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

другий (магістерський)
(рівень вищої освіти)

Розроблення автоматизованої системи контролю проходження пунктів пропуску на виробництві
(тема)

Виконав:
здобувач ІІ року навчання,
групи КІТПВм-23-1
Горбань А. Ю.
(прізвище, ініціали)

Спеціальність 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(код і повна назва спеціальності)

Тип програми освітньо-професійна
Освітня програма Комп'ютерно-інтегровані технологічні процеси і виробництва
(повна назва осітньої програми)

Керівник проф. Безкоровайний В. В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри КІТАР _____ Невлюдов І. Ш.
(підпис) (прізвище, ініціали)

2025

Я, як студент ХНУРЕ, розумію та підтримую політику закладу з академічної доброчесності. Я не надавав та не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

03.01.2025  Горбань А.Ю.

Харківський національний університет радіоелектроніки

Факультет АКТ
Кафедра КІТАР
Рівень вищої освіти другий (магістерський)
Спеціальність 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Тип програми Освітньо-професійна
Освітня програма Комп'ютерно-інтегровані технологічні процеси і виробництва
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«___»_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Горбаню Андрію Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Розроблення автоматизованої системи контролю проходження пунктів пропуску на виробництві
Затверджена наказом університету від 22.11.2024 №1231Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 11.01.2025р .
3. Вихідні дані до роботи: Розпізнавання обличчя; Ідентифікація користувачів; Удосконалення методу розпізнавання обличчя людини

4. Перелік питань, що потрібно опрацювати в роботі. Вступ. Аналіз структури та призначення автоматизованої системи контролю проходження пунктів пропуску на виробництві. Огляд систем-аналогів. Аналіз методів ідентифікації людини при проходженні пунктів контролю доступу. Аналіз апаратного забезпечення пункту контролю. Розробка структури макету системи та опис призначення структурних елементів. Аналіз та вибір апаратних модулів для системи. Розробка схеми підключення та складання макету системи. Розробка загального алгоритму роботи системи. Аналіз та вибір нейронної мережі для розпізнавання обличчя людини. Удосконалення методу розпізнавання обличчя людини на базі нейронної мережі. Обґрунтування вибору мови та середовища розробки. Розробка функцій розпізнавання обличчя людини. Результати експериментальних досліджень та аналіз отриманих результатів. Висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій Графічний матеріал у вигляді презентації (10–15 аркушів формату А4).

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання та аналіз завдання	09.09.2024	*Виконано*
2	Огляд проблеми автоматизації контролю		
	доступу на виробництві	23.09.2024	*Виконано*
3	Аналіз методів ідентифікації працівників	07.10.2024	*Виконано*
4	Розробка та складання макету системи	14.10.2024	*Виконано*
5	Розробка алгоритму роботи системи та		
	удосконалення методу ідентифікації	28.10.2024	*Виконано*
6	Розробка програмного забезпечення	04.11.2024	*Виконано*
7	Експериментальне дослідження системи	11.11.2024	*Виконано*
8	Підготовка публікацій	18.11.2024	*Виконано*
9	Подання кваліфікаційної роботи		
	керівнику	28.12.2024	*Виконано*
10	Підготовка презентації	31.12.2024	*Виконано*
11	Подання роботи для перевірки на плагіат	31.12.2024	*Виконано*
12	Подання роботи на рецензування	02.01.2025	*Виконано*
13	Попередній захист	08.01.2025	*Виконано*
14	Подання роботи до екзаменаційної комісії	11.01.2025	*Виконано*

Дата видачі завдання 2 вересня 2024 р.

Здобувач _____
(підпис)

Керівник роботи _____ проф. кафедри КІТАР Безкоровайний В. В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 103 с., 13 табл., 12 рис., 3 дод., 36 джерел.

АВТОМАТИЗОВАНА СИСТЕМА, ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ, КОНТРОЛЬ ДОСТУПУ, НЕЙРОННА МЕРЕЖА, РОЗПІЗНАВАННЯ ОБЛИЧЧЯ, MOBILENETV2, RFID.

Об’єкт дослідження – процес авторизації працівника на пункті пропуску виробництва.

Предмет дослідження – методи, алгоритми та програмне забезпечення ідентифікації працівника для проходження пунктів пропуску на виробництві.

Мета дослідження – підвищення ефективності системи доступу до виробничого приміщення за рахунок удосконалення технології контролю.

Методи дослідження – методи ідентифікації, штучного інтелекту, проєктування інформаціних систем.

У кваліфікаційній роботі запропоновано рішення з підвищення ефективності системи доступу до виробничого приміщення за рахунок розроблення системи контролю проходження пунктів пропуску на основі штучної нейронної мережі. За результатами аналізу сучасних аналогів запропоновано структуру макету макету, обрано необхідні апаратні модулі, розроблено схему підключення, загальний алгоритм роботи та відповідне програмне забезпечення. Результати есперименталь них досліджень підтвердили удосконалення методу розпізнавання обличчя з використанням нейронної мережі.

Результати кваліфікаційної роботи апробовані на двох наукових конференціях.

Отримані результати роботи можна віднести до пункту 9.4 Цілі сталого розвитку 9 «Промисловість, інновації та інфраструктура».

ABSTRACT

Explanatory note: 103 pages, 13 tables, 12 figures, 3 app, 36 sources.

AUTOMATED SYSTEM, ACCESS CONTROL, FACIAL RECOGNITION, NEURAL NETWORK, MOBILENETV2, RFID, USER IDENTIFICATION.

The object of the study is the process of employee authorization at the production checkpoint.

The subject of the study is methods, algorithms and software for employee identification for passing checkpoints at the production site.

The purpose of the study is to increase the efficiency of the access system to the production premises by improving control technology.

Research methods – identification methods, artificial intelligence, information systems design.

The qualification work proposes a solution to increase the efficiency of the access system to the production premises by developing a system for controlling the passage of checkpoints based on an artificial neural network. Based on the results of the analysis of modern analogues, the structure of the layout of the layout is proposed, the necessary hardware modules are selected, a connection diagram, a general algorithm of operation and the corresponding software are developed. The results of experimental research have confirmed the improvement of the facial recognition method using a neural network.

The results of the qualification work have been tested at two scientific conferences.

The obtained results of the work can be attributed to point 9.4 of the Sustainable Development Goals 9 “Industry, Innovation and Infrastructure”.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АСКПП – автоматизована система контролю проходження пунктів пропуску.

ММ – мікропроцесорний модуль.

NFC – Near Field Communication.

NC – Normally Closed.

NO – Normally Open.

RFID – Radio Frequency Identification.

USB – Universal Serial Bus.

ВСТУП

У сучасних умовах розвитку промислових підприємств виникає потреба у забезпеченні високого рівня контролю доступу до робочих зон для підвищення безпеки, запобігання несанкціонованому доступу та оптимізації внутрішніх процесів. Використання автоматизованих систем контролю доступу з елементами розпізнавання обличчя та RFID-технологій забезпечує ефективне вирішення цих завдань, що є особливо важливим для підприємств із високими вимогами до захисту інформації та матеріальних ресурсів.

Розвиток технологій машинного навчання та нейронних мереж створює нові можливості для підвищення точності та швидкості ідентифікації осіб, що сприяє зменшенню ймовірності помилок і покращенню користувацького досвіду. Водночас інтеграція різних модулів у єдину систему дозволяє оптимізувати витрати на впровадження та експлуатацію системи контролю доступу, що відповідає сучасним вимогам до ефективності виробництва.

Мета дослідження – підвищення ефективності контролю доступу до виробничого приміщення, за рахунок вдосконалення системи контролю.

Об’єкт дослідження – процес авторизації працівника на пункті пропуску виробництва.

Предмет дослідження – методи, алгоритми та програмне забезпечення ідентифікації працівника для проходження пунктів пропуску на виробництві.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз структури та призначення автоматизованої системи контролю проходження пунктів пропуску;

– провести аналіз аналогічних автоматизованих систем контролю;

– провести аналіз методів ідентифікації людини при проходженні пунктів контролю доступу;

– провести аналіз апаратного забезпечення пункту контролю проходження пунктів пропуску на виробництві;

– розробити структуру макета та описати призначення структурних блоків;

– провести аналіз та вибір апаратних модулів для розробки макета системи контролю проходження пунктів пропуску;

– розробити схему підключення та зібрати макет системи контролю проходження пунктів пропуску;

– розробити загальний алгоритм роботи системи контролю проходження пунктів пропуску;

– провести аналіз та вибір нейронної мережі для розпізнавання обличчя людини за особливостями їх рис;

– удосконалити метод розпізнавання обличчя людини на базі нейронної мережі MobileNetV2;

– провести обґрунтування вибору мови та середовища розробки;

– розробити функції розпізнавання обличчя людини;

– провести експериментальні дослідження та проаналізувати результати.

Науковою новизною є підвищення ефективності системи доступу до виробничого приміщення.

Кваліфікаційна робота виконана згідно ДСТУ 3008: 2015 [1], керуючись навчальним посібником з дипломного проектування [2] та методичними вказівками [3], а результати кваліфікаційної роботи пройшли апробацію на двох наукових конференціях [4-5].

1 АНАЛІЗ СУЧАСНИХ АВТОМАТИЗОВАНИХ СИСТЕМ КОНТРОЛЮ ПРОХОДЖЕННЯ ПУНКТІВ ПРОПУСКУ НА ВИРОБНИЦТВІ

1.1 Аналіз структури та призначення автоматизованої системи контролю проходження пунктів пропуску

Автоматизовані системи контролю проходження пунктів пропуску (АСКПП) є важливим елементом забезпечення безпеки та ефективності роботи підприємств. Їхнє основне призначення полягає в автоматизації процесів перевірки та реєстрації доступу співробітників і відвідувачів на об'єкти виробничого або іншого призначення, що дозволяє значно підвищити рівень контролю за рухом персоналу, забезпечуючи дотримання внутрішніх правил і зменшуючи ймовірність несанкціонованого доступу [6].

Структура типової АСКПП включає кілька основних компонентів: ідентифікаційний модуль, модуль обробки даних, фізичні засоби обмеження доступу (турнікети, двері з електрозамками тощо) та інтерфейс адміністратора. Ідентифікаційний модуль реалізує первинну функцію перевірки особи за допомогою електронних карток, біометричних даних або QR-кодів, а потім дані передаються до обробного модуля, де здійснюється аналіз інформації та приймається рішення щодо надання доступу. Одним із ключових завдань АСКПП є інтеграція з іншими інформаційними системами підприємства, як, наприклад, система може бути пов'язана з базою даних співробітників, системами відеоспостереження та обліку робочого часу, що дозволяє створити комплексне рішення для управління персоналом, яке забезпечує прозорість та аналітичну підтримку.

Для забезпечення надійності функціонування АСКПП використовуються резервні копії даних, а також засоби захисту від збоїв та несанкціонованого втручання, крім того, сучасні системи забезпечують масштабованість, що

дозволяє легко адаптувати їх до потреб зростаючого підприємства або змін у його структурі. На виробництві, призначення АСКПП включає не лише обмеження доступу, але й контроль за дотриманням розкладу роботи, облік робочого часу та запобігання надзвичайним ситуаціям, так як, у разі виникнення небезпеки система може виконувати функції евакуаційного контролю, забезпечуючи автоматичне відкриття турнікетів або дверей. Особливу увагу в АСКПП приділяють питанням конфіденційності та захисту персональних даних, а в зв'язку з цим застосовуються сучасні методи шифрування інформації, а також організуються регулярні перевірки безпеки системи. Це є особливо важливим у випадках використання біометричних даних, які потребують особливого захисту [7-8].

Ефективність роботи АСКПП значною мірою залежить від правильної організації їхньої структури. Розташування зчитувачів і турнікетів має бути зручним для користувачів і не створювати заторів у місцях із великим потоком людей, також важливо забезпечити чітку візуалізацію статусу доступу, щоб уникнути непорозумінь. Розробка АСКПП враховує різні сценарії роботи, включаючи змінний графік співробітників, доступ до різних зон підприємства та можливість швидкого оновлення прав доступу. Це забезпечує гнучкість системи та її здатність адаптуватися до специфічних потреб підприємства.

Окрім технічних аспектів, структура АСКПП, зазвичай, включає нормативно-правову базу, яка регулює використання систем контролю доступу. Це охоплює внутрішні положення підприємства, які визначають правила доступу, а також державні стандарти, які регламентують безпеку та захист даних. Можна сказати, що АСКПП є комплексними системами, які включають апаратні й програмні компоненти, а також організаційні та нормативні заходи, а успішне впровадження та експлуатація сприяють підвищенню безпеки, ефективності та дисципліни на виробництві [9].

1.2 Аналіз аналогічних автоматизованих систем контролю

В наш час, існує широкий спектр автоматизованих систем контролю доступу, які використовуються на виробничих підприємствах. Розглянемо основні приклади таких систем, їх характеристики, переваги, недоліки та можливості.

Система "Parsec" є однією з найбільш популярних на ринку. Вона забезпечує контроль доступу, облік робочого часу та інтеграцію з відеоспостереженням. Основні компоненти системи включають контролери, програмне забезпечення та різні засоби ідентифікації (карти, брелоки, біометричні дані). Переваги системи "Parsec" включають високу гнучкість у налаштуванні прав доступу, що дозволяє враховувати складні структури підприємства. Вона забезпечує надійну інтеграцію з іншими системами, такими як відеоспостереження та облік робочого часу. Крім того, інтерфейс адміністратора є інтуїтивно зрозумілим і зручним для користувачів, що спрощує управління доступом та моніторинг подій у реальному часі. Серед недоліків системи "Parsec" варто виділити високу вартість обладнання та програмного забезпечення, що може бути проблемою для малих підприємств. Також залежність від постачальника у випадку технічного обслуговування чи оновлення програмного забезпечення може створювати додаткові складнощі для компаній, які прагнуть зменшити зовнішню залежність [10].

Наступною системою є "ZKTeco", орієнтована на середній і малий бізнес. Вона включає в себе функції біометричної ідентифікації, контролю доступу та обліку робочого часу. Особливістю цієї системи є її доступність за ціною та компактність обладнання. Система "ZKTeco" вирізняється своєю доступністю та різноманітністю моделей обладнання, що дозволяє підприємствам вибирати рішення залежно від своїх потреб та бюджету. Вона підтримує широкий спектр методів ідентифікації, включаючи картки, PIN-коди, біометричні дані (відбитки пальців, розпізнавання обличчя), що забезпечує високий рівень адаптивності.

Система також відома своєю простою установкою та експлуатацією, що робить її привабливим варіантом для компаній із обмеженими ресурсами на навчання персоналу. Недоліками "ZKTeco" є обмежена інтеграція з іншими системами підприємства порівняно з більш дорогими аналогами. Крім того, іноді можуть виникати проблеми з точністю ідентифікації в умовах поганого освітлення або сильного забруднення. Ще одним мінусом є відносно базовий рівень технічної підтримки, який може стати перешкодою для вирішення складних технічних питань [11].

Система "Honeywell Access Control" належить до преміального сегмента і орієнтована на великі підприємства. Вона забезпечує високий рівень безпеки та має функції масштабованості для складних об'єктів. Honeywell Access Control відома своєю високою надійністю та інтеграцією з іншими корпоративними системами, такими як системи управління будівлями та відеоспостереження. Вона забезпечує широкий набір функцій для управління доступом, включаючи контроль у режимі реального часу, гнучкі налаштування рівнів доступу та можливості масштабування для великих підприємств. Однією з ключових переваг є потужна аналітика та звітність, що дозволяє керівникам відстежувати та аналізувати поведінку користувачів. Крім того, система підтримує сучасні методи ідентифікації, включаючи біометричні дані та мобільні рішення. Основним недоліком Honeywell Access Control є висока вартість впровадження та обслуговування, що може бути значним бар'єром для малих і середніх підприємств. Складність налаштування та інтеграції також потребує залучення висококваліфікованих спеціалістів, що збільшує витрати часу та ресурсів. Деякі користувачі відзначають, що інтерфейс може бути складним для новачків, що вимагає додаткового навчання персоналу. Ще однією проблемою може бути залежність від ліцензійного програмного забезпечення, що збільшує довгострокові витрати [12].

Після проведеного аналізу можна зробити висновки, що система "Parsec" є оптимальною для підприємств, які потребують багатофункціональності та

інтеграції з іншими системами, проте її вартість може бути недосяжною для малих компаній. "ZKTeco" підходить для малого та середнього бізнесу, однак її можливості можуть бути недостатніми для великих об'єктів. "Honeywell Access Control" ідеально підходить для великих підприємств, але вимагає значних фінансових вкладень і ресурсів для впровадження.

1.3 Аналіз методів ідентифікації людини при проходженні пунктів контролю доступу

Ефективність систем контролю доступу значною мірою залежить від застосовуваних методів ідентифікації. Основні етапи цього процесу включають збирання даних, перевірку особи, аналіз даних та прийняття рішення щодо надання доступу, кожен із цих етапів має свої особливості та вимоги:

– збирання даних, на цьому етапі система отримує інформацію, яка підтверджує особу користувача, це можуть бути дані з карток доступу, біометричних сканерів (відбитки пальців, розпізнавання обличчя), або цифрових кодів (PIN-код, QR-код). Надійність ідентифікації залежить від точності зчитування та якості обладнання;

– перевірка особи, зібрані дані передаються до модуля перевірки, який здійснює порівняння отриманої інформації з базою даних. Наприклад, сканований відбиток пальця порівнюється з шаблоном у системі, цей процес забезпечує підтвердження або відхилення доступу;

– аналіз даних, система оцінює відповідність отриманої інформації встановленим критеріям доступу, враховуються різні параметри: час, місце доступу, рівень дозволу. На цьому етапі можуть бути застосовані алгоритми штучного інтелекту для підвищення точності аналізу;

– прийняття рішення, на основі результатів аналізу приймається остаточне рішення: надати доступ або відмовити, рішення може

супроводжуватися відповідними діями, такими як відкриття дверей або активація сигналізації в разі несанкціонованої спроби доступу [13-14].

Наступним етапом, опишемо детальніше структуру процесу ідентифікації. Процес ідентифікації у системах контролю доступу складається з кількох етапів, які утворюють послідовну структуру, спрямовану на забезпечення надійного доступу до об’єктів. Перший етап – це реєстрація даних користувача. На цьому етапі до системи вносяться особисті дані співробітника, такі як ім’я, посада, номер картки, біометричні характеристики (відбитки пальців, скан обличчя) чи унікальні ідентифікатори, наприклад, QR-коди. Введені дані зберігаються в базі системи і асоціюються з правами доступу, які налаштовуються відповідно до зони чи часу роботи. Другим етапом є процес верифікації, під час верифікації система отримує ідентифікаційні дані користувача через відповідний зчитувач: картковий термінал, біометричний сенсор або QR-сканер. Цей етап передбачає порівняння отриманих даних із тими, що збережені в базі. Якщо введені дані збігаються з зареєстрованими, система підтверджує ідентичність користувача, переходячи до наступного етапу. Третій етап – це прийняття рішення щодо доступу. На основі результатів верифікації система аналізує права доступу користувача до конкретної зони або об’єкта. Якщо доступ дозволений, система надсилає команду на фізичний пристрій, наприклад, електрозамок або турнікет, відкриваючи прохід. У разі відсутності прав доступу користувач отримує відповідне сповіщення через індикатори, дисплей або звукові сигнали. Останнім етапом є реєстрація події доступу, де усі дії, включаючи успішні входи, відмови в доступі чи інші події, фіксуються в журналі системи. Ця інформація може бути використана для аналізу роботи підприємства, оцінки дотримання правил безпеки або вирішення спірних ситуацій. Таким чином, структура процесу ідентифікації забезпечує контроль, прозорість і ефективність роботи системи контролю доступу [15].

1.4 Аналіз апаратного забезпечення пункту контролю проходження пунктів пропуску на виробництві

При виборі варіантів побудови автоматизованої системи контролю проходження пунктів пропуску рішення приймаються за множиною показників, які враховують технічні, економічні та функціональні аспекти. Одним із ключових показників є надійність системи, яка визначається стабільністю роботи апаратного забезпечення, захистом від збоїв і зовнішніх впливів, а також здатністю до відновлення після неполадок. Важливе значення має також точність ідентифікації користувачів, адже помилкові спрацьовування або відмови можуть призвести до збоїв у роботі підприємства. Другий показник – вартість розробки та впровадження системи. Вона включає ціну апаратного забезпечення, розробку програмного забезпечення, інтеграцію з існуючими системами та експлуатаційні витрати. Крім того, важливо враховувати економічну ефективність: співвідношення вартості системи до її функціональності та тривалості експлуатації. Системи з низькою вартістю, але обмеженими можливостями можуть бути неефективними для великих підприємств, тоді як високовартісні системи виправдані лише в умовах підвищених вимог до безпеки. Ще одним важливим показником є гнучкість і масштабованість. Система повинна легко адаптуватися до змін у структурі підприємства, розширення зон доступу або збільшення кількості користувачів. Також враховуються можливості інтеграції з іншими інформаційними системами, такими як бази даних співробітників, системи відеоспостереження або обліку робочого часу. Сукупний аналіз цих показників дозволяє обрати оптимальний варіант побудови системи, який відповідає як технічним вимогам, так і бюджетним обмеженням підприємства [16].

Апаратне забезпечення пункту контролю є ключовим компонентом системи, оскільки воно забезпечує фізичне виконання перевірок доступу та управління потоками персоналу. Основними елементами апаратної частини є

зчитувачі, контролери, пристрої обмеження доступу (турнікети, шлагбауми), сервери для обробки даних і допоміжне обладнання (камери, кнопки виходу тощо). Проведемо аналіз кожного елемента, порівнюючи їхні характеристики, переваги та недоліки [17].

Зчитувачі – це пристрої, які отримують дані від користувача через картки, біометричні сенсори або QR-коди. Наприклад, RFID-зчитувачі є недорогими та простими в експлуатації, але вони менш надійні у випадках високої завантаженості. Біометричні зчитувачі, такі як сенсори відбитків пальців чи розпізнавання обличчя, забезпечують вищий рівень безпеки, але їхня точність може знижуватися через погане освітлення чи фізичні перешкоди. QR-зчитувачі є зручними для тимчасового доступу, але мають обмеження в інтеграції з іншими компонентами системи.

Наступним елементом є контролери, які виконують функцію управління всією системою на рівні об’єкта. Наприклад, централізовані контролери дозволяють об’єднувати велику кількість зчитувачів та інших пристроїв в єдину систему. Однак такі рішення потребують значних витрат на встановлення й обслуговування. Локальні контролери, навпаки, більш економічні й зручні у випадках, коли необхідно організувати невеликі точки доступу, але їхня масштабованість обмежена.

В свою чергу, турнікети, дверні електрозамки та шлагбауми є фізичними бар’єрами, які забезпечують або забороняють прохід. Наприклад, роторні турнікети забезпечують високий рівень безпеки, але створюють черги у випадках великого потоку людей. Прямі шлагбауми ефективні для контролю автомобільного руху, але можуть бути недостатньо безпечними для пішоходів. Дверні замки з електронним управлінням є зручними для офісів, але їхня робота залежить від стабільного електропостачання.

Сервери відіграють важливу роль у зберіганні й обробці даних, отриманих від зчитувачів та контролерів. Локальні сервери забезпечують високий рівень конфіденційності, але вимагають значних витрат на обладнання

та обслуговування. Хмарні сервери дозволяють зменшити витрати на інфраструктуру, забезпечуючи водночас доступність даних з будь-якого місця, але підвищують ризики кіберзагроз.

Кнопки виходу, камери спостереження та звукові/світлові індикатори доповнюють функціональність системи. Наприклад, камери спостереження інтегруються з контролем доступу для додаткової перевірки подій, але вони вимагають постійного моніторингу. Кнопки виходу є простими у використанні, але можуть бути об’єктом маніпуляцій з боку недобросовісних осіб. Зчитувачі й контролери повинні забезпечувати баланс між зручністю використання та рівнем захисту. Пристрої обмеження доступу обираються залежно від типу потоків (пішохідні або транспортні), а сервери та допоміжне обладнання – від потреб у зберіганні даних та інтеграції із суміжними системами, а їх ефективна комбінація цих елементів забезпечує надійність, безпеку та функціональність системи [18-19].

1.5 Постановка задач дослідження

В ході проведеного аналізу, було виявлено, що тема дослідження є актуальною. Метою дослідження є підвищення ефективності контролю доступу до виробничого приміщення, за рахунок вдосконалення системи контролю. Об’єктом дослідження є процес авторизації працівника на пункті пропуску виробництва. Предметом дослідження є методи, алгоритми та програмне забезпечення ідентифікації працівника для проходження пунктів пропуску на виробництві. Для досягнення поставленої мети потрібно вирішити наступні завдання:

– розробити структуру макета та описати призначення структурних блоків;

– провести аналіз та вибір апаратних модулів для розробки макета системи контролю проходження пунктів пропуску;

– розробити схему підключення та зібрати макет системи контролю проходження пунктів пропуску;

– розробити загальний алгоритм роботи системи контролю проходження пунктів пропуску;

– провести аналіз та вибір нейронної мережі для розпізнавання обличчя людини за особливостями їх рис;

– удосконалити метод розпізнавання обличчя людини на базі нейронної мережі MobileNetV2;

– провести обґрунтування вибору мови та середовища розробки;

– розробити функції розпізнавання обличчя людини;

– провести експериментальні дослідження та проаналізувати результати.

1.6 Висновки до першого розділу

У першому розділі кваліфікаційної роботи було виявлено, що АСКПП відіграють важливу роль у забезпеченні безпеки, ефективності та дисципліни на підприємствах. Їхня структура включає апаратні, програмні та організаційно-нормативні компоненти, які взаємодіють для забезпечення надійного та безпечного доступу до об'єктів. Проведений аналіз існуючих рішень, таких як "Parsec", "ZKTeco" і "Honeywell Access Control", дозволив виявити сильні та слабкі сторони кожної системи, що дасть змогу обрати оптимальний варіант в залежності від масштабу, потреб і бюджету підприємства, а особливу увагу слід приділяти інтеграції з іншими системами підприємства, захисту даних і можливості адаптації до змін у структурі або умовах роботи.

Результати аналізу показують, що впровадження АСКПП повинно враховувати не лише технічні параметри, але й організаційні аспекти, такі як розташування обладнання, зручність для користувачів і відповідність нормативно-правовим вимогам. Рекомендується обирати системи, що підтримують сучасні методи ідентифікації (біометрія, QR-коди) та мають

високу гнучкість у налаштуванні прав доступу. Ще одним важливим завданням є передбачити регулярне технічне обслуговування, оновлення програмного забезпечення та проведення перевірок безпеки, щоб мінімізувати ризики збоїв або несанкціонованого доступу. Для малих і середніх підприємств доцільно обирати більш доступні рішення, тоді як великі підприємства можуть інвестувати у масштабовані системи з розширеним функціоналом.

2 РОЗРОБКА СТРУКТУРИ МАКЕТА ТА ВИБІР АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Розробка структури макета та опис призначення структурних блоків

Проєктування структурної схеми є критично важливим етапом розробки АСКПП на виробництві, оскільки воно забезпечує комплексне бачення функціонування системи та взаємодію її компонентів. Структурна схема дозволяє визначити основні елементи системи, такі як датчики ідентифікації, контролери доступу, системи збору даних, обробки інформації та передачі сигналів. Це дає можливість чітко уявити всі процеси, що відбуваються в системі, та їх логічну послідовність. Також проєктування допомагає виявити потенційні ризики, як-от можливі збої в роботі системи або вразливі місця, що можуть бути використані для несанкціонованого доступу. Крім того, структурна схема допомагає розробникам оптимізувати взаємодію між компонентами, що сприяє підвищенню надійності та ефективності системи, а також її гнучкості до можливих модифікацій у майбутньому. Така схема також є ключовим інструментом для подальшої технічної документації та узгодження між різними підрозділами, які беруть участь у розробці та впровадженні системи [20-21].

При проєктуванні структурної схеми автоматизованої системи контролю проходження пунктів пропуску на виробництві, необхідно враховувати кілька ключових критеріїв, що забезпечують ефективність, надійність та безпеку. Одним із важливих критеріїв є можливість безконтактної ідентифікації працівників, що зменшує фізичний контакт та підвищує швидкість проходження. Це обумовлює необхідність використання систем комп'ютерного зору та бездротових мереж на основі RFID або NFC технологій. Комп'ютерний зір дозволяє автоматично розпізнавати осіб або інші ідентифікаційні ознаки без

необхідності додаткових носіїв, що зручно у великих виробництвах. Використання RFID або NFC забезпечує швидке зчитування даних, без потреби у фізичному контакті з пристроями, що значно підвищує ефективність системи. Ці технології також надають високий рівень безпеки, оскільки дозволяють уникнути підробок ідентифікаторів та несанкціонованого доступу. В таблиці 2.1 приведено аналіз обраних технологій та їх опис які будуть використовуватися для розробляємої автоматизованої системи контролю проходження пунктів пропуску на виробництві [22-23].

Таблиця 2.1 – Аналіз обраних технологій, які будуть використовуватися для розробки АСКПП на виробництві та їх опис

Технологія	Пояснення
Безконтактна ідентифікація	Забезпечує швидкість та безпеку при проходженні пунктів пропуску
RFID або NFC	Забезпечують надійне та швидке зчитування ідентифікаційних даних без фізичного контакту
Комп'ютерний зір	Дозволяє автоматично розпізнавати осіб, підвищуючи точність та зручність системи
Швидкість обробки даних	Важливо для великих потоків людей, щоб уникнути затримок у процесі ідентифікації
Безпека і захист даних	Гарантія того, що дані не будуть підроблені або доступ до системи не буде порушений

Виходячи з обраних критеріїв, які повинні виконуватися АСКПП на виробництві, що розробляється та обраних технологій, які приведено в таблиці 2.1, пропонується наступна структурна схема АСКПП на виробництві, що представлена на рисунку 2.1.

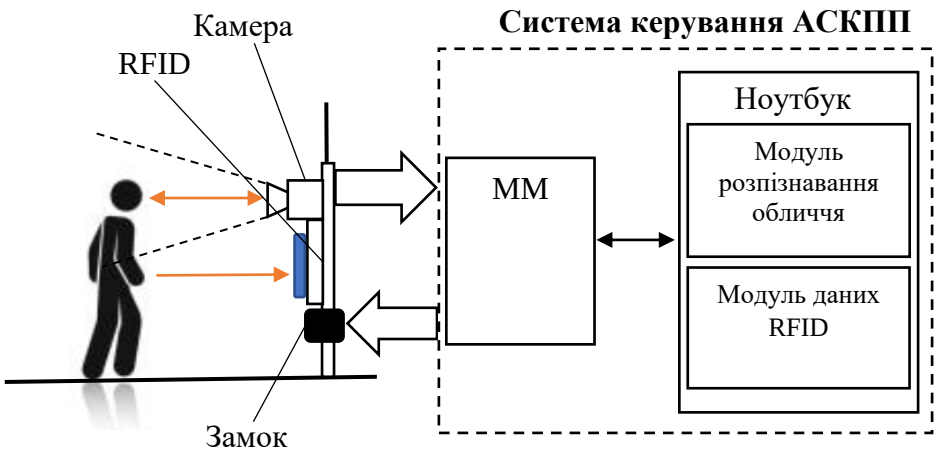


Рисунок 2.1 – Структурна схема макета АСКПП на виробництві, що розробляється

Приведена структура схема на рисунку 2.1, показує систему управління, в основі якої використовується АСКПП з інтеграцією різних модулів для розпізнавання осіб та ідентифікації за допомогою RFID. Нижче наведено опис призначення кожного з блоків:

– камера, відповідає за зчитування зображення або відео з обличчя людини для його подальшого аналізу. Використовується в модулі розпізнавання обличчя для ідентифікації користувача на основі біометричних даних;

– RFID, модуль зчитування RFID-карт або інших ідентифікаторів. В цьому блоці розташований зчитувач, який взаємодіє з RFID-чіпом, що може бути вбудований в картку або інший об'єкт, для підтвердження ідентифікації особи або об’єкта;

– замок, це електронний замок або механізм блокування доступу, який отримує сигнали від керуючої системи для відкриття або блокування дверей після успішної ідентифікації користувача через модулі розпізнавання обличчя або RFID;

– ММ (мікропроцесорний модуль), керуючий блок системи, який обробляє дані, отримані з модуля RFID. Він відповідає за зчитування даних з

карточки користувача, декодування інформації та передачі на ноутбук. Також ММ отримує дані з ноутбука та керує відкриттям або невідкриттям електричного замка;

– ноутбук (одноплатний комп’ютер) – пристрій, який виконує функцію обробки інформації та управління системою. Містить два основні програмні модулі: модуль розпізнавання обличчя та модуль даних RFID;

– модуль розпізнавання обличчя, програмна частина системи, яка аналізує дані з камери та визначає, чи відповідає зображення обличчя користувача заздалегідь записаним біометричним даним. Якщо ідентифікація успішна, дані передаються до модуля управління для надання доступу;

– модуль даних RFID, цей програмний модуль зберігає дані RFID-коду, які мають права доступу в виробниче приміщення.

Принцип роботи розробленої схеми макета АСКПП на виробництві, побудований наступним чином:

– об’єкт ідентифікації, підходить до пропускного пункту на виробництві;

– система сканує обличчя та зчитує дані з RFID-картки;

– отримані дані з камери напряму передаються на ноутбук або одноплатний комп’ютер, а дані з RFID-картки декодуються в ММ та у вигляді 16-го коду через порт USB теж передаються на ноутбук або одноплатний комп’ютер;

– на ноутбуці або одноплатному комп’ютері в модулі розпізнавання обличчя проводиться аналіз отриманого зображення обличчя та проводиться перевірка з існуючими зразками, та одночасно проводиться перевірка 16-го коду з RFID-картки. При умові, що два ці параметра мають позитивний відгук на запити, то система через ММ дає команду на відкриття замка. Якщо один, або всі параметри не відповідають, то система не дає команди на відкриття замка.

Розроблена система поєднує в собі два методи ідентифікації – біометричний (розпізнавання обличчя) і RFID, забезпечуючи багатофакторний підхід, що підвищує безпеку доступу [4].

2.2 Аналіз та вибір апаратних модулів для розробки макета системи контролю проходження пунктів пропуску

Проведення аналізу та вибір апаратних модулів для розробки макета системи контролю проходження пунктів пропуску на виробництві є необхідним для забезпечення ефективного та безпечного контролю доступу співробітників. Врахування специфіки виробництва, кількості працівників та рівня безпеки дозволяє визначити оптимальні компоненти, які забезпечать надійну ідентифікацію користувачів, мінімізуючи ризики несанкціонованого доступу. Наприклад, вибір камер високої роздільної здатності для розпізнавання обличчя або RFID-зчитувачів з великою дальністю дії дозволить адаптувати систему до вимог конкретного виробничого середовища. Також важливо підібрати надійні модулі управління та замки, щоб система працювала стабільно та без затримок. Ретельний аналіз дозволить створити прототип, який відповідає сучасним вимогам безпеки та продуктивності на підприємстві. Виходячи з розробленої схеми макета АСКПП на виробництві, проведемо аналіз та вибір апаратних модулів. Вибір веб-камери для реалізації ідентифікації людини в макеті АСКПП на виробництві обумовлений необхідністю отримання якісного зображення для точного розпізнавання обличчя. Камера повинна мати високу роздільну здатність, щоб забезпечити чіткі деталі обличчя, навіть при недостатньому освітленні, що часто зустрічається на виробництвах. Крім того, важливою характеристикою є висока частота кадрів для зниження затримок при обробці зображень у реальному часі. Сумісність з обраним програмним забезпеченням для аналізу та простота інтеграції в систему також відіграють важливу роль, оскільки це спрощує процес розробки та знижує витрати на

налаштування. В результаті аналізу, було обрано наступні камери, загальний вид яких приведено на рисунку 2.2, а технічні характеристики в таблиці 2.2.

а) б) в)

а) Logitech C920 HD Pro [24];

б) Microsoft LifeCam Studio [25];

в) Razer Kiyo [26]

Рисунок 2.2 – Вибір камери для реалізації макета АСКПП на виробництві

Таблиця 2.2 – Порівняння технічних характеристик камер: Logitech C920 HD Pro, Microsoft LifeCam Studio, Razer Kiyo

Характеристика	Камери		
	Logitech C920 HD Pro	Microsoft LifeCam Studio	Razer Kiyo
1	2	3	4
Максимальна роздільна здатність	1080p (Full HD)	1080p (Full HD)	1080p (Full HD)
Частота кадрів	30 fps (1080 p) / 60 fps (720 p)	30 fps	30 fps (1080 p) / 60 fps (720 p)
Кут огляду	78 °	75 °	81,6 °

Продовження таблиці 2.2

1	2	3	4
Автофокус	Так	Так	Так
Вбудоване підсвічування	ні	ні	Так (кільцеве підсвічування)
Інтерфейс підключення	USB 2.0		
Мікрофон	Стерео	Моно	Моно

Для реалізації макету системи АСКПП на виробництві важливо обрати веб-камеру, яка забезпечить високу якість зображення та надійність для ідентифікації осіб. Одним із ключових параметрів є роздільна здатність камери.

Модель Logitech C920 HD Pro пропонує Full HD 1080 p, що забезпечує чітке зображення для розпізнавання обличчя в реальному часі. Частота кадрів 30 fps на 1080 p дозволяє передавати плавне відео без затримок, що є важливим для системи контролю доступу. Важливим фактором є автофокус, який дозволяє точно ідентифікувати користувачів на різних відстанях, а стереомікрофон додає можливість захоплення звуку, якщо це потрібно для багатофункціональної системи. Крім того, камера легко інтегрується через USB 2.0, що спрощує її встановлення та налаштування. Завдяки цим характеристикам Logitech C920 HD Pro є кращим вибором для системи АСКПП, що розробляється та забезпечує високу продуктивність і сумісність із програмним забезпеченням для розпізнавання обличчя.

Наступним модулем для розробки макета системи АСКПП на виробництві є вибір модуля RFID. Відповідно до запропонованої структурної схеми (рис. 2.1), RFID модуль повинен відповідати наступним вимогам, які зазначені в таблиці 2.3.

Таблиця 2.3 – Вимоги, які пред’являються модулям RFID на виробництві

Вимога	Опис
Дальність зчитування	Модуль повинен забезпечувати достатню дальність зчитування для комфортного проходження осіб, що може бути критичним для великих виробничих зон
Швидкість реагування	Висока швидкість зчитування та ідентифікації міток для забезпечення неперервного руху осіб через контрольно-пропускні пункти без затримок
Безпека	Підтримка зашифрованих протоколів зв’язку для захисту даних, які передаються від RFID міток до читача, щоб уникнути несанкціонованого доступу або підробки міток
Надійність	Модуль повинен бути стійким до промислових умов, включаючи пил, бруд, вібрації, та коливання температур
Сумісність з існуючими системами	Здатність інтегруватися з іншими системами безпеки та автоматизації, які вже використовуються на виробництві
Сертифікація та стандарти	Відповідність міжнародним і місцевим стандартам та нормам для використання у виробничих умовах
Масштабованість	Можливість розширення системи для додавання нових міток або точок доступу без значних змін у існуючій інфраструктурі

Враховуючи вимоги, які пред’являються до модулів RFID на виробництві (табл. 2.3), було обрано наступні модулі, загальний вид яких представлено на рисунку 2.3.

Порівняння технічних характеристик обраних модулів подано в таблиці 2.4.

а) б) в)

а) модуль RFID-RC522 [27];

б) PN532 NFC RFID модуль [28];

в) RDM6300 125kHz RFID модуль [29]

Рисунок 2.3 – Загальний вид модулів RFID

Таблиця 2.4 – Порівняння технічних характеристик модулів RFID

Характеристики	Моделі модулів RFID		
	RFID-RC522	PN532 NFC RFID	RDM6300 125kHz
Частота	13,56 МГц	13,56 МГц	125 кГц
Дальність зчитування	до 5 см	до 10 см	до 10 см
Інтерфейс	SPI	I2C, SPI, UART	UART
Протоколи	ISO/IEC 14443-A	ISO/IEC 14443-A, NFC	EM4100
Живлення	3,3 В	3,3 В або 5 В	5 В
Швидкість передачі даних	До 10 Мбіт/с	До 424 кбіт/с	До 9600 біт/с
Додаткові функції	Підтримка MIFARE карток	Підтримка NFC міток і смарт-карток	Підтримка EM4100 стандарту
Розмір	40 мм x 60 мм	43 мм x 40 мм	37 мм x 25 мм
Сфера застосування	Контроль доступу, RFID мітки	NFC комунікації, RFID системи	Простий контроль доступу, ідентифікація

При виборі модуля для реалізації макету системи АСКПП на виробництві, модуль PN532 NFC RFID є найкращим варіантом у порівнянні з іншими, такими як RFID-RC522 та RDM6300, завдяки його розширеним функціям та універсальності. PN532 працює на частоті 13,56 МГц, аналогічно RFID-RC522, однак PN532 має більшу дальність зчитування до 10 см, що забезпечує зручніший доступ. Крім того, цей модуль підтримує не лише RFID технології, а й NFC, що дозволяє використовувати сучасні смартфони для ідентифікації, значно підвищуючи гнучкість системи. У порівнянні з RDM6300, який працює на застарілій частоті 125 кГц і підтримує тільки прості RFID карти, PN532 забезпечує більшу швидкість передачі даних, інтеграцію через кілька інтерфейсів (I2C, SPI, UART), що робить його зручнішим для інтеграції з Arduino. Це робить PN532 більш ефективним вибором для сучасної виробничої системи контролю доступу.

Останнім кроком для розробки макету системи АСКПП на виробництві, потрібно обрати модуль, який буде виконувати функції мікропроцесорного модуля, як це показано на рисунку 2.4, а в таблиці 2.5 приведено порівняння технічних характеристик.

а) б) в)

а) Arduino Nano [30];

б) Arduino Pro Mini [31];

в) Arduino Micro [32]

Рисунок 2.4 – Загальний вид мікроконтролерних модулів

Таблиця 2.5 – Порівняння технічних характеристик мікроконтролерних модулів: Arduino Nano, Arduino Pro Mini та Arduino Micro

Характеристики	Мікроконтролері модулі		
	Arduino Nano	Arduino Pro Mini	Arduino Micro
Мікроконтролер	ATmega328P	ATmega328P	ATmega32U4
Кількість цифрових виводів	14 (6 PWM)	14 (6 PWM)	20 (7 PWM)
Аналогові входи	8	8	12
Тактова частота	16 МГц		
Флеш-пам'ять	32 КБ		
ОЗП (SRAM)	2 КБ		2,5 КБ
EEPROM	1 КБ		
Інтерфейси підключення	UART, I2C, SPI	UART, I2C, SPI	UART, I2C, SPI, USB
USB-порт	microUSB	Немає (потрібен зовнішній FTDI адаптер)	microUSB
Розміри	18 мм x 45 мм	18 мм x 33 мм	18 мм x 48 мм
Живлення	5 В (через USB або Vin)	3,3 В / 5 В	5 В (через USB або Vin)
Споживання енергії	Низьке	Дуже низьке	Середнє

Вибір Arduino Nano для розроблюваного макету системи АСКПП на виробництві обґрунтований його компактністю, достатньою кількістю цифрових (14) та аналогових (8) виводів, що дозволяє підключати необхідну кількість датчиків і модулів, таких як RFID-модуль PN532. Завдяки мікроконтролеру ATmega328P, він забезпечує стабільну роботу при тактовій

частоті 16 МГц і має 32 КБ флеш-пам'яті, що дозволяє завантажити програму для управління системою контролю доступу. Наявність вбудованого microUSB порту спрощує підключення до комп'ютера для програмування та живлення, що особливо важливо для макетів на етапі розробки. Також, Arduino Nano має невелике енергоспоживання, що робить його ефективним для автономної роботи.

На останньому кроці необхідно обрати електромеханічний замок та модуль реле для керування ним. Відповідно до обраного модуля MM Arduino Nano, пропонується наступний електромеханічний замок та модуль реле, які представлено на рисунку 2.5.

а) б)

а) електромеханічний соленоїдний замок електрозамок засувка MIHI 12B;

б) 1-канальний модуль реле 12V для Arduino PIC ARM [33]

Рисунок 2.5 – Загальний вид обраного електромеханічного замка та модуля реле

Технічні характеристики для 1-канального реле 12V, сумісного з Arduino, PIC, ARM приведено в таблиці 2.6.

Таблиця 2.6 – Технічні характеристики для 1-канального реле 12V

Характеристика	Опис
1	2
Кількість каналів	1
Напруга живлення	12V DC
Максимальний струм комутації	10A при 250V AC або 10A при 30V DC

Продовження таблиці 2.6

1	2
Робоча напруга реле	12V DC
Інтерфейс управління	TTL логіка (3,3V / 5V для керування)
Споживання струму	Приблизно 20-30 мА
Контакти реле	NO (Normally Open), NC (Normally Closed), COM
Ізоляція	Оптична розв'язка для захисту мікроконтролера
Індикація стану	Світлодіод (LED)
Час спрацьовування	≤ 10 мс
Час відпускання	≤ 5 мс
Розмір	50 мм x 26 мм x 19 мм
Маса	15 г

Для розробки макета АСКПП на виробництві, обрані модулі забезпечують комплексне вирішення завдань. Одноканальне реле 12V дозволяє безпечно керувати електричними пристроями, такими як соленоїдний електрозамок, який забезпечує надійний механізм блокування доступу на виробничу територію. Електромеханічний соленоїдний замок працює з живленням 12V, є компактним і енергоефективним, що робить його гарним вибором для використання в обмежених просторах та забезпечення безпеки. Модуль PN532 NFC RFID забезпечує швидку та безконтактну ідентифікацію співробітників через RFID-карти або NFC, що підвищує зручність та безпеку контролю доступу. Arduino Nano завдяки компактному розміру та достатній потужності обробки добре підходить для підключення та керування різними модулями в межах макету системи. Камера Microsoft LifeCam Studio забезпечує високу якість відео для реалізації технологій розпізнавання облич, що додає ще один рівень безпеки системі, дозволяючи ідентифікувати особи працівників на виробничій лінії. Разом ці компоненти надають ефективне та надійне рішення для реалізації системи контролю доступу на виробництві.

2.3 Розробка схеми підключення та складання макета системи контролю проходження пунктів пропуску

Розробка схеми підключення макета АСКПП на виробництві є важливим етапом для забезпечення коректної роботи всіх модулів. Схема допоможе чітко визначити, як підключати такі компоненти, як камера, модуль RFID, реле, замок і контролер Arduino Nano, що запобіжить можливим помилкам у монтажі. Без правильної схеми можуть виникнути збої в роботі, що вплине на функціональність всієї системи.

Крім того, схема підключення дозволить виявити та усунути потенційні проблеми з живленням, забезпечити безпечне керування електронними компонентами, уникнути перевантаження або короткого замикання. Також вона полегшить майбутнє обслуговування та модернізацію системи, що є важливим для її ефективної експлуатації на виробництві. Розроблена схема підключення в середовищі Fritzing представлено на рисунку 2.6.

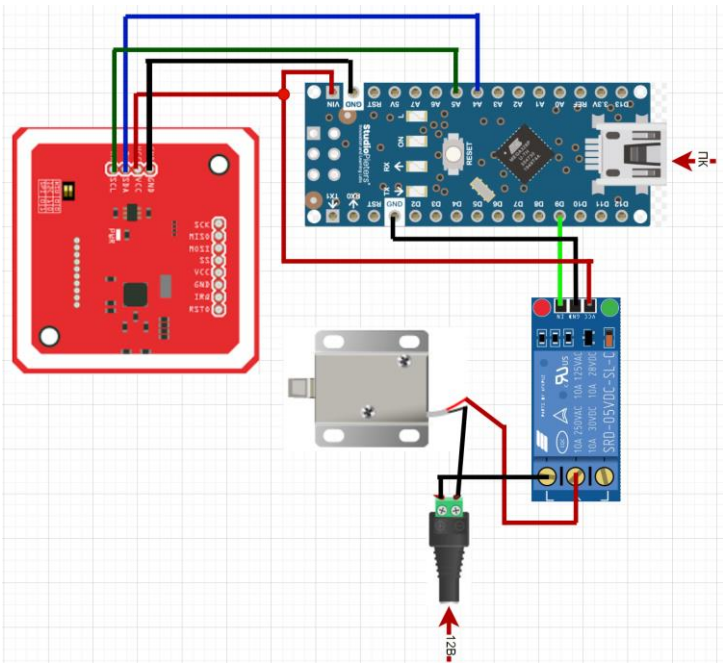


Рисунок 2.6 – Схема підключення апаратних модулів АСКПП на виробництві

На схемі підключення (рис. 2.6) розробленого макета АСКПП використовуються кілька апаратних модулів. В основі схеми знаходиться плата Arduino Nano, яка контролює всі компоненти. Модуль PN532 NFC RFID підключений до плати через 4 дроти: GND до землі Arduino, VCC до 5V для живлення, SDA до аналогового порту A4, і SCL до A5 для обміну даними через шину I2C. Також використовується 1-канальне реле 12V, яке управляється Arduino через цифровий вихід D6, що дозволяє комутувати електроживлення для замка. На реле подається живлення 12V, яке також використовується для електромеханічного соленоїдного замка. Arduino живить реле через GND і керує ним для замикання або відкриття дверей.

Живлення на 12V подається через окремий блок живлення, який підключений до реле та замка. Це дозволяє замку отримувати достатньо енергії для правильної роботи. Камера Logitech C920 HD Pro підключається до ноутбуку або мікроконтролера через порт USB. В рамках даної роботи, для реалізації макету буде використовуватися ноутбук з вбудованою веб-камерою. В наслідок чого, Arduino Nano буде напряму підключатися через USB порт до ноутбуку. Відповідно до розробленої схеми підключення (рис. 2.6) було зібрано макет АСКПП на виробництві, загальний вид якого представлено на рисунку 2.7.

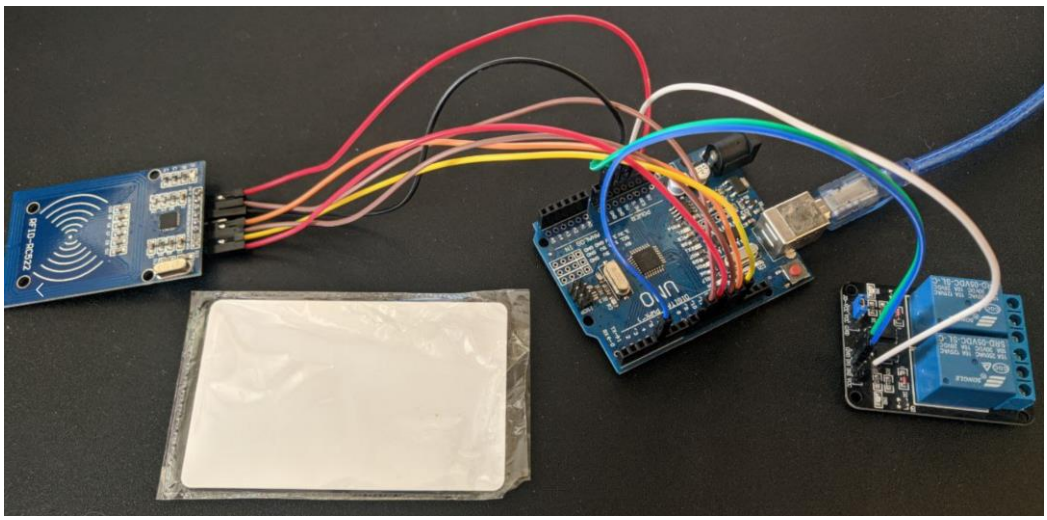


Рисунок 2.7 – Зібраний макет апаратної складової АСКПП на виробництві

2.4 Висновки до другого розділу

У другому розділі було розроблено структуру макета АСКПП із використанням сучасних апаратних та програмних модулів. Зокрема, визначено ключові функціональні блоки, такі як модуль розпізнавання обличчя, RFID-зчитувач, мікропроцесорний модуль, ноутбук як центральний обчислювальний пристрій, а також виконавчі механізми, такі як електронний замок. Усі блоки інтегровані в єдину систему, яка дозволяє забезпечити ідентифікацію користувачів шляхом використання біометричних даних та RFID-технологій. Розроблена схема була детально проаналізована та оптимізована для реалізації високого рівня безпеки й зручності експлуатації.

Під час вибору апаратного забезпечення було проаналізовано різні модулі та їхні характеристики з точки зору продуктивності, сумісності та економічної доцільності. Особливу увагу приділено розробці схеми підключення компонентів, що забезпечує надійність передачі даних і мінімізацію затримок. У результаті було створено макет системи, який дозволяє реалізувати принцип одночасного використання декількох методів ідентифікації, що підвищує стійкість і забезпечує відповідність сучасним вимогам до автоматизації контролю доступу на виробничих об'єктах.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ ПРОХОДЖЕННЯ ПУНКТІВ ПРОПУСКУ НА ВИРОБНИЦТВІ

3.1 Розробка загального алгоритму роботи системи контролю проходження пунктів пропуску

Розробка загального алгоритму роботи програмного забезпечення АСКПП на виробництві є необхідною для забезпечення узгодженої та ефективної роботи всіх компонентів системи. Алгоритм визначає послідовність дій, необхідних для коректної ідентифікації, аутентифікації та пропуску співробітників або відвідувачів. Він враховує інтеграцію різних апаратних модулів (камери, RFID, реле), а також обробку даних нейронними мережами для розпізнавання облич. Чіткий алгоритм дозволяє оптимізувати роботу системи, зменшити затримки та підвищити точність ідентифікації, що є критично важливим для безпеки та продуктивності виробництва. Також загальний алгоритм спрощує процес налагодження, тестування та майбутнього вдосконалення системи, забезпечуючи її масштабованість і адаптивність. Виходячи з цього пропонується наступний загальний алгоритм роботи АСКПП на виробництві, який представлено на рисунку 3.1.

Алгоритм, який представлено на рисунку 3.1, описує процес функціонування АСКПП на виробництві. Процес розпочинається із завантаження налаштувань системи. Після цього система очікує на піднесення картки RFID. Якщо картка не зчитується, система продовжує чекати. Як тільки картка зчитана, відбувається зчитування даних з неї. Якщо дані не отримані, система знову повертається до очікування картки.

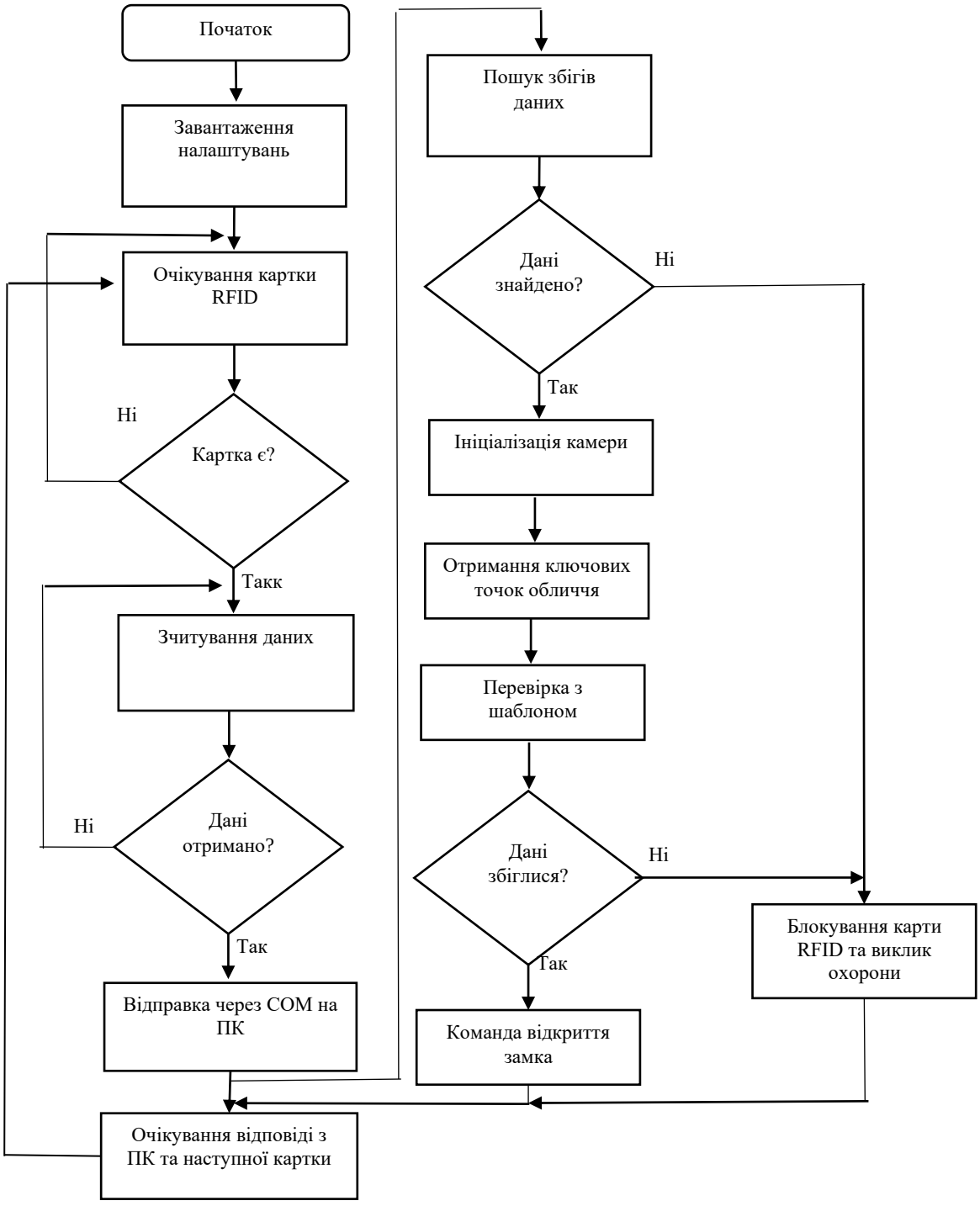


Рисунок 3.1 – Загальний алгоритм роботи АСКПП на виробництві

У випадку успішного зчитування даних, вони передаються через інтерфейс COM на ПК для подальшої обробки, після чого система чекає на відповідь від ПК. Паралельно на ПК запускається пошук збігів з базою даних.

Якщо дані знайдено, ініціалізується камера для захоплення зображення обличчя. Система отримує ключові точки обличчя та порівнює їх зі збереженим шаблоном у базі даних.

Якщо дані збігаються, надсилається команда на відкриття замка. У випадку невідповідності обличчя або якщо дані на картці не збігаються з базою, відбувається блокування картки та виклик служби охорони для забезпечення безпеки. Таким чином, алгоритм забезпечує два рівні аутентифікації: за карткою RFID та за розпізнаванням обличчя, що підвищує безпеку доступу до пункту пропуску.

Розроблений алгоритм забезпечує високий рівень безпеки доступу до пункту пропуску завдяки поєднанню двох методів аутентифікації: зчитування картки RFID та розпізнавання обличчя. Це мінімізує ризики несанкціонованого доступу, оскільки кожен етап контролює справжність користувача.

Алгоритм також забезпечує швидку ідентифікацію, оскільки паралельно виконується пошук збігів у базі даних та зчитування зображення. Інтеграція камери та обробки ключових точок обличчя підвищує надійність розпізнавання та зменшує ймовірність помилок.

У випадку виявлення невідповідності або підозрілих дій, система автоматично блокує картку та викликає охорону, що додає додатковий рівень захисту.

3.2 Аналіз та вибір нейронної мережі для розпізнавання обличчя людини за особливостями її рис

Для розробки макета АСКПП на виробництві важливим завданням є вибір нейронної мережі для розпізнавання обличь за їх рисами. Існує кілька ефективних архітектур, які можна застосувати для цієї мети:

– FaceNet, одна з провідних нейронних мереж для задач розпізнавання облич, використовує триплетну втрату для створення багатовимірних векторів

(ембеддингів) на основі характеристик обличь. Це дозволяє здійснювати ідентифікацію або верифікацію за допомогою порівняння векторних відстаней між різними обличчями. FaceNet демонструє високу точність і може використовуватися у завданнях, де критично важливе точне розпізнавання;

– VGG-Face, це глибока згорткова нейронна мережа (CNN), яка складається з великої кількості шарів, що забезпечують високу точність розпізнавання. Проте через велику кількість параметрів ця модель є ресурсоємною та може вимагати більше обчислювальних потужностей, що обмежує її застосування в системах з обмеженими ресурсами;

– ResNet-50, архітектура з глибокими залишковими зв'язками (Residual Connections), що допомагає вирішити проблему зникання градієнта при збільшенні глибини мережі. ResNet-50 є однією з найточніших моделей для розпізнавання облич і може використовуватися для високоточних систем контролю;

– MobileNetV2**,** одна з найбільш ефективних нейронних мереж для систем з обмеженими ресурсами є модель, яка оптимізована для швидкої роботи з обмеженими обчислювальними ресурсами, наприклад, на мобільних пристроях або вбудованих системах. MobileNetV2 використовує глибокі згорткові шари для досягнення балансу між точністю та швидкістю. Це дозволяє проводити розпізнавання облич у реальному часі з мінімальними затримками, що є критично важливим для систем контролю доступу на виробництві;

Проведемо порівняння переваг та недоліків вище представлених нейронних мереж з точки зору впровадження їх до системи ідентифікації людини по обличчю у АСКПП на виробництві, результати аналізу представлено у таблиці 3.1.

Таблиця 3.1 – Порівняння переваг та недоліків використання нейронних мереж з точки зору впровадження їх до системи ідентифікації людини по обличчю

Нейронна мережа	Переваги	Недоліки
FaceNet	Висока точність ідентифікації завдяки триплетній втраті; Підходить для задач верифікації та класифікації за векторами ембеддингів; Відмінна для обчислення подібності облич	Високі вимоги до обчислювальних ресурсів; Не підходить для систем з обмеженими ресурсами
VGG-Face	Глибока архітектура забезпечує високу точність розпізнавання; Може бути ефективною для великих баз даних облич	Велика кількість параметрів призводить до значних витрат на пам'ять і обчислення; Не оптимізована для реального часу або вбудованих систем
ResNet-50	Використовує залишкові зв'язки, що дозволяє будувати глибші мережі без втрати якості навчання; Висока точність при менших обчислювальних витратах порівняно з VGG-Face; Хороша продуктивність в задачах розпізнавання облич	Модель все ще залишається досить складною для вбудованих систем; Вимагатиме більшого часу на обробку порівняно з легкими моделями, як MobileNetV2
MobileNet V2	Легка архітектура, оптимізована для мобільних та вбудованих систем; Підтримує роботу в реальному часі завдяки низьким вимогам до ресурсів; Добре підходить для системи АСКПП з обмеженими ресурсами	Нижча точність у порівнянні з FaceNet або ResNet-50; Не така глибока і складна для великих баз даних облич

Отже, у виборі нейронної мережі для системи АСКПП, FaceNet і ResNet-50 підходять для високоточних задач, але MobileNetV2 з огляду на свою легковажну архітектуру є гарним вибором для реалізації системи, яка потребує обробки даних у реальному часі з обмеженими ресурсами.

3.3 Удосконалення методу розпізнавання обличчя людини на базі нейронної мережі MobileNetV2

Нехай $I(x, y)$ – це функція зображення обличчя, де x і y – це просторові координати пікселів зображення. Зображення проходить попередню обробку, таку як нормалізація (приведення до діапазону значень [0, 1]) і масштабування до стандартного розміру, наприклад 224 x 224 пікселя.

MobileNetV2 використовує архітектуру глибокої згорткової нейронної мережі з вузькими блоками, які називаються «інверсними залишковими блоками» (Inverted Residuals), для екстракції ключових ознак. З математичної точки зору кожен блок складається з таких операцій:

– групова згортка (Depthwise Convolution) використовується для ефективного зменшення кількості обчислень і параметрів у згорткових нейронних мережах. Вона полягає в застосуванні окремого фільтра до кожного каналу вхідного зображення замість традиційної згортки, яка одночасно обробляє всі канали. Це дозволяє значно зменшити обчислювальну складність, оскільки кількість операцій скорочується за рахунок розділення процесу згортки на дві окремі фази: спочатку групова згортка для кожного каналу, а потім точкова згортка для поєднання інформації з різних каналів. Така архітектура дозволяє зберегти важливі просторові ознаки з кожного каналу окремо, при цьому підвищуючи загальну продуктивність моделі. Групова згортка є ключовим компонентом для полегшених моделей, таких як MobileNet, де важливо зберегти баланс між швидкістю і точністю:

$$F(x, y) = W_d * I(x, y), \tag{3.1}$$

де $F(x, y)$ – вихідний результат після застосування групової згортки до вхідного зображення. Це карта ознак (Feature Map), яка відображає просторові

ознаки зображення після обробки згортковими фільтрами. Координати x і y вказують на положення пікселів у вихідній карті ознак;

W_d – це ядро або фільтр групової згортки (Depthwise Convolution Kernel). Воно відповідає за обробку кожного окремого каналу вхідного зображення. Важливо, що для кожного каналу застосовується окремий фільтр, тобто кількість фільтрів відповідає кількості каналів вхідного зображення;

$I(x, y)$ – це вхідне зображення або вхідний тензор, який містить інформацію про пікселі на позиціях x і y для кожного каналу. Із цього тензору беруться ознаки, які будуть оброблятися фільтрами групової згортки.

У контексті групової згортки W_d застосовується до кожного каналу окремо, тобто на відміну від традиційної згортки, де всі канали одночасно обробляються одним фільтром, тут операція виконується незалежно для кожного каналу вхідних даних;

– точкова згортка (Pointwise Convolution) використовується для зміни кількості каналів у тензорі без зміни його просторових розмірів. Основною її функцією є об'єднання інформації з різних каналів вхідного тензору шляхом застосування фільтра розміром 1 x 1. Точкова згортка дозволяє поєднати ознаки, отримані з різних каналів після застосування групової згортки, та інтегрувати їх у більш стисненому вигляді. Вона виконує важливу роль у побудові ефективних моделей глибокого навчання, таких як MobileNet, знижуючи обчислювальні витрати та кількість параметрів нейронної мережі, при цьому зберігаючи високу якість аналізу ознак:

$$F_{pw}(x, y) = W_p * F(x, y), \tag{3.2}$$

де $F_{pw}(x, y)$ – результат операції точкової згортки в точці з координатами x, y. Це вихідний тензор, в якому кількість каналів змінюється, але просторові розміри залишаються незмінними;

W_p – набір фільтрів розміром 1 x 1, що відповідають за перетворення вхідних каналів. Для кожного каналу вихідного тензора є свій фільтр W_p. Фільтри визначають ваги, які використовуються для зважування значень каналів у вхідному тензорі;

$F(x, y)$ – вхідний тензор ознак у точці x, y, який подається на операцію точкової згортки. Цей тензор містить набір каналів, отриманих після застосування групової згортки або попередніх шарів мережі.

Загалом точкова згортка об'єднує інформацію з усіх каналів вхідного тензора, змінюючи кількість каналів без зміни просторових розмірів.

Після кожного блоку виконується нелінійне перетворення через функцію активації, наприклад, ReLU6. Функція активації ReLU6 (Rectified Linear Unit 6) є варіацією класичної функції ReLU, яка обмежує значення виходу між 0 і 6. Її математичний вираз виглядає так:

$$ReLU6(x) = \min\left(\max(0, x), 6\right). \quad (3.3)$$

Це означає наступне:

– якщо вхідне значення x менше або дорівнює 0, вихід дорівнює 0 (як і в стандартній ReLU);

– якщо вхідне значення x більше 6, вихід обмежується на рівні 6;

– якщо x знаходиться в межах від 0 до 6, то вихід дорівнює самому x.

Тоді, для нашого випадку:

$$F_{out}(x, y) = \max\left(0, \min\left(F_{pw}(x, y), 6\right)\right), \quad (3.4)$$

де $F_{out}(x, y)$ – це результат нелінійного перетворення, тобто вихід функції активації ReLU6 для кожного пікселя чи елемента даних із координатами x, y. Значення виходу обмежене між 0 і 6;

$F_{pw}(x, y)$ – результат точкової згортки (Pointwise Convolution) для кожної пари координат x, y. Це проміжний результат після застосування згортки, який потім передається через функцію активації ReLU6;

$\max(0, \ldots)$ – ця частина функції відповідає за те, що вихідне значення не може бути меншим за 0. Якщо $F_{pw}(x, y)$ менше 0, результат буде 0, тобто негативні значення відсікаються, що є частиною стандартної функції ReLU;

$\min(\ldots, 6)$ – ця частина обмежує максимальне значення виходу на рівні 6. Якщо значення $F_{pw}(x, y)$ більше 6, то результат функції обмежується числом 6. Це специфічна властивість ReLU6, яка запобігає занадто великим значенням, що можуть негативно впливати на стабільність мережі.

Вираз (3.4) дозволяє:

– відсікання негативних значень через $\max(0, \ldots)$, запобігає проходженню негативних активацій далі по мережі;

– обмеження активацій зверху до 6 через $\min(\ldots, 6)$ допомагає зберігати стабільність обчислень, зменшуючи ймовірність перенасичення активацій, що особливо важливо для мобільних пристроїв і вбудованих систем.

Таким чином, вираз (3.4) визначає активацію для кожного елемента даних, обмежуючи вихід в межах [0, 6] для стабільної та ефективної роботи нейронної мережі. Завдяки такій обробці модель отримує набір ознак (Feature Map), що представляють ключові риси обличчя.

Наступним кроком необхідно зробити визначення ключових точок (Keypoint Detection) на обличчі людини. Кожна точка може бути описана координатами (x_i, y_i), де i відповідає номеру точки (наприклад, ліве око, праве око, ніс тощо). Якщо $P = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$ – це множина ключових точок, то модель має навчитися передбачати ці координати на основі отриманих ознак:

$$P = f(P_{out}), \tag{3.5}$$

де P – це координати ключових точок (наприклад, очей, носа, рота тощо) на обличчі або будь-які інші важливі особливості, які модель повинна передбачити. Це кінцевий результат, який генерує нейронна мережа після навчання. Як правило, це координати в 2D-просторі, виражені у вигляді пари (x, y) для кожної ключової точки;

f – це функція, яка відображає процес передбачення. Вона може бути частиною нейронної мережі, яка використовує різні нелінійні перетворення, згортки або повнозв'язні шари для того, щоб на основі отриманих ознак (фіч) визначити координати ключових точок. Функція f відповідає за обробку ознак і формування точних передбачень;

P_{out} – це ознаки (Feature Map або виходи попередніх шарів нейронної мережі), отримані після проходження зображення або даних через згорткові або інші шари моделі. Вони містять узагальнену інформацію про об'єкт на зображенні (в нашому випадку – обличчя), на основі якої і здійснюється передбачення. Ці ознаки описують структуру, текстури, контури, і на основі них модель будує передбачення координат.

Модель, представлена виразом (3.5), має навчитися передбачати координати ключових точок (P) на основі ознак, що описують об'єкт (P_{out}). Цей підхід дозволяє ефективно використовувати інформацію, отриману від зображення, для визначення точного розташування важливих точок (наприклад, рис обличчя) для подальшої ідентифікації або розпізнавання обличчя в автоматизованих системах контролю.

Отримавши координати ключових точок обличчя, система може порівняти їх з раніше збереженими шаблонами або пройти через наступний етап класифікації. При використанні MobileNetV2 для класифікації людини додається повнозв'язний шар:

$$\hat{y} = softmax(W_c \cdot F_{out} + b_c), \tag{3.6}$$

де $\hat{y}$ – це передбачуваний вихід моделі, тобто ймовірність належності вхідних даних до певного класу. У випадку класифікації людини це можуть бути різні класи, наприклад, конкретні особи. Вектор $\hat{y}$ містить ймовірності для кожного можливого класу, і сума всіх цих ймовірностей дорівнює 1 завдяки функції $softmax$;

$softmax$ – це функція активації, яка перетворює лінійну комбінацію ознак (результат $W_c \cdot F_{out} + b_c$) у ймовірності, які можна інтерпретувати як належність до кожного класу. Функція softmax нормалізує ці значення, щоб вони лежали в інтервалі від 0 до 1, і сума ймовірностей по всіх класах дорівнювала 1;

W_c – це матриця ваг повнозв'язного шару, що містить коефіцієнти, які застосовуються до ознак (F_{out}) для отримання кінцевих результатів перед класифікацією. Кожен рядок у матриці W_c відповідає окремому класу, і цей параметр навчається під час тренування моделі;

F_{out} – це вихід ознак, отриманий на попередніх шарах моделі. Ці ознаки є узагальненою інформацією, яка містить важливі характеристики об'єкта, зокрема обличчя. На основі цих ознак повнозв'язний шар виконує класифікацію;

b_c – це вектор зміщень (bias) для кожного класу. Зміщення додається до результатів лінійної комбінації $W_c \cdot F_{out}$ для кожного класу, що дозволяє моделі краще адаптуватися до даних і підвищити точність класифікації. Цей параметр також навчається під час тренування моделі.

Рівняння (3.6) описує процес класифікації у нейронній мережі, де повнозв'язний шар на основі ознак (F_{out}) генерує ймовірності належності до різних класів. Це ключовий етап в задачах ідентифікації, зокрема для розпізнавання осіб, коли модель визначає, до якого класу (особи) належить зображення обличчя.

Останній етап включає порівняння набору ознак або ключових точок поточного зображення зі збереженими шаблонами. Це можна зробити за допомогою обчислення евклідової відстані між векторами ознак:

$$d = \sqrt{\sum_{i=1}^{n}(P_i - T_i)^2}, \quad (3.7)$$

де d – евклідова відстань, яка є мірою схожості між двома векторами. Чим менше значення d, тим ближчі або подібніші вектори ознак, що відповідає більшій ймовірності того, що обидва вектори представляють одну і ту саму особу або об'єкт. Це результат обчислення, який використовується для класифікації або порівняння;

P_i – компоненти першого вектора ознак (наприклад, для поточного зразка), який був отриманий з нейронної мережі після обробки зображення обличчя. Кожен компонент вектора відповідає певній характеристиці або ознаці об'єкта (особи);

T_i – компоненти другого вектора ознак (еталонного або цільового вектора), з яким порівнюється перший вектор P_i. Це може бути вектор ознак для еталонного обличчя або шаблону, з яким проводиться порівняння;

n – кількість ознак або розмірність векторів. Це число визначає кількість компонентів, які використовуються для порівняння двох об'єктів. Вектор ознак зазвичай високорозмірний, і чим більша кількість ознак, тим точніше може бути порівняння;

$(P_i - T_i)$ – різниця між відповідними компонентами двох векторів ознак. Це різниця між конкретними ознаками двох порівнюваних об'єктів;

$(P_i - T_i)^2$ – квадрат різниці між відповідними компонентами векторів. Квадрат використовується для того, щоб зробити всі відхилення позитивними і посилити вплив більших відмінностей на загальну відстань.

Рівняння (3.7) використовується для обчислення відстані між векторами ознак двох об'єктів. У контексті розпізнавання обличчя, евклідова відстань d

дозволяє визначити, наскільки схожі або відрізняються обличчя. Мала відстань означає, що обличчя схожі, а велика відстань – що вони різні.

3.4 Обґрунтування вибору мови та середовища розробки

При розробці АСКПП на виробництві важливо правильно обрати мову програмування та середовище розробки, які будуть відповідати технічним вимогам проекту. Серед найбільш популярних мов програмування для таких задач виділяються Python, C++, Java та C#. Кожна з цих мов має свої переваги та недоліки.

Python є одним із найкращих виборів для розробки АСКПП через свою простоту, розвинуту екосистему бібліотек та модулів, які забезпечують швидку розробку програмного забезпечення. Основна перевага Python полягає в широкій підтримці наукових та нейронних бібліотек, таких як TensorFlow, Keras, та MediaPipe, які можуть бути використані для роботи з нейронною мережею MobileNetV2, що необхідна для розпізнавання облич. Окрім того, Python має модулі для роботи з COM-портами, такі як `pySerial`, що спрощує інтеграцію з апаратними пристроями, наприклад, RFID зчитувачами або замками. Важливою перевагою є підтримка Python на різних операційних системах, а також активна спільнота розробників.

C++ також широко використовується в промислових системах завдяки своїй високій продуктивності та контролю над апаратними ресурсами. Однак, розробка на C++ може бути складнішою та займати більше часу, особливо для реалізації та інтеграції нейронних мереж, де можуть знадобитися додаткові бібліотеки для машинного навчання.

Java та C# часто використовуються для розробки корпоративних рішень та десктопних додатків. Вони забезпечують високу продуктивність, але не мають такої потужної екосистеми для роботи з нейронними мережами та

машинним навчанням, як Python. Окрім того, інтеграція з COM-портами може бути складнішою порівняно з Python.

З огляду на всі ці фактори, вибір Python як мови програмування для розробки АСКПП є обґрунтованим рішенням. Це пояснюється можливістю легко працювати з нейронними мережами, такими як MobileNetV2, яка використовується для розпізнавання облич на базі ключових точок. MobileNetV2 є легкою моделлю для мобільних та вбудованих систем, що дозволяє швидко і ефективно розпізнавати обличчя при обмежених обчислювальних ресурсах.

Середовище розробки PyCharm є оптимальним вибором для роботи з Python, оскільки забезпечує повноцінний інструментарій для написання, налагодження та тестування коду. PyCharm має інтегровану підтримку для роботи з бібліотеками машинного навчання та нейронних мереж, а також забезпечує зручну інтеграцію з системами контролю версій та керування проектами. Це дозволяє ефективно працювати над великими проектами, зокрема такими, як АСКПП.

Також, для роботи з COM-портами в Python є доступні модулі, як-от `pySerial`, що дозволяє зчитувати дані з RFID-карток або інших пристроїв. Це критично важливо для роботи системи контролю пункту пропуску, де необхідно отримувати дані від фізичних пристроїв та приймати рішення на основі отриманої інформації [34].

Отже, поєднання мови програмування Python, середовища розробки PyCharm, нейронної мережі MobileNetV2 та можливості роботи з COM-портами забезпечує створення гнучкої, швидкої і ефективної автоматизованої системи контролю пункту пропуску. Це дозволить інтегрувати як сучасні методи біометричної ідентифікації, так і класичні RFID-технології для забезпечення безпеки та автоматизації на виробництві.

3.5 Розробка функцій розпізнавання обличчя людини

Розробка функцій розпізнавання обличчя людини є важливим етапом у створенні сучасних систем безпеки, ідентифікації користувачів та взаємодії з технічними засобами. Основним завданням такого процесу є коректне виявлення та аналіз ключових контрольних точок обличчя, які дозволяють відрізнити одного користувача від іншого. Для цього використовуються різні алгоритми та бібліотеки, зокрема MediaPipe, яка пропонує ефективний інструментарій для відстеження геометричних характеристик обличчя в режимі реального часу. Основна функціональність таких систем ґрунтується на порівнянні розташування контрольних точок з попередньо створеними зразками. Результати такого порівняння дають змогу визначити ступінь відповідності, що використовується для ухвалення рішень, наприклад, про надання доступу або ідентифікацію особи. Нижче приведемо фрагменти реалізації функції програми розпізнавання обличчя людини в рамках розробляємого макету АСКПП на виробництві:

- import cv2;
- import mediapipe as mp;
- import numpy as np.

Цей фрагмент коду імпортує необхідні бібліотеки для роботи з відео, зображеннями та розпізнаванням обличчя. cv2 використовується для роботи з відеопотоками та обробки зображень, дозволяючи читати та виводити відео. Бібліотека mediapipe застосовується для розпізнавання контрольних точок обличчя, забезпечуючи ефективне виявлення та трекінг обличчя в реальному часі. Numpy використовується для математичних операцій, таких як обчислення відстаней між контрольними точками обличчя для подальшого аналізу й порівняння:

mp_face_mesh = mp.solutions.face_mesh

face_mesh = mp_face_mesh.FaceMesh(static_image_mode=False, max_num_faces=1, min_detection_confidence=0.5)

Цей фрагмент коду відповідає за ініціалізацію модуля Mediapipe Face Mesh, який використовується для розпізнавання та відстеження обличчя. Він створює об'єкт face_mesh, який налаштовується на виявлення одного обличчя в кожному кадрі відео. Параметр static_image_mode=False вказує, що модуль працюватиме в режимі реального часу. max_num_faces=1 обмежує кількість розпізнаваних облич до одного, а min_detection_confidence=0.5 встановлює мінімальний поріг впевненості для успішного розпізнавання обличчя:

mp_drawing = mp.solutions.drawing_utils

Цей фрагмент коду відповідає за ініціалізацію модуля drawing_utils з бібліотеки Mediapipe, який використовується для візуалізації результатів розпізнавання. Він дозволяє малювати на зображенні контрольні точки або лінії, які відповідають положенню обличчя або інших об'єктів. Це допомагає користувачеві наочно бачити розпізнані риси обличчя в реальному часі. Завдяки цьому модулю програма може накладати графічні елементи, такі як сітки або контури, поверх відеопотоку:

```
def euclidean_distance(point1, point2):
    return np.linalg.norm(np.array(point1) - np.array(point2))
# Завантаження зразка контрольних точок обличчя для порівняння
sample_landmarks = np.load('venv/face_landmarks_sample.npy')
# Встановлюємо поріг для розпізнавання
RECOGNITION_THRESHOLD = 0.1
```

Цей фрагмент коду визначає функцію для обчислення евклідової відстані між двома точками у просторі, що дозволяє порівнювати позиції контрольних точок обличчя. Завантажується зразок контрольних точок обличчя з файлу для подальшого порівняння з новими даними, отриманими під час розпізнавання. Поріг для розпізнавання (RECOGNITION_THRESHOLD) визначає допустиму середню відстань між контрольними точками зразка та новими точками, при

якій система вважатиме обличчя ідентичним. Це важливо для точного розпізнавання та перевірки відповідності обличчя з певним шаблоном:

```
        # Перетворюємо кадр у RGB
        rgb_frame = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
        # Виконуємо обробку кадру для виявлення контрольних точок
        results = face_mesh.process(rgb_frame)
        if results.multi_face_landmarks:
            for face_landmarks in results.multi_face_landmarks:
                landmarks = []
                for lm in face_landmarks.landmark:
                    x = lm.x
                    y = lm.y
                    z = lm.z  # Додаємо координату Z для уникнення помилок
                    landmarks.append((x, y, z))
                # Перевірка чи обличчя відповідає зразку
            if is_face_matching(landmarks, sample_landmarks, RECOGNITION_THRESHOLD):
                cv2.putText(frame, "Access Granted", (50, 50), cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2, cv2.LINE_AA)
                else:
                cv2.putText(frame, "Access Denied", (50, 50), cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 0, 255), 2, cv2.LINE_AA)
                # Візуалізація контрольних точок
                mp_drawing.draw_landmarks(frame, face_landmarks, mp_face_mesh.FACEMESH_TESSELATION,
                                          landmark_drawing_spec=None,
                                          connection_drawing_spec=mp_drawing.DrawingSpec(color=(0, 255, 0),
```

```
                                                    thickness=1,
circle_radius=1))
        cv2.imshow('Face Recognition', frame)
```

Цей фрагмент коду спочатку перетворює кадр з формату BGR у RGB для подальшої обробки. Потім Mediapipe Face Mesh виконує розпізнавання контрольних точок обличчя, що повертає результати у вигляді списку точок на обличчі. Якщо обличчя було виявлено, контрольні точки зберігаються як координати (x, y, z). Далі, за допомогою функції порівняння, перевіряється, чи відповідають ці точки зразку обличчя, і залежно від результату на екран виводиться повідомлення "Access Granted" або "Access Denied". Окрім цього, контрольні точки візуалізуються на екрані для наглядності, відображаючи їх розташування на обличчі.

Розроблений програмний код для розпізнавання обличчя має кілька важливих переваг, які роблять його ефективним рішенням для АСКПП на виробництві. По-перше, використання бібліотек Mediapipe та OpenCV забезпечує швидку та точну обробку зображень у реальному часі. Це дозволяє системі оперативно розпізнавати обличчя співробітників, що підвищує ефективність роботи пункту пропуску. По-друге, алгоритм дозволяє виявляти ключові контрольні точки обличчя з урахуванням координат у просторі (x, y, z), що зменшує ймовірність помилок, пов'язаних з різними положеннями голови або кутами зйомки.

Третя перевага полягає в можливості порівняння зразків обличчя за допомогою евклідової відстані між контрольними точками, що робить процес розпізнавання більш точним і надійним. Порогове значення (Threshold), яке можна гнучко налаштовувати, забезпечує можливість адаптації алгоритму до різних умов виробничого середовища, таких як рівень освітлення чи якість відеопотоку. Завдяки цьому, система може працювати навіть у складних умовах, де якість зображення може бути компрометованою.

Іншою важливою перевагою є можливість налаштування системи для розпізнавання кількох осіб одночасно, що актуально для пунктів пропуску з високою інтенсивністю руху. Окрім цього, програмний код передбачає візуалізацію контрольних точок на обличчі, що полегшує процес налагодження та діагностики системи, дозволяючи оператору спостерігати, як система відстежує контрольні точки на обличчі в реальному часі.

Завдяки можливості відображати повідомлення "Access Granted" або "Access Denied", система може автоматично приймати рішення про допуск чи заборону доступу, що суттєво підвищує рівень безпеки на виробництві. Ця функціональність також дозволяє зменшити людський фактор у процесі контролю доступу, забезпечуючи більш надійний захист від несанкціонованого проникнення.

Загалом, розроблена система може легко інтегруватися у вже існуючі системи безпеки на підприємстві, використовуючи стандартні вебкамери або інші пристрої захоплення зображення. Такий підхід значно знижує витрати на обладнання та спрощує масштабування системи. Зручність у використанні, гнучкість налаштувань, а також висока точність і надійність алгоритму роблять цю систему ефективним інструментом для автоматизації процесу контролю доступу на підприємствах.

3.6 Висновки до третього розділу

У третьому розділі кваліфікаційної роботи було проведено комплексну розробку програмного забезпечення для автоматизованої системи контролю проходження пунктів пропуску на виробництві. Створено загальний алгоритм роботи системи, який інтегрує різні етапи ідентифікації, включаючи розпізнавання обличчя та обробку даних RFID-карток. В результаті аналізу обрано нейронну мережу MobileNetV2, яка продемонструвала високу точність і продуктивність для завдань розпізнавання облич. Алгоритм був вдосконалений

з урахуванням специфіки використання на виробничих об'єктах, що забезпечило зменшення часу обробки даних та підвищення надійності ідентифікації.

Розробка програмного забезпечення виконувалася із застосуванням Python, завдяки його потужній екосистемі бібліотек для роботи з нейронними мережами (TensorFlow, Keras) та обробки зображень (OpenCV).

Було реалізовано основні функції розпізнавання облич і перевірки відповідності біометричних даних, які забезпечують високу швидкість та точність роботи системи.

Обрані методи і технології дозволили створити ефективну програмну реалізацію, здатну до масштабування та інтеграції з іншими компонентами системи контролю доступу.

4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА АНАЛІЗ ОТРИМАНИХ РЕЗУЛЬТАТІВ

4.1 Постановка задач експерименту та умов проведення

Метою експерименту є перевірка точності та швидкості розпізнавання обличчя за допомогою розробленого програмного коду в умовах різного освітлення на виробничому пункті пропуску. Основними завданнями експерименту є:

– оцінити вплив рівня освітленості на точність розпізнавання обличчя;

– визначити час, необхідний для розпізнавання обличчя в реальному часі при різних умовах освітлення;

– виявити, як різні кути огляду та положення голови співробітника впливають на ефективність роботи системи;

– перевірити стійкість системи до зміни освітлення та якості відеопотоку;

– оцінити роботу системи за наявності сторонніх об'єктів або часткових перешкод (наприклад, маска, захисні окуляри);

– визначити оптимальні умови для ефективної роботи системи в реальних виробничих умовах.

Експерименти будуть проводитися на базі ноутбука Microsoft Surface Pro 4 з наступними параметрами: CPU Intel 6-го покоління Core i7; RAM – 16ГБ; SSD – 512 ГБ; GPU Intel Iris; Передня камера має роздільну здатність 5 мегапікселів і підтримує запис відео у форматі 1080p.

Умови експерименту. Освітленість, використовуватимуться різні рівні освітленості:

– низька (до 100 люкс) – темне приміщення або недостатнє освітлення;

– середня (від 100 до 500 люкс) – стандартне денне освітлення;

– висока (понад 500 люкс) – яскраве штучне або природне освітлення.

Кути огляду, випробування проводитимуться при різних положеннях голови:

– прямий погляд у камеру;

– легке відхилення голови вбік (15-30 градусів);

– погляд під кутом (45-60 градусів).

Перешкоди, перевірятиметься точність розпізнавання за наявності перешкод, таких як:

– часткове покриття обличчя (маска, захисні окуляри);

– наявність об'єктів на задньому плані.

Під час тестування системи розпізнавання обличчя важливо врахувати вплив різних факторів, які можуть вплинути на її ефективність. Один із таких факторів – освітленість приміщення. Для оцінки роботи системи потрібно провести серію тестів у різних умовах освітлення, визначити точність розпізнавання та час обробки кадру, а також виявити мінімальний рівень освітлення, за якого система здатна коректно функціонувати. Також слід провести тести на зміну положення голови співробітника, щоб визначити, як зміна кутів огляду впливає на точність роботи системи. Особливу увагу варто звернути на ситуації, коли частина обличчя закрита, наприклад, маскою або окулярами, і оцінити, наскільки ці перешкоди знижують ефективність розпізнавання. Крім того, важливо випробувати систему на здатність обробляти кілька облич одночасно, що дозволить визначити її продуктивність під час підвищеного навантаження. Останній аспект, який варто перевірити – це стійкість до раптових змін освітлення, наприклад, коли співробітник переходить із темного приміщення до яскраво освітленого простору, і швидкість адаптації системи до таких змін.

За результатами експериментів буде зроблено висновки щодо ефективності роботи системи розпізнавання обличь в умовах виробництва, та визначено оптимальні умови для її використання.

4.2 Проведення експерименту та отримання даних

Проведення експерименту з оцінки впливу рівня освітленості на точність розпізнавання обличчя в АСКПП має велике значення для підвищення ефективності та надійності цієї системи. Оскільки освітленість на виробництві може змінюватися, важливо визначити, як різні рівні освітлення впливають на здатність програми точно розпізнавати осіб. Зібрані дані допоможуть оптимізувати алгоритми обробки зображень, що підвищить точність і швидкість розпізнавання. Це, в свою чергу, забезпечить безпеку на пункті пропуску, зменшуючи ймовірність помилкових спрацьовувань або невизнання осіб. Експеримент також надасть можливість виявити оптимальні умови для роботи системи, адаптуючи її до реальних умов експлуатації. Результати дослідження можуть бути використані для вдосконалення не лише АСКПП, а й інших технологій розпізнавання облич, що важливо для розвитку автоматизованих систем в цілому. Таким чином, цей експеримент стане важливим кроком до створення більш надійних і ефективних систем контролю доступу. Отримані дані з проведеного експерименту оцінки впливу рівня освітленості на точність розпізнавання обличчя представлено в таблиці 4.1.

Таблиця 4.1 – Експеримент оцінки впливу рівня освітленості на точність розпізнавання обличчя

Номер експерименту	Освітленість (люкс)	Точність розпізнавання обличчя (%)
1	2	3
1	56	70
2	76	75
3	100	81
4	140	88
5	250	92
6	300	94

Продовження таблиці 4.1

1	2	3
7	400	97
8	500	93
9	650	91
10	700	89

Результати першого експерименту представлено у вигляді графіка на рисунку 4.1.

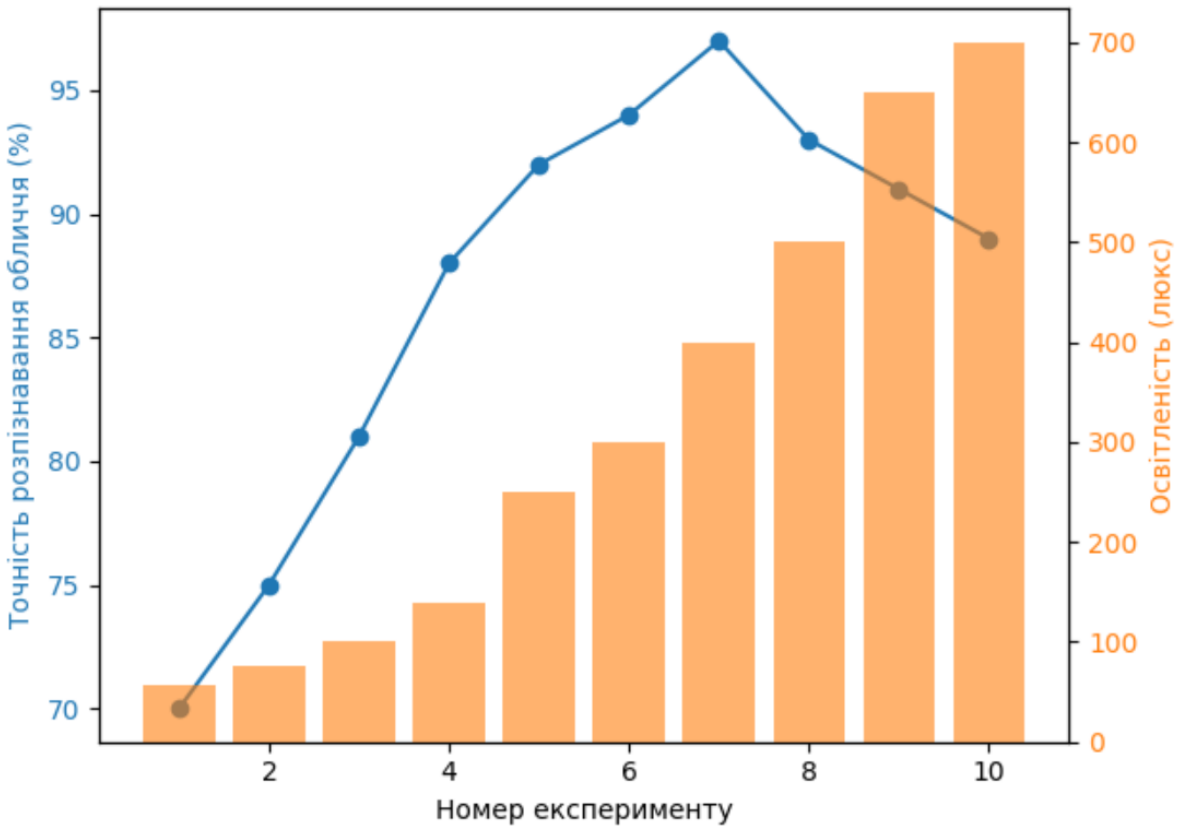


Рисунок 4.1 – Залежність точності розпізнавання обличчя від освітленності

В отриманих даних (таблиця 4.1 та рисунок 4.1) спостерігається позитивна кореляція між освітленістю в люксах і точністю розпізнавання обличчя. На початкових етапах експерименту, при освітленості 56 люкс, точність розпізнавання становила 70 %, що є досить низьким показником. З підвищенням освітленості до 140 люкс, точність розпізнавання покращується до 88 %. Однак після досягнення освітленості 400 люкс точність максимально

зростає до 97 %. Цікаво, що при освітленості 500 люкс точність знижується до 93 %, а при 650 і 700 люкс спостерігається незначне зниження до 91 % і 89 % відповідно. Це може свідчити про те, що надмірне освітлення може призводити до відблисків або інших оптичних артефактів, які негативно впливають на якість розпізнавання.

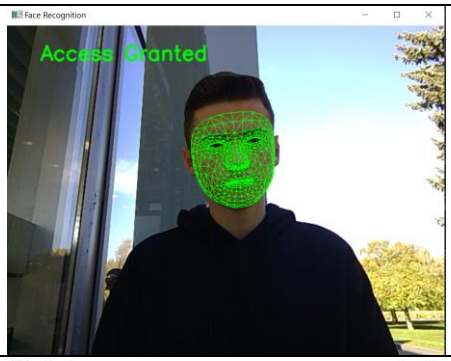
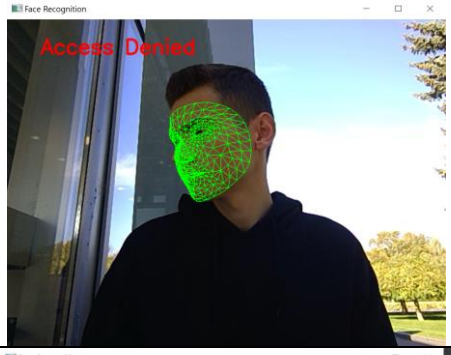
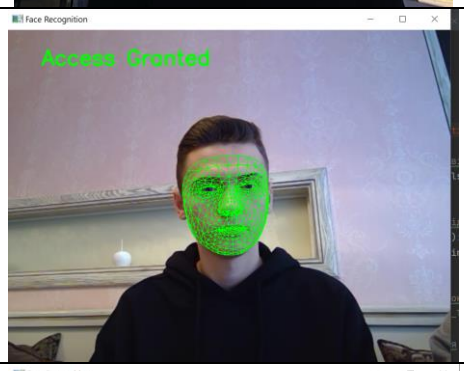
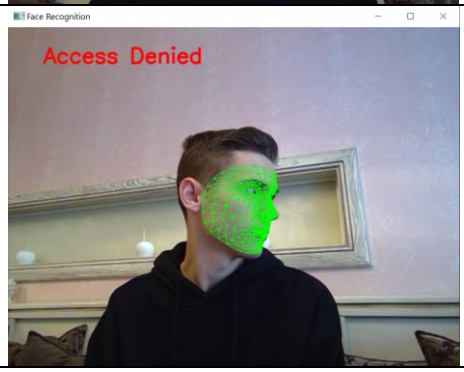
Загалом, дані підтверджують, що оптимальна освітленість є критично важливою для ефективної роботи системи розпізнавання обличчя, і показники точності демонструють чітку залежність від рівня освітленості в середовищі.

Проведення експерименту для оцінки швидкості розпізнавання обличчя в реальному часі при різних умовах освітлення є критично важливим для вдосконалення АСКПП на виробництві. Цей експеримент дозволить з'ясувати, як зміна освітлення впливає на швидкість обробки даних і ефективність роботи програмного забезпечення. Визначення оптимальних умов освітлення допоможе знизити затримки в розпізнаванні, що підвищить загальну продуктивність системи.

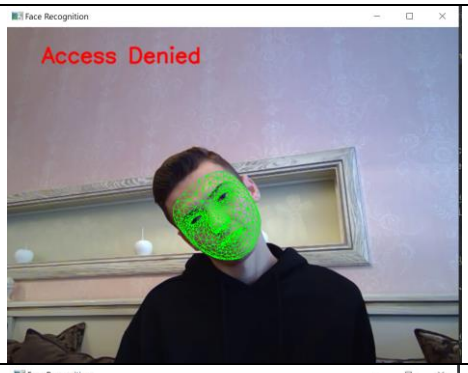
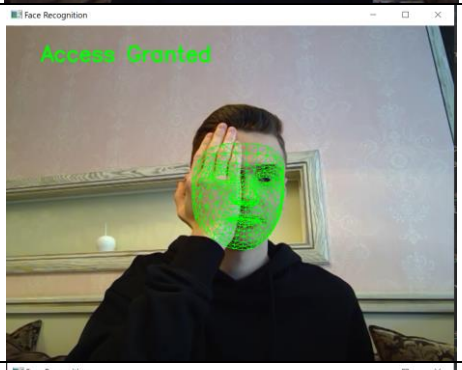
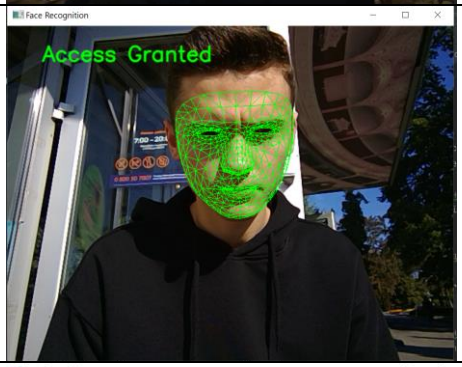
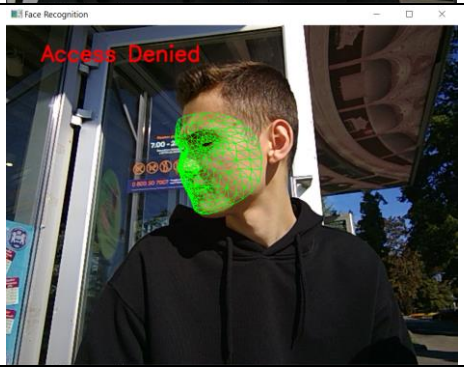
Швидкість розпізнавання має велике значення, оскільки вона безпосередньо впливає на оперативність обслуговування людей на пункті пропуску. Зібрані дані дозволять розробникам адаптувати алгоритми, щоб вони могли працювати ефективно в різних умовах. Це також сприятиме підвищенню точності розпізнавання, оскільки швидка реакція системи зменшує ймовірність помилок у ідентифікації.

Таким чином, результати експерименту можуть стати основою для поліпшення системи, що сприятиме безпеці та зручності користувачів. Усе це робить експеримент важливим кроком у розвитку сучасних технологій контролю доступу. Отримані результати експерименту з швидкості розпізнавання обличчя в реальному часі при різних умовах освітлення, представлено в таблиці 4.2.

Таблиця 4.2 – Швидкість розпізнавання обличчя в реальному часі при різних умовах освітлення

Номер експерименту	Зображення	Швидкість Розпізнавання (мс)	Освітленість (люкс)
1	2	3	4
1		100	56
2		90	76
3		78	100
4		70	140

Продовження таблиці 4.2

1	2	3	4
5		63	250
6		60	300
7		55	400
8		60	500
9		60	650
10		68	700

Результати другого експерименту представлено у вигляді графіка на рисунку 4.2.

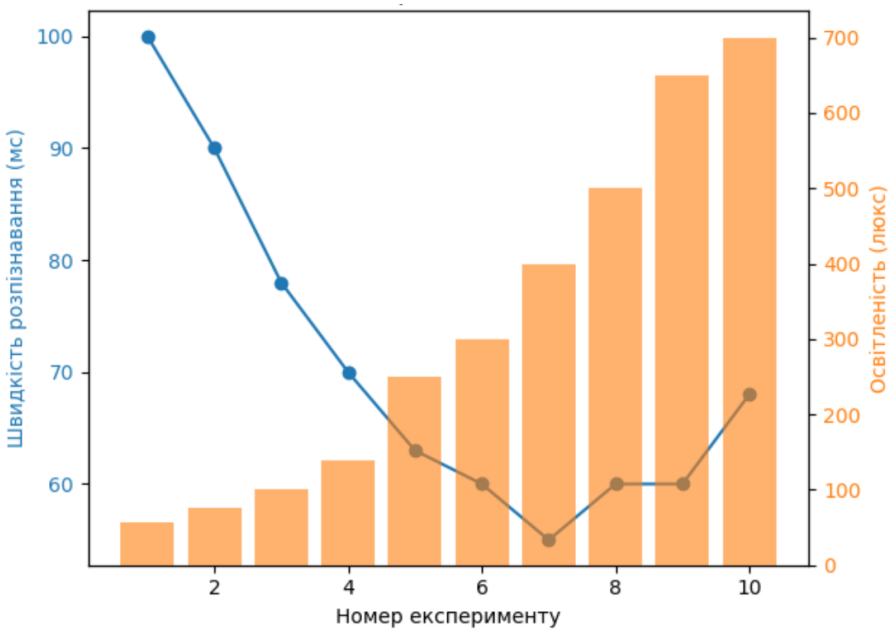


Рисунок 4.2 – Графік залежності швидкості розпізнавання обличчя від освітленості

Аналіз даних (таблиця 4.2 та рисунок 4.2), отриманих з другого експерименту, показує чітку залежність між швидкістю розпізнавання обличчя та рівнем освітленості. Починаючи з освітленості 56 люкс, швидкість розпізнавання становить 100 мс, що є найвищим показником. Як освітленість зростає до 140 люкс, швидкість розпізнавання знижується до 70 мс, вказуючи на те, що підвищення освітленості може ускладнити обробку зображення. При подальшому збільшенні освітленості до 250 люкс швидкість розпізнавання падає до 63 мс, а при 400 люкс – до 55 мс, досягаючи свого мінімуму. Варто помітити, що при освітленості 500 люкс швидкість розпізнавання відновлюється до 60 мс, що може свідчити про адаптивні можливості системи в умовах високої освітленості. Проте, при освітленості 650 і 700 люкс швидкість залишається сталою на рівні 60 і 68 мс відповідно. Загалом, ці дані свідчать про те, що оптимальна освітленість є критично важливою для забезпечення ефективної роботи системи розпізнавання облич. Висновки з даних можуть бути корисними для покращення алгоритмів обробки зображень, адаптуючи їх до змінних умов освітлення.

Проведення експерименту для виявлення впливу різних кутів огляду та положення голови співробітника на ефективність роботи АСКПП є важливим етапом у розробці програмного забезпечення. Цей експеримент дозволяє зрозуміти, як зміни в позиції голови впливають на точність і швидкість розпізнавання обличчя, що є критично важливим для функціонування системи. Визначення оптимальних кутів огляду допоможе підвищити надійність і ефективність системи, адже співробітники можуть перебувати в різних положеннях під час проходження контролю. Дослідження також дозволить виявити можливі проблеми, які можуть виникнути при специфічних положеннях голови, та розробити алгоритми для їх усунення. Зібрані дані можуть стати основою для адаптації системи до реальних умов роботи, що підвищить її продуктивність. Розуміння цих факторів також допоможе у створенні рекомендацій для користувачів щодо оптимального положення під час проходження контролю. Загалом, результати експерименту матимуть безпосередній вплив на покращення безпеки та зручності використання АСКПП на виробництві. Отримані результати експерименту виявлення, як різні кути огляду та положення голови співробітника впливають на ефективність роботи системи представлено у таблиці 4.3.

Таблиця 4.3 – Експеримент виявлення, як різні кути огляду та положення голови співробітника впливають на ефективність роботи системи

Номер експерименту	Кут огляду (градуси)	Точність розпізнавання (%)	Швидкість розпізнавання (мс)
1	0	96	55
2	15	90	61
3	20	85	66
4	30	74	69
5	45	0	-
6	50	0	-
7	60	0	-

Результати третього експерименту представлено у вигляді графіка на рисунку 4.3.

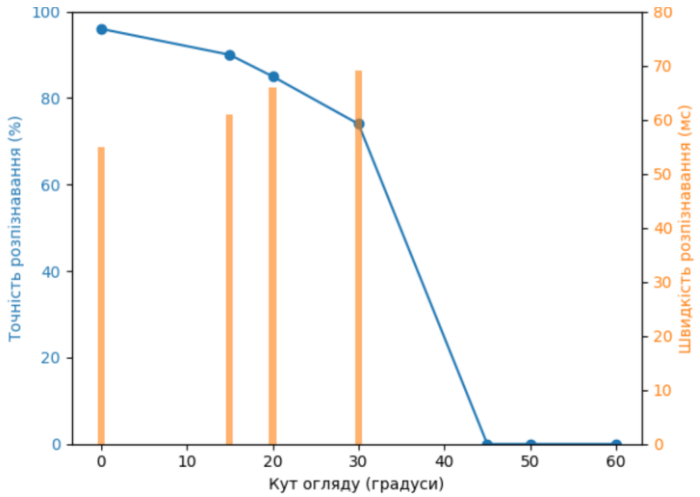


Рисунок 4.3 – Графік впливу кута огляду на точність і швидкість розпізнавання облич

В експериментах, що досліджували вплив кута огляду на точність та швидкість розпізнавання облич (таблиця 4.3 та рисунок 4.3), було проведено сім експериментів. Перші чотири експерименти, при кутах огляду від 0 до 30 градусів, показали високу точність розпізнавання, яка варіювалася від 96 % до 74 %. Це свідчить про те, що система ефективно розпізнає обличчя при безпосередньому та легкому боковому погляді. Проте, з відхиленням голови більше ніж 30 градусів, точність різко падає до 0 %.

Швидкість розпізнавання демонструє позитивну тенденцію: зменшення затримки з 55 мс при прямому погляді до 69 мс при 30 градусах. Однак при кутах огляду 45 градусів та більше система не змогла виконати розпізнавання, що призвело до відсутності даних по швидкості. Це вказує на те, що система потребує оптимізації для роботи з великими відхиленнями. Таким чином, результати свідчать про те, що система найбільш ефективна при невеликих кутах огляду, і для покращення її роботи необхідно враховувати фактори, які впливають на розпізнавання облич у нестандартних умовах.

Проведення дослідження впливу різних перешкод на точність розпізнавання обличчя є важливим кроком у вдосконаленні програмного забезпечення АСКПП. Це дослідження допомагає виявити, які конкретні перешкоди, такі як часткове покриття обличчя або наявність об'єктів на задньому плані, можуть негативно впливати на ефективність системи. Розуміння цих впливів дозволяє розробникам адаптувати алгоритми розпізнавання, щоб вони могли краще справлятися з такими ситуаціями. Завдяки цьому можна підвищити точність системи, що, у свою чергу, забезпечить більшу надійність контролю на пунктах пропуску. Результати дослідження також можуть слугувати основою для рекомендацій щодо покращення умов роботи системи, таких як оптимізація освітлення або уникнення певних розташувань об'єктів. Врешті-решт, це дозволить забезпечити безпечніший і ефективніший процес контролю для співробітників і відвідувачів підприємства, що є критично важливим для сучасних виробництв. Отримані результати експерименту дослідження вплив різних перешкод на точність розпізнавання обличчя приведені в таблиці 4.4.

Таблиця 4.4 – Результати четвертого експерименту, дослідження впливу різних перешкод на точність розпізнавання обличчя

Номер експер.	Тип перешкоди	Точність розпізнавання (%)	Примітки
1	2	3	4
1	Часткове покриття (маска)	80	Вплив на область рота та носа
2	Часткове покриття (захисні окуляри)	85	Вплив на область очей
3	Об'єкти на задньому плані (високі)	70	Деформація зображення
4	Об'єкти на задньому плані (низькі)	75	Погіршення контрасту
5	Часткове покриття (салонні окуляри)	72	Вплив на контури обличчя
6	Комбіновані перешкоди	65	Маска + об'єкти на задньому плані

Продовження таблиці 4.4

1	2	3	4
7	Наявність тіні на обличчі	78	Зменшення чіткості зображення
8	Змішане освітлення	73	Вплив на експозицію та кольори
9	Відблиски від стекол	68	Деформація зображення
10	Витягнуті форми на задньому плані	71	Деформація та відволікання уваги

Результати четвертого експерименту представлено у вигляді графіка на рисунку 4.4.

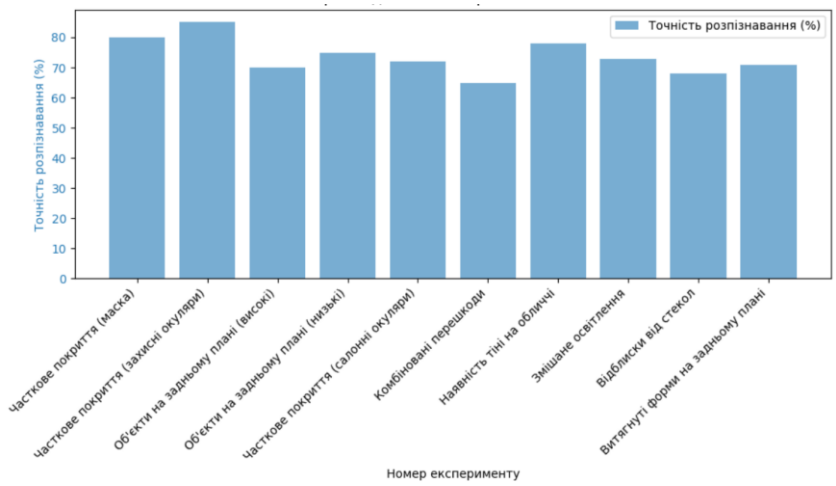


Рисунок 4.4 – Графік впливу перешкод на точність розпізнавання обличчя

В результаті проведених експериментів щодо впливу різних типів перешкод на точність розпізнавання обличчя (таблиця 4.4 та рисунок 4.4) було виявлено значні варіації в отриманих показниках. Найвищу точність розпізнавання (85 %) було зафіксовано при частковому покритті обличчя захисними окулярами, що свідчить про хорошу адаптивність системи до даного виду перешкоди. Натомість при частковому покритті маскою точність склала 80 %, що також демонструє відносно високий рівень розпізнавання, проте область рота та носа залишалася проблемною. З іншого боку, наявність високих об'єктів на задньому плані призвела до значного зниження точності до 70 %, що

вказує на критичний вплив фонових об'єктів на процес розпізнавання. Комбіновані перешкоди продемонстрували ще більшу проблемність, з точністю лише 65 %, що підтверджує, що накладення декількох перешкод суттєво погіршує результати. Зменшення чіткості зображення через тіні призвело до точності 78%, тоді як змішане освітлення зменшило точність до 73 %, що вказує на важливість контролю освітлення для системи розпізнавання. В цілому, отримані результати вказують на те, що тип і комбінація перешкод істотно впливають на ефективність розпізнавання обличчя, і для підвищення точності необхідно враховувати ці фактори в подальших розробках.

4.3 Аналіз отриманих даних та підготовка рекомендацій

Загальний аналіз отриманих результатів експерименту показує, що розроблена АСКПП має значний потенціал для ефективного розпізнавання обличчя. В результаті проведених досліджень були виявлені ключові фактори, які впливають на точність і швидкість розпізнавання.

Якісний аналіз показав наступні результати:

– вплив освітленості, результати експерименту показали, що підвищення рівня освітленості суттєво покращує точність розпізнавання облич. Найвища точність спостерігалася при максимальному рівні освітленості, що свідчить про важливість належного освітлення на пунктах пропуску. Це може бути критично важливим для функціонування системи в умовах різного природного та штучного освітлення;

– кути огляду, результати свідчать про те, що точність розпізнавання зменшується при відхиленні голови від прямого погляду. Значні відхилення (більше 30 градусів) призводять до різкого зниження ефективності системи. Це підкреслює необхідність налаштування камер для оптимального захоплення зображень облич при різних кутах;

– перешкоди, дослідження показали, що наявність часткового покриття обличчя або об'єктів на задньому плані може суттєво вплинути на точність. Найбільш значні втрати точності спостерігалися при комбінації маски та об'єктів на фоні. Це свідчить про важливість належної організації робочого простору на пунктах пропуску.

Цифровий аналіз показав наступні результати проведених експериментів, які приведено в таблиці 4.5.

Таблиця 4.5 – Зведена таблиця цифрового аналізу отриманих результатів проведених експериментів

Параметри	Аналіз
Точність розпізнавання	Максимальна точність при прямих кутах (96%).
	Зниження точності до 65% при комбінованих перешкодах
	Суттєве зниження (0%) при кутах огляду 45 градусів і більше
Швидкість розпізнавання	Найшвидше розпізнавання (55 мс) при прямому погляді.
	Зростання часу розпізнавання до 69 мс при відхиленні голови до 30 градусів
	Час розпізнавання збільшується до недоступності (не визначено) при кутах 45 градусів і більше

Виходячи з отриманих даних при проведенні експериментів над розробленим макетом автоматизованої системи контролю проходження пунктів пропуску на виробництві можна запропонувати наступні рекомендації, які приведено в таблиці 4.6.

Таблиця 4.6 – Рекомендації

Параметр	Рекомендацій
1	2
Оптимізація освітлення	Рекомендується забезпечити стабільне та рівномірне освітлення на всіх пунктах пропуску, що дозволить підвищити точність системи

Продовження таблиці 4.6

1	2
Налаштування камер	Систему потрібно обладнати камерами, здатними до адаптації при зміні кута огляду, або використовувати декілька камер для покриття різних напрямків
Планування простору	Необхідно мінімізувати можливі перешкоди в полі зору камер. Рекомендується проводити регулярні перевірки і очищення території, щоб уникати відволікань, які можуть знижувати точність розпізнавання
Інструктаж персоналу	Персонал на пунктах пропуску повинен бути навчений правилам поведінки при проходженні контролю, зокрема про необхідність уникати швидких рухів головою та використання предметів, що закривають обличчя
Оцінка ефективності	Регулярний моніторинг і оцінка ефективності системи в реальних умовах експлуатації допоможе вчасно виявляти проблеми і коригувати налаштування для покращення результатів

Загалом, отримані дані підтверджують доцільність використання розробленого макету АСКПП, проте для досягнення максимальної ефективності слід вжити заходів для покращення умов роботи системи.

4.4 Охорона праці

Забезпечення безпеки праці під час розробки та експлуатації автоматизованих систем контролю доступу є важливою складовою успішного виконання проєкту. Основні аспекти охорони праці включають забезпечення безпеки роботи з апаратним обладнанням, мінімізацію впливу електромагнітного випромінювання, організацію робочих місць розробників програмного забезпечення та забезпечення ергономічності. Основні ризики, пов'язані з роботою над системою, включають можливість ураження електричним струмом, травмування під час роботи з інструментами та устаткуванням, а також вплив електромагнітного випромінювання від

обладнання. Крім того, довготривала робота за комп’ютером може викликати зорове та фізичне перенапруження. При роботі з апаратними модулями необхідно дотримуватись правил електробезпеки. Роботи з підключенням системи виконуються при відключеному живленні. Для захисту користувачів і обладнання встановлюються автоматичні вимикачі та заземлення корпусу системи.

Для забезпечення комфортних умов роботи виконується розрахунок штучного освітлення. Для розрахунку використовуємо формулу:

$$E = \Phi \cdot N / S, \tag{4.1}$$

де E – освітленість, лк;

Φ – світловий потік однієї лампи, лм;

N – кількість ламп;

S – площа приміщення, м².

Припустимо, площа приміщення — 12 м², використовується 4 лампи зі світловим потоком 1600 лм кожна.

$$E = 1600 \cdot 4 / 12 = 533 \text{ лк}.$$

Отримане значення відповідає нормам для робочих приміщень (не менше 500 лк).

Обладнання, що використовується, має відповідати нормам щодо рівня електромагнітного випромінювання. Для зменшення впливу необхідно дотримуватись безпечних відстаней між джерелами випромінювання та користувачами. Також рекомендовано використовувати екрановані кабелі [35].

4.5 Висновки до четвертого розділу

У четвертому розділі кваліфікаційної роботи було виконано експериментальні дослідження функціонування автоматизованої системи контролю проходження пунктів пропуску на виробництві. В рамках постановки задач експерименту визначено ключові метрики для оцінювання ефективності системи: точність розпізнавання обличь, швидкість обробки даних та надійність ідентифікації.

Проведення експерименту здійснювалося в умовах, максимально наближених до реальних виробничих сценаріїв, з урахуванням різних зовнішніх факторів, таких як освітлення, кут огляду та зайві перешкоди.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було досягнуто поставлену мету – підвищення ефективності системи доступу до виробничого приміщення за рахунок удосконалення технології контролю.

У першому розділі проведено аналіз структури та призначення автоматизованої системи контролю проходження пунктів пропуску, аналіз аналогічних автоматизованих систем контролю, аналіз методів ідентифікації людини при проходженні пунктів контролю доступу та аналіз апаратного забезпечення пункту контролю проходження пунктів пропуску на виробництві. За результатами аналізу у другому розділі запропоновано структуру макету та здійснено опис призначення структурних блоків, проведено аналіз та вибір апаратних модулів для розробки макета системи контролю проходження пунктів пропуску, розроблено схему підключення та зібрано макет системи контролю проходження пунктів пропуску.

Третій розділ присвячено розробці загального алгоритму роботи системи контролю проходження пунктів пропуску. У ньому проведено аналіз та вибір нейронної мережі для розпізнавання обличчя людини за особливостями їх рис, удосконалено метод розпізнавання обличчя людини на базі нейронної мережі MobileNetV2. Для її реалізації попередньо проведено обґрунтування вибору мови та середовища розробки, що дозволило реалізувати функції розпізнавання обличчя людини. У четвертому розділі було проведено експериментальні дослідження та проаналізовано отримані результати.

Експериментальні дослідження підтвердили ефективність обраного підходу, продемонструвавши високу точність розпізнавання обличь та швидкість обробки даних.

Результати кваліфікаційної роботи пройшли апробацію на двох наукових конференціях [4-5].

Отримані результати роботи можна віднести до Цілі сталого розвитку 9 «Промисловість, інновації та інфраструктура», а саме 9.4 «Сприяти прискореному розвитку високо- та середньовисокотехнологічних секторів переробної промисловості, які формуються на основі використання ланцюгів «освіта – наука – виробництво» та кластерного підходу за напрямами: розвиток інноваційної екосистеми; розвиток інформаційнотелекомунікаційних технологій (ІКТ); застосування ІКТ в АПК, енергетиці, транспорті та промисловості; високотехнологічне машинобудування; створення нових матеріалів; розвиток фармацевтичної та біоінженерної галузей» [36].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ДСТУ 3008: 2015. Документація. Звіти у сфері науки та техніки. структура та правила оформлення. Введ. 2015-06-22. К. Держстандарт України, 2017. 29 с.

2. Невлюдов І.Ш. Дипломне проектування для студентів усіх форм навчання спеціальностей 151 «Автоматизація та комп'ютерно-інтегровані технології» [Текст]: навч. посіб. / І.Ш. Невлюдов, А.О. Андрусевич, О.В. Токарєва, Г.В. Пономарьова. Київ-58, пр. Космонавта Комарова, 1, 2016. 320 с.

3. Методичні вказівки з підготовки та захисту кваліфікаційної роботи здобувачами другого (магістерського) рівня вищої освіти спеціальності 174 Автоматизація та комп'ютерно-інтегровані технології, освітньо-професійних програм: «Автоматизоване управління технологічними процесами»; «Комп'ютерно-інтегровані технологічні процеси і виробництва»; «Комп'ютеризовані та робототехнічні системи» / Упоряд.: І. Ш. Невлюдов Р. В. Артюх В. В. Безкоровайний Н. П. Демська В. В. Євсєєв О. І. Филипенко О. М. Цимбал. Харків: ХНУРЕ, 2021. 55 с.

4. Horban A. Development of an Automated Access Control and Management System for Enhanced Security in Industrial Facilities / A. Horban // Digital innovation & sustainable development 2024 : Proceedings of I-st International Conference, November 15, 2024. Kharkiv, 2024. P. 14-15.

5. Горбань А. Ю., Безкоровайний В. В. Структурний синтез системи контролю доступу на промислових об'єктах / А. Горбань // Комп'ютерно-інтегровані технології автоматизації технологічних процесів на транспорті та у виробництві. Матеріали всеукраїнської науково-практичної конференції здобувачів вищої освіти і молодих учених. – Харків, ХНАДУ, 2024. С. 146–149.

URL: https://mf.khadi.kharkov.ua/departments/avtomatizaciji-ta-kompjuterno-integrovanikh-tekhnologii/konferencija-kit/ (дата звернення: 15.12.2024).

6. Beskorovainyi V., Kolesnyk L., Chinwi Mgbere Dr. Mathematical models for determining the Pareto front for building technological processes options under the conditions of interval presentation of local criteria // Innovative Technologies and Scientific Solutions for Industries. 2023. No. 2 (24). P. 16–26. URL: https://www.itssi-journal.com/index.php/ittsi/article/view/386 (дата звернення: 14.11.2024).

7. Сидорович, О. (2023). Проблематика використання новітніх інформаційно-комунікаційних технологій у митному просторі України. Світ фінансів, (4 (73)), 89-101.

8. Ковальов І. О. Розроблення засобів автоматизації теплових пунктів із застосуванням технології IoT : пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 151 - Автоматизація та комп`ютерно-інтегровані технології / І.О. Ковальов ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки, кафедра Комп’ютерно-інтегрованих технологій, автоматизації та мехатроніки. Харків, 2021. 84 с.

9. Bezkorovainyi V., Kolesnyk L., Gopejenko V., Kosenko V. The method of ranking effective project solutions in conditions of incomplete certainty // Advanced Information Systems, 2024. v. 8, no 2. P 27–38. URL: http://ais.khpi.edu.ua/article/view/305462/297067 (дата звернення 15.11.2024).

10. Комплексні системи безпеки для вашого бізнесу // ParSec, 2024. URL: https://parsec.com.ua/ (дата звернення: 10.11.2024).

11. Lenko, F. (2021). Specifics of RFID based access control systems used in logistics centers. Transportation Research Procedia, 55, 1613-1619.

12. Yusupbekov, N., Adilov, F., Astafurov, M., & Ivanyan, A. (2023, August). Honeywell Experion HIVE as breakthrough approach in control systems evolution.

In International Conference on Intelligent and Fuzzy Systems (pp. 19-25). Cham: Springer Nature Switzerland.

13. Тітова, В., Кльоц, Ю., Мостовий, . С., & Колісник, В. (2023). Система контролю та управління доступом на основі rfid-технологій. Measuring and computing devices in technological processes, (4), 44–48. https://doi.org/10.31891/2219-9365-2023-76-5.

14. Усенко, В. В. Система контролю доступу з розпізнаванням облич: магістерська дис.: 126 Назва спеціальності Інформаційні системи та технології / Усенко Вадим Вікторович. Київ, 2024. 103 с.

15. Podvisotsky O. Methods and tools for biometric user identification in a smart home system : Master Thesis „123 — Computer Engineering“ / Oleksandr Podvisotsky. Ternopil, TNTU, 2023. 75 p.

16. Beskorovainyi V. V., Petryshyn L. B., Shevchenko O. Yu. Specific subset effective option in technology design decisions // Applied Aspects of Information Technology. 2020. Vol. 3. No.1. P. 443–455. URL: https://aait.op.edu.ua/?fetch=articles&with=info&id=40 (дата звернення: 16.11.2020).

17. Beskorovainyi V. Combined method of ranking options in project decision support systems // Innovative Technologies and Scientific Solutions for Industries. 2020. No 4 (14). P. 13–20. URL: http://journals.uran.ua/itssi/article/view/ITSSI.2020.14.013 (дата звернення 16.11.2024).

18. Бєльский А. С. Автоматизована охоронна система для комерційних приміщень : робота на здобуття кваліфікаційного ступеня бакалавра : спец. 151 – автоматизація та комп’ютерно-інтегровані технології / наук. кер. В. О. Журба. Суми : Сумський державний університет, 2023. 71 с.

19. Гузенко Б. М. Автоматизований моніторинг доступу до виробничого приміщення на основі однопалатного комп’ютера Raspberry Pi : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому

(магістерському) рівні, спеціальність 151 – Автоматизація та комп`ютерно-інтегровані технології / Б. М. Гузенко ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків, 2022. 122 с.

20. Yevsieiev, V., Abu-Jassar, A., Maksymova, S., & Gurin, D. (2024). Human Operator Identification in a Collaborative Robot Workspace within the Industry 5.0 Concept. Multidisciplinary Journal of Science and Technology, 4(9), 95-105.

21. Moiseev, M., Maksymova, S., Yevsieiev, V., & Alkhalaileh, A. (2024). Program Algorithm for Monitoring System Development. Journal of Universal Science Research, 2(7), 33–43. Retrieved from https://inlibrary.uz/index.php/universal-scientific-research/article/view/36023.

22. Nevliudov, I. S., Yevsieiev, V. V., Maksymova, S. S., Omarov, A. O. M., & Klymenko, O. M. (2023). Conveyor Belt Object Identification: Mathematical, Algorithmic, and Software Support.

23. Nataliya, M., & Olexander, P. (2024). Development of a cyberphysical system for monitoring fire safety. System technologies, 1(150), 100-107.10.

24. Web камера Logitech C920x Pro HD (960-001335) // Сайт ELMIR, 2024. URL: https://elmir.ua/ua/web_camera/web-camera-logitech-c920x-pro-hd-960001335.html?gclid=Cj0KCQjwm5e5BhCWARIsANwm06ha4WDmD7uQF1Bny9tKKnlw2RHxn1tJPVZoxpdhfB71MmR7Jf466N8aApivEALw_wcB (дата звернення: 14.10.2024).

25. Web камера Logitech C920x Pro HD (960-001335) // Сайт ELMIR, 2024. URL: https://elmir.ua/ua/web_camera/web-camera-logitech-c920x-pro-hd-960001335.html?gclid=Cj0KCQjwm5e5BhCWARIsANwm06g3RvTliyzkrMUgmZKs2amLr6H26OGinNapo1nTZqE_tr_DBuR3RYaAu3mEALw_wcB (дата звернення: 14.10.2024).

26. Web камера Razer Kiyo (RZ19-02320100-R3M1) // Сайт ELMIR, 2024. URL: https://elmir.ua/ua/web_camera/web_camera_razer_kiyo_rz19-02320100r3m1.html?gclid=Cj0KCQjwm5e5BhCWARIsANwm06hK6NqcywqdypEl

vRzPR97wfxF_wdFaD50TW6uLRrNCWJ-aIi1GIDEaAsdrEALw_wcB (дата звернення: 14.10.2024).

27. RFID набір з тегами RC522 // Сайт МікроАмпер, 2024. URL: https://uamper.com/index.php?route=product/product&path=224&product_id=127&gad_source=1&gclid=Cj0KCQjwm5e5BhCWARIsANwm06iFAD5IrTjrAsv0qJZEvRSv4w5gdGlJy0F3vV-aWtFer7hjwoyz4aAnyyEALw_wcB (дата звернення: 15.10.2024).

28. Модуль nfc pn532 13,56 мгц для arduino // Сайт Електроніка, 2024. URL:https://electronica.in.ua/p2202568417modulnfcpn532.html?source=merchant_center&utm_source=google&utm_medium=cpc&utm_campaign=20496384634&utm_term=&utm_content=&utm_position=&utm_matchtype=&utm_placement=&utm_network=x&gad_source=1&gclid=Cj0KCQjwm5e5BhCWARIsANwm06iNKGN0WtDkw_4qZ2ENMvP7UlUuFyih3j3BsCWvzqAytV7KuFWaQJYaAn6OEALw_wcB (дата звернення: 15.10.2024).

29. RFID модуль 125 кГц (RDM6300) // Сайт МікроАмпер, 2024. URL: https://uamper.com/index.php?route=product/product&path=224&product_id=459&gad_source=1&gclid=Cj0KCQjwm5e5BhCWARIsANwm06iSl9rKo8rCAGoFTo-PEeh7dlvH_yNnUzvHfPgAj2WWLqhpGDpgoe0aAlfrEALw_wcB (дата звернення: 15.10.2024).

30. Arduino Nano V3 розпаяна з кабелем // Сайт МікроАмпер, 2024. URL:https://uamper.com/index.php?route=product/product&path=60&product_id=335&gad_source=1&gclid=Cj0KCQjwm5e5BhCWARIsANwm06jwev2sbEU9eiLVooORS2wUJNtT8beJuQQBR3juQJc7uNb6jwobcKIaArx9EALw_wcB (дата звернення: 17.10.2024).

31. Arduino Pro Mini 5V // Сайт МікроАмпер, 2024. URL:https://uamper.com/index.php?route=product/product&path=60&product_id=27&gad_source=1&gclid=Cj0KCQjwm5e5BhCWARIsANwm06gNYnZnIlvLoBfO15wmVgMnpoD-0DBuj6pp_4L7wC9XDnS7U8Iqu28aAg6pEALw_wcB (дата звернення: 17.10.2024).

32. Arduino Pro Micro // Сайт МікроАмпер, 2024. URL: https://uamper.com/index.php?route=product/product&path=60&product_id=204&gad_source=1&gclid=Cj0KCQjwm5e5BhCWARIsANwm06iOJb0vSsrJno3q1dH3oVchtgs-c4QKHkzJJRsDua9g3abuw4-FH4kaAkYMEALw_wcB (дата звернення: 17.10.2024).

33. 1-канальный модуль реле 12V для Arduino PIC ARM // Сайт Evse.com.ua, 2024. URL: https://evse.com.ua/ru/1-kanalnyj-modul-rele-12v-dlya-arduino-pic-arm?gclid=Cj0KCQjwm5e5BhCWARIsANwm06hkZHYM_JbN-YeWHQMDjHzssKggH-n2rGi1BeIW418fw-4NzQzAbXgaAuJlEALw_wcB (дата звернення: 05.12.2024).

34. Python // Python, 2024. URL: https://www.python.org/ (дата звернення: 28.11.2024).

35. Охорона праці на виробництві // Сайт GCC, 2024. URL: https://gc.ua/uk/oxorona-pracivofisivimogidorobochogomiscyaofisnogopracivnika/ (дата звернення: 10.12.2024).

36. Ціль 9. Промисловість, інновації та інфраструктура // Diia business, 2024. URL: https://business.diia.gov.ua/entrepreneur-handbook/item/cil_9_promislovist_innovaciyi_ta_infrastruktura (дата звернення: 15.12.2024).