Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА
# Пояснювальна записка

перший (бакалаврський)
(рівень вищої освіти)

Розроблення автоматичної підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технології комп'ютерного зору
(тема)

Виконав:
здобувач 4 року навчання,
групи АКТАКІТ-21-1
Андрій НОРИК
(власне ім'я, прізвище)

Спеціальність 151 Автоматизація та комп'ютерно інтегровані технології
(код і повна назва спеціальності)
Тип програми освітньо-професійна
Освітня програма АКІТ
( повна назва освітньої програми)

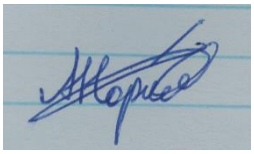
Керівник асистент Андрій СЛЮСАР
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри КІТАР _____ Ігор НЕВЛЮДОВ
(підпис) (власне ім'я, прізвище)

2025 р.

Я, Норик Андрій Олександрович, як здобувач вищої освіти ХНУРЕ, розумію і підтримую політику закладу із академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Я не використовував штучний інтелект для підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

«23» червня 2025 р.  Андрій НОРИК

Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій

Кафедра Комп'ютерно-інтегрованих технологій автоматизації та робототехніки

Рівень вищої освіти перший (бакалаврський)

Спеціальність 151 Автоматизація та комп'ютерно-інтегровані технології
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Автоматизація та комп'ютерно-інтегровані технології
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«30» квітня 2025 р.

# ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Норику Андрію Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення автоматичної підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технології комп'ютерного зору
затверджена наказом університету від 19 травня 2025 р. № 390 Ст
2. Термін подання здобувачем роботи до екзаменаційної комісії 27 червня 2025 р.
3. Вихідні дані до роботи
3.1 Можливість інтеграції комп'ютерного зору з сенсорними пристроями для підвищення надійності спрацювань
3.2 Середовище та мова розробки: Python, OpenCV, MediaPipe; середовище розробки – PyCharm.
3.3 Використання алгоритмів розпізнавання облич для ідентифікації особи
3.4 Сумісність з апаратними платформами Raspberry Pi, Arduino
3.6 Інтерфейс взаємодії інформативний і придатним для сповіщення адміністратора
4. Перелік питань, що потрібно опрацювати в роботі
4.1 Аналіз існуючих засобів та методів контролю доступу до приміщення
4.2 Розробка структурної схеми, алгоритм роботи та схему підключення підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технології комп'ютерного зору
4.3 Розроблення програмної частини підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технології комп'ютерного зору
4.4 Охорона праці
4.5 Висновки
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних

ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
Демонстраційний матеріал, представлений у форматі презентації Power Point (*ppt) – 12 ст. формату А4 _____
_____
_____
_____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1 )

| Найменування розділу | Консультант (посада, прізвище, ім'я, по батькові) | Позначка консультанта про виконання розділу | |
|---|---|---|---|
| | | підпис | дата |
| | | | |
| | | | |

**КАЛЕНДАРНИЙ ПЛАН**

| № | Назва етапів роботи | Строк / терміни виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Аналіз технічного завдання | 30.04.2025 | виконано |
| 2 | Аналіз методів контролю доступу на об'єктах з підвищеними вимогами до безпеки | 01.05.2025 | виконано |
| 3 | Аналіз існуючих методів, засобів та програмних рішень для систем відеоспостереження та комп'ютерного зору | 10.05.2025 | виконано |
| 4 | Розробка структурної схеми підсистеми моніторингу та сповіщення | 18.05.2025 | виконано |
| 5 | Створення програмного забезпечення для розпізнавання санкціонованого доступу | 25.05.2025 | виконано |
| 6 | Розробка апаратно-програмного модуля системи моніторингу | 01.06.2025 | виконано |
| 7 | Оформлення пояснювальної записки | 14.06.2025 | виконано |
| 8 | Подання роботи на перевірку Інтернет-сервісом StrikePlagiarism | 24.06.2025 | виконано |
| 9 | Подання роботи на рецензію | 25.06.2025 | виконано |
| 10 | Подання роботи на підпис завідувачу кафедри | 26.06.2025 | виконано |
| 11 | Подання роботи до Екзаменаційної комісії (ЕК) | 27.06.2025 | виконано |

Дата видачі завдання 30 квітня 2025 р.

Здобувач _____ Андрій НОРИК
(підпис)

Керівник роботи _____ асистент Андрій СЛЮСАР
(підпис) (посада, власне ім'я, прізвище)

# РЕФЕРАТ

Пояснювальна записка: 57 с., 24 рис., 2 дод., 16 джерел.

КОМП'ЮТЕРНИЙ ЗІР, МОНІТОРИНГ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, РОЗПІЗНАВАННЯ ОБЛИЧ, ВІДЕОСПОСТЕРЕЖЕННЯ, ДАТЧИКИ, PYTHON, MEDIAPIPE, СИГНАЛІЗАЦІЯ.

Мета роботи – покращення якості контролю доступу до приміщення за рахунок впровадження автоматичної підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технологій комп'ютерного зору.

Об'єкт дослідження – процес контролю доступу до приміщення.

Предмет дослідження – апаратно-програмна підсистема моніторингу та сповіщення з використанням відеоаналітики і сенсорних засобів.

У ході кваліфікаційної роботи проведено аналіз сучасних технологій контролю доступу: механічних, електронних та біометричних систем, а також огляд комерційних рішень на ринку.

Розроблено структурну схему системи, алгоритм її роботи, схему підключення апаратних компонентів, а також виконано підбір елементної бази.

Програмну частину реалізовано на мові Python з використанням бібліотеки MediaPipe, що дозволило забезпечити розпізнавання облич у режимі реального часу.

Експериментально досліджено ефективність використаного алгоритму розпізнавання облич у порівнянні з іншими методами (HOG + SVM, FaceNet). Наведено графічні результати та описано поведінку системи в різних ситуаціях.

Отримані результати роботи можно віднести до Цілі сталого розвитку 9 «Промисловість, інновації та інфраструктура», а саме п. 9.1 «Розвивати якісну надійну, сталу та доступну інфраструктуру, яка базується на використанні інноваційних технологій, у т.ч. екологічно чистих видів транспорту».

# ABSTRACT

Explanatory note: 57 pages, 24 figures, 2 appendices, 16 sources.

KEYWORDS: COMPUTER VISION, MONITORING, UNAUTHORIZED ACCESS, FACE RECOGNITION, VIDEO SURVEILLANCE, SENSORS, PYTHON, MEDIAPIPE, ALARM SYSTEM.

The purpose of this work is to improve the quality of access control to the premises by implementing an automated monitoring and notification subsystem for unauthorized access based on computer vision technologies.

The object of research – the process of controlling access to the premises.

The subject of the study is a hardware and software monitoring and notification subsystem using video analytics and sensors.

During the qualification work, an analysis of modern access control technologies, including mechanical, electronic, and biometric systems, and a review of commercial solutions on the market was conducted.

The system's block diagram, algorithm of its operation, hardware component connection diagram, and selection of the element base were developed.

The software part was implemented in Python using the MediaPipe library, which made it possible to provide real-time face recognition.

The effectiveness of the face recognition algorithm in comparison with other methods (HOG + SVM, FaceNet) has been experimentally investigated. Graphical results are presented, and the system's behavior in different situations is described.

The obtained results can be attributed to Sustainable Development Goal 9, 'Industry, innovation, and infrastructure,' namely, clause 9.1, 'Develop high-quality reliable, sustainable and affordable infrastructure based on the use of innovative technologies, including environmentally friendly modes of transport.'

# ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ

САПР – система автоматизованого проєктування;

СКБ – спеціалізоване конструкторське бюро;

СКУД – система контролю та управління доступом;

УСАРВ – Українська система автоматизованого розрахунку відрахувань;

CAD – Computer-Aided Design (автоматизоване проєктування);

CAM – Computer-Aided Manufacturing (автоматизоване виробництво);

CAE – Computer-Aided Engineering (автоматизовані інженерні розрахунки й аналіз);

RFID – Radio Frequency Identification (радіочастотна ідентифікація).

# ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій та зростання рівня загроз кібер- і фізичної безпеки, все більшої актуальності набуває створення ефективних автоматизованих систем безпеки. Особливої уваги потребують технології, здатні в режимі реального часу здійснювати моніторинг обстановки, ідентифікувати потенційні загрози та оперативно реагувати на них. Одним із перспективних напрямів у цій галузі є застосування методів комп’ютерного зору для виявлення несанкціонованого доступу до об'єктів.

Комп’ютерний зір дозволяє реалізувати автоматичне розпізнавання облич, аналіз поведінки осіб, виявлення підозрілої активності та формування відповідних сповіщень. Це значно підвищує ефективність систем контролю доступу, особливо у випадках, коли необхідно забезпечити безперервний контроль за великою кількістю об’єктів або територій.

Ця кваліфікаційна робота присвячена розробленню автоматизованої підсистеми моніторингу та сповіщення про несанкціонований доступ на основі технологій комп’ютерного зору. Рішення має на меті забезпечення надійного та швидкого виявлення спроб доступу сторонніх осіб, що дозволяє своєчасно вживати відповідних заходів безпеки.

У межах кваліфікаційної роботи здійснюється проєктування апаратної частини системи, включаючи вибір та обґрунтування елементної бази (камери, обчислювальний модуль, мережеві пристрої, засоби зв’язку та сповіщення), розроблення структурної та алгоритмічної схеми функціонування, а також опис логіки взаємодії між її компонентами.

Мета роботи – покращення якості контролю доступу до приміщення за рахунок впровадження автоматичної підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технологій комп’ютерного зору.

Об’єкт розробки – процес контролю доступу до приміщень.

Предмет розробки – підсистема моніторингу та сповіщення про несанкціонований доступ на базі комп’ютерного зору.

Для досягнення поставленої мети необхідно вирішити такі основні задачі:

– провести аналіз сучасних методів, засобів та систем контролю доступу до приміщень;

– дослідити комерційно доступні рішення у сфері автоматизованого моніторингу доступу;

– розробити структурну та алгоритмічну схему функціонування підсистеми;

– здійснити підбір оптимальних технічних компонентів системи з урахуванням вимог до продуктивності, енергоефективності, надійності та вартості;

– розробити програмну частину автоматичної підсистеми моніторингу та сповіщення;

– провести симуляцію роботи розробленого алгоритму розпізнавання облич;

– розробити та оформити пояснювальну записку, використовуючи навчальний посібник з дипломного проектування [3], методичні вказівки [2] та ДСТУ 3008-15 [1].

# 1 АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ТА МЕТОДІВ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

## 1.1 Аналіз сучасних технологій контролю доступу до приміщення

На сьогоднішній день впровадження систем контролю доступу до приміщень стає все більш актуальним через постійне збільшення кількості випадків крадіжок, незаконних проникнень та інших порушень. Останнім часом питання забезпечення безпеки приміщень набуває дедалі більшої актуальності, незалежно від типу об'єкта – чи то житлові будівлі або офісні приміщення. Вибір ефективної системи контролю доступу є важливим завданням, що постає перед користувачем.

Одним із традиційних методів контролю доступу є механічні замки різних типів. Головними перевагами таких замків є простота у використанні, низька вартість, а також широке поширення комплектів замків із ключами для зручності монтажу та експлуатації. Водночас механічні замки мають суттєві недоліки: їх можна легко зламати, а ключі – загубити чи втратити, що призводить до неможливості точно ідентифікувати особу, яка отримала доступ до приміщення.

З огляду на зазначені обмеження, все більшої популярності набувають електронні системи контролю доступу. До таких систем належать замки, що відкриваються за допомогою карток, брелків або введення спеціальних кодів. Основні переваги цих систем полягають у можливості швидкого керування доступом, оперативному блокуванні або виданні електронних ключів, зміні кодів доступу та ідентифікації осіб, які отримують доступ у певний час. Саме завдяки цим перевагам електронні замки отримали широке застосування в офісах великих компаній, готелях, фінансових установах, освітніх закладах та інших об'єктах, де необхідний ретельний контроль за доступом. Водночас слід враховувати, що електронні системи також не є абсолютно надійними, оскільки існує можливість злому електронних ключів, карток або кодових замків.

Вищий рівень безпеки надають біометричні системи контролю доступу. Ці системи забезпечують високий рівень безпеки, оскільки використовують унікальні біометричні характеристики людини, такі як відбитки пальців, особливості обличчя, райдужну оболонку ока та голос. Завдяки цьому вони здатні дуже точно ідентифікувати особу, практично унеможливлюючи помилки та виключаючи можливість підробки, адже ці характеристики індивідуальні для кожної людини.

Останнім часом біометричні технології набувають дедалі більшої популярності, оскільки користувачам не потрібно носити із собою ключі або картки, які можна загубити чи забути вдома. Проте ці рішення мають і певні недоліки: вони дорожчі, складніші у встановленні та налаштуванні, вимагають регулярного технічного обслуговування і все ж залишається ризик злому.

Продуктивні системи контролю доступу також використовують інтегровані продукти, що поєднують декілька методів в єдиному технологічному рішенні. Наприклад, дуже популярні системи, які поєднують електронні замки з біометричними технологіями. В результаті можна суттєво підвищити ступінь надійності й ефективності захисту приміщень.

Таким чином, під час вибору засобів доступу до приміщення слід враховувати, що багатоаспектність не дозволяє застосовувати універсальний підхід або єдиний метод вирішення в усіх випадках. Як правило, необхідно брати до уваги специфічні умови, серед яких рівень потенційних загроз та наявність фінансових ресурсів.

## 1.2 Класифікація технологій контролю доступу до приміщення

Сучасні технології контролю доступу поділяють на кілька основних категорій. Кожна з цих категорій має свої особливості, переваги та недоліки, що полегшує аналіз і допомагає зрозуміти, який саме спосіб контролю доступу найкраще підходить у конкретних умовах.

Перша й найпростіша категорія систем контролю доступу – це механічні замки. Саме вони є найдавнішими та знайомими всім вже багато років. До них належать, передусім, звичайні замки. Циліндрові замки, замки із засувом, навісні замки, кодові замки та багато інших. Усі вони відкриваються за допомогою звичайного металевого ключа або механічної комбінації [4].

До наступної категорії належать електронні замки. Вони значно сучасніші та більш безпечні порівняно з механічними. До таких типів замків належать магнітні картки, RFID-мітки, електронні ключі, кодові замки, домофони. Наприклад, одними з найбільших виробників вважаються компанії, що випускають замки з магнітними картками – HID Global, Salto Systems, ZKTeco. Вони допомагають точно керувати доступом до приміщень, легко змінювати рівень доступу, а також вести облік кожної події. Наприклад, якщо співробітник загубив картку, її можна легко деактивувати та видати іншу, чого неможливо зробити зі звичайними замками з механічним ключем.

Третій тип електронного доступу – ідентифікація особи за допомогою особистих біометричних даних. Такі системи контролюються найбільш точно й вважаються найбезпечнішими. Особливість цього типу доступу полягає в підтвердженні особистості людини за її унікальними фізіологічними характеристиками – такими як відбитки пальців, сітківка або райдужка ока – або за поведінковими особливостями. Сучасні смартфони й планшети з технологією розпізнавання обличчя – це яскравий приклад біометричних технологій.

Серед виробників, які випускають системи біометричного контролю доступу, можна виділити компанії Suprema (FaceStation 2, BioStation), ZKTeco (SpeedFace, SilkID) або BioSmart. Головними перевагами таких систем є максимально високий рівень захисту (адже скопіювати біометричні дані дуже і дуже складно), зручність використання (немає необхідності носити із собою ключ чи брелок), а також точність ідентифікації особи.

Однак біометричні системи мають і певні недоліки. Це висока вартість обладнання, складність монтажу, необхідність регулярного сервісного обслуговування. Крім того, існує ряд проблем із безпекою зберігання самих

біометричних даних, оскільки їх неможливо замінити так легко, як звичайний пароль чи пропуск.

Таким чином, всі ці системи працюють разом. Вибір залежить від типу об’єкта, фінансів та рівня безпеки. Біометрія – правильне рішення для великих систем безпеки, електронний контроль доступу підходить для більшості підприємств та офісів, а механічні замки також актуальні для багатьох звичайних житлових приміщень та приміщень з обмеженим бюджетом.

Ще один важливий напрямок – це системи, що поєднують у собі різні технічні засоби. Наприклад, RFID-карти та біометрія (відбиток пальця та розпізнавання обличчя). Вони дозволяють повною мірою використовувати всі переваги кожної технології та згладжують їхні недоліки. Вони відмінно підходять для систем із найвищими вимогами безпеки (великі банки, дата-центри, державні установи) [5].

Отже, сучасні системи контролю доступу, які представлені на ринку, характеризуються різним рівнем безпеки, варіюються за ціною, складністю експлуатації та монтажу. Вибір конкретного пристрою залежить від особливостей приміщення, у якій планується його встановлення, а також фінансових можливостей власників.

### 1.2.1 Механічні засоби санкціонованого доступу до приміщення

Для контролю доступу дуже часто обирають механічні замки. Вони існують вже давно і поширені тому, що коштують недорого, прості у використанні та мають досить високу надійність.

Основним елементом механічного замка стає механізм (рис. 1.1), що запускається за допомогою витриманого у специфічному вигляді ключа або відмикання за допомогою даної комбінації. Механічні замки діють досить просто: ключ змінює параметри замка механічно (рухає циліндри, зсуває сувальди тощо), що дозволяє відчинити або закрити двері.

Переваги механічних замків – це простота установки, незалежність від джерел енергії, надійність роботи у звичайних умовах та низькі ціни. Механічні замки мають серйозні недоліки.

Не зважаючи на це, механічні замки досі залишаються дуже затребуваними через простоту монтажу та доступні ціни, проте вони забезпечують лише базовий ступінь безпеки. Тому для важливих чи дорогих об’єктів переважно встановлювати системи з електронними або навіть біометричними засобами контролю доступу, завдяки чому безпека умов ще більше зростає.

Рисунок 1.1 – Механічний замок з циліндричним механізмом

Хоча замки все ще популярні, завдяки своїй простоті та доступності, більшої безпеки вдалося б досягти при використанні додаткових сучасних та надійних систем контролю доступу.

### 1.2.2 Електроні засоби санкціонованого доступу до приміщення

З метою виключення потенційних проблем, пов’язаних із втратою або втратою ключів, та їх несанкціонованим виготовленням, а також з метою фіксації фактів відкриття замків на важливих об’єктах, механічні замки та засуви все частіше поступаються місцем сучасним електронним. Можливо, невдовзі механічні засоби будуть мінімально використовуватись, або навіть зовсім не використовуватимуться.

Так як у механічних замків і засувів при всій їх надійності є і фундаментальні недоліки: ключ можна втратити, і можна виготовити некеровану кількість фізичних ключів без відома і дозволу власника приміщення. Тим більше, що у механічної системи немає відстеження часу відкриття та запису моменту відкриття. Сучасні електронні системи мають технічні можливості автоматично фіксувати інформацію про кожну спробу доступу. Це включає точну ідентифікацію особи, яка використовує електронний ключ або картку, а також час входу та виходу з приміщення.

Широке поширення сучасних електронних замків обумовлено їх можливістю багато в чому вирішувати проблеми, які раніше не могли бути вирішені за допомогою звичних механічних замків. Що робить системи безпеки більш надійними, та забезпечує рівень безпеки, що відповідає завданням охорони об'єктів.

Сучасні замки поділяються на кілька типів за принципом ідентифікації користувачів та типів доступу.

Електронні замки без механічного ключа використовують для керування доступом спеціалізовані електронні носії інформації – картки з інтегрованими мікросхемами або з магнітною смугою. Для забезпечення доступу такі картки необхідно помістити у відповідний пристрій зчитування інформації, вбудований у замок. Подібні рішення є особливо популярними у готельній сфері завдяки простоті їх програмування, можливості швидкого перекодування або блокування ключа у випадку його втрати. Картки з магнітною смугою зазвичай виготовляються з пластику та містять додаткову службову інформацію. Для

відкривання дверей необхідно провести карткою через зчитувальний пристрій замка. Такі рішення широко використовуються у корпоративному секторі через їхні переваги, серед яких економічність і простота експлуатації (рис. 1.2).

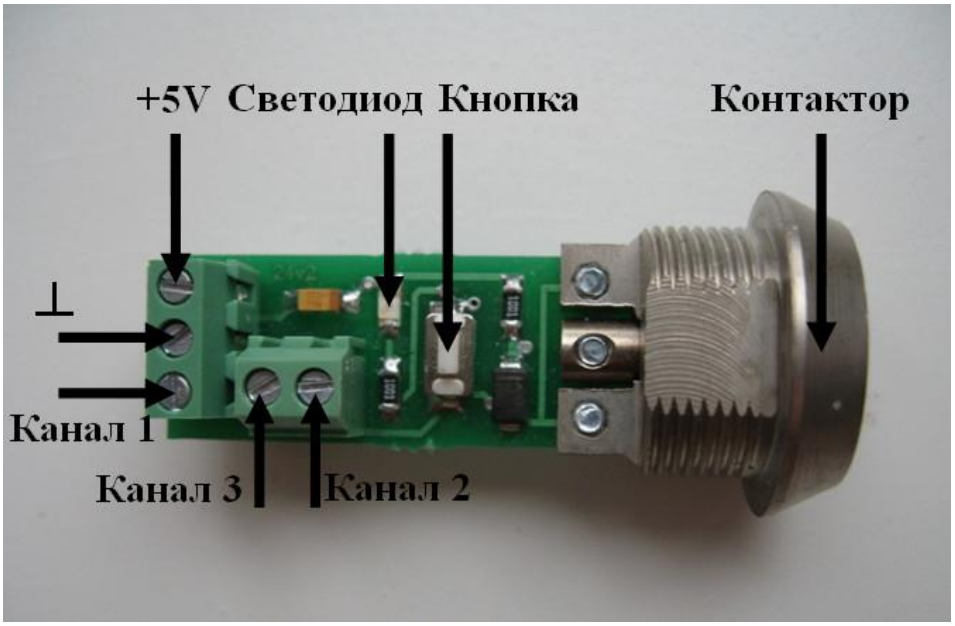



Рисунок 1.2 – Електронний замок та опис його компонентів

Безконтактна система доступу з використанням RFID. Для відкриття дверей потрібно просто піднести картку або брелок до зчитувача. Такі системи часто використовується в усьому світі, у тому числі у великих компаніях, таких як Google, Microsoft, Amazon. Основні виробники – SEVEN, HID, Dahua.

Контролер SEVEN CR-772m – це автономний пристрій для організації системи контролю доступу з використанням безконтактних RFID-ідентифікаторів стандарту EM-Marine (частота 125 кГц). Він поєднує функції контролера та зчитувача та дозволяє ефективно контролювати доступ через один прохід без підключення до центральної системи.

Замки з цифровими клавіатурами, які відкриваються після введення власного PIN-коду. Очевидно, найчастіше такі замки використовують у офісах, на складах, в лабораторіях тощо. Відомим брендом таких замків є Samsung.

Проте, з іншого боку, є й недоліки електронних систем. Ми говоримо про вразливості, такі як копіювання RFID-ідентифікаторів, ламання коду від замку, а

також зламування електронних замків кіберзлочинцями. Все це спонукає розробників покращувати технології, шифрувати дані та зміцнювати захист від можливих атак.

### 1.2.3 Біометричні засоби санкціонованого доступу

Сьогодні найбільш сучасним та комфортним є розпізнавання людини за допомогою біометрії. Біометрична система контролю доступу базується на ідентифікації особистості за унікальними фізіологічними ознаками людини. До таких ознак належать відбитки пальців, геометрія обличчя, структура райдужної оболонки ока та геометрія долоні руки. Зазначені біометричні параметри є індивідуальними для кожної людини, що робить їх високонадійним засобом аутентифікації.

Масове впровадження біометричних технологій має низку переваг порівняно з традиційними механічними та електронними системами контролю доступу. Основними перевагами таких систем є високий ступінь надійності та точність ідентифікації користувачів, що унеможливлює підробку або втрату ідентифікаційних даних. На відміну від традиційних ключів чи перепусток, біометричні дані завжди знаходяться при користувачеві, що суттєво зменшує ризик їх втрати або несанкціонованого використання сторонніми особами.

Сьогодні біометрія – це не лише забезпечення безпеки приміщень. Але й різних пристроїв, наприклад, смартфонів та персональних комп'ютерів. Два відомих приклади – це технології з розпізнавання обличчя Face ID та відбитків пальців Touch ID фірми Apple, аналогічні рішення є у Samsung, що реалізує їх у своїх смартфонах та інших мобільних пристроях.

У контексті забезпечення безпеки об’єктів, де зберігається конфіденційна інформація чи матеріальні цінності, на сьогодні найбільш затребуваними є біометричні системи контролю доступу. Такі системи застосовуються для захисту приміщень та офісів великих компаній, банківських установ, сховищ даних, державних організацій і стратегічних промислових об'єктів. Серед провідних виробників, що інтегрують біометричні технології у свої рішення для

професійного сектору, можна виділити, зокрема, компанію Suprema з її пристроями FaceStation 2 та BioStation A2.

Особливо активно біометричні технології впроваджуються у фінансовій сфері. Так, у банківських установах (наприклад, у ПриватБанку та Monobank) вже реалізовано рішення, що дозволяють ідентифікувати клієнтів за відбитками пальців або шляхом розпізнавання обличчя для підвищення безпеки під час здійснення карткових транзакцій та операцій у мобільних додатках.

Однак, попри очевидні переваги, впровадження біометричних систем пов’язане з певними труднощами. Серед головних недоліків – висока вартість обладнання, складність його встановлення та значні витрати на регулярне технічне обслуговування. Крім того, важливо враховувати потенційні ризики, пов’язані з безпекою: у разі компрометації біометричних даних неможливо здійснити їх заміну так само легко, як пароль чи електронний ключ, що робить наслідки витоку цих даних особливо критичними.

Тому розпізнавання по біометрії займає провідну позицію серед сучасних засобів контролю доступу завдяки своїй точності ідентифікації, зручності та надійності, хоча до його реалізації потрібен особливий підхід, оскільки використання біометрії пов’язане з проблемами конфіденційності та безпеки даних.

Проте, попри численні переваги біометричних систем, необхідно враховувати й низку недоліків, що обмежують їх застосування.

По-перше, застосування біометричних систем контролю доступу пов’язане зі значними фінансовими витратами, що зумовлюється необхідністю повної модернізації обладнання та програмного забезпечення на всіх точках входу у приміщення. Таке обладнання є технічно складним, потребує регулярного кваліфікованого монтажу, налаштування та сервісного обслуговування, що може бути виконано лише спеціально навченими фахівцями. Крім апаратного обслуговування, біометричні системи вимагають ретельного програмного калібрування з урахуванням індивідуальних особливостей користувачів, режиму

роботи об’єкта та інших параметрів експлуатації, що потребує високої точності та ретельності на етапі впровадження.

По-друге, навіть найсучасніші біометричні системи не є повністю захищеними від помилок. Імовірність збоїв виникає через зовнішні фактори, такі як пошкодження або забруднення сканованих біометричних ознак (наприклад, стирання відбитків пальців), нерівномірність освітлення при розпізнаванні обличчя чи інші умови, що погіршують якість отриманої інформації. Відповідно, система біометричної аутентифікації завжди потребує регулярного моніторингу і, за необхідності, додаткового налаштування обладнання для забезпечення високої точності розпізнавання.

Ще однією важливою проблемою використання біометричних систем є безпека зберігання та обробки біометричних даних користувачів. Ця проблема є особливо актуальною, оскільки, на відміну від паролів чи електронних карток, у разі компрометації біометричних даних неможливо здійснити їх заміну. Тому питання конфіденційності та надійності зберігання біометричних ознак висуваються на перший план серед завдань, які має вирішувати експлуатуюча організація.

Зважаючи на вищезазначені виклики, дедалі більшої популярності набувають багатофакторні системи контролю доступу, що поєднують кілька методів автентифікації. Подібні системи можуть одночасно використовувати електронні засоби ідентифікації (наприклад, RFID-картки або введення паролю) та біометричні технології (сканування відбитків пальців, розпізнавання обличчя). Багатофакторна автентифікація широко застосовується на об'єктах із підвищеним рівнем безпеки, таких як фінансові установи (банки), державні організації (наприклад, Міністерство внутрішніх справ України), великі промислові підприємства та стратегічні компанії (наприклад, АТ «Укрзалізниця», ДП «НАЕК Енергоатом»), де вимоги до безпеки є надзвичайно високими.

## 1.3 Аналіз сучасних комерційних систем контролю доступу до приміщень

### 1.3.1 SEVEN CR-772m

SEVEN CR-772m оснащений релейним виходом для підключення електромагнітного або електромеханічного замка, а також входом для кнопки виходу. Програмування пристрою здійснюється за допомогою інфрачервоного пульта дистанційного керування та майстер-карт, що входять до комплекту постачання. Додатково, контролер (рис. 1.3) має вбудований світлочутливий резистор для захисту від несанкціонованого відкриття корпусу та триколірний світлодіодний індикатор стану. Нижче наведено фото SEVEN CR-772m контролера [6].

Технічні характеристики SEVEN CR-772m:

– підтримка ідентифікаторів: EM-Marine 125 кГц;

– максимальна кількість користувачів: до 2000;

– дальність зчитування: від 3 см до 10 см;

– режими роботи: імпульсний та фіксації;

– живлення: DC від 12 В до 24 В;

– ступінь захисту: IP66;

– робочий температурний діапазон: від –40°C до +60°C;

– матеріал корпусу: нержавіюча сталь.

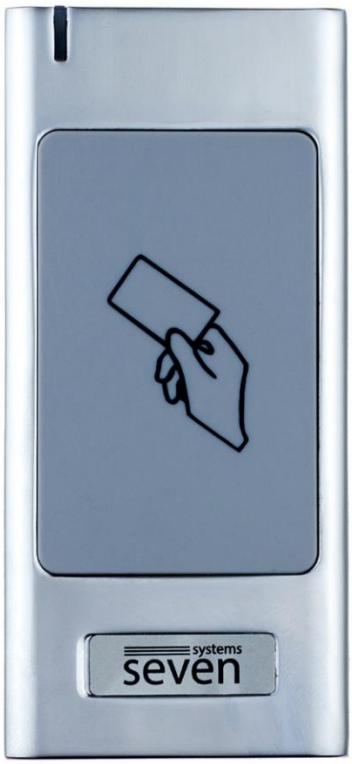



Рисунок 1.3 – Контролер зі зчитувачем магнітної картки SEVEN CR-772m

1.3.2 Suprema FaceStation 2

Suprema FaceStation 2 – біометричний термінал для контролю доступу до приміщення, який використовує технологію розпізнавання обличчя. Завдяки передовим алгоритмам та потужному апаратному забезпеченню, цей пристрій забезпечує швидку та точну ідентифікацію користувачів [7].

Основні технічні характеристики:

– процесор: 1,4 ГГц Quad-Core;

– пам'ять: 8 ГБ Flash + 1 ГБ RAM;

– дисплей: 4-дюймовий кольоровий TFT LCD з роздільною здатністю 800 пікселів x 480 пікселів;

– ємність користувачів: до 30000;

– швидкість розпізнавання: до 4000 порівнянь в секунду;

– журнали подій: до 5000000 текстових записів та 50000 зображень;

– інтерфейси: Ethernet, wi-fi , RS-485, Wiegand, USB 2.0;

– діапазон робочих температур: від – 20°C до +50°C.

Цей пристрій (рис. 1.4) також оснащений інфрачервоною підсвіткою, що дозволяє йому працювати в умовах низького освітлення до 25000 лк, та підтримує функцію виявлення живого обличчя для запобігання спробам обману системи за допомогою фотографій або відео.


Рисунок 1.4 – Пристрій для біометричного контролю доступу з функцією розпізнавання обличчя Suprema FaceStation 2

### 1.3.3 Suprema FaceStation F2

Suprema FaceStation F2 – високотехнологічний багатофункціональний термінал контролю доступу, який поєднує в собі передові біометричні технології та підтримку різноманітних методів ідентифікації. Цей пристрій забезпечує високий рівень безпеки та зручності використання, що робить його ідеальним рішенням для сучасних систем контролю доступу [8].

Основні технічні характеристики:

– біометричні методи ідентифікації: розпізнавання обличчя та відбитків пальців;

– технологія Fusion Matching: поєднання візуального та інфрачервоного розпізнавання обличчя з використанням алгоритмів глибокого навчання для досягнення високої точності та захисту від спроб обману системи;

– підтримка RFID: сумісність з картками 125 кГц EM, HID Prox, 13,56 МГц MIFARE, MIFARE Plus, DESFire EV1/EV2/EV3, FeliCa, а також мобільний доступ через NFC та BLE;

– ємність пам’яті: до 100000 користувачів. 50000 користувачів для розпізнавання обличчя. 100000 користувачів для відбитків пальців. З можливістю зберігання до 5000000 текстових логів та 50000 зображень;

– дисплей: 7-дюймовий кольоровий IPS LCD з роздільною здатністю 800 x 1280 пікселів;

– швидкість розпізнавання: менше 0,5 с;

– інтерфейси: Ethernet, RS-485, Wiegand, USB 2.0, два TTL входи, один релейний вихід;

– живлення: 12 В або 24 В DC, максимальний струм 2,5 А;

– робочі умови: температура від – 20°C до +50°C, вологість від 0% до 80% (без конденсації).

Suprema FaceStation F2 (рис. 1.5) також підтримує функції виявлення живого обличчя та відбитків пальців, що забезпечує додатковий рівень безпеки.

Завдяки своїм можливостям, цей термінал ідеально підходить для використання в офісах, виробничих підприємствах, медичних закладах та інших об'єктах, де необхідний високий рівень контролю доступу.


Рисунок 1.5 – Пристрій для біометричного контролю доступу з функцією розпізнавання обличчя Suprema FaceStation F2

# 2 РОЗРОБЛЕННЯ СТРУКТУРНОЇ СХЕМИ ТА АЛГОРИТМ РОБОТИ ПІДСИСТЕМИ МОНІТОРИНГУ ТА СПОВІЩЕННЯ ПРО НЕСАНКЦІОНОВАНИЙ ДОСТУП ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ КОМП'ЮТЕРНОГО ЗОРУ

## 2.1 Структурна схема

В ході розробки, яка складається з поетапної інтеграції апаратних і програмних компонентів, було створено цілісну архітектуру підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням комп'ютерного зору та сенсорних засобів (рис. 2.1). Основу цієї архітектури становить блок обробки даних, який функціонує як центральний елемент логічного управління. Він приймає, обробляє та аналізує сигнали від усіх елементів системи: сенсорів, камер та модулів контролю.

Контроль доступу здійснюється за трьома напрямами: дверей, стелі й підлоги. У зоні дверей використовується IP-камера, герконовий датчик і електронний замок, що взаємодіє з базою авторизованих осіб. Контроль стелі реалізовано за допомогою вібраційних сенсорів, ІЧ-бар'єрів та камери «fish-eye» для огляду зверху. Аналогічні засоби, зокрема вібраційні датчики й інфрачервоні сенсори, застосовуються для спостереження за підлогою.

Уся зібрана інформація надходить до блоку обробки даних, де в реальному часі виконується аналіз активності. У разі виявлення об'єкта система ініціює процедуру розпізнавання особи. Якщо особа є в базі, фіксується вхід, відбувається відкриття замка та продовжується спостереження. Якщо ж авторизацію не підтверджено або зафіксовано порушення (наприклад, перетин ІЧ-бар'єра чи вібрація), активується модуль сигналізації, який інформує охорону чи адміністратора.

Паралельно з цим відеопотік передається на сервер зберігання та аналізу, що дозволяє накопичувати архів даних і використовувати їх для подальшої

аналітики та навчання моделей комп’ютерного зору. Уся система функціонує як 9 злагоджений механізм, де кожен компонент виконує свою функцію, а взаємодія координується через блок обробки даних.

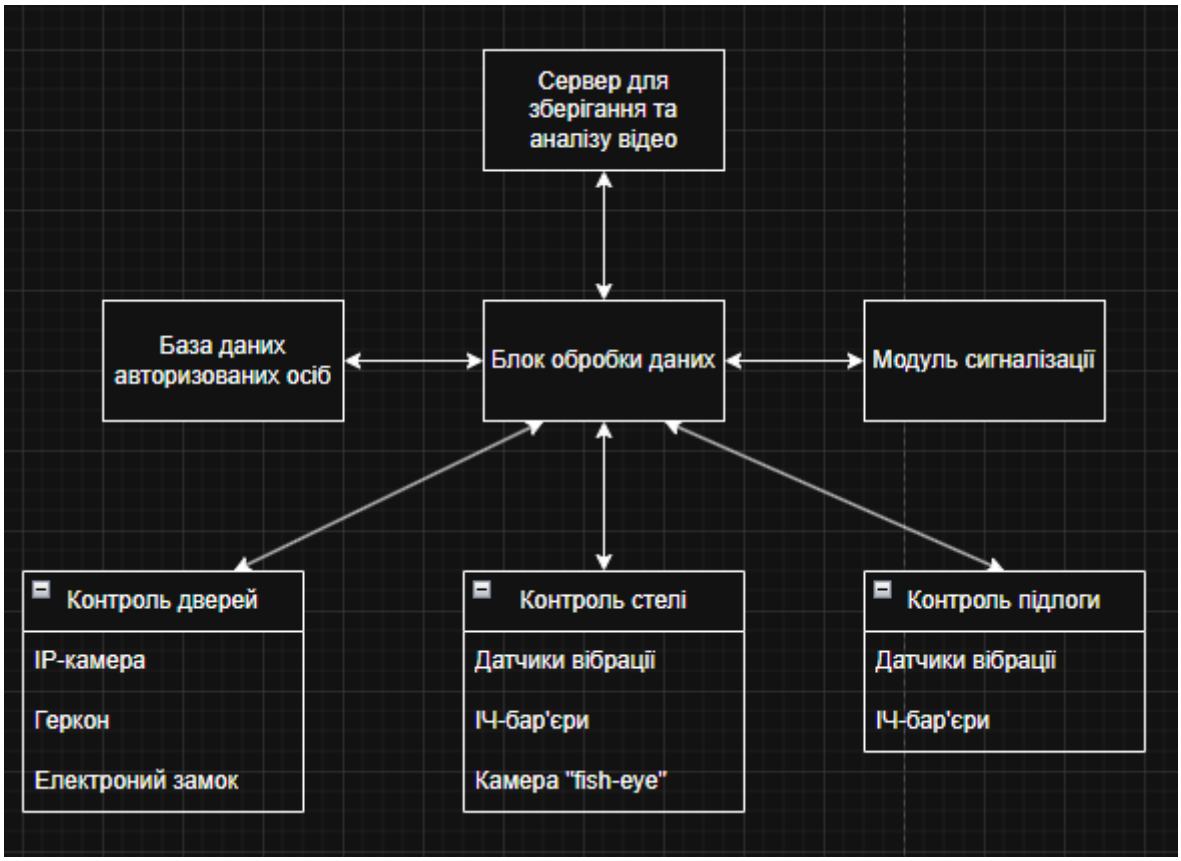



Рисунок 2.1 – Структурна схема

## 2.2 Алгоритм роботи

Підсистема моніторингу та сповіщення про несанкціонований доступ ґрунтується на поєднанні апаратних та програмних засобів, зокрема сенсорів, відеокамер і засобів обробки даних (рис. 2.2). Робота системи починається з ініціалізації, під час якої здійснюється перевірка стану всіх компонентів: IP-камери, камери типу «fish-eye», ІЧ-бар’єрів, герконів, електронного замка та вібраційних датчиків. У разі виявлення несправності система фіксує подію в журналі та повідомляє адміністратора. Якщо все працює коректно, запускається моніторинг у реальному часі. Відеопотік з камер обробляється у спеціальному

блоці, де також враховуються сигнали від сенсорів. У разі виявлення руху відбувається розпізнавання об’єкта та перевірка особи в базі даних. Якщо особа авторизована, фіксується вхід і продовжується відеоспостереження. У протилежному випадку активується система сигналізації та надсилається повідомлення охороні. Усі дані записуються на сервер для подальшого аналізу.

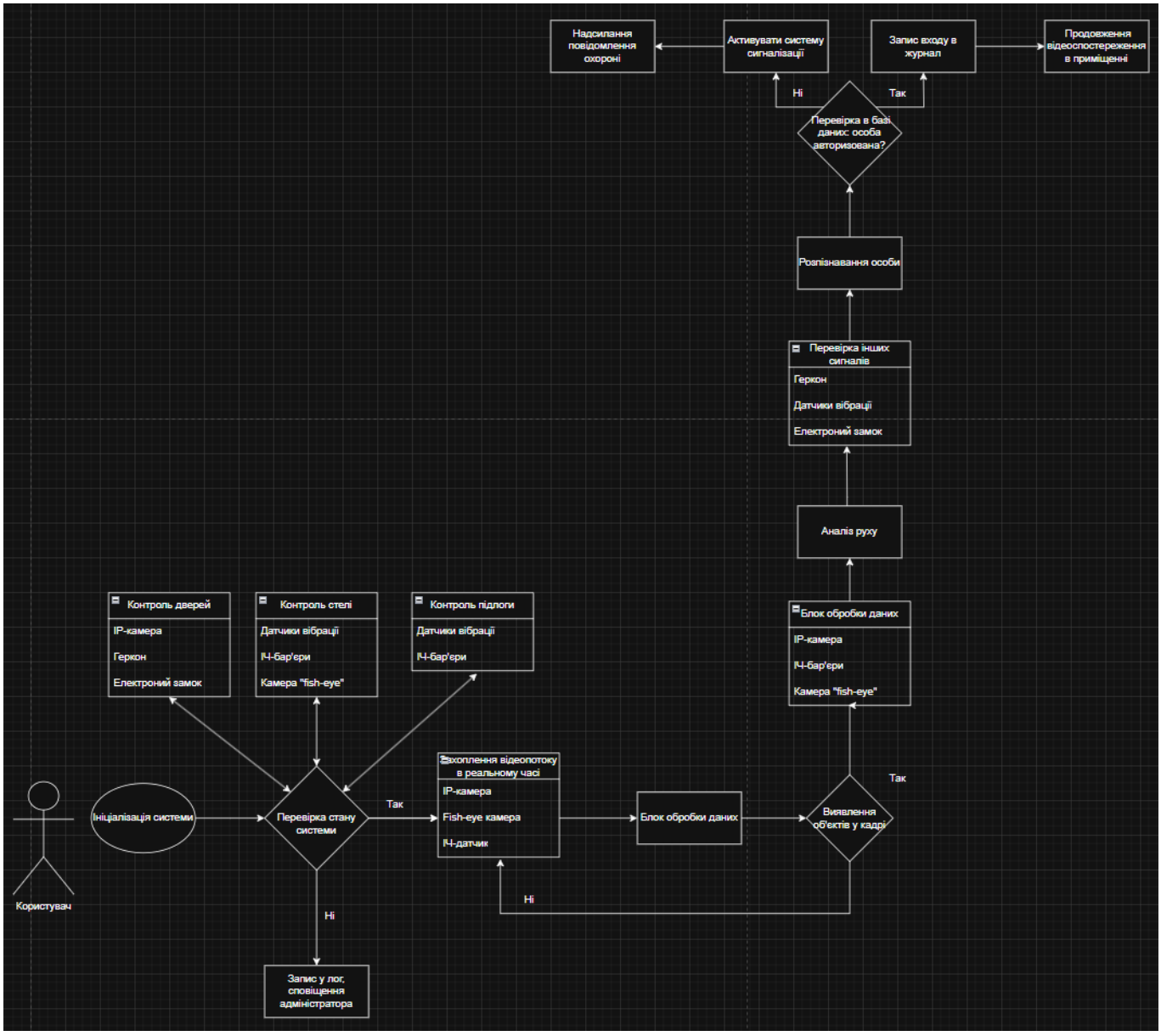



Рисунок 2.2 – UML роботи системи

## 2.3 Схема підключення

У цьому розділі подано схему підключення компонентів, що використовуються у системі (рис. 2.3). Вона демонструє, як саме з'єднуються між собою датчики руху, кнопки «вібрація» (імітація датчика вібрації) та кнопка “геркон” (імітація відкриття дверей), світлодіод (сигналізація), сервопривід (імітація електронного замка) та виконавчі пристрої для забезпечення коректної роботи підсистеми моніторингу та сповіщення. Схема реалізована у віртуальному середовищі моделювання Wokwi, що дозволяє перевірити логіку взаємодії всіх елементів до створення фізичного пристрою.

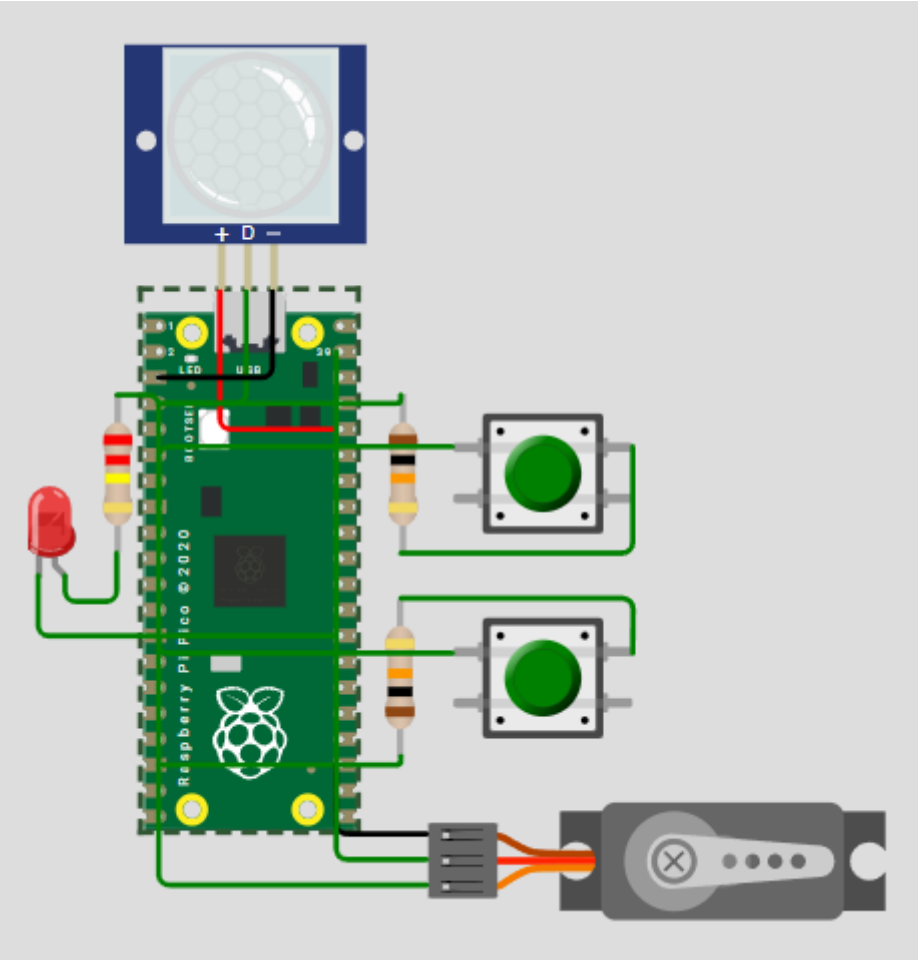



Рисунок 2.3 – Схема підключення

## 2.4 Підбір елементної бази

### 2.4.1 Підбір камери «fish-eye»

Raspberry Pi HQ Camera – це високоякісна модульна камера з 12-мегапіксельним сенсором Sony IMX477, яка підтримує змінні об'єктиви, включаючи надширококутні та "fish-eye", що дозволяє досягати кута огляду понад 180° (рис. 2.4). Завдяки високій роздільній здатності та повній сумісності з Raspberry Pi, вона є ідеальним рішенням для систем відеоспостереження, машинного зору та аналітики, де критично важливо деталізоване охоплення великої площі [9].

Основні технічні характеристики:

– сенсор: Sony IMX477, 12,3 МП;

– розмір сенсора: 1/2,3 дюйма;

– роздільна здатність: 4056 пікселів ×3040 пікселів;

– відео: до 1080p при 60 кадрах/с;

– об'єктив: Підтримка змінних об'єктивів з кріпленням C/CS;

– кут огляду: Залежить від встановленого об'єктива;

– підключення: CSI-інтерфейс для підключення до Raspberry Pi;

– сумісність: Raspberry Pi 4 Model B, 3B+, 3B, 2B, Zero W;

– додаткові функції: Можливість використання з різними об'єктивами для досягнення бажаного кута огляду та фокусної відстані;

– розміри: 38 мм × 38 мм × 19,8 мм;

– живлення: Через CSI-інтерфейс.


Рисунок 2.4 – Камера "fish-eye" Raspberry Pi HQ Camera

2.4.2 Підбір ІЧ-датчику

HC-SR505 – компактний інфрачервоний датчик руху, розроблений для точного виявлення присутності людини (рис. 2.5). Він поєднує в собі енергоефективність, швидкий відгук і високу чутливість, що робить його оптимальним вибором для побудови охоронних або автоматизованих систем керування [10].

Основні технічні характеристики:

– пасивний інфрачервоний (PIR);

– робоча напруга: від 4,5 В до 20 В DC (рекомендовано 5 В);

– струм споживання: до 50 мкА;

– вихідний сигнал: цифровий (високий рівень ≈ 3,3 В при виявленні руху);

– зона виявлення: до 3 м радіус;

– кут виявлення: до 100° та 120° по горизонталі;

– затримка вимкнення: приблизно 8 с (фіксована, без налаштування);

– час реакції: до 1 с;

– робоча температура: –20°C до +80°C;

– розміри модуля: приблизно 10 мм на 23 мм;

– призначення: для мікроконтролерних систем (Arduino, ESP32, STM32, Raspberry Pi тощо).


Рисунок 2.5 – ІЧ-датчику HC-SR505

2.4.3 Підбір IP-камери

Raspberry Pi Camera Module v2 – компактний та високоякісний модуль камери, розроблений спеціально для використання з одноплатними комп'ютерами Raspberry Pi (рис. 2.6). Оснащений 8-мегапіксельним сенсором Sony IMX219, цей модуль забезпечує чітке зображення та підтримку відеозйомки у форматах до 1080p при 30 кадрах на секунду. Завдяки простому підключенню через CSI-інтерфейс та широкій сумісності з програмним забезпеченням, камера є ідеальним інструментом для реалізації проєктів у сфері комп'ютерного зору, систем моніторингу, розпізнавання об'єктів та інших інтелектуальних рішень [11].

Основні технічні характеристики:

– роздільна здатність: 8 МП (3280 пікселів × 2464 пікселів);

– об'єктив: Фіксований, фокусна відстань ≈ 3,04 мм;

– кут огляду: Приблизно 62,2° по горизонталі;

– ІЧ-підсвітка: Відсутня (потребує окремого ІЧ-модуля для нічного бачення);

– стиснення відео: Підтримка зйомки відео у форматі H.264 (із застосуванням GPU Raspberry Pi);

– підключення: Шлейф CSI (Camera Serial Interface);

– сумісність: Повна підтримка Raspberry Pi OS, libcamera, Picamera2;

– додаткові функції: Можливість захоплення фото та відео, інтеграція з системами комп'ютерного зору (OpenCV);

– захист: Відсутній корпус (потребує окремого захисного корпусу для зовнішнього використання);

– робоча температура: від 0°C до +50°C;

– живлення: Через порт CSI камери (від Raspberry Pi);

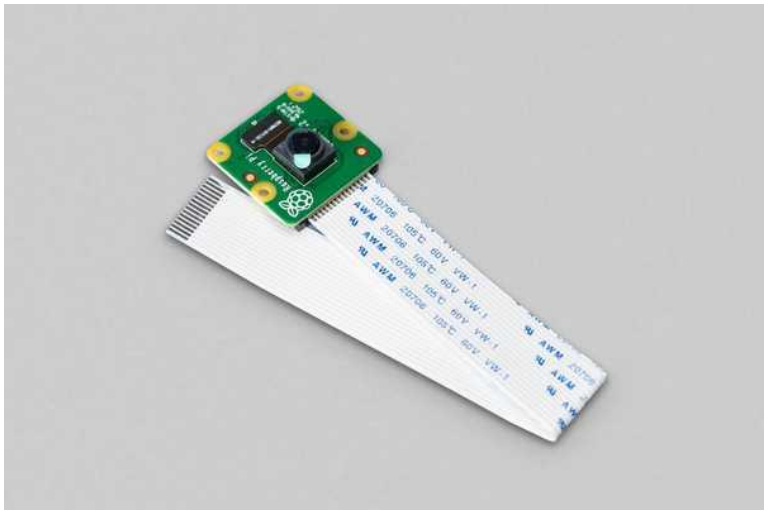


Рисунок 2.6 – IP-камера Raspberry Pi Camera Module v2

2.4.4 Підбір датчику вібрації

Модуль вібрації SW-420 – це високочутливий сенсор, що дозволяє виявляти коливання або удари на поверхні (рис. 2.7). Завдяки використанню компаратора LM393, пристрій забезпечує стабільну роботу в різних умовах, що робить його ідеальним для систем сигналізації, контролю стану обладнання або безпеки [12].

Основні технічні характеристики:

– напруга живлення: 3,3 В – 5 В DC;

– інтерфейс виходу: цифровий (DO);

– індикатор стану: вбудований світлодіод (LED) сигналізує спрацювання;

– чутливість: регулюється за допомогою вбудованого потенціометра;

– споживання струму: до 15 мА;

– затримка спрацювання: < 1 с після закінчення вібрації;

– робоча температура: від –10°C до +70°C;

– розміри модуля: 32 мм × 14 мм × 11 мм;

– смісність: Arduino, STM32, ESP32, Raspberry Pi, AVR та інші мікроконтролери.

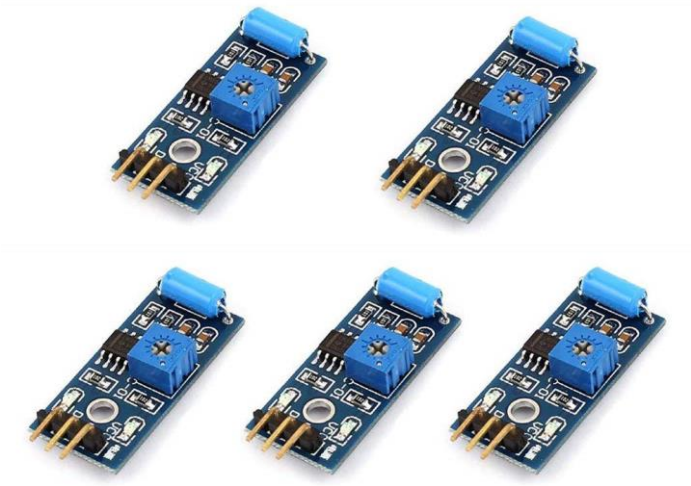


Рисунок 2.7 – Модуль вібрації SW-420

2.4.5 Підбір електронного замка

Електронний замок YLI YE-304NO – компактний та надійний електромеханічний замок, який забезпечує ефективне блокування доступу у складі сучасних систем контролю доступу (рис. 2.8). Завдяки нормально розімкненій конструкції (замок відкритий без подачі живлення) він дозволяє

організувати контрольований прохід у різні зони приміщення. Пристрій відзначається низьким енергоспоживанням, стійкістю до зносу та простотою інтеграції з контролерами, зчитувачами і кнопками виходу. YLI YE-304NO ідеально підходить для застосування в офісах, сервісних зонах та інших об’єктах з підвищеними вимогами до безпеки [13].

Основні технічні характеристики:

– живлення: DC 12 В точка зап’ята;

– споживання струму: 100 мА;

– сила утримання: до 150 кг;

– розміри замка: 50 мм × 30,2 мм × 26,8 мм;

– розміри замикаючого елементу: 31 мм;

– вага: 180 г;

– діапазон робочих температур: від -40°C до +50°C;

– сумісність: кодові клавіатури, зчитувачі, контролери, кнопки виходу та інші пристрої СКУД.

Рисунок 2.8 – Електронний замок YLI YE-304NO

2.4.6 Підбір геркона

Геркон Y213 – це надійний магнітоконтактний сенсор (рис. 2.9)., який забезпечує безконтактне зчитування положення металевих чи магнітних об'єктів. Завдяки простій конструкції та високій чутливості, пристрій широко використовується у системах безпеки, дверних або віконних датчиках та інших автоматизованих рішеннях [14].

Основні технічні характеристики:

– робоча напруга: до 100 В DC;

– максимальний струм комутації: до 0,5 А;

– опір замкнених контактів: ≤ 200 мОм;

– діелектрична міцність: до 150 В;

– робоча температура: від –40°C до +50°C;

– розміри: 28 мм × 14 мм × 8 мм (сенсорна частина); магніт аналогічного розміру.

Рисунок 2.9 – Геркон Y213

2.4.7 Підбір блоку обробки даних

Raspberry Pi 4 Model B – це потужний одноплатний комп’ютер, призначений для реалізації складних інженерних задач (рис. 2.10). Завдяки багатоядерному процесору, великій кількості інтерфейсів та підтримці

операційних систем на базі Linux, він ідеально підходить як центральний елемент у розумних системах керування та моніторингу [15].

Основні технічні характеристики:

– процесор: 4-ядерний ARM Cortex-A72 (64-бітний, 1,5 ГГц);

– оперативна пам’ять: 2 ГБ / 4 ГБ / 8 ГБ LPDDR4 (залежно від модифікації);

– графіка: Broadcom VideoCore VI, підтримка 4K-відео;

– зовнішні дисплеї: 2 × micro-HDMI (до 4K 60fps);

– мережеві інтерфейси;

– gigabit Ethernet;

– wi-Fi 802.11ac (2,4 ГГц / 5 ГГц) ;

– bluetooth 5.0;

– порти USB: 2 × USB 3.0 , 2 × USB 2.0;

– розширення та периферія;

– GPIO 40 пінів;

– CSI (інтерфейс камери) ;

– DSI (інтерфейс дисплея) ;

– зберігання даних: microSD-слот (підтримка карт до 1 ТБ);

– живлення: 5 В / 3 А через USB-C;

– розміри: 85,6 мм × 56,5 мм;

– робочі умови: температура від 0°C до +50°C.

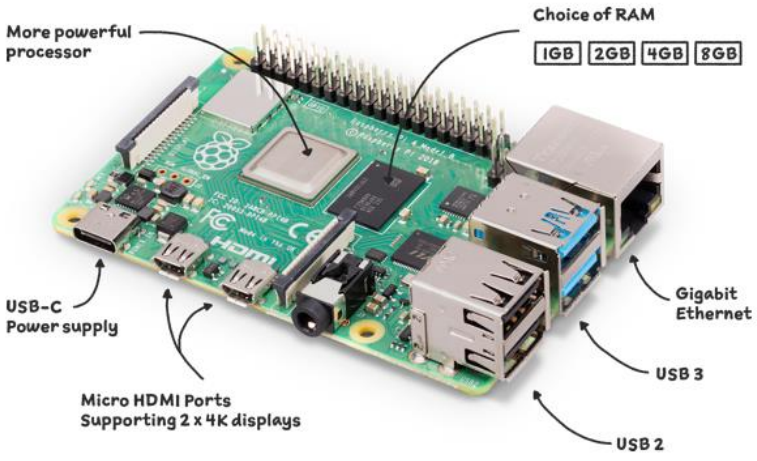



Рисунок 2.10 – Одноплатний комп’ютер Raspberry Pi 4 Model B

# 3 РОЗРОБЛЕННЯ ПРОГРАМНОЇ ЧАСТИНИ ПІДСИСТЕМИ МОНІТОРИНГУ ТА СПОВІЩЕННЯ ПРО НЕСАНКЦІОНОВАНИЙ ДОСТУП ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ КОМП'ЮТЕРНОГО ЗОРУ

## 3.1 Огляд методів розпізнавання облич

### 3.1.1. MediaPipe Face Detection

MediaPipe – це відкритий фреймворк від компанії Google, призначений для побудови систем комп'ютерного зору в реальному часі. Його модуль Face Detection базується на легкій згортковій нейронній мережі BlazeFace, яка забезпечує високу швидкість роботи навіть на мобільних пристроях. Після виявлення обличчя, система може використовувати додаткові модулі, зокрема Face Mesh, для побудови детальної тривимірної сітки з 468 контрольних точок.

MediaPipe оптимізований для продуктивності: він використовує буферизацію кадрів, повторне використання попередніх результатів та прискорене обчислення ознак, що робить його особливо ефективним для задач реального часу. Основні переваги MediaPipe – це кросплатформеність, відносно мала вага моделей та інтеграція в мобільні та веб-додатки.

### 3.1.2. HOG + SVM (Histogram of Oriented Gradients + Support Vector Machine)

Це методи які побудовані на тому що формують гістограми орієнтованих градієнтів, які описують локальні контури обличчя. Потім ці ознаки подаються на вхід SVM. Такий підхід є більш точним у порівнянні з Haar Cascades та забезпечує вищу стабільність при різноманітних умовах.

Реалізація цього методу присутня в популярній бібліотеці dlib. Його основною перевагою є баланс між якістю розпізнавання та відносною простотою реалізації без потреби в глибокому навчанні. Однак, у випадках складних сцен

(наприклад, з великою кількістю облич або різкими поворотами голови) ефективність методу помітно знижується в порівнянні з MediaPipe.

### 3.1.3. FaceNet

FaceNet – це один із перших підходів на основі глибокого навчання, який використовує згорткову нейронну мережу для побудови векторного представлення обличчя. Кожне обличчя проєктується у вектор простору ознак (зазвичай 128-вимірного), де обличчя однієї особи розміщуються поруч, а різних – на відстані.

Особливістю є використання функції втрат типу triplet loss, яка навчає модель так, щоб скорочувати відстань між векторами облич однієї особи та збільшувати – між різними.

### 3.1.4. Haar Cascades / Viola – Jones Detector

Haar Cascades – це один із найперших методів автоматичного виявлення облич, запропонований у 2001 році. Алгоритм базується на простих контрастних ознаках (наприклад, темні та світлі області обличчя), які швидко обчислюються за допомогою інтегрального зображення. Для класифікації використовується метод AdaBoost у вигляді каскаду слабких класифікаторів.

Попри свою історичну важливість, Haar Cascades мають суттєві недоліки. Вони малостійкі до змін кута зору, освітлення, перекриттів, а також часто дають хибні спрацьовування. Тим не менш, метод і досі використовується через простоту та надзвичайно високу швидкість обчислень.

### 3.1.5. MTCNN (MULTI-TASK CASCADED CONVOLUTIONAL NETWORKS)

MTCNN складається з каскаду нейронних мереж, кожна з яких відповідає за різну стадію обробки: перша – виявляє обличчя, друга – уточнює його позицію, третя – знаходить ключові точки (очі, ніс, рот). Такий підхід дозволяє досягати

як високої точності, так і знаходити положення обличчя в просторі для подальшого вирівнювання.

MTCNN часто використовується як попередній етап для моделей на кшталт FaceNet або ArcFace. Головна перевага – точне виявлення облич і ключових точок навіть при складних положеннях голови. Недолік – відносно більша затримка порівняно з MediaPipe.

## 3.2 Порівняння алгоритмів розпізнавання облич

У сучасних системах комп'ютерного зору розпізнавання облич є однією з найбільш важливих задач. Для її вирішення застосовується низка методів, кожен з яких має свої особливості, переваги та обмеження. Серед найбільш поширених алгоритмів варто виокремити MediaPipe, Haar Cascades, HOG + SVM, MTCNN та FaceNet. Кожен із цих підходів представляє різні покоління й технічні рівні розвитку методів машинного навчання.

Алгоритм MediaPipe, розроблений компанією Google, є сучасним високопродуктивним рішенням, орієнтованим на роботу в реальному часі, зокрема на мобільних пристроях. Його ключовою перевагою є оптимізована легка згорткова нейронна мережа BlazeFace, яка забезпечує швидке виявлення облич навіть за обмежених обчислювальних ресурсів. Система добре масштабована та підтримує модуль Face Mesh, що дозволяє відслідковувати до 468 ключових точок на обличчі, що важливо для задач трекінгу міміки чи доповненої реальності. За точністю MediaPipe дещо поступається найсучаснішим глибоким моделям, проте її продуктивність і кросплатформеність роблять її ідеальною для прикладних систем.

Haar Cascades – це класичний метод, який має історичне значення як один з перших ефективних алгоритмів розпізнавання облич. Він базується на простих візуальних ознаках, що описують контраст між світлими і темними ділянками зображення, та на каскадному застосуванні слабких класифікаторів (наприклад, AdaBoost). Незважаючи на свою швидкість, Haar Cascades демонструє низьку

точність, особливо в умовах зміни освітлення, кута зору або часткового перекриття обличчя. У сучасних системах він здебільшого використовується в демонстраційних або обмежених за ресурсами проєктах.

Іншим традиційним методом є HOG + SVM, який спирається на побудову гістограм орієнтованих градієнтів, що описують контури обличчя. Після цього ознаки подаються на вхід SVM-класифікатору. Такий підхід забезпечує кращу точність у порівнянні з Haar, особливо на фронтальних зображеннях, однак також демонструє зниження ефективності при поворотах голови чи при складних фонах. Перевагою цього методу є його простота та невибагливість до ресурсів, що робить його придатним для застосування в реальному часі на невисокопродуктивному обладнанні.

Метод MTCNN (Multi-task Cascaded Convolutional Networks) є більш складним з технічної точки зору, оскільки використовує каскад із трьох нейронних мереж, кожна з яких виконує власну задачу: первинне виявлення облич, уточнення його меж та локалізацію ключових точок. Така каскадна архітектура дозволяє значно підвищити точність виявлення, зокрема при змінах положення голови, часткових перекриттях та різному освітленні. MTCNN часто використовується як попередній етап у складніших системах розпізнавання, зокрема для вирівнювання облич перед подачею на більш потужні моделі.

Одним із найпотужніших методів є FaceNet, що реалізує концепцію порівняння облич не шляхом прямої класифікації, а шляхом побудови векторного представлення обличчя у багатовимірному просторі ознак. У цьому просторі обличчя однієї особи розміщуються ближче одне до одного, ніж до облич інших людей. Це досягається завдяки використанню спеціальної функції втрат triplet loss, яка навчає мережу порівнювати відстані між ембеддингами. Проте цей метод є дуже ресурсоємним і не призначений для використання на мобільних пристроях без спеціалізованих апаратних засобів.

Порівнюючи усі розглянуті алгоритми, можна зробити висновок, що їх ефективність значною мірою визначається контекстом застосування. Серед них найбільш універсальним і практичним рішенням є MediaPipe, який поєднує

високу швидкодію, низьке навантаження на систему та достатній рівень точності для складних задач, зокрема верифікації особи. Завдяки своїй легкій архітектурі та гнучкості, MediaPipe може ефективно виконувати виявлення й ідентифікацію облич у реальному часі навіть на пристроях із обмеженими обчислювальними ресурсами. Це робить його оптимальним варіантом для широкого спектру прикладних систем біометричної верифікації – від мобільних застосунків до вбудованих рішень у пристроях доступу.

У той час як такі моделі, як FaceNet, демонструють надзвичайну точність у лабораторних умовах, вони вимагають значних обчислювальних ресурсів і не завжди придатні для використання у практичних системах з обмеженим обладнанням. Аналогічно, MTCNN забезпечує високу точність локалізації облич і ключових точок, але поступається MediaPipe в реальному часі за швидкодією та енергоефективністю. Методи HOG + SVM та Haar Cascades залишаються актуальними переважно в задачах з мінімальними вимогами до точності, де головною є швидкість реакції системи.

Таким чином, у задачах верифікації особи, особливо в умовах обмежених ресурсів, MediaPipe виступає найбільш збалансованим рішенням, що забезпечує належний рівень точності, високу швидкодію та легку інтеграцію. Вибір алгоритму розпізнавання облич повинен враховувати вимоги до ефективності, точності, масштабованості та ресурсної доступності, і саме MediaPipe часто найкраще відповідає цим критеріям у реальних прикладних сценаріях

## 3.3 Вибір мови програмування та алгоритму розпізнавання облич

У межах реалізації кваліфікаційної роботи «Розроблення автоматичної підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технології комп’ютерного зору» було обрано мову програмування Python та бібліотеку MediaPipe**,** що зумовлено низкою важливих технічних та практичних переваг, які безпосередньо впливають на ефективність розробки, продуктивність системи та простоту її масштабування.

Мова Python є однією з найпопулярніших у сфері комп’ютерного зору та штучного інтелекту. Вона відзначається лаконічним синтаксисом, високою читабельністю коду та широкою підтримкою з боку спільноти розробників. Завдяки величезній кількості відкритих бібліотек, таких як OpenCV, NumPy, TensorFlow, а також гнучким засобам інтеграції, Python забезпечує швидку реалізацію алгоритмів обробки зображень та дозволяє сконцентруватися на логіці системи, а не на низькорівневій реалізації. Окрім того, Python підтримується більшістю сучасних апаратних платформ, що спрощує перенесення коду на різні пристрої – від серверів до одноплатних комп’ютерів (наприклад, Raspberry Pi).

У якості основного інструменту для виявлення облич було обрано бібліотеку MediaPipe, яка поєднує у собі точність, високу продуктивність та кросплатформеність. MediaPipe розроблена компанією Google та оптимізована для роботи в реальному часі, навіть на пристроях із обмеженими обчислювальними ресурсами. Завдяки внутрішній моделі BlazeFace, MediaPipe забезпечує стабільне й точне виявлення облич, а її модульна структура дозволяє легко інтегрувати функціональність трекінгу, побудови сітки обличчя та подальшої ідентифікації. Важливо також, що бібліотека надає інструменти для обробки відеопотоків із камери в режимі реального часу, що є критично важливим для задачі моніторингу та негайного сповіщення про несанкціонований доступ.

Таким чином, поєднання Python і MediaPipe дозволило реалізувати ефективну, масштабовану та продуктивну підсистему, яка відповідає сучасним вимогам до швидкодії, точності та зручності впровадження. Цей вибір забезпечив оптимальний баланс між технологічною гнучкістю та прикладною цінністю розробленого рішення.

## 3.4 Експериментальні результати застосування розробленого алгоритму розпізнавання облич та їх порівняння з іншими алгоритмами

У цьому розділі представлено експериментальне порівняння розробленої системи розпізнавання облич на основі бібліотеки MediaPipe із двома іншими поширеними підходами – FaceNet та HOG + SVM. Основна мета експерименту полягала в оцінці точності, швидкодії та стабільності роботи кожного з методів у типових умовах, які моделюють сценарій несанкціонованого доступу.

Для наочності до звіту включено скріншоти з прикладами роботи кожного з алгоритмів, що ілюструють якість виявлення та ідентифікації облич у реальних відеопотоках. Порівняння проводилося за однакових умов – із використанням однієї камери, однакової роздільної здатності зображення та набору тестових осіб.

Результати розпізнавання особистості (рис. 3.1 – 3.9) наведено на скріншотах нижче.

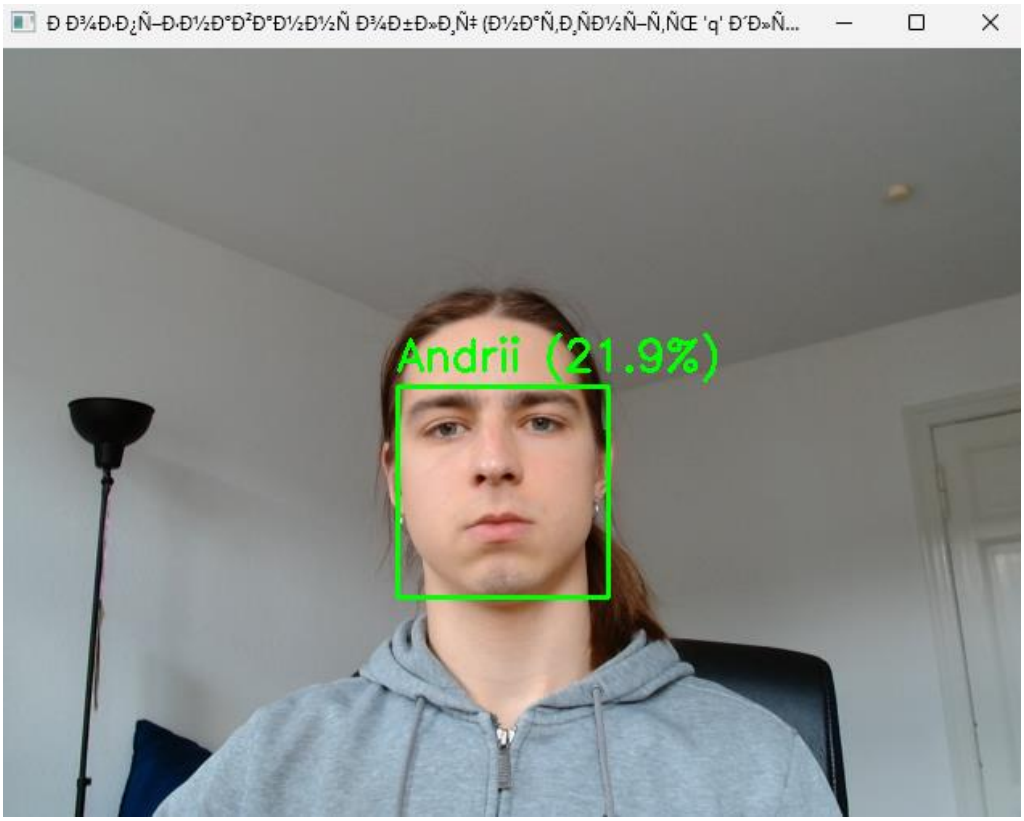



Рисунок 3.1 – Результати MediaPipe в анфас

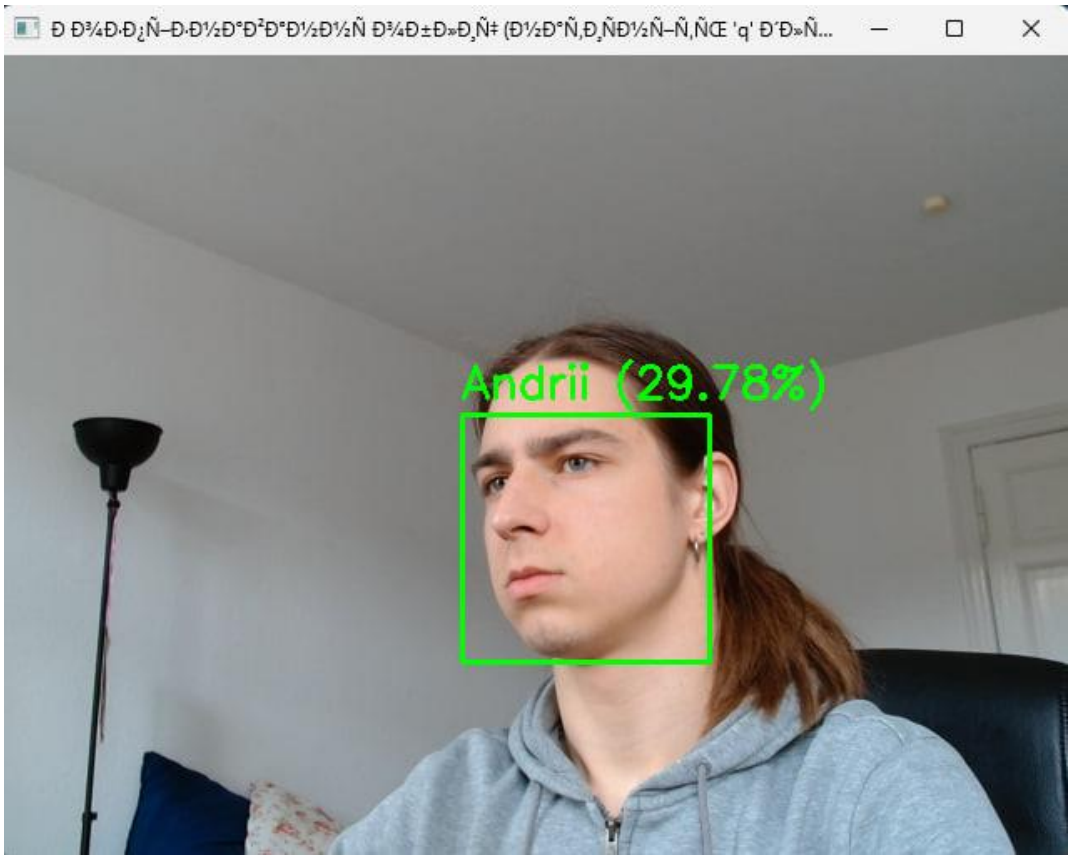



Рисунок 3.2 – Результати MediaPipe в профіль з повернутою головою праворуч

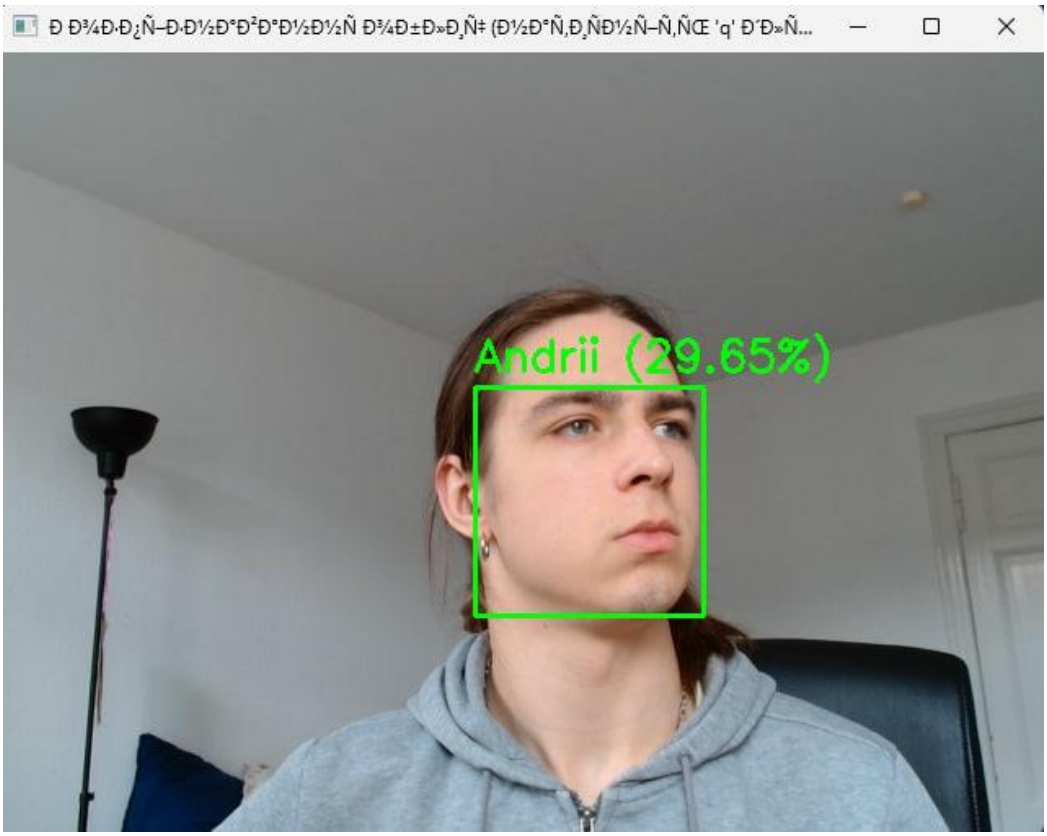



Рисунок 3.3 – Результати MediaPipe в профіль з повернутою головою ліворуч

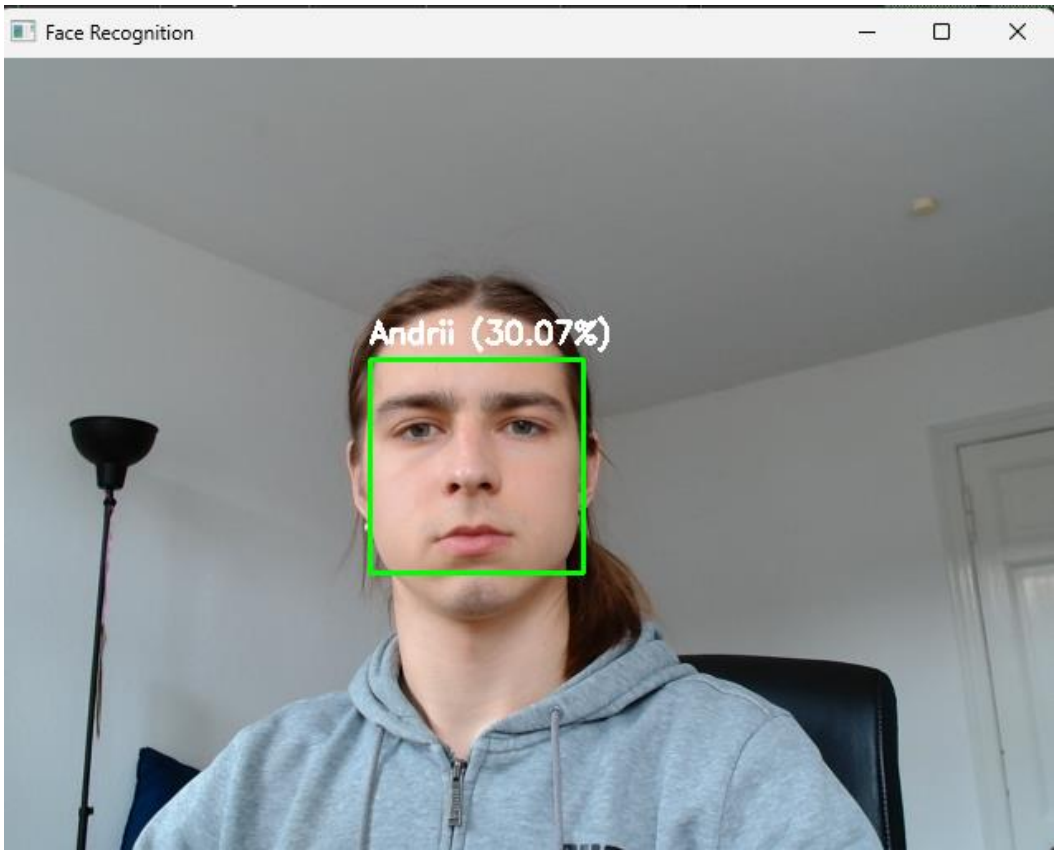



Рисунок 3.4 – Результати HOG+SVM в анфас

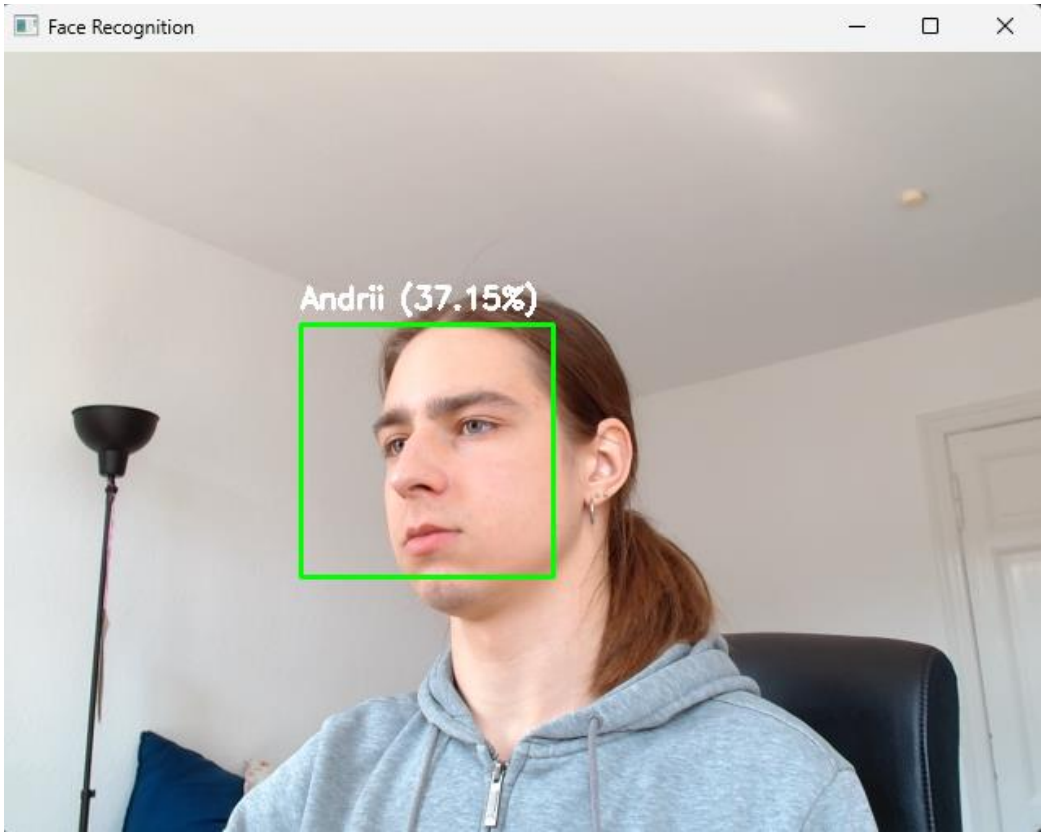



Рисунок 3.5 – Результати HOG+SVM в профіль з повернутою головою праворуч

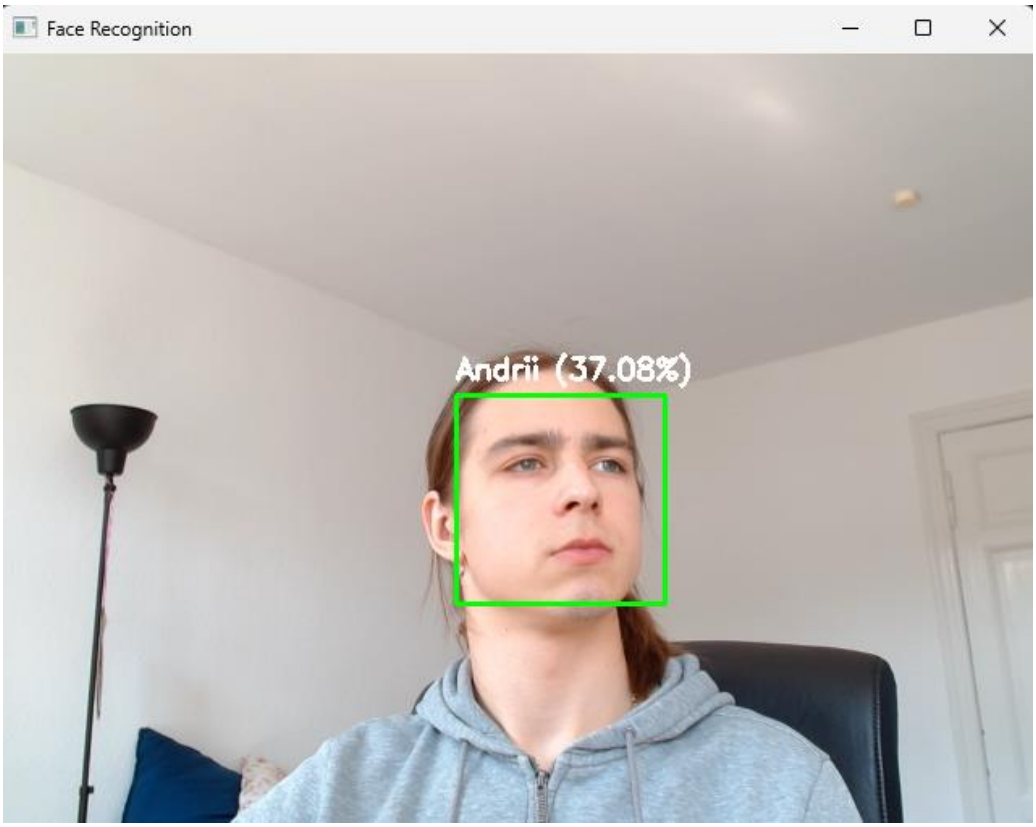



Рисунок 3.6 – Результати HOG+SVM в профіль з повернутою головою ліворуч

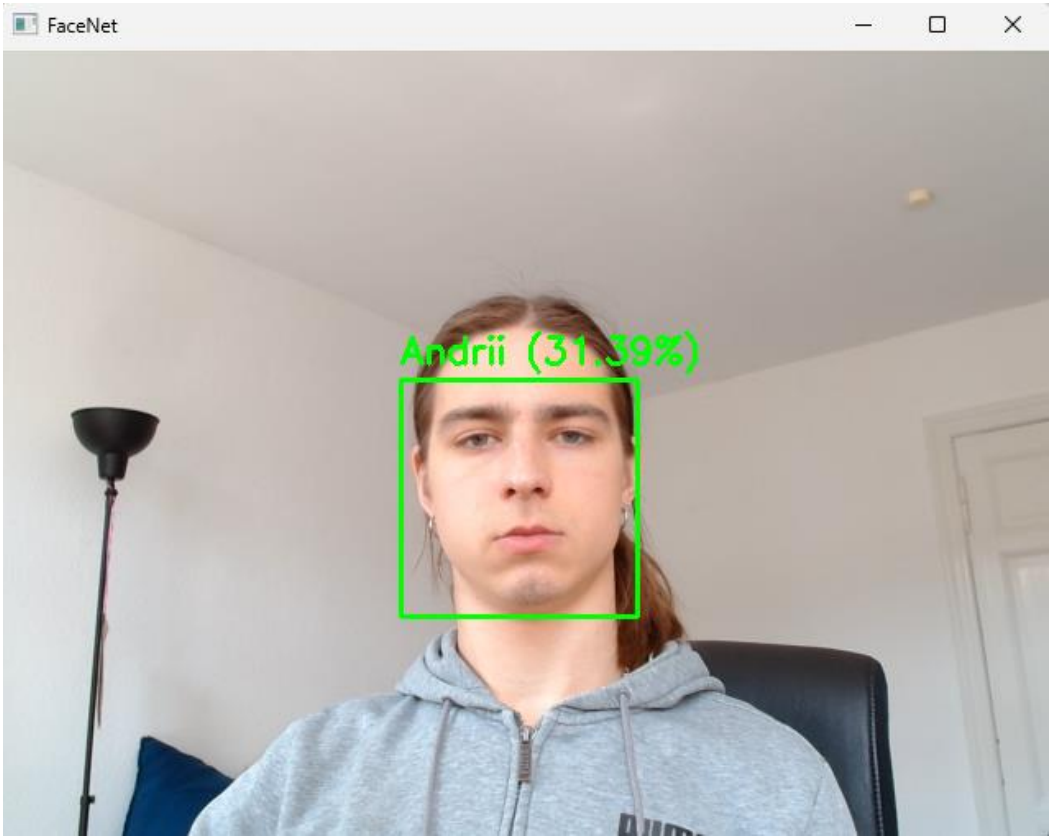



Рисунок 3.7 – Результати FaceNet в анфас

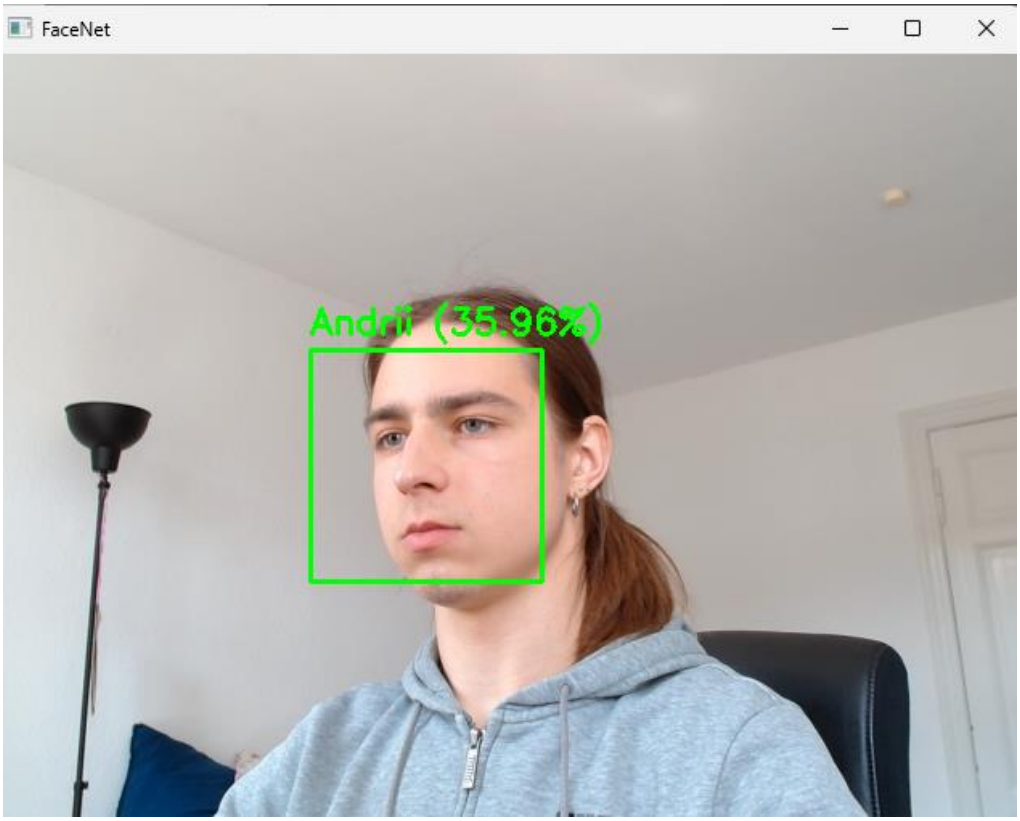



Рисунок 3.8 – Результати FaceNet в профіль з повернутою головою праворуч

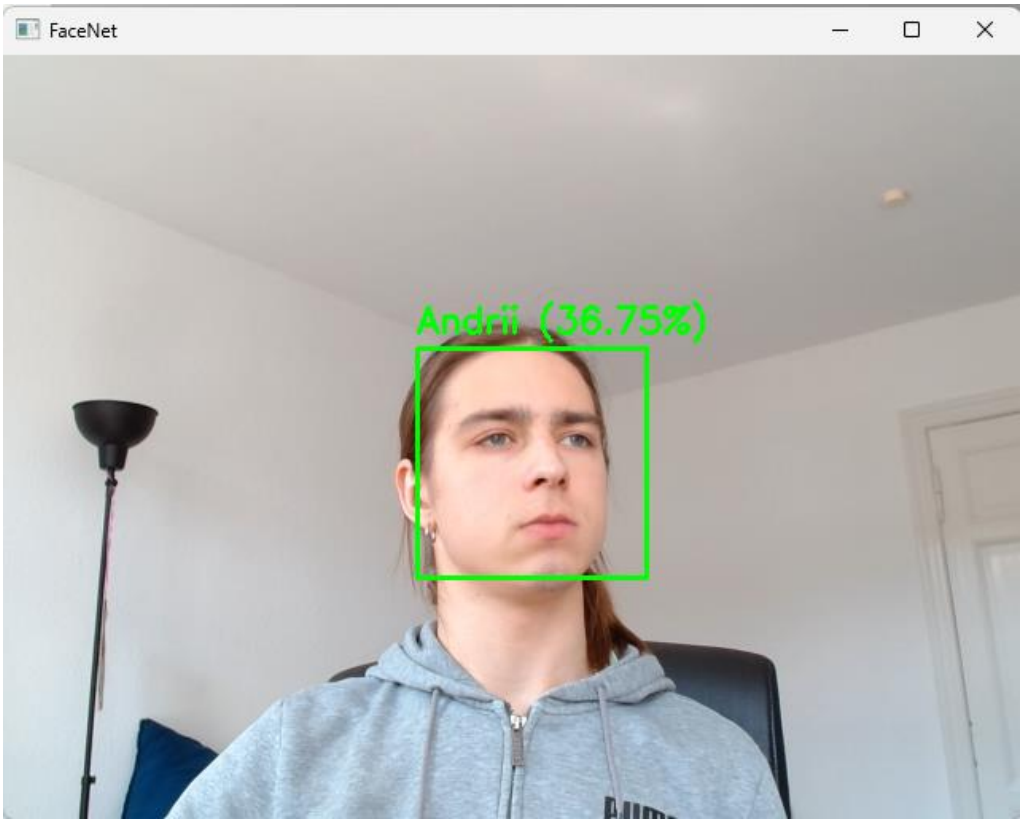



Рисунок 3.9 – Результати FaceNet в профіль з повернутою головою ліворуч

# 4 ОХОРОНА ПРАЦІ

## 4.1 Аналіз умов праці в лабораторії

Приміщення, де ведеться проектування, являє собою лабораторію. Площа даного приміщення становить – 35 м$^2$, об’єм – 105 м$^3$, має чотири робочих місця. Розміри приміщення 5 м × 7 м × 3 м.

Електроживлення здійснюється від трифазної мережі з глухозаземленою нейтраллю та напругою 220 В, з частотою 50 Гц.

Для забезпечення нормальних умов праці ДСанПіН 3.3.2–007–98 встановлює на одне робоче місце площу виробничого приміщення не менше 6 м$^2$, висота приміщення повинна бути не менше 3,2 м, об'єм повітряного простору 20 м$^3$. В даному випадку реальна площа на одного працюючого становить 10 м, об’єм – 25 м$^3$, що відповідає санітарним нормам.

Розглядаючи людину в нерозривному зв'язку і в безперервній взаємодії з навколишнім середовищем, як об'єкт вивчення можна виділити систему «Людина-машина-середовище» («Л-М-С»), а предметом вивчення – небезпеки і їх вплив на людину в процесі функціонування і розвитку системи «Л-М-С». Головним в системі «Л-М-С» є безпека людини.

Згідно ДСТУ 12.0.003–74 можна виділити небезпечні та шкідливі виробничі фактори в приміщенні.

Фізичні:

– підвищена рухливість повітря;

– недостатня освітленість робочої зони;

– підвищений рівень електромагнітного випромінювання;

– підвищення значення напруги в електричному ланцюзі, замикання якого може відбутися через тіло людини.

Психофізіологічні:

– фізичні (статичні) перевантаження;

– розумове перенапруження;

– перенапруження зорових аналізаторів.

## 4.2 Промислова безпека в лабораторії

Електричне живлення устаткування здійснюється від трифазної мережі з глухозаземленою нейтраллю напругою 220 В, частотою 50 Гц. Захист персоналу від ураження електричним струмом, необхідно здійснювати за допомогою занулення НПАОП 40.1–1.32–01. Для цього треба з'єднати металеві неструмоведучі частини обладнання з нульовим дротом мережі, за допомогою алюмінієвого дроту, перетин якого дорівнювати перерізу фазного дрота мережі.

При замиканні фази на занулення корпус електроустановки автоматично відключається, якщо значення струму однофазного короткого замикання Ік, А, задовольняє умові [16]

$$I_k \geq kI_{\text{ном}}, \tag{4.1}$$

де $I_{\text{ном}}$ – номінальний струм плавкої вставки запобіжника або струм спрацьовування автоматичного вимикача, А;

$k$ – коефіцієнт кратності струму.

Він приймається в залежності від типу захисту електроустановки. Якщо захист здійснюється автоматичним вимикачем, що має тільки електромагнітне відсічення, тобто, який спрацьовує без витримки часу, то $k$ = 1,25. Якщо установка захищена плавкими запобіжниками, час перегорання яких залежить від величини струму, то $k \geq 3$ (у вибухонебезпечних приміщеннях $\geq 4$) [16].

$$I_{\text{кз}} = \frac{U_{\text{ф}}}{\frac{Z_T}{3} + Z_{\text{П}}}, \tag{4.2}$$

де $\frac{Z_T}{3}$ – повний опір обмоток трансформатора, визначається з [16], виходячи з потужності трансформатора, $\frac{Z_T}{3}$ = 0,075 Ом;

$Z_П$ – опір петлі "фаза-нуль", $Z_П$ = 0,8 Ом.

Розрахуємо $I_{кз}$ за формулою (4.2)

$$I_{кз} = \frac{220}{0{,}075 + 0{,}8} = 251 \text{ А}.$$

З умови формули (4.1)

$$I_н \leq \frac{I_{кз}}{k}, \quad (4.3)$$

де $k$ =1,25 – коефіцієнт кратності струму.

$$I_н \leq \frac{251}{1{,}25} = 200 \text{ А}.$$

Вибираємо автоматичний вимикач TemBreak від 50 А до 250 А у якого, $I_н$= 100 А, який має тільки напівпровідниковий розчеплювач (відсічення).

Відповідно до НПАОП 0.00–4.12–05, всі працівники проходять інструктажі з охорони праці: вступний, первинний на робочому місці, повторний і, при необхідності, позаплановий та цільовий.

# ВИСНОВКИ

У результаті проведеної роботи було досягнуто поставленої мети – покращення якості контролю доступу до приміщення за рахунок впровадження автоматичної підсистеми моніторингу та сповіщення про несанкціонований доступ із використанням технологій комп’ютерного зору. Розроблена підсистема становить сучасне інженерне рішення, орієнтоване на актуальні виклики в галузі фізичної безпеки, та інтегрує засоби комп’ютерного зору і штучного інтелекту для реалізації ефективного доступ-контролю. Зокрема, використання алгоритмів автоматичного виявлення присутності людини, розпізнавання облич та генерації сповіщень у режимі реального часу дозволило значно підвищити точність, оперативність і надійність роботи підсистеми.

Перший розділ присвячено здійсненню комплексної аналітичної роботи, спрямованої на вивчення сучасного стану систем контролю доступу. Особливу увагу було приділено виявленню їхніх основних переваг, типових недоліків, а також окресленню сфер ефективного застосування зазначених технологій у різних умовах експлуатації.

На основі отриманих результатів аналізу було сформульовано вимоги до майбутньої підсистеми контролю доступу з урахуванням особливостей її функціонування в реальному середовищі. Ці вимоги включали як технічні, так і функціональні аспекти, що забезпечують практичну придатність запропонованого рішення.

Другий розділ було присвячено проєктуванню підсистеми у ході якого було розроблено алгоритмічну модель її функціонування, а також створено структурну схему, яка відображає взаємозв’язки між основними модулями та логіку їхньої взаємодії. Це дозволило забезпечити цілісне розуміння архітектури системи.

З метою реалізації запропонованих рішень було підібрано відповідну апаратну базу, до складу якої увійшли високоточна камера, обчислювальний

модуль, мережеві компоненти та засоби сповіщення. Така конфігурація забезпечує стабільну та безперебійну роботу підсистеми в умовах реального часу.

Проєктування архітектури підсистеми було здійснено з урахуванням принципів відкритості, що дозволяє її подальше масштабування та інтеграцію з іншими інформаційно-безпековими сервісами. Це значно розширює потенціал системи в контексті майбутнього розвитку.

Окрему увагу було приділено сценаріям критичних ситуацій, у межах яких передбачено можливість оперативного втручання оператора. Такий підхід сприяє підвищенню загальної надійності підсистеми та зменшенню ризику прийняття хибних рішень у нестандартних умовах.

У третьому розділі виконано програмну реалізацію, результати якої підтвердили, що підсистема здатна з високою точністю ідентифікувати особу та швидко реагувати на загрозу, значно зменшуючи ризики хибних спрацювань і затримок при реагуванні. Технологія комп’ютерного зору не лише дозволяє автоматизувати процес ідентифікації, а й забезпечує підвищену адаптивність до змін навколишнього середовища, завдяки можливості подальшого навчання моделей.

Особливістю запропонованого рішення є його гнучкість: підсистема може бути адаптована до різного типу об’єктів – від малих офісів до великих державних установ. Крім того, вона має перспективу подальшого розвитку: впровадження поведінкового аналізу, хмарної синхронізації даних, захищеного резервного зберігання та інтеграції з системами відеоаналітики, що розширює функціональність і підвищує загальний рівень безпеки.

Таким чином, розроблена підсистема відповідає сучасним вимогам до безпеки, забезпечує автоматизований моніторинг доступу, скорочує витрати на охоронний персонал та мінімізує людський фактор. Отримані результати можуть бути використані як основа для впровадження у реальні об’єкти з підвищеними вимогами до безпеки, а також слугувати базою для подальших досліджень і вдосконалення в галузі інтелектуальних систем контролю доступу.

Загалом, виконана робота засвідчує доцільність використання технологій комп’ютерного зору в системах безпеки нового покоління, що відповідають актуальним викликам часу та дозволяють створити більш безпечне та контрольоване середовище.

Також, отримані результати роботи можно віднести до Цілі сталого розвитку 9 «Промисловість, інновації та інфраструктура», а саме п. 9.1 «Розвивати якісну надійну, сталу та доступну інфраструктуру, яка базується на використанні інноваційних технологій, у т.ч. екологічно чистих видів транспорту».

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ДСТУ 3008:2015 Інформація та документація «Звіти у сфері науки і техніки». Структура та правила офомрлювання. / В. Земцева; Ю. Поліщук, канд. фіз.-мат. наук; Р. Санченко, канд. техн. наук; Л. Шрамко; А. Ямчук (науковий керівник) ДП «УкрНДНЦ» від 22 червня 2015р. No 61 з 2017- 07-01.

2. Методичні вказівки з підготовки кваліфікаційної роботи для здобувачів першого (бакалаврського) рівня вищої освіти денної і заочної форми навчання спеціальності 151 «Автоматизація та комп'ютерно- інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології» / Упоряд.: І. Ш. Невлюдов, О. І. Филипенко, О. В. Токарєва, С. П. Новоселов, О. В. Сичова. – Харків: ХНУРЕ, 2023. – 64 с.

3. Навчальний посібник з підготовки кваліфікаційної роботи бакалавра для здобувачів вищої освіти денної і заочної форм навчання спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології»: Навчальний посібник / І. Ш. Невлюдов, В.А. Андрусевич, О. В. Токарєва, С. П. Новоселов, О. В. Сичова. – Харків : Видавництво Іванченка І. С., 2022. – 151 с.

4. What Are Mechanical Door Locks? [Електронний ресурс] – Режим доступу до ресурсу: https://www.pdqlocks.com/blog/what-are-mechanical-door-locks – 19.04.2025.

5. Система контролю та управління доступом на основі RFID-технологій – Віра Тітова та ін. [Електронний ресурс] – Режим доступу до ресурсу: https://vottp.khmnu.edu.ua/index.php/vottp/article/view/175/174 – 20.04.2025.

6. Автономний контролер доступу Seven CR-772m [Електронний ресурс] – Режим доступу до ресурсу: https://worldvision.com.ua/seven-cr-772m/ – 14.04.2025.

7. Smart Facial Authentication Terminal FaceStation 2 [Електронний ресурс] – Режим доступу до ресурсу: https://www.supremainc.com/en/hardware/facial-authentication-terminal-facestation2.asp – 14.04.2025.

8. Fusion Multimodal Terminal Suprema FaceStation F2 [Електронний ресурс] – Режим доступу до ресурсу: https://www.supremainc.com/en/hardware/fusion-multimodal-terminal-facestation-f2.asp?iHARDWARE_NO=226 – 15.04.2025.

9. Камера Raspberry Pi High Quality Camera [Електронний ресурс] – Режим доступу до ресурсу: https://evo.net.ua/kamera-raspberry-pi-high-quality-camera/?srsltid=AfmBOoq-Ucv9JS3oUEOGB1xQMGQOsMMpi5nTYW1Yk8KVM2Qt8ilfPA6q – 15.05.25.

10. ІЧ-датчик HC-SR505 Mini PIR [Електронний ресурс] – Режим доступу до ресурсу: https://www.makershop.de/sensoren/infrarot-2/mini-pir-bewegungsmelder-infrarot-ir-sr505-sensor-modul-arduino/ – 15.05.25.

11. IP-камера Raspberry Pi Camera Module 2 [Електронний ресурс] – Режим доступу до ресурсу: https://www.raspberrypi.com/products/camera-module-v2/ – 15.05.25.

12. Датчик вібрації Hiletgo SW-420 Vibration Sensor Module [Електронний ресурс] – Режим доступу до ресурсу: https://www.amazon.com/Hiletgo-SW-420-Vibration-Sensor-Arduino/dp/B00HJ6ACY2 – 16.05.25.

13. Електрозамок Yli Electronics YE-304NO [Електронний ресурс] – Режим доступу до ресурсу: https://www.bezpeka-shop.com/ua/product/elektrozamok-ye-304no-power-open-dlya-sistemy-kontrolya-dostupa/?srsltid=AfmBOoojxPIc79KKP3HnuZsNP1155b3v4YXAFEBqyTFWvY3kfwKld8j9 – 16.05.25.

14. Геркон Y213 [Електронний ресурс] – Режим доступу до ресурсу: https://www.mini-tech.com.ua/gerkon – 16.05.25.

15. Блок обробки даних Raspberry Pi 4 Model B [Електронний ресурс] – Режим доступу до ресурсу: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/ – 17.05.25.

16. Комплекс навчально-методичного забезпечення навчальної дисципліни «Безпека праці в індустрії ІТ-технологій» підготовки освітнього рівня бакалавр усіх спеціальностей та усіх напрямів університету [http://catalogue.nure.ua/knmz] / ХНУРЕ; розроб.: Т. Є. Стиценко, Г. В. Пронюк, Н. М. Сердюк. – Харків, 2017. – 122 с.