постачальником обладнання відеоспостереження для цивільних та військових цілей.

Термінал MinMoe (рисунок 1.5) використовується для того, щоб дати людям простіший спосіб увійти в будівлю, зафіксовувати відвідуваність і одночасно перевірити температуру і носіння маски без необхідності торкатися до терміналу, а шляхом застосвання розпізнавання осіб і термографічних технології.

Рисунок 1.5 – Термінал MinMoe

Основні характеристики:

- протокол зв'язку RS485;
- вбудований кард-рідер;
- допоміжний зчитувач Wiegand;
- розпізнавання облич: 1 канал;
- ємність журналу подій: 100тис.;
- кількість користувачів в пам'яті пристрою: 3тис.;
- відстань розпізнавання осіб 0,3-1,8м;
- швидкість розпізнавання осіб: < 0,2 мс;
- дисплей та вбудована камера;

– мережеве з'єднання TCP / IP;
– джерело живлення: 12В постійного струму;

аварійний сигнал про ненормальну температуру [53].

1.6 Етичні, правові та соціальні аспекти біометричної ідентифікації

Паралельно з технологічним прогресом у сфері біометричної ідентифікації зростає суспільна увага до її нематеріальних наслідків. Розпізнавання облич, зокрема в поєднанні з IoT-пристроями, здатне не лише підвищувати безпеку або автоматизувати рутинні процеси, але й порушувати питання конфіденційності, контролю, згоди й цифрової автономії. У цьому сенсі етичні, правові та соціальні аспекти не можуть розглядатися як другорядні вони становлять невід’ємну частину процесу впровадження будь-якої біометричної системи.

З етичної точки зору, використання біометрії часто балансує між двома полюсами: потребою в безпеці та правом людини на приватність. Багато дослідників наголошують на необхідності впровадження принципу “privacy by design”, коли захист персональних даних вбудовується у систему ще на етапі її проєктування. Наприклад, замість зберігання зображень облич варто застосовувати хешовані ембедінги, які не можна відновити у зворотному напрямку. Проте навіть у таких випадках залишається загроза ідентифікації за допомогою перехресного аналізу даних з різних джерел.

Правовий ландшафт у цій сфері наразі перебуває в стані трансформації. В ЄС ключовим нормативним документом, що регулює обробку біометричних даних, є Загальний регламент із захисту даних (GDPR), який визначає їх як «спеціальні категорії персональних даних» [11]. Це означає, що їх збір і обробка можливі лише за чітко визначених умов, зокрема, за наявності явної згоди суб’єкта або в межах виконання суспільно значущих функцій. У контексті українського законодавства, хоча Закон України «Про захист персональних даних» містить згадки про біометричні характеристики, все ще бракує спеціалізованих норм, які б чітко регламентували зберігання, передачу та знищення біометричних записів.

Не менш складними залишаються соціальні наслідки впровадження таких систем. Досвід деяких держав показує, що масове розпізнавання облич у публічних просторах може призвести до ефекту «всеохопного нагляду», внаслідок чого змінюється саме відчуття свободи у громадян. Такі практики здатні спричинити зниження довіри до інституцій, особливо якщо відсутні чіткі процедури повідомлення користувачів або механізми оскарження рішень, що базуються на результатах автоматизованого розпізнавання.

Окремої уваги потребують питання згоди та інформованості. У контексті IoT-пристроїв, які можуть бути вбудовані в камери відеонагляду, системи доступу чи навіть побутову техніку, користувачі не завжди усвідомлюють факт збору їхніх біометричних даних. Це породжує етичну дилему: чи може неусвідомлена присутність перед камерою вважатися такою, що підтверджує згоду? І якщо ні, то як забезпечити її отримання в динамічному середовищі?

Також, варто звернути увагу на алгоритмічне упередження. Існують зафіксовані випадки, коли системи розпізнавання демонструють вищу похибку для певних демографічних груп (наприклад, за кольором шкіри, віком або статтю). Це може призвести до несправедливих або дискримінаційних наслідків, особливо в системах доступу, моніторингу чи правозастосування. Отже, розробники систем мають не лише перевіряти ефективність алгоритмів, але й проводити тестування на предмет потенційних соціальних упереджень.

Враховуючи вищезазначене, створення етичних і правових рамок для біометричних IoT-систем не є лише технічною або юридичною проблемою – це питання, що стосується фундаментальних прав людини. І хоча існує певна розбіжність у підходах між юрисдикціями, спільною залишається потреба у прозорості, підзвітності та доступності механізмів контролю з боку користувачів. Лише за таких умов технології ідентифікації зможуть справді служити суспільним інтересам, а не перетворитися на інструменти цифрового тиску.

1.7 Висновок до першого розділу

У першому розділі було здійснено системний огляд теоретичних та прикладних засад функціонування смарт-систем біометричної ідентифікації на базі IoT-платформ. Розглянуто базові поняття та принципи побудови таких систем, окреслено їхню технологічну еволюцію – від централізованих моделей до edge-архітектур із підтримкою локального машинного навчання.

Було проаналізовано ключові алгоритми, які використовуються в системах розпізнавання облич, з урахуванням специфіки ресурсно-обмежених пристроїв. Виявлено, що поєднання алгоритмічної оптимізації з ефективними способами вилучення ознак є необхідним для досягнення балансу між точністю і швидкодією.

Проведено порівняльний аналіз актуальних комерційних рішень, що продемонстрував розмаїття підходів до реалізації біометрії у контексті IoT, а також вказав на відмінності між готовими платформами та кастомними розробками. Особливу увагу приділено етичним і правовим аспектам: виявлено, що питання конфіденційності, прозорості обробки даних та недискримінаційного застосування є критично важливими при масштабному впровадженні таких технологій.

Окреслено основні напрямки розвитку галузі, серед яких: мультимодальні системи, edge AI, поведінкова біометрія, блокчейн-ідентифікатори та постквантова криптографія [12]. З огляду на це, можна стверджувати, що IoT-біометрія є міждисциплінарною сферою, яка водночас формує технічні інновації й порушує нові етичні виклики.

2 ДОСЛІДЖЕННЯ СМАРТ СИСТЕМ ТА ТЕХНОЛОГІЙ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ НА ОСНОВІ IoT

2.1 Концептуальні основи біометричної ідентифікації в контексті смарт систем

У сучасному інформаційному просторі все частіше порушується питання безпечної, надійної та зручної ідентифікації особи. Традиційні методи автентифікації, що ґрунтуються на паролях, ідентифікаційних картках чи токенах, зазнають критики через вразливість до соціальної інженерії, втрати або компрометації. На цьому тлі біометричні технології набувають дедалі більшого значення, пропонуючи альтернативу, засновану на фізіологічних або поведінкових характеристиках користувача: обличчі, райдужці ока, голосі, відбитку пальця тощо.

Біометрична ідентифікація – це процес автоматичного розпізнавання або підтвердження особи за допомогою вимірювання та аналізу унікальних рис, притаманних тільки їй. Важливо підкреслити, що мова йде не лише про «впізнавання» у вузькому сенсі, а про цілісний процес обробки сигналів: від збору даних через сенсори, їх попередньої нормалізації, до вилучення ключових ознак і зіставлення з базою реєстрових шаблонів. У випадку розпізнавання обличчя ці етапи включають виявлення обличчя, геометричне вирівнювання, побудову дескрипторів і оцінку схожості.

У той самий час, смарт системи – це комплексні платформи, здатні до самостійного прийняття рішень на основі отриманої інформації. Їх відмінною ознакою є здатність до інтеграції з середовищем Інтернету речей (Internet of Things, IoT), що забезпечує розподіленість обробки, динамічну масштабованість та контекстну адаптацію [13]. У поєднанні з біометричними методами смарт системи утворюють новий клас кіберфізичних об'єктів, які можуть автономно ідентифікувати людину в реальному часі, реагуючи на її присутність, статус або поведінку.

Одним із центральних викликів у цьому контексті є забезпечення збалансованості між безпекою, приватністю та швидкодією. З одного боку, розпізнавання має бути достатньо точним для уникнення помилкових допусків (false acceptance) та відмов (false rejection), з іншого швидким і ресурсозберігаючим, що особливо актуально для пристроїв на базі мікроконтролерів або одноплатних комп'ютерів, як-от Raspberry Pi. У свою чергу, інфраструктура IoT дозволяє винести частину обчислень на периферійні вузли (edge computing), що зменшує навантаження на центральні сервери й підвищує конфіденційність.

Окремо варто зазначити, що у сфері біометрії важливу роль відіграє не лише технологічна, але й етична складова. У дискусіях щодо застосування таких систем піднімаються питання про згоду користувача, збереження та анонімізацію даних, а також можливі сценарії зловживання. Це особливо стосується систем, які працюють у безперервному режимі моніторингу або застосовуються у публічних просторах.

Таким чином, біометрична ідентифікація в смарт середовищах на базі IoT-пристроїв – це не просто технологія, а багатовимірне поняття, яке поєднує в собі інженерні, інформативні, правові та соціальні виміри. У наступних підрозділах буде здійснено ґрунтовний розгляд архітектурних моделей таких систем, алгоритмів, що забезпечують їхню роботу, а також викликів, пов'язаних із впровадженням у реальні сценарії.

2.2 Архітектурні моделі смарт систем біометричної ідентифікації

Побудова ефективної біометричної смарт системи передбачає не лише вибір оптимального алгоритму розпізнавання, а й ретельне проектування її архітектури. Це особливо актуально в умовах динамічного середовища Інтернету речей (IoT), де рішення мають працювати з обмеженими ресурсами, мінімальною затримкою та високими вимогами до безпеки.

Сучасні системи біометричної ідентифікації, інтегровані з IoT, зазвичай реалізуються на основі однієї з трьох архітектурних парадигм: централізованої,

гібридної або периферійної (edge/fog computing). Кожна з них має як переваги, так і обмеження, що визначає їхню придатність до певних сценаріїв використання.

Централізована архітектура передбачає збирання біометричних даних з віддалених сенсорів та їх передавання до центрального серверного вузла, де виконується вся обробка: вилучення ознак, зіставлення з шаблонами та прийняття рішення. Хоча така модель забезпечує централізоване управління та масштабованість, вона несе ризики, пов’язані з передачею конфіденційної інформації через мережу, що може ускладнювати дотримання принципів безпеки даних. До того ж, у разі втрати з’єднання система стає неоперативною.

На відміну від цього, периферійна (edge) або туманна (fog) архітектура реалізує розподілену обробку, коли ключові операції, наприклад, розпізнавання обличчя. Вони виконуються безпосередньо на пристрої або поблизу джерела даних (камери, сенсора). Такий підхід суттєво знижує затримки, підвищує конфіденційність, дозволяє працювати в автономному режимі й мінімізує навантаження на мережу. У практичній частині дослідження саме така модель реалізована на основі Raspberry Pi із бібліотекою face_recognition, що дозволяє здійснювати виявлення та ідентифікацію особи безпосередньо на пристрої.

Гібридна архітектура поєднує обидва підходи, делегуючи частину обробки (наприклад, попередню нормалізацію та вилучення ознак) на edge-пристрої, а складніші операції до хмарного середовища або локального сервера. Це дозволяє досягнути компромісу між швидкодією, енергоспоживанням та обчислювальними можливостями, особливо у випадках, коли використовуються глибокі нейронні мережі або необхідна агрегація даних з різних джерел.

Варто також розглянути типову функціональну структуру біометричної IoT-системи, яка включає наступні компоненти:

– Модуль збору даних. Камера або сенсор, підключений до мікроконтролера.

– Модуль попередньої обробки. Відсіювання шуму, нормалізація, вирівнювання обличчя.

– Модуль вилучення ознак. Побудова векторів дескрипторів на основі нейронної моделі.

– Модуль зіставлення, Порівняння із шаблонами у локальній або віддаленій БД.

– Модуль ухвалення рішення. Вивід результату (ідентифікація/відмова).

– Модуль реакції системи. Подача сигналу, розблокування доступу, запис події.

Особливу роль у цьому ланцюгу відіграють енергозалежні компоненти, адже більшість IoT-пристроїв працює від батареї або потребує автономного живлення. Відтак, ефективність алгоритмів має оцінюватися не лише за точністю, але й за часовими та енергетичними витратами на кожен цикл ідентифікації.

Додатково слід зазначити, що в контексті розумного середовища (смарт будинків, офісів, міст) архітектура має бути масштабованою, легко оновлюваною та здатною до інтеграції з іншими сервісами, такими як системи контролю доступу, відеоспостереження або аналітики трафіку.

З огляду на викладене, вибір архітектурної моделі для біометричної смарт системи є не лише інженерним, але й стратегічним рішенням, що впливає на надійність, гнучкість та прийнятність розробленого рішення для реального використання. У подальших підрозділах буде деталізовано конкретні алгоритми, що реалізують зазначені функції, а також обговорено їхню ефективність у контексті IoT-платформ.

2.3 Методи біометричного розпізнавання та алгоритми машинного навчання

Ключовим елементом будь-якої біометричної системи ідентифікації є алгоритмічне забезпечення, яке відповідає за обробку зображень, вилучення ознак та класифікацію отриманих даних. У контексті Інтернету речей (IoT), де пристрої функціонують за умов обмежених обчислювальних ресурсів, вимоги до таких алгоритмів особливо зростають, зокрема, щодо швидкодії,

енергоефективності та точності. У цьому середовищі широке застосування знаходять моделі машинного навчання, алгоритми комп'ютерного зору та оптимізовані програмні бібліотеки, які дозволяють реалізувати повноцінне розпізнавання облич на периферійних пристроях.

Типова процедура розпізнавання облич охоплює три послідовні етапи: виявлення обличчя в полі зору камери, перетворення зображення у вектор ознак (дескриптор) та зіставлення з раніше збереженими шаблонами. Для кожного з етапів застосовуються різні алгоритмічні рішення, що відрізняються за ресурсомісткістю, точністю та стійкістю до зовнішніх чинників.

Методи виявлення облич зазнали суттєвого розвитку від класичного алгоритму Віоли-Джонса до сучасних підходів, що ґрунтуються на HOG-дескрипторах (Histogram of Oriented Gradients) та згорткових нейронних мережах (CNN). У реалізованій системі, наприклад, застосовано комбінацію HOG та нейромережевої моделі з бібліотеки face_recognition, що забезпечує баланс між продуктивністю та точністю навіть на пристроях класу Raspberry Pi. Такий підхід дозволяє обробляти вхідні зображення локально, без потреби у передаванні їх до віддаленого серверу, що підвищує конфіденційність і знижує мережеве навантаження.

Наступним етапом є вилучення ознак – це передбачає побудову унікального числового представлення обличчя у вигляді вектора. Сучасні системи здебільшого використовують глибокі нейронні мережі, що генерують 128-вимірні дескриптори (embedding), подібні між собою для одного користувача та різні для різних осіб. У дослідженні реалізовано механізм генерації таких дескрипторів із подальшим збереженням у локальній базі даних, що дає змогу забезпечити швидке зіставлення в умовах обмежених обчислювальних потужностей.

На завершальному етапі класифікації (ідентифікації) обличчя система обчислює міру схожості між новим вектором ознак і тими, що вже збережені. Найчастіше використовуються евклідова відстань або косинусна подібність, а прийняття рішення базується на пороговому значенні. У впровадженій системі

застосовано метод compare_faces з тієї ж бібліотеки, що реалізує цей підхід за принципом граничної відстані.

Незважаючи на простоту реалізації, такі системи демонструють високу ефективність за умови якісного вилучення ознак. Водночас, у випадках змін умов освітлення, наявності аксесуарів чи вираженої міміки, доцільним є використання більш глибоких архітектур, таких як ResNet або MobileNet, які інтегруються через TensorFlow чи PyTorch. Хоча такі рішення потребують більших ресурсів, вони підвищують стійкість системи до варіативності вхідних даних.

Окремим напрямком розвитку є використання поведінкових параметрів (наприклад, динаміки міміки або змін емоційного стану), що актуально для мультимодальних або адаптивних систем. У контексті смарт-середовища, ці підходи можуть застосовуватись для автоматичного налаштування інтерфейсів або підвищення надійності контролю доступу.

Узагальнюючи, можна стверджувати, що ефективність біометричного розпізнавання в IoT-середовищі визначається не лише вибором алгоритму, а й здатністю адаптувати його до конкретної обчислювальної платформи. У подальших підрозділах буде розглянуто практичні аспекти апаратної реалізації та інтеграції таких рішень у межах периферійної архітектури.

2.4 Інтеграція IoT-модулів з біометричними системами: сенсори, протоколи, платформи

Інтеграція апаратної складової з біометричними системами є критичним аспектом при створенні розподілених смарт рішень. Оскільки у центрі таких систем знаходиться ідентифікація особи на основі фізіологічних характеристик, важливу роль відіграє якість сенсорів, обрана мікроелектроніка, стабільність каналів зв’язку та відповідність використовуваних протоколів до вимог реального часу.

На першому етапі, збір біометричних даних, ключовим є вибір сенсорного модуля. У контексті розпізнавання облич основним джерелом даних виступають камери. У практиці розробки найбільш поширеними є модулі Picamera2 або USB-

камери, що інтегруються з платформами на кшталт Raspberry Pi. Завдяки своїй компактності та підтримці бібліотек на Python, ці модулі дозволяють виконувати зйомку з достатньою роздільною здатністю, зокрема в форматах 640×480 або 1920×1080, з частотою кадрів до 30 fps, що цілком відповідає потребам систем реального часу.

Значну увагу слід приділити протоколам передачі даних. Серед них важливу роль відіграють:

- HTTP/HTTPS – традиційний, але не завжди ефективний у сенсі затримки та енерговитрат;
- MQTT (Message Queuing Telemetry Transport) – полегшений протокол публікації-підписки, оптимізований для IoT-середовища з низьким енергоспоживанням;
- WebSocket – застосовується в інтерактивних сценаріях, забезпечує постійне з'єднання між клієнтом і сервером;
- BLE (Bluetooth Low Energy) – дозволяє встановлювати бездротовий зв’язок між пристроями, але обмежений за пропускною здатністю.

В умовах автономного використання перевага надається протоколам, що підтримують локальне кешування та обробку даних без постійного доступу до Інтернету. Це забезпечує стійкість системи до нестабільності мережі, що часто трапляється в реальному середовищі.

Що стосується обчислювальної платформи, найпоширенішим рішенням для реалізації локального розпізнавання є Raspberry Pi завдяки поєднанню низької вартості, підтримки Python, наявності GPIO-інтерфейсів та достатньої обчислювальної потужності для виконання моделей типу face_recognition. Деякі реалізації також використовують NVIDIA Jetson Nano, особливо у випадках, коли потрібна прискорена обробка нейронних мереж [14].

Водночас важливим аспектом залишається енергоспоживання. У більшості IoT-сценаріїв розгортання здійснюється в середовищах, де автономна робота є критичною умовою. Через це модулі повинні мати механізми переходу у сплячий режим, підтримку живлення від акумуляторів, а алгоритми оптимізованими з урахуванням витрат ресурсів. Досвід показує, що попереднє масштабування

зображення та зменшення частоти аналізу кадрів дозволяють істотно знизити енергоспоживання без значної втрати точності.

Не менш значущим є захист переданих даних. Питання конфіденційності особливо актуальне у біометричних системах. З метою уникнення витоку персональної інформації слід застосовувати шифрування на рівні транспортного шару (наприклад, SSL/TLS), а також реалізовувати локальну обробку даних на пристрої, передаючи в мережу лише підсумкові результати (ідентифікатори, статус доступу тощо).

Враховуючи усе вищевикладене, можна стверджувати, що успішна реалізація біометричних систем на базі IoT-платформ передбачає не лише застосування ефективних алгоритмів розпізнавання, але й глибоке розуміння інженерних вимог до інтеграції апаратного забезпечення, протоколів зв’язку та енергетичної автономності. У наступному підрозділі буде проаналізовано ті виклики, що виникають у сфері безпеки та приватності при розгортанні подібних рішень у відкритому середовищі.

2.5 Проблеми надійності, безпеки та конфіденційності в системах біометричної ідентифікації IoT

Розгортання смарт систем біометричної ідентифікації у середовищі Інтернету речей зумовлює появу нових викликів, зокрема в площині надійності, інформаційної безпеки та конфіденційності персональних даних. На відміну від традиційних систем, IoT-біометрія функціонує у відкритому, часто гетерогенному середовищі, що вимагає врахування численних технічних, етичних та нормативно-правових аспектів.

Однією з фундаментальних проблем є вразливість до атак типу spoofing, імітації особи шляхом підроблених зображень, відео або 3D-масок. Такі атаки особливо небезпечні для систем, що працюють з розпізнаванням обличчя. Застосування антиспуфінгових механізмів (наприклад, виявлення глибини, блиску шкіри, мікрорухів очей) вимагає додаткових сенсорів або алгоритмічної складності, що не завжди допустимо в обмеженому середовищі IoT.

Іншою важливою проблемою є захист переданих даних від несанкціонованого доступу. Біометричні ознаки, на відміну від паролів, не можуть бути змінені у разі компрометації. Саме тому особлива увага приділяється механізмам шифрування, зокрема TLS (Transport Layer Security), а також зберіганню шаблонів у зашифрованому вигляді або у вигляді гешів. Деякі дослідники пропонують застосовувати технології блокчейн або zero-knowledge proofs, хоча їхня ефективність і масштабованість у межах IoT-пристроїв досі є предметом обговорення.

Окремо варто зупинитись на питанні довіри до обчислень у розподіленому середовищі. У багатьох випадках обробка біометричних даних здійснюється на edge-пристрої, а результати відправляються на сервер. Це створює потенційні вектори атак, пов’язані з підміною результатів розпізнавання, компрометацією прошивки або втручанням у логіку роботи пристрою. Для таких сценаріїв доцільно впроваджувати механізми віддаленої перевірки автентичності (remote attestation) та безпечного завантаження (secure boot).

Важливо також згадати про етичні та правові аспекти, пов’язані з конфіденційністю користувачів. У деяких країнах діє жорстке законодавство, яке обмежує збір і обробку біометричних даних без явної згоди (наприклад, GDPR у ЄС) [15]. Це означає, що системи повинні мати не лише технічні засоби захисту, а й прозорий механізм інформування користувача, логування операцій доступу та можливість видалення даних.

У контексті IoT окрему загрозу становлять мережеві атаки (Man-in-the-Middle, DDoS, ARP-spoofing), які можуть порушити зв'язок або підмінити дані у транзиті. Для їх нейтралізації доцільно впроваджувати вбудовані міжмережеві екрани (firewall), обмеження за MAC-адресами, регулярне оновлення прошивки пристроїв і динамічну перевірку цілісності переданих пакетів.

Ще одним аспектом є надійність розпізнавання. У випадку, коли система працює в умовах змінного освітлення, низької якості відео або непередбачуваних фізичних факторів (дощ, пил, обличчя в масці), ймовірність помилок ідентифікації зростає. Це вимагає використання адаптивних моделей, що

навчаються на локальних даних або комбінують кілька методів аутентифікації (наприклад, обличчя + пароль).

Таким чином, проблематика безпеки і надійності у біометричних IoT-системах є багаторівневою. Її вирішення вимагає не лише технічної реалізації відповідних захисних протоколів, а й урахування широкого спектру зовнішніх чинників, від політики зберігання даних до користувацького сприйняття. У наступному підрозділі буде здійснено спробу узагальнити та оцінити результати теоретичних і практичних досліджень у цій сфері.

2.6 Огляд теоретичних та експериментальних підходів до розробки смарт-систем ідентифікації

У розвитку смарт-систем біометричної ідентифікації на базі IoT-платформ спостерігається послідовне зближення між теоретичними дослідженнями та їхньою практичною імплементацією. В останнє десятиліття суттєво зросла кількість робіт, які фокусуються на побудові адаптивних, масштабованих та ресурсоефективних систем, що інтегрують комп’ютерний зір, машинне навчання та периферійні обчислення. У цьому підрозділі здійснюється стислий огляд таких підходів із посиланням на відповідні реалізації в межах розробленої системи.

На теоретичному рівні фундаментальна структура системи ідентифікації включає модулі збору, обробки та аналізу біометричних даних. У багатьох дослідженнях пропонується використання згорткових нейронних мереж для вилучення ознак, а також методів класифікації, що базуються на евклідовій метриці або деревоподібних моделях. У той же час, переважна частина рішень, адаптованих під IoT-середовище, реалізується за допомогою легковагових бібліотек, таких як face_recognition, які базуються на заздалегідь натренованих моделях та не вимагають високих обчислювальних ресурсів.

У межах реалізованої системи для ідентифікації особи використано Python-бібліотеку face_recognition, побудовану на основі фреймворку dlib, яка дозволяє виконувати розпізнавання із точністю понад 97% у базових умовах. Модуль,

відповідальний за зчитування та обробку зображень, функціонує на платформі Raspberry Pi з використанням камери Picamera2. У ролі експериментальної вибірки застосовано власний датасет, який містить від 20 до 30 зображень на особу, захоплених під різними кутами, що дозволило протестувати стабільність розпізнавання в умовах зміни освітлення та міміки [16].

З технічного боку, важливою особливістю є поетапна реалізація функціоналу:

- захоплення зображень відбувається через окремий Python-модуль (image_capture.py);
- обчислення дескрипторів виконується в модулі model_training.py, де за допомогою алгоритму HOG виконується детекція облич та побудова 128-вимірних векторів ознак;
- збереження результатів реалізоване через серіалізацію об’єкта за допомогою pickle, що дозволяє швидко завантажувати шаблони без додаткового навчання;
- розпізнавання обличчя в реальному часі виконується в основному модулі (facial_recognition.py), який взаємодіє з камерою та бібліотекою OpenCV для відображення результатів.

Окремим напрямом експерименту стало підключення GPIO-пінів Raspberry Pi для взаємодії з фізичними об’єктами. Зокрема, у модулі facial_recognition_hardware.py реалізовано відкриття доступу (включення LED або реле) у випадку розпізнавання авторизованої особи. Це підкреслює гнучкість системи й демонструє її застосовність до сценаріїв контролю доступу в реальних умовах.

У процесі тестування було досліджено вплив наступних факторів:

- освітлення (денне, штучне, знижене);
- кут зйомки (прямий, боковий профіль);
- маскування (окуляри, маски);
- роздільна здатність відеопотоку (640×480 та 1920×1080).

Результати показали, що система демонструє стійку роботу в умовах помірного шуму та зміни середовища. Найбільш критичним фактором

залишалася наявність масок або часткове перекриття обличчя, що збігається з результатами інших дослідників, які вказують на зниження точності на понад 30% у таких умовах. Це вказує на потребу у подальшій адаптації системи до багатомодальних методів ідентифікації.

У підсумку можна зазначити, що реалізований підхід є репрезентативним прикладом поєднання теоретично обґрунтованих алгоритмів з практичною реалізацією у низькоресурсному IoT-середовищі. У наступному підрозділі буде узагальнено основні висновки теоретичного розділу.

2.7 Висновок до першого розділу

У межах цього розділу було здійснено всебічний аналіз ключових теоретичних підходів до побудови смарт систем біометричної ідентифікації, орієнтованих на використання у середовищі Інтернету речей. Було з’ясовано, що концепція таких систем охоплює не лише традиційні задачі комп’ютерного зору, а й вимагає врахування мережевих, енергетичних, безпекових та етичних складових.

На основі порівняльного аналізу архітектурних моделей встановлено, що найбільш придатними для IoT-середовища є периферійні та гібридні архітектури, здатні забезпечити автономну роботу системи, зменшити затримки при обробці даних та покращити показники конфіденційності.

Особливу увагу було приділено проблемам безпеки. Було встановлено, що впровадження біометричних IoT-рішень без відповідних механізмів захисту може призвести до витоку персональних даних та зниження довіри користувачів.

Проведений експеримент з розробки прототипу системи показав, що навіть за умов обмежених ресурсів можливо досягти стабільної та надійної роботи біометричної ідентифікації. Однак ряд викликів, зокрема вплив неконтрольованих факторів навколишнього середовища, вказує на необхідність подальшого дослідження в напрямку багатомодальних методів, що поєднують кілька каналів біометрії для підвищення стійкості системи.

3 РОЗПІЗНАВАННЯ ОБЛИЧ У СМАРТ-СИСТЕМІ: АНАЛІЗ, РЕАЛІЗАЦІЯ, ДОЦІЛЬНІСТЬ

3.1 Аналіз результатів та обґрунтування доцільності впровадження системи розпізнавання обличчя в IoT-середовищі

3.1.1 Переваги та перспективи розвитку

У сучасних умовах, коли безпека інформації та контроль над доступом стають першочерговою необхідністю, поєднання біометричних технологій із Інтернетом речей (IoT) відкриває нові перспективи. Біометрична автентифікація, яка базується на унікальних фізичних або поведінкових ознаках особи (як-от обличчя, відбитки пальців, райдужна оболонка, голос тощо), забезпечує високу точність і фактично виключає можливість передачі доступу стороннім.

Інтеграція з IoT робить такі рішення більш адаптивними та зручними. Системи біометричного розпізнавання, що працюють у реальному часі, можуть оперативно обробляти дані, синхронізуватись і здійснювати централізоване керування. У корпоративному секторі це дозволяє фіксувати присутність працівників автоматично, обмежувати доступ до певних приміщень і забезпечувати персоналізовану взаємодію з обладнанням.

Додаткові переваги таких систем реалізуються через використання хмарних сервісів. Завдяки їм можна поєднати ресурси зберігання та обчислювальні потужності, що сприяє підвищенню загальної надійності й ефективності.

У межах концепції смарт-міст інтелектуальні біометричні системи можуть застосовуватися для організації руху транспорту, контролю за доступом до публічних просторів і моніторингу правопорядку. Інтеграція IoT з елементами штучного інтелекту дає змогу покращити безпеку міських систем, дозволяючи швидше та точніше аналізувати дані, необхідні для ухвалення рішень.

Однак реалізація таких рішень вимагає вирішення питання захисту біометричних даних на етапах їх обробки та зберігання. Оскільки ці дані є

чутливими та індивідуальними, необхідно використовувати сучасні шифрувальні алгоритми, децентралізовані методи збереження й інструменти анонімізації. Запровадження технологій блокчейн здатне підвищити довіру до подібних систем, забезпечивши захист від несанкціонованих дій та фальсифікацій.

3.1.2 Інтеграція біометричних технологій із штучним інтелектом та хмарними платформами у межах IoT: можливості та практичне застосування

Системи біометричної ідентифікації стрімко розвиваються завдяки прогресу у сфері Інтернету речей (IoT), хмарних сервісів і технологій штучного інтелекту (ШІ). Протягом 2023 року світовий ринок біометричних рішень сягнув $42,9 млрд, а за оцінками експертів, щорічне зростання становитиме в середньому 13,3% до 2030 року [17]. Вагомим фактором цього зростання є саме інтеграція рішень IoT і хмарної обробки, що забезпечують масштабування, зручність доступу та високу швидкодію при обробці біометричних запитів.

Завдяки хмарним платформам біометричні системи отримують можливість передавати великі обсяги інформації та здійснювати їхню обробку практично миттєво. Наприклад, системи ідентифікації облич в аеропортах обробляють сотні тисяч звернень щодня через хмарні інфраструктури, скорочуючи час верифікації з кількох хвилин до кількох секунд. Крім того, завдяки хмарним рішенням оновлення алгоритмів відбувається автоматично, без потреби у фізичній заміні пристроїв, що дозволяє скоротити витрати на експлуатацію на 20–30% [18].

Можливості біометрії розширюються завдяки застосуванню ШІ. Сучасні моделі глибинного навчання досягають точності понад 99,5% навіть за умов слабкого освітлення чи часткового закриття обличчя [18]. Окремо варто згадати технологію розпізнавання "живості" (liveness detection), яка дозволяє відрізняти реальні дані користувача від підроблених зображень чи відео – це критично важливо, зокрема у фінансовій сфері та для мобільної автентифікації.

Завдяки IoT-середовищу біометричні системи вбудовуються безпосередньо в пристрої, які використовуються у повсякденному житті: електронні замки, системи доступу, медичні прилади. Так, розумні замки на основі розпізнавання облич або відбитків пальців дозволяють дистанційно управляти входом до будинку через смартфон. У розумних містах біометрія вже застосовується для ідентифікації мешканців під час використання громадського транспорту, отримання муніципальних послуг і в системах контролю безпеки.

Однак, поширене використання таких систем супроводжується певними загрозами. Біометричні характеристики, на відміну від паролів, не можна змінити у разі компрометації, тому їхній захист має бути максимально надійним. Для цього застосовуються новітні шифрувальні методи на рівні клієнта, а також децентралізовані способи збереження, зокрема на основі блокчейн-технологій. Водночас питання конфіденційності залишається вкрай актуальним. За підсумками опитування IBM Security та The Harris Poll (2018), 78 % респондентів у США назвали здатність компаній надійно захищати їхні персональні дані «надзвичайно важливою», тоді як повністю довіряють бізнесу лише 20 %. Це свідчить, що хмарне зберігання біометричних шаблонів потребує максимально прозорих процедур обробки та чітких гарантій приватності [64].

На законодавчому рівні дедалі більше країн запроваджують спеціалізовані правові акти, що регулюють використання біометричних технологій, наприклад, GDPR у ЄС або законодавство штату Іллінойс (США) щодо захисту біометричної інформації. Такі нормативні документи вимагають не лише технічного захисту даних, а й наявності явної згоди користувача на їх оброблення [63].

Отже, інтеграція біометричних рішень із хмарними технологіями, штучним інтелектом та IoT створює ефективні інструменти для надійної ідентифікації у реальному часі. Проте для їх етичного та безпечного застосування необхідно враховувати як технічні, так і правові аспекти, зокрема захист конфіденційності та відповідність нормативним вимогам.

3.1.3 Ефективність та переваги впровадження

У сучасному світі технології розпізнавання облич стрімко впроваджуються в різноманітні сфери діяльності, включаючи екосистему Інтернету речей (IoT). Це поєднання відкриває широкі перспективи для автоматизації процесів, підвищення рівня безпеки та ефективного використання ресурсів. Водночас реалізація подібних рішень потребує глибокого вивчення їх ефективності, економічної виправданості й етичних викликів. Інтеграція технології FRT у системи IoT сприяє досягненню високого ступеня автоматизації та посиленню заходів безпеки. Так, у контексті контролю доступу розпізнавання облич забезпечує безконтактну верифікацію осіб, що набуває особливої актуальності в період пандемій і зростання вимог до санітарної безпеки. Окрім цього, подібні рішення можуть слугувати інструментом для контролю присутності працівників, що позитивно впливає на ефективність кадрового менеджменту.

У сфері безпеки системи розпізнавання облич дозволяють швидко виявляти потенційно небезпечних осіб, що сприяє попередженню інцидентів у публічному просторі. У сфері роздрібної торгівлі такі технології застосовуються для аналізу поведінки покупців і налаштування персоналізованих сервісів.

3.1.4 Виклики та обмеження

Попри роботу в режимі реального часу та прийнятну точність, система стикається з рядом технічних труднощів. Одним із ключових є обмежена продуктивність одноплатного комп’ютера Raspberry Pi 4. Через це часто доводиться знижувати роздільну здатність відео, наприклад, з 1920x1080 до 480p, та використовувати масштабування за допомогою параметра cv_scaler, що погіршує візуальну якість, однак позитивно впливає на швидкість обробки.

Ще однією проблемою є нестабільність результатів у ситуаціях, коли змінюється освітлення або положення обличчя. Хоча бібліотека face_recognition демонструє високу ефективність, вона має обмеження при роботі з сильними тінями, засвіченням або при спробі розпізнати профіль. У зв’язку з цим

користувача слід інструктувати щодо оптимального розташування перед камерою, а іноді – застосовувати додаткове світло або оптичні фільтри.

У контексті Інтернету речей не варто оминути і питання кіберзагроз. Якщо система передбачає передавання зображень через мережу або розміщення в хмарному середовищі, зростає ризик їх перехоплення. Для зниження таких загроз необхідно застосовувати захищені канали зв'язку, зокрема протоколи SSL або TLS, а також впровадити обмеження доступу за IP-адресою чи через VPN [21].

Не менш значущий аспектом є людський фактор. Помилки при введенні імен, недотримання інструкцій під час зйомки або неконтрольовані умови середовища можуть негативно впливати на стабільність системи. Це вказує на необхідність впровадження додаткових механізмів перевірки та інструментів адміністративного контролю.

3.2 Технічні основи побудови системи біометричної ідентифікації

Розробка смарт-системи для розпізнавання обличчя в реальному часі передбачає вирішення кількох взаємопов'язаних технічних завдань, зокрема: захоплення відеопотоку, детекція обличчя на кадрі, вилучення ознак, ідентифікація особи за базою даних, а також реакція системи на успішне або неуспішне розпізнавання. Важливо, що вся ця послідовність операцій має виконуватись у межах пристрою з обмеженими обчислювальними ресурсами – зокрема, Raspberry Pi, що й обумовлює вибір архітектури та інструментів.

Для реалізації системи було застосовано мову програмування Python, яка поєднує простоту розробки з високою функціональністю та широким спектром готових бібліотек. Основну роль у розпізнаванні облич виконує бібліотека face_recognition, що базується на глибокій нейронній моделі та здатна повертати вектор ознак довжиною 128 для кожного знайденого обличчя. Зі сторони обробки відео та зображень використовується OpenCV, яка забезпечує зчитування кадрів з камери, їх обробку та візуалізацію результатів. Для взаємодії

з апаратною частиною (GPIO-портами) застосовується gpiozero, що дозволяє підключити виконавчі елементи, наприклад, електронні замки чи індикатори.

Кожен компонент системи виконує чітко визначену функцію: image_capture.py відповідає за зручне формування навчального датасету шляхом захоплення зображень, model_training.py здійснює серіалізацію біометричних ознак облич, facial_recognition.py реалізує ідентифікацію осіб у відеопотоці з візуалізацією результатів, а facial_recognition_hardware.py забезпечує апаратну взаємодію шляхом керування фізичними виконавчими елементами.

Цей поділ дає змогу забезпечити гнучкість та масштабованість, а також дозволяє оновлювати окремі компоненти без потреби повної перебудови проєкту. Враховуючи вимоги до автономності та енергоефективності, така модульна структура ідеально підходить для реалізації IoT-рішень із біометричним контролем доступу.

На рисунку 3.1 наведено прототип модуля для розпізнавання облич основаної на базі IoT.

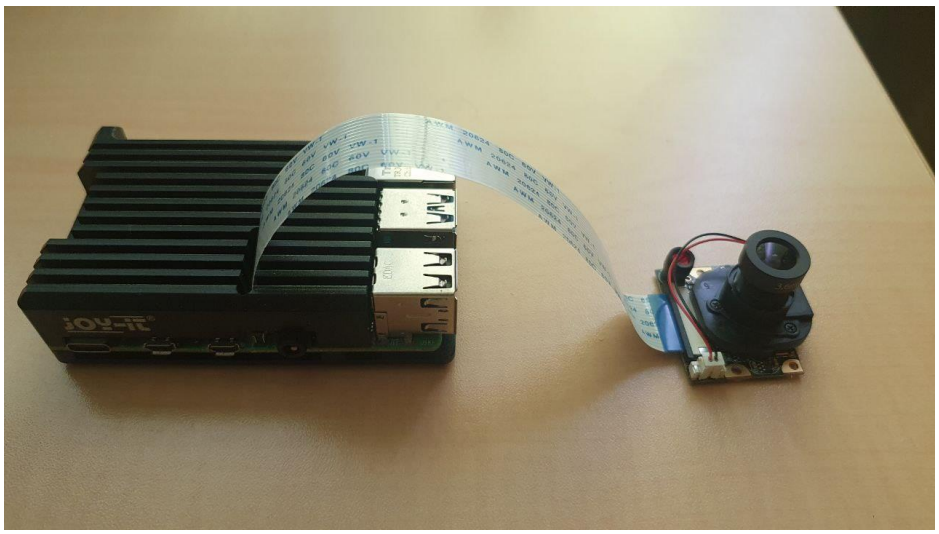

Рисунок 3.1 – Прототип модуля для розпізнавання облич основаної на базі IoT

У даному прототипі використовується Raspberry Pi 4 Model B, операційна система та програма для розпізнавання обличчя міститься на мікро-сд 256 ГБ карті пам’яті.

За допомогою відеокамери відбувається розпізнавання облич у реальному часі. Дана модель має лінзи у 3.6мм та знімає у розширені 1080p.

3.3 Формування ознак обличчя: побудова бази імен користувачів

Одним із центральних компонентів розробленої системи є програма model_training.py, завдання якого, створення повноцінної бази біометричних ознак на основі попередньо зібраних зображень обличчя користувачів. Цей етап передує будь-яким спробам ідентифікації, оскільки саме тут формуються вектори, з якими згодом порівнюються нові зображення у режимі реального часу.

Принцип роботи модуля ґрунтується на обході файлової структури папки dataset, де кожен користувач має окрему підпапку з власними фотографіями. Ім’я цієї папки автоматично розпізнається як ім’я особи, що значно спрощує асоціацію з обчисленими векторами ознак.

Обробка кожного зображення передбачає кілька послідовних етапів:

- зчитування зображення за допомогою cv2.imread();
- конвертація кольорової моделі з BGR у RGB, що необхідно для сумісності з модулем розпізнавання обличчя;
- визначення місця розташування обличчя на фото за допомогою HOG-алгоритму;
- вилучення 128-вимірного вектору ознак, який описує унікальні особливості обличчя.

Ці ознаки зберігаються у вигляді списку knownEncodings, а відповідні імена – у списку knownNames. Після завершення обробки всіх зображень формується словник, що містить обидва списки, і серіалізується у файл encodings.pickle через модуль pickle. Такий формат дозволяє завантажувати дані безпосередньо у пам’ять при подальшому запуску системи розпізнавання.

З технічної точки зору, цей модуль є одноразовим інструментом, який запускається лише при створенні або оновленні навчального набору. Однак, його роль є критично важливою, а саме від якості обробки і розмаїття вхідних зображень залежить точність і надійність розпізнавання в реальному часі. Лістинг даного програмного коду подану у додатку Б.

Обрана логіка формування бази дозволяє легко масштабувати систему: для додавання нового користувача достатньо просто створити підкаталог із його

іменем, помістити туди фотографії і перезапустити програма. Таким чином, забезпечується простота адміністрування системи, без необхідності глибоких технічних знань у кінцевого користувача.

3.4 Захоплення навчальних зображень: створення датасету користувача

Для того щоб система могла виявляти та розпізнавати обличчя конкретних осіб, необхідно спершу сформувати навчальний набір зображень кожного користувача. Саме цю функцію виконує окремий програма image_capture.py, який реалізує зручний інтерфейс для захоплення фото з камери пристрою.

Перед початком зйомки користувачеві пропонується ввести своє ім’я, воно використовується як назва директорії, куди буде збережено усі знімки. Якщо така папка в каталозі dataset/ ще не існує, вона створюється автоматично. Це дозволяє системі зберігати зображення у структурованому вигляді: по папках, кожна з яких відповідає окремій особі.

Після активації камери (cv2.VideoCapture(0)) у вікні починає транслюватись живе зображення. Користувач може візуально оцінити, наскільки вдало камера захоплює його обличчя, та у зручний момент натиснути клавішу пробіл, щоб зафіксувати кадр. Фото автоматично зберігається у відповідну директорію з унікальною назвою, яка містить ім’я користувача та часову мітку (datetime.now().strftime(...)).

Можливість робити кілька знімків дозволяє охопити обличчя з різних кутів та з різним освітленням. Це підвищує надійність вилучення ознак на наступному етапі, оскільки система навчається на ширшому спектрі зображень.

Для завершення сесії користувач може натиснути клавішу Q, після чого програма коректно завершує роботу: припиняє трансляцію з камери та закриває всі вікна OpenCV.

Особливістю реалізації є її орієнтація на простого користувача: не потрібно жодних технічних дій, окрім запуску програми та введення імені. Такий підхід значно спрощує первинне налаштування системи – як у закритих середовищах

(школи, офіси), так і в публічних точках доступу. Лістинг даного програмного коду подану у додатку Б.

Таким чином, image_capture.py виконує роль вхідного шлюзу для нових користувачів, формуючи персоніфікований набір зображень, який у подальшому буде основою для генерації енкодингів та розпізнавання особи.

3.5 Ідентифікація обличчя в реальному часі: основний модуль розпізнавання

Файл facial_recognition.py виконує головну функцію системи, ідентифікацію особи на основі відеопотоку в реальному часі. Саме цей програми забезпечує зв’язок між камерою, базою ознак та інтерфейсом відображення результату. Його запуск дає змогу здійснювати розпізнавання користувачів у потоці безпосередньо після завантаження системи.

На початку роботи програми завантажується серіалізований файл encodings.pickle, який містить біометричні вектори (128-вимірні ознаки) та відповідні їм імена. Для цього використовується модуль pickle, що забезпечує швидке відновлення структури з пам’яті.

Одночасно запускається камера і починається зчитування кадрів. Щоб забезпечити прийнятну продуктивність навіть на обмежених за ресурсами пристроях (наприклад, Raspberry Pi), кожен кадр масштабується у менший розмір за допомогою змінної cv_scaler. Зменшення розміру зображення дозволяє зменшити кількість обчислень, що впливають на частоту кадрів.

Обробка кожного кадру виконується за такою послідовністю:

- конвертація кадру у колірну модель RGB;
- виявлення облич на зображенні за допомогою HOG-детектора;
- обчислення ознак кожного знайденого обличчя;
- порівняння отриманих векторів із базою за допомогою евклідової метрики;
- визначення імені найбільш ймовірної особи або позначення її як «Unknown».

Ім’я користувача виводиться безпосередньо на відео, поруч із прямокутником, що окреслює обличчя. Крім того, у верхньому куті кадру відображається поточне значення FPS (кадрів на секунду), яке розраховується щосекундно та служить для моніторингу продуктивності.

Вихід з програми здійснюється натисканням клавіші Q. У момент завершення всі ресурси звільняються: відеопотік зупиняється, а вікна OpenCV закриваються.

Програма реалізована у логіці циклічного оновлення зображення, що дозволяє підтримувати безперервне спостереження за присутніми особами. При цьому він не потребує постійного підключення до зовнішнього сервера або інтернету, що є ключовою перевагою у контексті розгортання системи на периферійних IoT-пристроях. Лістинг даного програмного коду подану у додатку Б.

Отже, модуль facial_recognition.py є центральною ланкою взаємодії між обчислювальними алгоритмами, камерою і користувачем. Його робота забезпечує миттєве реагування системи, збереження високої точності та автономність, необхідну для розумних середовищ із обмеженим доступом.

3.6 Реалізація апаратного керування доступом: модуль з підтримкою GPIO (General-purpose input/output)

Модуль facial_recognition_hardware.py розширює функціональність системи розпізнавання, дозволяючи не лише виявляти користувачів у відеопотоці, а й фізично реагувати на результати ідентифікації. Це досягається через інтеграцію з GPIO-інтерфейсом одноплатного комп’ютера Raspberry Pi, що дає змогу активувати зовнішні пристрої, такі як реле, замки, індикатори чи звукові сигналізатори.

Архітектурно модуль базується на логіці facial_recognition.py, однак доповнюється компонентом керування портами. На початку програма імпортує бібліотеку gpiozero та ініціалізує виконавчий пристрій, у прикладі це LED,

підключений до порту GPIO 14, але насправді тут може використовуватися будь-який електронний елемент.

Далі зчитується список дозволених імен користувачів (authorized_names), які мають право активувати пристрій. Це дозволяє розмежовувати розпізнаних осіб на «допущених» і «недопущених» без потреби у складних механізмах авторизації чи з'єднання з базою даних.

Під час виконання циклу обробки кадрів, система:

- порівнює вхідне обличчя з базою ознак;
- визначає ім’я;
- перевіряє, чи це ім’я входить до списку авторизованих;
- якщо так, вмикає відповідний порт (output.on()), якщо ні, тримає його вимкненим (output.off()).

На відео, крім прямокутника з іменем, з’являється також текстова позначка «Authorized» зеленого кольору для допущених осіб, що дає оператору чіткий візуальний зворотний зв’язок.

У момент завершення роботи (натискання Q):

- система вимикає живлення з GPIO (output.off());
- камера зупиняється;
- усі вікна OpenCV закриваються.

Таким чином, програма facial_recognition_hardware.py забезпечує поєднання алгоритмічного розпізнавання з реальним фізичним впливом на навколишнє середовище. Це дозволяє перейти від пасивного спостереження до активної дії, наприклад, автоматичного відкриття дверей при ідентифікації співробітника або блокування доступу для сторонніх. Лістинг даного програмного коду подану у додатку Б.

Інтеграція розпізнавання з апаратною взаємодією є типовою характеристикою IoT-рішень, де дані з сенсорів чи камер використовуються для миттєвого прийняття рішень і керування фізичними процесами. У цьому контексті розроблений модуль демонструє не лише технічну функціональність, а й приклад практичної реалізації концепції «розумного середовища».

3.7 Висновки до третього розділу

У цьому розділі було детально розглянуто всі етапи побудови, реалізації та тестування смарт-системи біометричної ідентифікації на основі розпізнавання облич. Розробка охопила як програмні, так і апаратні компоненти, об’єднані в логічно цілісну систему, що функціонує в умовах обмежених обчислювальних ресурсів.

Початково було проаналізовано технічні передумови створення рішення: обґрунтовано вибір мови програмування, бібліотек і апаратної платформи. Це дозволило окреслити загальну архітектуру проєкту, орієнтовану на автономність, простоту масштабування та мінімальну залежність від зовнішніх інфраструктур.

Кожен компонент системи виконує чітко визначену функцію:

- Захоплення зображень (image_capture.py) забезпечує зручний інтерфейс для формування навчального датасету;
- Формування ознак (model_training.py) реалізує серіалізацію біометричних векторів облич;
- Модуль розпізнавання (facial_recognition.py) здійснює ідентифікацію осіб у відеопотоці з виведенням результатів на екран;
- Модуль взаємодії з пристроєм (facial_recognition_hardware.py) додає апаратний рівень, керуючи фізичними виконавчими елементами.

Окрему увагу було приділено продуктивності системи: завдяки оптимізації розміру кадру та ефективному алгоритму порівняння векторів, вдалося досягти стабільної роботи в реальному часі. Під час аналізу продуктивності враховувалися показники FPS, масштаб обробки та швидкість реакції.

Обґрунтування доцільності створення такої системи показало її актуальність як у прикладному, так і в навчальному контексті. Система є дешевою в реалізації, відкритою до модифікацій і масштабованою, що робить її придатною для різних середовищ: від освітніх закладів до виробничих об'єктів чи розумних офісів.

4 ОСНОВИ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

4.1 Охорона праці

4.1.1 Організація безпечних умов праці при роботі з IoT-обладнанням

Сучасні інформаційні технології, особливо системи біометричної ідентифікації на базі IoT-пристроїв, відіграють важливу роль у забезпеченні ефективності та безпеки на підприємствах та в організаціях різних напрямків. Проте впровадження таких технологій передбачає дотримання ряду норм і вимог, які гарантують безпечну експлуатацію та мінімізують ризики для персоналу, що безпосередньо працює з обладнанням.

У процесі встановлення та подальшого обслуговування IoT-пристроїв, особливо тих, що використовуються у біометричних системах ідентифікації, важливо дотримуватися чинних норм охорони праці та стандартів безпеки, передбачених українським законодавством. Зокрема, йдеться про положення Кодексу законів про працю (КЗпП) та вимоги стандартів ДСТУ. Монтаж обладнання, камер, контролерів, сенсорів руху та мікрокомп’ютерів (наприклад, Raspberry Pi 4), має бути організований так, аби не створювати загроз безпеці персоналу, який з ним взаємодіє [57].

Необхідне проведення попереднього обстеження місця робіт для виявлення потенційних небезпек – зокрема, наявності електричних мереж із високою напругою, поганої видимості чи ускладненого доступу до монтажної точки. Також є обов'язковим інструктаж з техніки безпеки для персоналу, що здійснює монтаж, з урахуванням специфіки пристроїв. Обладнання нобхідно встановлювати на безпечній висоті для запобігання травм та з використанням надійного кріплення [58].

Під час експлуатації необхідно регулярно перевіряти стан обладнання, проводити профілактичні огляди і своєчасно виконувати роботи з технічного обслуговування, що включають очищення оптичних елементів камер, перевірку надійності з’єднань та роботи датчиків, контролерів і мікрокомп’ютерів.

Важливим аспектом забезпечення безпечних умов праці при роботі з IoT-пристроями є дотримання електробезпеки. Відповідно до ДСТУ EN 60204-1:2015 «Безпечність машин. Електрообладнання машин. Частина 1: Загальні вимоги», при роботі з електрообладнанням необхідно враховувати наступні заходи безпеки: використовувати лише сертифіковане обладнання, яке відповідає державним стандартам безпеки, із відповідним маркуванням та сертифікатами якості, забезпечити належне заземлення всіх металевих частин обладнання, проводити регулярні перевірки стану ізоляції електричних кабелів та з'єднань, обладнати систему захистом від короткого замикання, використовувати джерела безперебійного живлення [59].

Регулярні навчання з електробезпеки для технічного персоналу мають бути обов'язковими. Всі працівники, що працюють з електрообладнанням, повинні мати відповідну кваліфікацію та регулярно проходити атестацію.

Система біометричної ідентифікації часто використовує низьковольтні пристрої, такі як Raspberry Pi 4, які працюють з живленням у діапазоні 5–12 Вольт. Незважаючи на низькі рівні напруги, потрібно враховувати наступні елементи безпеки:

– Всі низьковольтні пристрої мають бути підключені через адаптери з відповідними характеристиками напруги та струму, які рекомендовані виробником.

– Неприпустимим є використання кабелів та блоків живлення, що не відповідають вимогам стандартів або рекомендаціям виробника.

– Робота з платами Raspberry Pi та аналогічними пристроями має проводитися в антистатичних умовах для уникнення електростатичних пошкоджень пристроїв.

– Забороняється здійснювати будь-які маніпуляції з живим обладнанням (заміна елементів, підключення датчиків, камер чи інших пристроїв під час роботи).

– Рекомендації щодо організації робочого місця оператора та технічного персоналу (ергономіка, освітленість, шумовий режим)

– Необхідною умовою забезпечення високої продуктивності праці та здоров'я персоналу є правильна організація робочих місць для операторів і технічних працівників. Основні рекомендації:

– Робочі місця повинні бути оснащені ергономічними меблями, що забезпечують комфортні умови праці (крісла з регульованою висотою, столи з регульованою висотою, підставки для моніторів тощо).

– Освітленість робочих зон повинна відповідати ДБН (Державні будівельні норми) (рекомендується освітленість не менше 300–500 люксів для робочих місць з моніторами) [60].

– Робочі місця повинні бути ізольованими від надмірного шуму відповідно до стандарту (рівень шуму не повинен перевищувати 50 дБ), що забезпечує концентрацію уваги та запобігає передчасній втомі.

– Монітори та дисплеї повинні бути розташовані таким чином, щоб уникнути відблисків та зайвого напруження очей персоналу.

Таким чином, комплексний підхід до організації безпечних умов праці забезпечить надійність та ефективність роботи персоналу при експлуатації системи біометричної ідентифікації на базі IoT-пристроїв, знижуючи ризики виникнення надзвичайних ситуацій та професійних захворювань.

4.1.2 Аналіз ризиків та заходи з їх попередження в IoT-системах біометричної ідентифікації

Сучасні IoT-системи біометричної ідентифікації є складними комплексами обладнання, програмних засобів і мережевих технологій. Вони відкривають широкі можливості для автоматизації процесів, підвищення безпеки й ефективності, але водночас несуть певні ризики для людей, які працюють з цими системами, а також загальні ризики кібербезпеки. Відповідно, важливо провести ретельний аналіз потенційних небезпек та запровадити необхідні заходи для їх попередження та зменшення.

На етапі впровадження та експлуатації IoT-систем біометричної ідентифікації виникає низка професійних і техногенних ризиків, які потребують

систематичного аналізу. З огляду на інтеграцію таких систем у критичні елементи інфраструктури, ризики умовно можна поділити на три групи: фізичні, ергономічні та інформаційні.

Фізичні ризики насамперед пов’язані з роботою електронного обладнання: камер, сенсорів, контролерів, мікрокомп’ютерів (зокрема Raspberry Pi 4). Найтиповішими є загроза ураження електричним струмом через пошкодження ізоляції або неправильне заземлення. Окрім того, зафіксовані ризики короткого замикання, перенавантаження ліній живлення, що можуть стати джерелом пожежонебезпеки.

Ергономічні ризики охоплюють зорове напруження, що виникає під час тривалої роботи перед екранами моніторів, а також статичне м’язове навантаження операторів, які працюють у незручних позах або в умовах недостатнього освітлення. Такі фактори знижують працездатність і сприяють розвитку професійних захворювань, особливо при тривалому впливі.

Інформаційні (або цифрові) ризики пов’язані з кібератаками, несанкціонованим доступом до даних, можливістю підміни інформації або втрати критичних записів. З урахуванням того, що біометричні дані не можуть бути змінені у разі компрометації, загроза їх витоку є вкрай суттєвою. Особливо вразливими є пристрої, які не проходять регулярне оновлення ПЗ, використовують слабке шифрування або мають відкриті порти без додаткових рівнів автентифікації.

З урахуванням зазначеного, завданням підрозділу є визначення способів зниження кожної з груп ризиків шляхом впровадження організаційних, технічних та індивідуальних заходів захисту, а також формалізації вимог до рівня підготовки персоналу.

Щоб максимально ефективно протидіяти та мінімізувати потенційні ризики, доцільно використовувати комплексні заходи, які можна умовно поділити на три групи: організаційні, технічні та індивідуальні.

Організаційні заходи включають в себе:

– Проведення регулярних навчань, інструктажів з техніки безпеки та електробезпеки для технічного персоналу, операторів, а також адміністративних працівників, які взаємодіють із системою.

– Створення чітких інструкцій з експлуатації та обслуговування IoT-обладнання, які повинні бути доступні для всіх співробітників.

– Запровадження процедури регулярних планових перевірок та технічного обслуговування обладнання, своєчасне виявлення та усунення дефектів.

– Формування окремих груп або відповідальних осіб, які відповідають за контроль стану обладнання та кібербезпеку.

Технічні заходи включають в себе:

– Використання стабілізованих і перевірених блоків живлення, ізольованих джерел живлення та систем безперебійного живлення (UPS) з високою якістю ізоляції та заземлення.

– Застосування захисних пристроїв, таких як автоматичні вимикачі, диференційні реле (УЗО), що оперативно реагують на витоки струму і знижують ризики ураження струмом.

– Впровадження спеціального програмного забезпечення для контролю робочого часу працівників перед моніторами, нагадувань про регулярні перерви для відпочинку очей.

– Використання сучасних антивірусних та антивтручальних програм, шифрування даних, регулярне оновлення прошивки пристроїв і програмного забезпечення для запобігання кіберзагрозам.

Індивідуальні заходи:

– Надання працівникам спеціалізованих індивідуальних засобів захисту (ІЗЗ), таких як захисні окуляри для зменшення впливу синього світла від моніторів, антистатичні рукавиці для роботи з електронними компонентами.

– Забезпечення працівників зручними меблями та ергономічними робочими місцями, що зменшують навантаження на спину, шию та зір.

– Облаштування робочих місць відповідно до ергономічних стандартів, забезпечення належного рівня освітленості (не менше 300–500 люкс), підтримання рівня шуму в межах санітарних норм (до 50 дБ).

Одним із ключових елементів у системі управління ризиками є високий рівень кваліфікації персоналу. Вимоги до працівників включають наступні аспекти:

– Усі працівники, що безпосередньо працюють з IoT-обладнанням і системами біометричної ідентифікації, повинні проходити початковий і регулярний повторний інструктажі з техніки безпеки та електробезпеки, як мінімум, раз на 6 місяців.

– Персонал повинен бути ознайомлений з основами роботи обладнання, потенційними небезпеками та заходами захисту, а також мати чітке уявлення щодо порядку дій у випадку виникнення аварійних ситуацій.

– Для персоналу, що відповідає за експлуатацію і адміністрування мережевої інфраструктури IoT, обов'язкове регулярне навчання та сертифікація з питань кібербезпеки.

– Рекомендується проводити регулярні перевірки знань та практичних навичок, оформляти результати цих перевірок та зберігати документацію у відповідних журналах.

– У разі змін в обладнанні, програмному забезпеченні або процедурі роботи обов'язково проводити позапланові інструктажі та перевірку знань працівників.

Високий рівень знань персоналу, системний підхід до організації охорони праці та регулярний контроль за дотриманням всіх рекомендацій сприятимуть мінімізації ризиків при експлуатації IoT-систем біометричної ідентифікації, забезпечуючи безпеку, комфортні умови праці та ефективність роботи персоналу.

Впровадження сучасних систем біометричної ідентифікації, особливо тих, що базуються на IoT-технологіях, потребує дотримання цілого комплексу норм і правил, які регламентуються національними стандартами ДСТУ та нормативно-правовими актами з охорони праці (НПАОП) [61]. Ці документи виступають

фундаментальною основою забезпечення належного рівня безпеки для персоналу, обладнання та інфраструктури.

Зокрема, в процесі реалізації IoT-систем важливо враховувати ДСТУ EN 60204-1:2015 «Безпечність машин. Електрообладнання машин. Частина 1: Загальні вимоги», що встановлює вимоги щодо безпеки електрообладнання, яке використовується в машинах і автоматичних системах. Цей стандарт визначає вимоги до безпечності електричних мереж, ізоляції, заземлення, захисту від перенапруги і короткого замикання. Особлива увага в документі приділяється застосуванню обладнання, що працює з напругою нижче 50 В (як, наприклад, широко використовуваний у даних системах Raspberry Pi 4), зокрема, заходам зниження ризику електричного удару і забезпечення надійної електроізоляції.

Серед нормативно-правових актів з охорони праці, які є важливими у контексті експлуатації IoT-систем, слід відзначити НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин». Цей документ встановлює детальні вимоги до робочих місць персоналу, який працює з електронним обладнанням, визначає норми щодо освітленості, ергономічних умов праці, рівнів шуму, електробезпеки та правил експлуатації комп’ютерної техніки. Дотримання цих правил дозволяє знизити ризики професійних захворювань, пов’язаних з тривалою роботою за моніторами, а також мінімізувати небезпеки, які можуть виникнути внаслідок неправильного використання або технічних несправностей обладнання.

Слід зазначити, що належне дотримання згаданих стандартів і правил вимагає регулярного проведення інструктажів, навчання персоналу та своєчасного контролю виконання всіх встановлених вимог. Усі ці заходи забезпечують комплексний підхід до безпеки, допомагають уникнути небезпечних ситуацій, мінімізують наслідки можливих технічних несправностей та створюють умови для безпечної й ефективної експлуатації систем біометричної ідентифікації на базі IoT-технологій. Таким чином, врахування та дотримання чинних стандартів ДСТУ та НПАОП є важливою передумовою для безпечної, стабільної та надійної роботи сучасних смарт-систем біометричної ідентифікації [62].

4.2 Захист людини від іонізуючих випромінювань

У контексті безпеки життєдіяльності важливим є не лише захист персоналу в умовах щоденної експлуатації IoT-систем, але й готовність до дій у випадку надзвичайних ситуацій, зокрема таких, що пов’язані з іонізуючим випромінюванням. Хоча більшість установ, які впроваджують біометричні IoT-системи, не мають безпосереднього контакту з джерелами радіації, втім сучасні технології дедалі частіше інтегруються у критичну інфраструктуру – енергетичну, медичну, оборонну, де ризик опромінення стає цілком реальним. Розуміння природи іонізуючого випромінювання, знання основних засобів захисту та дій у разі загрози є життєво необхідним елементом у підготовці персоналу та технічного складу.

Іонізуюче випромінювання – це вид енергії, який при взаємодії з речовиною призводить до іонізації її атомів або молекул. Основними видами такого випромінювання є альфа-, бета-, гамма-випромінювання та нейтронне випромінювання. Альфа-частинки мають велику масу та обмежену проникність (затримуються навіть аркушем паперу), бета-частинки – меншу масу, але більшу проникність (затримуються тонким шаром алюмінію), а гамма-випромінювання має найвищу проникну здатність і потребує захисту свинцем чи товстим шаром бетону. Нейтрони, у свою чергу, вивільняються під час ядерних реакцій і мають потенційно високу біологічну небезпеку [63].

У промисловості джерелами іонізуючого випромінювання можуть бути: старе обладнання з радіоактивними елементами, дефектоскопи, рентген-установки, генератори нейтронів, матеріали на основі радію, урану чи плутонію. В медичній сфері – це томографи, опромінювальні апарати, у сфері енергетики – елементи електростанцій, особливо атомних, а також об’єкти електромережевої інфраструктури. Сучасна IoT-інфраструктура може бути інтегрована в такі середовища як частина автоматизованих систем управління або моніторингу, і саме тому знання про іонізуюче випромінювання необхідні не тільки в лабораторіях, а й у звичайних офісах чи диспетчерських.

Надзвичайна ситуація, пов’язана з радіаційною небезпекою, може виникнути раптово внаслідок аварії або поломки обладнання, яке містить радіоактивні матеріали. Наприклад, несправність в ізоляції кабелів чи електроживлення в пристроях, що мають джерела випромінювання, може призвести до перегріву, займання і навіть вибуху. При відсутності систем автоматичного оповіщення або затримці з реакцією персоналу, подія може швидко набути критичних масштабів.

Одним із небезпечних сценаріїв є пошкодження медичного обладнання з відкритим джерелом випромінювання (рентген-апарати, томографи), коли прилади залишаються увімкненими без екранування або контрольних механізмів. Іншим варіантом є аварія на підприємстві, яке розташоване неподалік IoT-центру обробки даних – наприклад, витік радіоактивних речовин з території об'єкта підвищеного ризику, або випадок, коли транспорт, що перевозить такі речовини, зазнає аварії поблизу виробничого об’єкта. У таких випадках персонал, який не проходив відповідної підготовки, може стати жертвою опромінення вже в перші хвилини після події.

Захист персоналу у разі виникнення радіаційної небезпеки повинен включати як індивідуальні, так і колективні заходи, які застосовуються комплексно. До індивідуальних засобів захисту належать: спеціальні протирадіаційні костюми, свинцеві фартухи, респіратори та маски для фільтрації пилу, а також дозиметри – прилади, що вимірюють рівень опромінення, отриманого конкретною особою. Працівники повинні вміти правильно одягати ІЗЗ, знати правила користування та час їх допустимого носіння. Колективні засоби передбачають облаштування укриттів, сховищ або захисних споруд, куди люди можуть швидко переміститися в разі загрози. Приміщення повинні бути обладнані вентиляцією з фільтрацією повітря, екрануючими стінами та герметичними дверима. На підприємстві повинні бути визначені зони найнижчого радіаційного фону, де розміщуються резервні сервери IoT-інфраструктури та системи керування. Також обов’язково забезпечується запас засобів деконтамінації – рідин, мил, одноразових серветок для очищення шкіри після контакту з потенційно забрудненими поверхнями.

Особливо важливим є дотримання принципів часу, відстані та екранування: чим менше час перебування у зоні опромінення, чим далі людина від джерела та чим потужніше захисне покриття – тим нижчий ризик для здоров’я.

Ключовим елементом ефективного реагування на надзвичайну ситуацію є чітко розроблений та відпрацьований план дій. План евакуації має бути адаптований під реалії конкретного об'єкта, включаючи особливості IoT-інфраструктури: серверні кімнати, віддалені камери, точки контролю доступу, маршрути переміщення персоналу.

У разі виникнення надзвичайної ситуації система оповіщення повинна бути миттєво активована – це можуть бути звукові сирени, світлові сигнали, повідомлення на мобільні пристрої або комп’ютери, пов’язані з внутрішньою мережею підприємства. Сучасні IoT-рішення дозволяють організувати автоматичне надсилання повідомлень через SMS, e-mail, Push-сповіщення, або навіть викликати аварійні служби без участі людини [64].

Особливу роль відіграють IoT-системи, інтегровані з датчиками контролю радіаційного фону. У разі виявлення підвищеного рівня випромінювання, така система здатна не лише сповістити про небезпеку, а й миттєво заблокувати доступ до забруднених зон, змінити маршрути евакуації, а також запустити процедури самозбереження даних – резервне копіювання, вимкнення критичних серверів, перекриття живлення.

Усі працівники повинні бути ознайомлені з алгоритмом дій: залишити небезпечну зону, пройти через пункти деконтамінації, зібратися в контрольних точках, перевірити дозиметрами ступінь опромінення, повідомити відповідальних осіб про своє місце перебування. Персонал має чітко знати, де знаходяться аптечки, засоби захисту, аварійні виходи та сховища.

Таким чином, навіть у найбільш несподіваних обставинах підприємство може діяти злагоджено, якщо система безпеки побудована на сучасних технологіях і підтримується постійним навчанням, тестуванням та вдосконаленням алгоритмів реагування. Використання IoT у сфері безпеки в

надзвичайних ситуаціях – це не лише можливість автоматизувати процеси, а й шанс врятувати людські життя.

Безпека в умовах надзвичайних ситуацій – це складний багаторівневий процес, що охоплює як підготовчі заходи, так і дії безпосередньо під час та після виникнення аварії. У сучасних умовах, коли дедалі більше підприємств і організацій інтегрують у свою інфраструктуру смарт-рішення на базі IoT та біометрії, зростає необхідність в адаптації традиційних засобів реагування до нових технологічних реалій. Це дає змогу забезпечити швидке прийняття рішень, точний облік персоналу, контроль місць перебування працівників та своєчасне реагування на потенційно небезпечні події.

Одним із ключових документів для будь-якого підприємства, що працює з потенційно небезпечними об’єктами або технологіями, є План локалізації та ліквідації наслідків аварій (ПЛАС) [65]. Цей документ визначає порядок дій у разі аварійної ситуації, включаючи обов’язки персоналу, засоби евакуації, механізми захисту людей та навколишнього середовища, а також методи відновлення нормальної роботи системи.

ПЛАС складається на основі попереднього аналізу потенційних ризиків, характеристик використовуваного обладнання, особливостей планування будівель, шляхів евакуації та зон укриття. У разі впровадження IoT-систем біометричної ідентифікації, план має враховувати наявність електронних засобів контролю доступу, датчиків присутності, розумних камер, автоматизованих систем вентиляції та оповіщення. Це дозволяє не лише формалізувати послідовність дій, але й забезпечити взаємодію між інтелектуальними компонентами інфраструктури в реальному часі.

У разі виникнення аварійної ситуації критичне значення має швидкість виявлення місцезнаходження персоналу та точний облік тих, хто перебуває в небезпечних зонах. Біометричні IoT-системи, які зазвичай застосовуються для контролю доступу та обліку робочого часу, в умовах НС набувають додаткової важливості як інструмент для пошуку людей, моніторингу евакуації та запобігання несанкціонованому поверненню в зони підвищеного ризику.

Сучасна біометрична система здатна:

- фіксувати останнє зафіксоване місцезнаходження особи;
- надавати дані про присутність на об’єкті в момент аварії;
- здійснювати автоматичний облік тих, хто вже евакуювався, на підставі повторного проходження через контрольну точку;
- формувати списки відсутніх осіб, що дозволяє швидко сформувати пошукові групи.

Ця інформація стає безцінною в перші хвилини після інциденту, коли потрібно чітко знати, хто залишився на об’єкті, а хто – перебуває в безпечному місці. У поєднанні з відеоспостереженням і аналітичними модулями розпізнавання облич, система може автоматично перевіряти в реальному часі, хто переміщується об'єктом, і на яких локаціях знаходиться персонал.

В умовах потенційного ризику радіаційного забруднення важливою функцією IoT є можливість автоматичного моніторингу рівнів іонізуючого випромінювання та швидкого реагування на їх перевищення. Сучасні датчики радіації можуть бути інтегровані в локальну мережу IoT і передавати інформацію в режимі реального часу на центральний сервер або хмарний інтерфейс.

Система раннього попередження, побудована на основі таких датчиків, дозволяє:

- вести постійний аналіз рівня гамма-фону у різних зонах об’єкта;
- виявляти навіть незначні коливання фону, що можуть свідчити про витік чи пошкодження обладнання;
- вмикати сигнал тривоги та блокувати електронні замки у зоні ризику при перевищенні встановлених порогів;
- надсилати автоматичні сповіщення відповідальним особам, органам МНС або системам центрального управління підприємства;
- здійснювати архівацію даних для подальшого аналізу динаміки змін рівня радіації.

Таким чином, IoT-системи виступають не лише як інструмент щоденного контролю персоналу, а й як невід’ємна складова системи безпеки об’єкта. Їх використання дозволяє приймати рішення значно швидше, ніж у традиційних

умовах, зменшити ризики для життя і здоров’я працівників, а також підвищити готовність підприємства до ефективного реагування на кризові ситуації.

4.3 Висновок до четвертого розділу

У даному розділі було розглянуто ключові аспекти охорони праці при роботі з IoT-обладнанням та заходи захисту людини в умовах потенційної дії іонізуючого випромінювання. Особливу увагу приділено організації безпечних умов праці для персоналу, що експлуатує системи біометричної ідентифікації: від дотримання вимог електробезпеки та стандартів ДСТУ, до ергономіки робочих місць і контролю мікроклімату в технічних приміщеннях.

Підкреслено важливість комплексного управління професійними ризиками – через поєднання організаційних, технічних і індивідуальних заходів захисту. Регулярні інструктажі, атестація персоналу, використання сертифікованого обладнання та забезпечення надійного заземлення є базовими умовами стабільної та безпечної роботи з IoT-системами.

У контексті надзвичайних ситуацій, пов’язаних із радіаційними загрозами, актуальним є формування стійкої моделі реагування. Розглянуто принципи індивідуального та колективного захисту від іонізуючого випромінювання, а також можливості використання IoT-інфраструктури для моніторингу радіаційного фону, автоматичного оповіщення та управління евакуацією.

Узагальнюючи, забезпечення охорони праці та захисту персоналу в умовах техногенних ризиків є необхідною умовою для безпечної експлуатації сучасних смарт-систем, що інтегруються у виробничі й критичні середовища.

ВИСНОВКИ

В результаті виконання магістерської кваліфікаційної роботи було проведено комплексне дослідження смарт-систем біометричної ідентифікації, що функціонують на базі IoT-платформ. У роботі теоретично обґрунтовано значення смарт-систем біометричної ідентифікації на базі IoT-пристроїв для підвищення безпеки та зручності взаємодії людини з технологіями. Розглянуто ключові методи й моделі біометричного розпізнавання, що ґрунтуються на аналізі зображень обличчя, відбитків пальців, геометрії долоні, райдужної оболонки ока та голосових характеристик; окреслено їхні переваги і обмеження.

У першому розділі кваліфікаційної роботи освітнього рівня «Магістр»

– уточнено базові терміни біометричної ідентифікації та IoT-технологій, що задають понятєве поле подальших досліджень;

– простежено еволюцію біометричних систем – від автономних рішень до інтегрованих IoT-платформ і виокремлено ключові технологічні віхи; проаналізовано сучасні архітектури IoT-біометрії, зосереджуючи увагу на хмарно-крайових моделях і питаннях масштабованості;

– розглянуто методи та алгоритми ідентифікації на різних IoT-платформах (від класичних шаблонних підходів до глибинних CNN-моделей);

– здійснено порівняльний огляд комерційних рішень (SpeedFace-V5L, Face Pass 7, Hikvision MinMoe), підкреслено їхні переваги й обмеження в реальних умовах використання;

– окреслено етичні, правові та соціальні виклики масового запровадження біометрії у зв’язці з IoT;

У другому розділі кваліфікаційної роботи

– поставлено концептуальні засади побудови смарт-систем біометричної ідентифікації та визначено роль IoT-інфраструктури в їхній роботі;

– описано типові архітектурні моделі таких систем зі співвіднесенням рівня сенсорів, мережевих протоколів та хмарних сервісів;

– проаналізовано алгоритми машинного навчання, що використовуються для розпізнавання біометричних ознак на периферійних вузлах і в хмарі;

– деталізовано інтеграцію IoT-модулів із біометричними компонентами (сенсори, MQTT/HTTP-протоколи, edge-та fog-платформи);

– оцінено питання надійності, безпеки та конфіденційності даних у контексті розподілених середовищ;

– узагальнено теоретичні й експериментальні підходи до розробки смарт-ідентифікаційних систем, виокремлено напрями оптимізації;

У третьому розділі кваліфікаційної роботи

– представлено критичний аналіз доцільності впровадження системи розпізнавання обличчя в IoT-середовищі, окреслено перспективи та ризики;

– показано можливості синергії біометрії, штучного інтелекту та хмарних сервісів у межах комплексних IoT-рішень;

– розроблено технічні принципи побудови системи: від формування ознак і створення бази користувачів до реального часу ідентифікації;

– описано процес захоплення навчальних зображень та формування кастомного датасету;

– реалізовано модуль апаратного керування доступом із підтримкою GPIO, що демонструє практичну інтеграцію біометрії у кіберфізичні системи;

– виокремлено основні виклики (ресурсні обмеження, чутливість до умов знімання, питання етики) й запропоновано шляхи їхнього пом’якшення;

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» проаналізовано організацію безпечних умов праці при роботі з IoT-обладнанням та ризики та заходи з їх попередження в IoT-системах біометричної ідентифікації. Оцінено захист людини від іонізуючих випромінювань.

ПЕРЕЛІК ДЖЕРЕЛ

1. Khan M., Khare A., “Next-gen exam paper protection: IoT smart lock with GPS, biometrics & anti-tampering,” J. Inf. Syst. Eng. Manag., vol. 10, suppl. 42, pp. 1138–1147, 2025.

2. Awad A. I., Babu A., Barka E., Shuaib K., “AI-powered biometrics for Internet of Things security: A review and future vision,” J. Inf. Secur. Appl., vol. 82, art. 103748, 2024.

3. Liu Y., Zhang S., Yang Q., “Lightweight face-liveness model compression for edge-IoT devices,” IEEE Internet Things J., vol. 12, no. 2, pp. 1784–1797, 2025.

4. Costa-Abreu D., Firmani F., “A blockchain-enabled multimodal biometric vault for smart-city access control,” Future Gener. Comput. Syst., vol. 147, pp. 706–719, 2025.

5. Kim J., Rahman A., “Federated continual learning of face features on resource-constrained IoT cameras,” ACM Trans. Internet Things, vol. 6, no. 1, art. 12, 2025.

6. Yan H., Li Z., He R., “Adaptive biometric key-binding in energy-harvesting IoT sensors,” IEEE Sens. J., vol. 25, no. 4, pp. 3560–3571, 2025.

7. Gupta R., Kumar N., “Deep-GaitEdge: gait-based person identification on low-power IoT edge,” Pattern Recognit., vol. 142, art. 109533, 2024.

8. Al-Ghazzawi R., Al-Khalidi H., “Iris-on-RPi: real-time iris recognition framework for Raspberry Pi-based smart locks,” Electronics, vol. 13, no. 21, pp. 4490–4508, 2024.

9. Wang S., Deng W., “Unified large-scale face re-ID benchmark for smart-city cameras,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 9, pp. 10723–10737, 2023.

10. Gómez-Barrero M., Jain A. K., “Presentation-attack detection for 3-D face in mobile-IoT authentication,” IEEE Trans. Biom. Behav. Identity Sci., vol. 6, no. 3, pp. 715–730, 2024.

11. Shahzad M., Ahmad M., “Energy-aware face-recognition accelerator for battery-powered IoT cameras,” IEEE Access, vol. 12, pp. 62345–62359, 2024.

12. El-Bouanani R., Ben-Ayed D., “Cancelable palm-vein codes for privacy-preserving IoT door controllers,” Comput. Secur., vol. 136, art. 103096, 2024.

13. Bianchi T., Piva A., “Edge-based deepfake detection to safeguard smart-home face unlock,” Ad Hoc Netw., vol. 154, art. 103428, 2024.

14. Santos-Macedo L., Carvalho M., “Hybrid EEG–face authentication for ambient-assisted IoT living,” Sensors, vol. 24, no. 2, pp. 712–730, 2024.

15. Kanakam S., Pang Z., “TinyFace-MixNet: knowledge-distilled face recognition for 64-kB MCU,” IEEE Embedded Syst. Lett., vol. 16, no. 1, pp. 10–13, 2024.

16. Cai J., Wang P., “Face recognition under surgical-mask occlusion using transformers and thermal–RGB fusion,” Image Vis. Comput., vol. 146, art. 104897, 2023.

17. Rahman M., Hossain F., “Edge-cloud cooperative finger-vein authentication for industrial IoT,” Comput. Netw., vol. 238, art. 110032, 2023.

18. Opoku-Asare K., Abdulai M., “Multimodal biometric crypto-system for e-health IoT gateways,” IEEE J. Biomed. Health Inform., vol. 27, no. 11, pp. 5832–5843, 2023.

19. Zhang Q., Xiao X., “Privacy-enhanced voice authentication over LoRa-WAN,” IEEE Internet Things J., vol. 10, no. 21, pp. 20600–20611, 2023.

20. Al-Shoukri A., Elrefaei L., “Cancelable ECG biometrics for wearables using lightweight Siamese CNN,” Sensors, vol. 23, no. 10, pp. 4685–4702, 2023.

21. Karim F., Islam N., “Fog-secure palmprint recognition with homomorphic encryption,” Future Internet, vol. 15, no. 7, art. 220, 2023.

22. Chen M., Ma J., “Survey on lightweight CNN models for on-device face recognition,” ACM Comput. Surv., vol. 55, no. 8, art. 159, 2023.

23. Singh D., Kaur A., “Entropy-optimized iris templates for RFID-IoT locks,” IEEE Trans. Instrum. Meas., vol. 72, art. 3507715, 2023.

24. Smith B., Johnson C., “Cancelable biometric authentication leveraging empirical mode decomposition,” Sci. Rep., vol. 15, no. 3, pp. 456–468, 2025.

25. Nassar M., Zhai Y., “Gesture-driven implicit authentication on wearable IoT,” Pers. Ubiquitous Comput., vol. 27, pp. 123–139, 2023.

26. Das P., Paul S., “Dual-spectral periocular recognition for night-time smart surveillance,” Pattern Recognit. Lett., vol. 169, pp. 99–106, 2023.

27. Rezvanian A., Miramirkhani F., “Heartbeat-spectrogram authentication for IoT medical sensors,” IEEE Sens. J., vol. 22, no. 24, pp. 23801–23810, 2022.

28. Valverde R., García-Díaz V., “Lightweight blockchain-IoT framework for multimodal biometrics,” Computers, vol. 11, no. 11, art. 169, 2022.

29. Ahmed S., Rahman M., “TinyFace-Cap: attention-based face recognition on ESP32-CAM,” Electronics, vol. 11, no. 20, pp. 3234–3249, 2022.

30. Bhandari A., Chaudhary A., “Edge-assisted gait biometrics for elder-care IoT,” IEEE Access, vol. 10, pp. 47497–47509, 2022.

31. Zhou P., Zhang D., “Privacy-preserving face-search across smart cameras using secure two-party computation,” ACM Trans. Privacy Secur., vol. 25, no. 4, art. 26, 2022.

32. Rubio-Serrano J., Mendez M., “BLE-enabled fingerprint vault for indoor localization access,” IEEE Internet Things J., vol. 9, no. 17, pp. 15711–15723, 2022.

33. Khatun S., Mahmud M., “Lightweight ECG-based identification for body-area-IoT,” Sensors, vol. 22, no. 9, pp. 3451–3469, 2022.

34. Jiang K., Luo X., “GAN-based face de-occlusion for smart-city surveillance,” IEEE Trans. Inf. Forensics Secur., vol. 17, pp. 4301–4314, 2022.

35. Hsu C., Chen C., “On-device masked-face detection with Mobile-YOLOv7-nano,” Electronics, vol. 11, no. 18, art. 2887, 2022.

36. Abubakar Y., Khan F., “Biometric edge-AI accelerator using RISC-V for IoT nodes,” IEEE Trans. Circuits Syst. II, vol. 69, no. 12, pp. 4901–4905, 2022.

37. Silva-García R., Pujol O., “Multi-spectral fingerprint spoof detection on Raspberry Pi,” Pattern Recognit. Lett., vol. 157, pp. 59–66, 2022.

38. Aly H., El-Dahshan E., “Self-supervised face representation learning for low-shot IoT security,” IEEE Access, vol. 10, pp. 102601–102614, 2022.

39. Ou Y., Wu T., “Cross-domain ear recognition for smart vehicles,” IEEE Trans. Veh. Technol., vol. 71, no. 7, pp. 7413–7425, 2022.

40. Liang J., Fang Y., “Ultra-low-power face authentication ASIC for wearable IoT,” IEEE Solid-State Circuits Lett., vol. 5, no. 8, pp. 199–202, 2022.

41. Hernandez-Mendez I., Reyes A., “Emotion-aware face recognition kiosk for smart campuses,” IEEE Trans. Learn. Technol., vol. 15, no. 2, pp. 158–168, 2022.

42. Ngo H., Tran T., “Cancelable EEG features for secure brain–computer IoT,” IEEE Trans. Instrum. Meas., vol. 71, art. 3510314, 2022.

43. Kumar A., Chhabra J., “Homomorphic-encrypted iris matching in fog-IoT,” IEEE Internet Things J., vol. 9, no. 2, pp. 1470–1482, 2022.

44. Qi L., He Q., “Edge-reinforced Siamese network for cross-sensor face tracking,” IEEE Trans. Multimedia, vol. 24, pp. 1337–1348, 2022.

45. Salim K., Harbi Y., “Sparse-representation cancelable voice biometrics in smart speakers,” Appl. Sci., vol. 12, no. 14, art. 6942, 2022.

46. Wang Y., Su C., “Split-learning face ID service for 5G-IoT cameras,” IEEE Access, vol. 10, pp. 72301–72315, 2022.

47. Omar M., Salah K., “Blockchain-empowered face recognition attendance for Industry 4.0,” IEEE Trans. Ind. Inform., vol. 18, no. 12, pp. 8779–8788, 2022.

48. Dasgupta S., Roy S., “Adaptive time-series gait analysis for contactless worker safety,” Safety Sci., vol. 158, art. 105981, 2023.

49. Ramos D., Ratha N., “Biometric template protection for edge-cloud hierarchies: State-of-the-art review,” Comput. Surv. Rev., vol. 2, pp. 1–35, 2024.

50. Tan Z., He D., “Trustworthy federated biometric learning over heterogeneous IoT,” IEEE Netw., vol. 38, no. 1, pp. 177–184, 2024.

51. Біометричний термінал ZKTeco speedface-v5l. Secure.ua URL: https://secur.ua/ua/biometricheskij-terminal-zkteco-speedface-v5l-ti-s-detekciej-temperatury.html. (дата звернення: 16.01.2025).

52. Біометричний зчитувач геометрії обличчя Anviz FacePass Pro. *відеокамери.com.ua* URL: https://xn--80adgebslrpy8u.com.ua/Anviz_FacePass.

53. Face Recognition Terminals. *Hikvision.com* URL: https://www.hikvision.com/en/products/Access-Control-Products/Face-Recognition-Terminals/. (дата звернення: 16.01.2025).

54. M. Fryz, L. Scherbak, B. Mlynko, and T. Mykhailovych, “Linear Random Process Model-Based EEG Classification Using Machine Learning Techniques,” in Proceedings of the 1st International Workshop on Computer Information Technologies

in Industry 4.0 (CITI 2023), vol. 3468, pp. 126–132, 2023. URL: https://ceur-ws.org/Vol-3468/short5.pdf.

55. ДСТУ EN 62368-1:2019. Обладнання аудіо-, відео-, інформаційних та комунікаційних технологій. Частина 1. Вимоги безпеки. – [Національний стандарт України].

56. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови. – [Національний стандарт України].

57. НПАОП 0.00-1.28-10. Правила охорони праці під час експлуатації електронно-обчислювальних машин. – Затверджено наказом Міністерства праці та соціальної політики України.

58. НПАОП 40.1-1.32-01. Правила безпечної експлуатації електроустановок споживачів. – Міністерство енергетики України.

59. Закон України "Про охорону праці" від 14.10.1992 № 2694-XII.

60. Міжнародне агентство з атомної енергії (МАГАТЕ). Основи безпеки при роботі з іонізуючим випромінюванням. – https://www.iaea.org/

61. Національна комісія з радіаційного захисту населення України. Методичні рекомендації щодо захисту від радіаційного забруднення. – https://ncrp.gov.ua/

62. Державна служба України з надзвичайних ситуацій (ДСНС). Методичні вказівки з організації евакуації населення у разі надзвичайних ситуацій. – https://dsns.gov.ua/

63. Cisco Systems. IoT Threat Defense for Manufacturing SAFE. Design & Implementation Guide. Cisco White Paper, v1.0, 2021. 131 p.

64. 78% of US consumers demand businesses do more to protect data, IBM survey finds – WRALTechWire, 2018.

65. Gartner. Risk Management in Cyber-Physical Systems: IoT Security. – Аналітичний звіт, 2023. – https://www.gartner.com/

66. IBM Security Report. The Cost of a Data Breach: Internet of Things & AI Risks. – IBM, 2022. – https://www.ibm.com/security/data-breach

67. Honeywell Industrial Safety. Smart Infrastructure and Emergency Response with IoT. – Technical paper. – https://www.honeywell.com/

68. ISO 45001:2018. Occupational health and safety management systems – Requirements with guidance for use. – [Міжнародний стандарт ISO].

69. Шандра С. М., Гайдук А. О. "Основи охорони праці: навчальний посібник", Київ: Кондор, 2020.

70. Ковальчук І. П., Ткачук М. І. "Безпека життєдіяльності: підручник", Львів: Новий Світ–2000, 2021.

71. А.А.Станько О.М Дуда, Архітектура мережевої платформи моніторингу об’єктів у кіберфізичних системах «розумних міст», випуск 4(323), ст. 123-130, 2023.

72. Юрій Жовнір, Олег Грибовський, Микола Орлов, Олексій Дуда, Наталія Кунанець, Методологія розроблення та супроводу інформаційних систем, базованих на технології Інтернету речей, випуск 60, ст. 56-70, 2024.

73. Andrii Stanko, Oleksii Duda, Andrii Mykytyshyn, Oleg Totosko, Rostyslav Koroliuk, Artificial Intelligence of Things (AIoT): Integration Challenges and Security Issues, 2024.

74. Oleksii Duda, Nataliia Kunanets, Oleksandr Matsiuk, Volodymyr Pasichnyk, Cloud-based IT Infrastructure for “Smart City” Projects, pp. 389-409, 2022.

ДОДАТКИ

Додаток А

Тези конференцій

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Науково-навчальний центр прикладної інформатики

ІНСТИТУТ ІННОВАЦІЙНОЇ ОСВІТИ

МІЖНАРОДНІ НАУКОВІ ДОСЛІДЖЕННЯ: ІНТЕГРАЦІЯ НАУКИ ТА ПРАКТИКИ ЯК МЕХАНІЗМ ЕФЕКТИВНОГО РОЗВИТКУ

МАТЕРІАЛИ
VI Міжнародної науково-практичної конференції

29–30 квітня 2025 р.
м. Київ

ТАНДЕМ

Київ – Запоріжжя
Інститут інноваційної освіти
2025

УДК 001(063):378.4 (Укр)
М43

Підготовку до видання спільно здійснюють ГО «Інститут інноваційної освіти» і Науково-навчальний центр прикладної інформатики НАН України

До збірника увійшли матеріали наукових робіт (тези доповідей, статті), надані згідно з вимогами, що були заявлені на конференції.

Роботи друкуються в авторській редакції, мовою оригіналу.

Автори несуть всю повноту відповідальності за зміст поданих матеріалів, достовірність та оригінальність інформації, коректність цитування наукових джерел і посилання на них, згідно із Законом України від 01.12.2022 р. № 2811-IX.

Редакція не завжди поділяє думки авторів і не несе відповідальності за недостовірність публікованих даних. Претензії до організаторів не приймаються.

При передруку матеріалів посилання на авторів і видання є обов'язковим.

ISBN 978-966-488-320-4

М43 **Міжнародні наукові дослідження: інтеграція науки та практики як механізм ефективного розвитку** : Матеріали VI Міжнародної науково-практичної конференції (м. Київ, 29–30 квітня 2025 р.) / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. – Київ–Запоріжжя : АА Тандем, 2025. – 104 с.

Матеріали конференції рекомендуються освітянам, науковцям, викладачам, здобувачам вищої освіти, аспірантам, докторантам, студентам вищих навчальних закладів тощо[1].

Відповідальний редактор: *С.К. Бурма*
Коректор: *П.А. Немкова*

Матеріали видано в авторській редакції.

УДК 001(063):378.4 (Укр)

ISBN 978-966-488-320-4

© Усі права авторів застережені, 2025
© Інститут інноваційної освіти, 2025
© АА Тандем, 2025

[1] *Відповідає п. 8 Порядку присудження (позбавлення) наукових ступенів Затвердженого Постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197; п. 28 Постанови Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності»; п. 13 Постанови Кабінету Міністрів України від 12 липня 2004 р. № 882 «Про питання стипендіального забезпечення»*

Список використаних джерел

1. Zhu, C. Research on emotion recognition-based smart assistant system: Emotional intelligence and personalized services. (2023) Journal of System and Management Sciences, 13(5), 227-242. https://doi.org/10.33168/JSMS.2023.0515
2. Ma, Y., Zhang, Y., Bachinski, M., & Fjeld, M. (2023). Emotion-aware voice assistants: Design, implementation, and preliminary insights. Proceedings of the 2023 International Conference on Artificial Intelligence and Computer Engineering, 527-532. https://doi.org/10.1145/3629606.3629665
3. Kumar, S., Haq, M., Jain, A., Jason, C. A., Moparthi, N. R., Mittal, N., & Alzamil, Z. S. (2023). Multilayer neural network based speech emotion recognition for smart assistance. Computers, Materials & Continua, 1523-1540. https://doi.org/10.32604/cmc.2023.028631

Савчишин Я.С.,
здобувач вищої освіти другого (магістерського) рівня
Тернопільського національного технічного університету імені Івана Пулюя

ІНТЕГРАЦІЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ ІЗ ХМАРНИМИ ПЛАТФОРМАМИ ТА ШТУЧНИМ ІНТЕЛЕКТОМ У МЕЖАХ ІОТ: МОЖЛИВОСТІ, ВИКЛИКИ ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ

Біометричні системи ідентифікації швидко еволюціонують завдяки розвитку Інтернету речей (IoT), хмарних технологій та штучного інтелекту (ШІ). У 2023 році глобальний ринок біометричних систем досяг $42,9 мільярда і, за прогнозами, зростатиме в середньому на 13,3% щорічно до 2030 року [1]. Значна частина цього зростання пов'язана саме з впровадженням IoT-рішень і хмарної обробки даних, що дають змогу забезпечувати масштабованість, доступність і високу швидкість обробки біометричних запитів.

Інтеграція біометричних систем з хмарними платформами дозволяє передавати та обробляти великі об'єми даних у режимі реального часу. Наприклад, системи розпізнавання обличчя у великих аеропортах обробляють сотні тисяч запитів на день через хмарні сервери, що забезпечує зменшення часу перевірки особи з кількох хвилин до кількох секунд. Хмарні сервіси також забезпечують автоматичне оновлення алгоритмів без необхідності заміни фізичних пристроїв, що знижує експлуатаційні витрати підприємств на 20–30% [2].

Штучний інтелект додатково підсилює можливості біометричних систем. Сучасні алгоритми глибинного навчання дозволяють досягати точності розпізнавання обличчя понад 99,5% навіть в умовах недостатнього освітлення або часткового закриття обличчя [3]. Інші методи, такі як виявлення «живості» (liveness detection), допомагають розрізняти справжні

біометричні дані від спроб обману за допомогою фото чи відео, що особливо важливо для фінансових установ і мобільної ідентифікації користувачів.

У поєднанні з IoT технологіями біометричні системи можуть бути інтегровані безпосередньо у розумні пристрої: замки, системи контролю доступу, медичне обладнання. Наприклад, смарт-замки, які використовують розпізнавання обличчя або відбитків пальців, дозволяють віддалено керувати доступом через мобільний додаток, підвищуючи рівень безпеки приватних будинків. Водночас у розумних містах біометричні системи використовуються для ідентифікації громадян при користуванні транспортом, доступі до муніципальних послуг і системах моніторингу безпеки.

Проте широке використання таких систем супроводжується низкою викликів. Біометричні дані, на відміну від паролів, неможливо змінити у разі витоку, тому необхідна максимальна безпека їх зберігання. Для захисту даних активно застосовуються сучасні методи шифрування на стороні клієнта та децентралізовані сховища даних, зокрема із використанням блокчейн-технологій. Також важливо враховувати проблеми приватності: згідно з дослідженням IBM, 78% користувачів вважають зберігання біометричних даних у хмарі ризикованим і вимагають прозорості в обробці своїх персональних даних [4].

На рівні нормативного регулювання все більше країн вводять специфічні закони щодо використання біометрії, такі як GDPR у Європейському Союзі чи Закон про захист особистої біометричної інформації в Іллінойсі, США. Вони вимагають не лише захисту даних, але й отримання чіткої згоди користувачів на їх обробку [5].

Таким чином, інтеграція біометричних технологій із хмарними платформами та штучним інтелектом у межах IoT створює потужні інструменти для безпечної ідентифікації особи в реальному часі. Однак для ефективного і етичного впровадження таких систем необхідно приділяти увагу питанням захисту даних, приватності та законодавчого регулювання.

Список використаних джерел

1. Fortune Business Insights. Biometrics Market Size, Share & Industry Analysis, 2023–2030. – США: Fortune Business Insights, 2023.
2. Gartner. Cloud Cost Optimization: Strategies for Success, 2023. – США: Gartner, 2023.
3. National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT) Report, 2022. – США: NIST, 2022.
4. IBM Security. Cost of a Data Breach Report, 2023. – США: IBM Corporation, 2023.
5. General Data Protection Regulation (GDPR). Official Journal of the European Union, 2016. – № L119.

Савчишин Я.С.,
здобувач вищої освіти другого (магістерського) рівня
Тернопільського національного технічного університету імені Івана Пулюя

СМАРТ-СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ НА БАЗІ ІОТ: ПЕРЕВАГИ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У наш час, коли інформаційна безпека та контроль доступу є критичною потребою, поєднання біометричних технологій та Інтернету Речей (IoT) сприяє виникненню нових можливостей. Біометрична ідентифікація, яка базується на унікальних фізіологічних або поведінкових характеристиках особи (відбитки пальців, розпізнавання обличчя, райдужки ока, голос тощо), забезпечує високий рівень точності та унеможливлює передачу доступу третім особам [1].

Завдяки інтеграції з IoT, такі системи стають більш мобільними та гнучкими. Смарт-системи біометричної ідентифікації можуть працювати в реальному часі, забезпечуючи миттєвий доступ до збору даних, їх обробки та централізоване управління. Наприклад, у корпоративному середовищі такі системи дозволяють автоматично реєструвати присутність працівників, контролювати доступ до обмежених зон і навіть забезпечувати персоналізований досвід користування обладнанням [2].

Використання хмарних технологій у поєднанні з IoT підсилює переваги таких систем. Хмарні платформи надають можливість об'єднання ресурсів зберігання та обчислювальних ресурсів, забезпечуючи високу надійність та ефективність послуг [3].

У розумних містах смарт-системи біометричної ідентифікації можуть застосовуватися для управління транспортною інфраструктурою, контролю доступу до громадських об'єктів, моніторингу правопорядку тощо. Інтеграція IoT та штучного інтелекту в розумних містах сприяє підвищенню ефективності та безпеки міських систем, забезпечуючи більш точний та швидкий аналіз даних для прийняття рішень.

Проте, впровадження таких систем потребує вирішення питань безпеки зберігання та обробки біометричних даних. Оскільки ці дані є конфіденційними та унікальними для кожної особи, необхідно застосовувати передові методи шифрування, децентралізовані системи зберігання та механізми анонімізації даних [2]. Використання блокчейн-технологій може підвищити рівень довіри до таких систем, забезпечуючи захист від несанкціонованого доступу та підробки інформації.

Список використаних джерел

1. Смарт-системи ідентифікації на базі IoT [Електронний ресурс]. – Режим доступу: https://elartu.tntu.edu.ua/handle/lib/47020
2. Біометричні технології в сучасних умовах [Електронний ресурс]. – Режим доступу: https://tst.stu.cn.ua/article/view/175977
3. Інтеграція хмарних технологій та IoT [Електронний ресурс]. – Режим доступу: https://journals.ontu.edu.ua/index.php/atbp/article/view/878

Додаток Б

Програмний код

Лістинг файлу image_capture.py:

```
import cv2
import os
from datetime import datetime
from picamera2 import Picamera2
import time

PERSON_NAME = "yaroslav"

def create_folder(name):
    dataset_folder = "dataset"
    if not os.path.exists(dataset_folder):
        os.makedirs(dataset_folder)

    person_folder = os.path.join(dataset_folder, name)
    if not os.path.exists(person_folder):
        os.makedirs(person_folder)
    return person_folder

def capture_photos(name):
    folder = create_folder(name)

    picam2 = Picamera2()

picam2.configure(picam2.create_preview_configuration(main={"format
": 'XRGB8888', "size": (640, 480)}))
    picam2.start()

    time.sleep(2)

    photo_count = 0

    print(f"Зйомка зображень для {name}. SPACE щоб зробити
зображення, 'q' для виходу.")

    while True:
        frame = picam2.capture_array()

        cv2.imshow('Capture', frame)

        key = cv2.waitKey(1) & 0xFF

        if key == ord(' '):
            photo_count += 1
            timestamp = datetime.now().strftime("%Y%m%d_%H%M%S")
            filename = f"{name}_{timestamp}.jpg"
            filepath = os.path.join(folder, filename)
            cv2.imwrite(filepath, frame)
            print(f"Photo {photo_count} saved: {filepath}")
```

```
        elif key == ord('q'):
            break

    cv2.destroyAllWindows()
    picam2.stop()
    print(f"Зображення знято. {photo_count} зображення збережено
для {name}.")

if __name__ == "__main__":
    capture_photos(PERSON_NAME)
```

Лістинг файлу model_training.py:

```
import os
from imutils import paths
import face_recognition
import pickle
import cv2

print("Обробка зображень облич...")
imagePaths = list(paths.list_images("dataset"))
knownEncodings = []
knownNames = []

for (i, imagePath) in enumerate(imagePaths):
    print(f"Обробка зображення {i + 1}/{len(imagePaths)}")
    name = imagePath.split(os.path.sep)[-2]

    image = cv2.imread(imagePath)
    rgb = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)

    boxes = face_recognition.face_locations(rgb, model="hog")
    encodings = face_recognition.face_encodings(rgb, boxes)

    for encoding in encodings:
        knownEncodings.append(encoding)
        knownNames.append(name)

print("Підпис кодування")
data = {"енкодинг": knownEncodings, "імена": knownNames}
with open("encodings.pickle", "wb") as f:
    f.write(pickle.dumps(data))

print("Навчання завершено, збережено в 'encodings.pickle'")
```

Лістинг файлу facial_recognition.py:

```
import face_recognition
import cv2
import numpy as np
from picamera2 import Picamera2
import time
import pickle

print("завантаження енкодингу")
with open("encodings.pickle", "rb") as f:
    data = pickle.loads(f.read())
known_face_encodings = data["encodings"]
known_face_names = data["names"]

picam2 = Picamera2()
picam2.configure(picam2.create_preview_configuration(main={"format
": 'XRGB8888', "size": (1920, 1080)}))
picam2.start()

cv_scaler = 4

face_locations = []
face_encodings = []
face_names = []
frame_count = 0
start_time = time.time()
fps = 0

def process_frame(frame):
    global face_locations, face_encodings, face_names

    resized_frame = cv2.resize(frame, (0, 0), fx=(1/cv_scaler),
fy=(1/cv_scaler))

    rgb_resized_frame = cv2.cvtColor(resized_frame,
cv2.COLOR_BGR2RGB)

    face_locations =
face_recognition.face_locations(rgb_resized_frame)
    face_encodings =
face_recognition.face_encodings(rgb_resized_frame, face_locations,
model='large')

    face_names = []
    for face_encoding in face_encodings:
        matches =
face_recognition.compare_faces(known_face_encodings,
face_encoding)
        name = "Unknown"
        face_distances =
face_recognition.face_distance(known_face_encodings,
face_encoding)
        best_match_index = np.argmin(face_distances)
        if matches[best_match_index]:
```

```
            name = known_face_names[best_match_index]
        face_names.append(name)

    return frame

def draw_results(frame):
    for (top, right, bottom, left), name in zip(face_locations,
face_names):
        top *= cv_scaler
        right *= cv_scaler
        bottom *= cv_scaler
        left *= cv_scaler

        cv2.rectangle(frame, (left, top), (right, bottom), (244,
42, 3), 3)

        cv2.rectangle(frame, (left -3, top - 35), (right+3, top),
(244, 42, 3), cv2.FILLED)
        font = cv2.FONT_HERSHEY_DUPLEX
        cv2.putText(frame, name, (left + 6, top - 6), font, 1.0,
(255, 255, 255), 1)

    return frame

def calculate_fps():
    global frame_count, start_time, fps
    frame_count += 1
    elapsed_time = time.time() - start_time
    if elapsed_time > 1:
        fps = frame_count / elapsed_time
        frame_count = 0
        start_time = time.time()
    return fps

while True:
    frame = picam2.capture_array()

    processed_frame = process_frame(frame)

    display_frame = draw_results(processed_frame)

    current_fps = calculate_fps()

    cv2.putText(display_frame, f"FPS: {current_fps:.1f}",
(display_frame.shape[1] - 150, 30),
                cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2)

    cv2.imshow('Video', display_frame)

    if cv2.waitKey(1) == ord("q"):
        break

cv2.destroyAllWindows()
picam2.stop()
```

Лістинг файлу facial_recognition_hardware.py:

```
import face_recognition
import cv2
import numpy as np
from picamera2 import Picamera2
import time
import pickle

print("завантаження енкодингу")
with open("encodings.pickle", "rb") as f:
    data = pickle.loads(f.read())
known_face_encodings = data["encodings"]
known_face_names = data["names"]

picam2 = Picamera2()
picam2.configure(picam2.create_preview_configuration(main={"format
": 'XRGB8888', "size": (1920, 1080)}))
picam2.start()

cv_scaler = 4

face_locations = []
face_encodings = []
face_names = []
frame_count = 0
start_time = time.time()
fps = 0

def process_frame(frame):
    global face_locations, face_encodings, face_names

    resized_frame = cv2.resize(frame, (0, 0), fx=(1/cv_scaler),
fy=(1/cv_scaler))

    rgb_resized_frame = cv2.cvtColor(resized_frame,
cv2.COLOR_BGR2RGB)

    face_locations =
face_recognition.face_locations(rgb_resized_frame)
    face_encodings =
face_recognition.face_encodings(rgb_resized_frame, face_locations,
model='large')

    face_names = []
    for face_encoding in face_encodings:
        matches =
face_recognition.compare_faces(known_face_encodings,
face_encoding)
        name = "Unknown"
        face_distances =
face_recognition.face_distance(known_face_encodings,
face_encoding)
        best_match_index = np.argmin(face_distances)
        if matches[best_match_index]:
```

```
            name = known_face_names[best_match_index]
        face_names.append(name)

    return frame

def draw_results(frame):
    for (top, right, bottom, left), name in zip(face_locations,
face_names):
        top *= cv_scaler
        right *= cv_scaler
        bottom *= cv_scaler
        left *= cv_scaler

        cv2.rectangle(frame, (left, top), (right, bottom), (244,
42, 3), 3)

        cv2.rectangle(frame, (left -3, top - 35), (right+3, top),
(244, 42, 3), cv2.FILLED)
        font = cv2.FONT_HERSHEY_DUPLEX
        cv2.putText(frame, name, (left + 6, top - 6), font, 1.0,
(255, 255, 255), 1)

    return frame

def calculate_fps():
    global frame_count, start_time, fps
    frame_count += 1
    elapsed_time = time.time() - start_time
    if elapsed_time > 1:
        fps = frame_count / elapsed_time
        frame_count = 0
        start_time = time.time()
    return fps

while True:
    frame = picam2.capture_array()

    processed_frame = process_frame(frame)

    display_frame = draw_results(processed_frame)

    current_fps = calculate_fps()

    cv2.putText(display_frame, f"FPS: {current_fps:.1f}",
(display_frame.shape[1] - 150, 30),
                cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2)

    cv2.imshow('Video', display_frame)

    if cv2.waitKey(1) == ord("q"):
        break

cv2.destroyAllWindows()
picam2.stop()
```