

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка програмного забезпечення пропускнуої системи з використанням штучного інтелекту»

Здобувача вищої освіти першого (бакалаврського) рівня,
IV курсу, групи КБ-20-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології (за галузями)»



(підпис)

Ковпака Дениса
Васильовича

(прізвище, ім'я, по батькові)

Науковий керівник



(підпис)

Редич Олександр
Володимирович, к.е.н.

(прізвище, ім'я, по батькові,
науковий ступінь, вчене звання)

Керівник освітньо-
професійної програми



(підпис)

Омельчук Антон
Анатолійович, к.т.н.

(прізвище, ім'я, по батькові, науковий
ступінь, вчене звання)

Допущено до захисту за рішенням кафедри комп'ютерних та інформаційних
технологій і систем протокол від «22» травня 2024 №15

Завідувач кафедри



(підпис)

Філоненко Михайло
Миколайович, к.ф.-м.н.,

доцент

(прізвище, ім'я, по батькові,
науковий ступінь, вчене звання)

Реєстрація № 25

24.05.2024

(дата)



(підпис відповідальної особи)

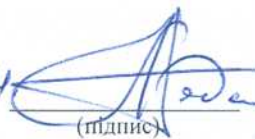
Результати перевірки

до захисту

(до захисту, на доопрацювання)

22.05.24

(дата)



(підпис)

Результат захисту

5 (відмінно)

(оцінка)

06.06.2024

(дата)



(підпис)

Голова комісії:



(підпис)

В.М. Франчук

Члени комісії:



(підпис)

М.М. Філоненко



(підпис)

С.М. Грищенко



(підпис)

В.О. Ніжегородцев

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	30		06.06.2024 Франчук В.М. <i>В.М.</i> Філоненко М.М. <i>М.М.</i> Грищенко С.М. <i>С.М.</i> Ніжегородцев В.О. <i>В.О.</i> Суховерхівка Л.П. <i>Л.П.</i>
2. Дотримання вимог щодо оформлення	від 0 до 10	9		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	5		
4. Рецензент	від 0 до 5	5		
РАЗОМ БАЛІВ	від 0 до 50	49		

Оцінювання кваліфікаційної роботи науковим керівником - 49 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
98	A	5 (відмінно)	06.06.2024	Франчук В.М. <i>В.М.</i> Філоненко М.М. <i>М.М.</i> Грищенко С.М. <i>С.М.</i> Ніжегородцев В.О. <i>В.О.</i> Суховерхівка Л.П. <i>Л.П.</i>

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	
50-59	E	3 (задовільно)
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
Кафедра комп'ютерних та інформаційних технологій і систем
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 122 «Комп'ютерні науки»
Освітня програма: «Інформаційні управляючі системи і технології (за галузями)»

Затверджую

Завідувач кафедри  Філоненко М.М.
«23» жовтня 2023

**Завдання на кваліфікаційну роботу
здобувачу вищої освіти**

Ковпаку Денису Васильовичу

(прізвище, ім'я, по батькові)

Затверджена наказом ректора від «20» жовтня 2023 № 1411

1. Тема кваліфікаційної роботи «Розробка програмного забезпечення пропускнуої системи з використанням штучного інтелекту»

Затверджена наказом ректора від «20» жовтня 2023 № 1411

2. Строк здачі закінченої роботи «20» травня 2024

3. Мета роботи: розробка та реалізація модулю пропускнуої системи для розпізнавання облич з використанням штучного інтелекту

Об'єкт дослідження: системи контролю допуску та технології розпізнавання облич

Предмет дослідження: системи керування допусками на об'єкт за допомогою камер відеоспостереження та веб-серверів з обробкою даних облич. Технології згорткових нейромереж глибокого навчання (CNN) та Open CV

Орієнтовна база дослідження: інфраструктура ДПУ як об'єкт впровадження системи доступу

4. Вихідні дані до роботи: база даних сканованих облич працівників, студентів ДПУ

5. Перелік графічного матеріалу: рисунки та графіки, формули, що пояснюють суть застосованих методів та засобів. Структурні схеми та таблиці, графіки результатів моделювання

6. Зміст кваліфікаційної роботи (перелік питань за кожним розділом)

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ АСПЕКТИ РОЗРОБКИ СИСТЕМ ДОПУСКУ

1.1. Існуючі системи контролю доступу

1.2. Розвиток штучного інтелекту в сфері розпізнавання об'єктів та облич

1.3. Огляд технологій для розробки програмного забезпечення

РОЗДІЛ 2. ПРОЄКТУВАННЯ, РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1. Проектування системи контролю доступу

2.2. Моделювання системи розпізнавання облич

2.3. Компонування системи розпізнавання облич з системою контролю доступу

РОЗДІЛ 3. ОЦІНКА ТА ТЕСТУВАННЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1. Тестування системи контролю доступу

3.2. Тестування системи розпізнавання облич

3.3. Тестування скомп'юованої системи контролю доступу з розпізнаванням облич

7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури кваліфікаційної роботи	До 15.10.2023	15.10.2023
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	29.12.2023	29.12.2023
3	II розділ (аналіз експериментальної частини про методики досліджень)	15.02.2024	15.02.2024
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	15.04.2024	15.04.2024
5	Висновки	01.05.2024	01.05.2024
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	06.05.2024	06.05.2024
7	Отримання відгуку керівника	28.05.2024	28.05.2024
8	Отримання зовнішньої рецензії	30.05.2024	30.05.2024

8. Дата видачі завдання «23» жовтня 2023

9. Керівник кваліфікаційної роботи


(підпис)

О.В. Редич

10. Керівник освітньо-професійної програми


(підпис)

А.А. Омельчук

11. Завдання до виконання отримав здобувач вищої освіти


(підпис)

Д.В. Ковпак

АНОТАЦІЯ

Метою даної кваліфікаційної роботи на тему «Розробка програмного забезпечення пропускнуої системи з використанням штучного інтелекту» є розробка системи контролю доступу, для підвищення рівня безпеки працівників та студентів в Державному податковому університеті.

Завданням роботи є вивчення сучасних методів і технологій для створення безпечної та ефективної системи контролю доступу, що здатна розпізнавати обличчя користувачів і приймати рішення в режимі реального часу.

Предметом дослідження є технології штучного інтелекту та методи розпізнавання облич, які застосовуються для автоматизації процесу контролю доступу.

Об'єктом дослідження є процес розробки, тестування та впровадження системи контролю доступу з використанням методів штучного інтелекту.

Базою дослідження є теоретичні аспекти розпізнавання облич та практичні підходи до створення інтегрованих систем безпеки, з особливою увагою до архітектури системи, алгоритмів розпізнавання, методів захисту персональних даних та інтеграції нових рішень у існуючу інфраструктуру.

За результатами дослідження сформульовані рекомендації щодо впровадження системи контролю доступу на основі штучного інтелекту в різних організаціях, а також визначені перспективи подальшого розвитку таких систем у сфері інформаційних технологій.

Одержані результати можуть бути використані для підвищення рівня безпеки та ефективності управління доступом у різних установах.

Ключові слова: система контролю доступу, штучний інтелект, розпізнавання облич, безпека, інтеграція, бази даних, серверні системи, мережеві технології.

Кваліфікаційна робота містить 52 сторінки, 11 рисунків, 3 додатки.

Рік виконання кваліфікаційної роботи: 2024.

Рік захисту роботи: 2024.

ABSTARCTS

The purpose of this qualification work on the topic “Development of access control system software using artificial intelligence” is to develop an access control system using artificial intelligence to improve the security of employees and students at the State Tax University.

The task of the work is to study modern methods and technologies for creating a secure and efficient access control system capable of recognizing users' faces and making real-time decisions.

The subject of the research is artificial intelligence technologies and face recognition methods applied to automate the access control process.

The object of the research is the process of developing, testing, and implementing an access control system using artificial intelligence methods.

The research base includes theoretical aspects of face recognition and practical approaches to creating integrated security systems. Special attention is paid to studying the system architecture, recognition algorithms, personal data protection methods, and the integration of new solutions into the existing infrastructure.

The research results formulate recommendations for implementing an artificial intelligence-based access control system in various organizations and identify the prospects for further development of such systems in the field of information technology.

The obtained results can be used to enhance security and access management efficiency in various institutions.

Keywords: access control system, artificial intelligence, face recognition, security, integration, databases, server systems, network technologies.

The qualification work contains 52 pages, 11 figures, 3 appendices.

Year of completion: 2024.

Year of defense: 2024.

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ АСПЕКТИ РОЗРОБКИ СИСТЕМ ДОПУСКУ.....	6
1.1. Існуючі системи контролю доступу.....	6
1.2. Розвиток штучного інтелекту в сфері розпізнавання об'єктів та облич.....	10
1.3. Огляд технологій для розробки програмного забезпечення.....	13
РОЗДІЛ 2. ПРОЄКТУВАННЯ, РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ.....	18
2.1. Проектування системи контролю доступу.....	18
2.2. Компонування системи розпізнавання облич з системою контролю доступу	29
РОЗДІЛ 3. ОЦІНКА ТА ТЕСТУВАННЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ.....	32
3.1. Тестування системи контролю доступу.....	32
3.2. Тестування системи розпізнавання облич.....	35
3.3. Тестування скомпонованої системи контролю доступу з розпізнаванням облич.....	36
ВИСНОВКИ.....	38
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	40
ДОДАТКИ.....	46

ВСТУП

У сучасному світі високих технологій питання безпеки та контролю доступу набувають все більшого значення. Розвиток штучного інтелекту відкриває нові можливості для створення ефективних систем контролю за доступом. Дана дипломна робота присвячена розробці пропускнуої системи з використанням штучного інтелекту, яка спрямована на підвищення рівня безпеки та зручності управління доступом.

Сьогодні, в епоху швидкої технологічної трансформації, питання безпеки та контролю доступу до приміщень, об'єктів та інформації стає надзвичайно актуальним для різноманітних сфер діяльності. Системи, які використовують штучний інтелект для контролю доступу, виявляються необхідними з точки зору підвищення ефективності та надійності захисту.

Зловмисники постійно шукають нові шляхи взлому систем безпеки, тому необхідно постійно удосконалювати засоби контролю та запобігання несанкціонованому доступу. Застосування штучного інтелекту у системах контролю доступу дозволяє створити більш інтелектуальні та адаптивні системи, здатні вчасно реагувати на загрози та підвищувати загальний рівень безпеки.

Крім того, у сучасному світі зростає значення використання розумних технологій для забезпечення комфорту та безпеки користувачів. Системи контролю доступу на базі штучного інтелекту можуть підвищити рівень комфорту для користувачів, забезпечуючи швидкий та зручний доступ до об'єктів при максимальній безпеці.

Таким чином, розробка пропускнуої системи з використанням штучного інтелекту є надзвичайно актуальною та важливою завданням, яке вирішує важливі проблеми безпеки та комфорту в сучасному світі.

Метою даної дипломної роботи є розробка та реалізація модулю пропускнуої системи для розпізнавання облич з використанням штучного інтелекту. Для досягнення цієї мети необхідно вирішити наступні завдання:

Аналіз існуючих систем контролю доступу: вивчення сучасних підходів та їхніх переваг і недоліків;

Розробка алгоритмів штучного інтелекту: створення інтелектуальних алгоритмів для ефективного контролю доступу;

Програмна реалізація системи та тестування: розроблення програмного забезпечення для системи та перевірка його на практиці;

Оцінка ефективності системи: проведення тестів та аналіз результатів для оцінки працездатності та ефективності системи.

Об'єктом дослідження є системи контролю допуску та технології розпізнавання облич для інфраструктур де важливо забезпечити високий рівень безпеки та зручності для користувачів.

Предметом дослідження є технології згорткових нейромереж глибокого навчання (CNN), які використовують алгоритми штучного інтелекту для підвищення ефективності контролю доступу [2].

У процесі дослідження використані такі методи:

Аналіз наукової літератури та публікацій: вивчення існуючих наукових робіт з питань контролю доступу та штучного інтелекту;

Моделювання та розробка алгоритмів штучного інтелекту: створення математичних моделей та розробка алгоритмів для контролю доступу;

Програмування та тестування системи: реалізація розробленої системи та перевірка її функціональності;

Експериментальне дослідження: проведення експериментів для оцінки ефективності та працездатності розробленої системи.

Базою дослідження є інфраструктура ДПУ як об'єкт впровадження системи доступу, де можливе її застосування як пропускнуої системи. Дані для системи є , також, об'єкти підприємств, установ, фінансових інститутів та інших

організацій, де забезпечення безпеки та контроль доступу є критично важливими аспектами діяльності.

Особистий внесок автора : у даній роботі автором апробовано і застосовано модель ШІ, на основі OpenCV для модулю розпізнавання облич пропускної системи ДПУ .

Практична значимість результатів: результати роботи можуть бути використані у проекті пропускної системи ДПУ до критичних об'єктів та приміщень.

Апробація досліджень відбулась на 1-й конференції молодих вчених “Математичні методи та цифрові технології в економіці”, теза “Система контролю доступу з використанням штучного інтелекту” ,15.03.20245 р., ДПУ, Ірпінь.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ АСПЕКТИ РОЗРОБКИ СИСТЕМ ДОПУСКУ

1.1. Існуючі системи контролю доступу

Системи управління доступом є ключовим елементом забезпечення безпеки у різноманітних областях, включаючи корпоративні будівлі та публічні місця. Вони застосовуються для регулювання входу до приміщень, будинків, інформаційних систем, а також для гарантування безпеки на об'єктах з інтенсивним рухом людей, наприклад, в аеропортах, на стадіонах і в готелях.

Існує широкий спектр систем контролю доступу, категоризація яких може бути здійснена на основі різних параметрів, включаючи способи ідентифікації користувачів, технічні особливості та сфери використання[24]. Нижче наведено декілька з найбільш розповсюджених типів цих систем[1].

Ключові системи доступу.

Системи доступу на основі ключів відносяться до найбільш базових та інтуїтивно зрозумілих методів управління доступом. Ці системи дозволяють контролювати доступ до об'єктів за допомогою традиційних ключів або карток доступу.

Принцип роботи фізичних ключів є металеві інструменти, які вставляють у замкову щілину та повертають для розблокування дверей чи воріт. Кожен ключ має індивідуальний дизайн або набір зубців, що взаємодіють з компонентами замку, дозволяючи його відкрити. Перевагами таких ключів є простота використання, невисока вартість, можливість легкої заміни у випадку втрати або крадіжки.

Карткові системи доступу.

Системи на основі карток використовують пластикові ідентифікаційні картки, оснащені магнітною стрічкою або вбудованим чіпом для зберігання інформації. Для доступу користувачам достатньо провести картокою по картрідеру або наблизити її до пристрою зчитування. Вони мають більшу безпеку порівняно з фізичними ключами, можливість швидкого і легкого скасування або заміни в разі втрати або крадіжки, можливість зберігання більшої кількості інформації на картці. З недоліків можна виокремити потребу у спеціальному читачі для карток,

вразливість до втрати або крадіжки картки, можливість несанкціонованого копіювання чи підробки картки.

Обидва ці типи систем є популярними в багатьох сферах, однак існують більш сучасні та безпечніші альтернативи, такі як біометричні системи або RFID, які відображають прогрес у технологіях контролю доступу.

PIN-коди (Personal Identification Numbers) є популярним методом контролю доступу, який базується на введенні унікального числового коду користувачем. Кожен користувач обирає або отримує унікальний числовий код, який він повинен ввести для отримання доступу. Код зазвичай складається з 4 або більше цифр і може бути встановлений або змінений користувачем у відповідності до правил безпеки системи.

Найпоширеніший спосіб введення PIN-коду - через клавіатуру, де користувач вручну вводить числову комбінацію. У деяких випадках PIN-код можна ввести, натискаючи відповідні числа на сенсорному екрані або панелі.

Перевагами PIN-кодів є те що їх введення не вимагає додаткових пристроїв або карток. Порівняно з біометричними системами, реалізація PIN-кодів зазвичай менш витратна. Адміністраторам системи легко управляти та змінювати PIN-коди для користувачів. Щодо вразливостей, якщо хтось переглядає користувача під час введення коду, можливо, цей код буде скопійовано. Більшість систем PIN-кодів мають обмежену довжину, що знижує рівень безпеки порівняно з довгими кодами. PIN-коди залишаються популярним методом контролю доступу, особливо там, де потрібна простота використання та невисокі витрати реалізації, але їх безпека може бути підвищена за допомогою додаткових заходів, таких як двофакторна аутентифікація.

Перейдемо до картрідерів. Картрідери використовують картки з магнітною смугою або чіпом для ідентифікації користувача. Користувач просто подає картку до читача або прокручує її через нього, і система перевіряє інформацію на картці для надання або відмови в доступі. Такі Картки можуть бути захищені паролем або кодом доступу. Вони комфортні та легкі у використанні тому що надають можливість швидко скасувати або змінити права доступу, відключити втрачені або викрадені картки. Мінусом є те що при втраті або викраденні картки, інша

особа може використовувати її для незаконного доступу. Зараз цю дилему вирішують багато установ, тому створюються технології для віддаленого блокування картки у випадку її втрати, але якщо по неухважності швидко цього не помітити, можна прогавити момент коли зловмисники витягнуть потрібну собі або інформацію або гроші, тощо.

Щодо біометричних систем. Біометричні системи контролю доступу ідентифікують особу на основі її унікальних біологічних ознак, таких як відбитки пальців, риси обличчя, структура сітківки ока чи голосовий відбиток. Ці дані скануються та перевіряються на відповідність із записами в базі даних для надання доступу. Фізичні характеристики унікальні для кожної особи, що робить біометричні системи важко підробити чи обійти. Хоча з появою технологій штучного інтелекту різко підвищився попит на потужне вдосконалення рівня кібербезпеки, адже нейромережі в силах підробити чужий голос, чи створити фейк-відео з будь яким обличчям. Користувач не потребує додаткових предметів, таких як картка або ключ, для отримання доступу.

Біометричні системи можуть бути вартісні у встановленні та підтримці. Зберігання біометричних даних може стати об'єктом порушення приватності та потенційних загроз для безпеки даних.

Технологія RFID (Ідентифікація за допомогою радіочастот) представляє собою ефективний засіб для ідентифікації осіб, товарів або об'єктів без фізичного контакту, використовуючи радіочастотні теги та сканери. Ця технологія знаходить застосування у широкому спектрі галузей, включаючи виробництво, логістику, охорону здоров'я та системи контролю доступу.

Такі системи розділяються на два типи: активні та пасивні.

Активні системи RFID: В цих системах, мітки мають вбудоване джерело живлення та можуть випромінювати сигнал навіть на великі відстані (декілька метрів). Вони зазвичай використовуються для відстеження великих об'єктів, таких як контейнери або транспортні засоби.

У пасивних системах мітки не мають власного джерела живлення і активуються радіосигналами, що випромінюються читачем. Вони зазвичай мають

обмежену дальність дії (декілька десятків сантиметрів) і використовуються для відстеження товарів або контролю доступу.

RFID-мітки оснащені мікрочіпом та антенною, що дозволяє здійснювати зчитування даних без необхідності фізичного контакту. На мікрочіпі записаний унікальний код або інформація, доступна для ідентифікації спеціальними скануючими пристроями. Пристрої для зчитування RFID використовують радіочастотні хвилі для ідентифікації та запису даних на RFID-теги. Вони генерують радіохвилі, що стимулюють мітки до передачі збереженої на них інформації.

Системи RFID широко застосовуються у різноманітних робочих сферах населення, таких як, до прикладу логістика і управління ланцюгом постачання. Використання RFID дозволяє автоматизувати відстеження та контроль за рухом товарів від виробника до кінцевого споживача.

Системи RFID використовуються для контролю доступу до об'єктів, будівель, транспорту тощо. Вони можуть бути використані для безконтактного відкриття дверей або шлагбаумів на автостоянках.

RFID дозволяє відстежувати рух та місцезнаходження активів, таких як обладнання або інструменти на виробництві або в складських приміщеннях.

Технологія RFID відіграє важливу роль у автоматизації та оптимізації численних процедур у різноманітних областях. Завдяки своїй здатності до точного відстеження та ідентифікації, ці системи набувають все більшої популярності та поширення.

Остання система про яку варто згадати це система "розумних" дверей і домофонів.

Представляють собою інноваційні технології, які комбінують у собі елементи безпеки, зручності та доступності для контролю доступу до приміщень.

До цих систем належать електронні замки, які можна керувати через мобільні програми чи інші електронні засоби. Вони пропонують різноманітні способи розпізнавання особи, включаючи біометричне сканування, RFID-технології або введення PIN-коду.

Домофонні системи надають можливість комунікації з гостями на відстані, дозволяючи користувачам відмикати двері дистанційно, здійснювати відео або аудіо зв'язок, а також фіксувати інформацію про всі візити.

Користувачі можуть керувати доступом до своїх приміщень з будь-якої точки світу за допомогою мобільного телефону або планшета. Системи можуть використовувати різні методи аутентифікації, щоб гарантувати лише авторизований доступ до приміщень. Домофони можуть мати вбудовані камери і мікрофони для взаємодії з відвідувачами, що дозволяє відстежувати та спілкуватися з ними в реальному часі. Деякі системи можуть зберігати записи про вхідні події, включаючи час та дату відвідування, інформацію про осіб, які входили та виходили.

1.2. Розвиток штучного інтелекту в сфері розпізнавання об'єктів та облич

Протягом останніх років, штучний інтелект значно просунувся у поліпшенні технологій ідентифікації об'єктів та розпізнавання осіб. Цей прогрес став реальністю завдяки інтеграції високорозвинених методів машинного та глибинного навчання, посилення обчислювальних потужностей та збільшення кількості даних, доступних для тренування моделей[8;20;22].

Автоматизоване визначення об'єктів є технологією, яка дозволяє ідентифікувати та класифікувати об'єкти на фотографіях чи відеозаписах без людського втручання. Цей процес є важливою частиною області комп'ютерного бачення та штучного інтелекту і знаходить застосування в широкому спектрі секторів, включаючи охорону здоров'я, самокеровані транспортні засоби, системи безпеки, робототехніку, маркетинг та інші[21].

Системи безпеки від злочинності.

Sighthound. Це рішення для відеоспостереження, яке використовує розпізнавання облич для ідентифікації людей на відео та виявлення небажаних осіб.

Avigilon Control Center (ACC). Це програмне забезпечення відеоспостереження, яке має функцію автоматичного виявлення та відстеження об'єктів на відео.

Системи моніторингу безпеки.

Hikvision[5]. Компанія Hikvision виробляє відеокамери та програмне забезпечення для відеоспостереження, яке має функції автоматичного виявлення об'єктів та розпізнавання облич.

Axis Communications. Ця компанія також виробляє відеокамери та програмне забезпечення для відеоспостереження з функціями автоматичного розпізнавання об'єктів.

Виробничі процеси.

ABB Robotics. Компанія ABB використовує системи розпізнавання об'єктів для автоматичного визначення розташування та орієнтації предметів у виробничих процесах.

Amazon Robotics. Amazon використовує системи розпізнавання об'єктів у своїх складських роботах для автоматичного сортування та інвентаризації товарів.

Система проводить аналіз фото чи відеоматеріалів за допомогою методів комп'ютерного бачення, виявляючи на зображеннях ділянки, що відповідають певним зразкам чи атрибутам об'єктів, які необхідно ідентифікувати. Опісля ідентифікації потенційних цільових сегментів, система застосовує треновані моделі машинного навчання для їх класифікації. Ці моделі, які часто базуються на нейронних мережах типу CNN нейронних мереж, володіють високою ефективністю у визначенні об'єктів на графічних зображеннях.

CNN становлять фундаментальний підхід у розпізнаванні об'єктів. Їх застосовують для того, щоб автоматизовано ідентифікувати та категоризувати об'єкти на фотографіях, використовуючи виявлення ключових особливостей та візерунків.

Глибоке навчання є ключовою технологією для автоматичного розпізнавання об'єктів, оскільки воно дозволяє системам вчитися виконувати завдання без потреби експліцитного програмування шаблонів для кожного типу об'єкта.

Використання певних функцій активації та архітектур згорткових нейронних мереж дозволяє системам ефективно виявляти та класифікувати об'єкти на зображеннях.

Застосування штучного інтелекту для цих задач, мають відгуки в багатьох професійних сферах.

Медицина. Автоматичне розпізнавання об'єктів в медичних зображеннях, таких як рентгенівські знімки, може допомогти лікарям в діагностуванні хвороби та виявляти патології.

Zebra Medical Vision. Ця компанія використовує системи розпізнавання об'єктів для автоматичного виявлення патологій та хвороб на медичних зображеннях, таких як рентгенівські знімки та КТ.

Google DeepMind Health. Використовує глибоке навчання для розпізнавання та аналізу медичних зображень для виявлення ознак патологій та захворювань.

Системи розпізнавання об'єктів використовуються в автономних автомобілях для виявлення інших транспортних засобів, пішоходів, дорожніх знаків та перешкод на дорозі.

Вони використовуються для виявлення підозрілих об'єктів або поведінки на відео з камер відеоспостереження для забезпечення безпеки.

Waymo. Компанія Waymo використовує системи розпізнавання об'єктів для виявлення автомобілів, пішоходів, велосипедистів та інших об'єктів на дорозі в своїх автономних автомобілях.

Tesla Autopilot. Система Autopilot в автомобілях Tesla використовує комп'ютерний зір для виявлення та відстеження інших транспортних засобів на дорозі.

Системи розпізнавання об'єктів можуть бути використані для аналізу зображень та відео для отримання інформації про споживачів, їхній вік, стать, емоції та інші характеристики.

Паралельно з розпізнаванням об'єктів може застосовуватися сегментація зображень, яка дозволяє виділяти окремі області на зображенні, що відповідають різним об'єктам.

Деякі системи можуть визначати не лише тип об'єкта, але і його положення або орієнтацію в просторі.

Тривимірне розпізнавання об'єктів.

Деякі системи можуть аналізувати тривимірні дані, такі як дані зі стереокамер або лідарів, для розпізнавання об'єктів у тривимірному просторі. Для точного визначення положення об'єктів у тривимірному просторі системи розпізнавання можуть використовувати облікові системи координат.

Застосування цих систем в реальному часі.

Деякі системи спроможні працювати в реальному часі, що дозволяє їм розпізнавати об'єкти відразу під час їх появи на зображенні або відео. Лайв розпізнавання об'єктів може бути використане у системах моніторингу безпеки для автоматичного виявлення небезпечних ситуацій або подій. Або можна ще згадати футбол, де використовується система VAR для вирішення спірних рішень під час гри, яка в реальному часі транслює необхідний момент, і дає можливість оглядати його з різних кутів, для найточнішого рішення арбітру в результаті перегляду.

Системи розпізнавання можуть бути модернізовані шляхом навчання для підвищення точності та ефективності розпізнавання. Використання ансамблевих методів, дерев рішень, може допомогти підвищити точність розпізнавання. Автоматичне розпізнавання об'єктів продовжує розвиватися, і його застосування в різних галузях відкриває нові можливості для автоматизації та оптимізації багатьох процесів.

1.3. Огляд технологій для розробки програмного забезпечення

У моїй системі контролю доступу використовується набір технологій, до якого входить Python в якості головної мови програмування, OpenCV та бібліотека розпізнавання облич для аналізу зображень, MySQL для управління даними, а також PHPMyAdmin для керування базами даних[19]. Використання цих інструментів забезпечить ефективну роботу вашої системи зі штучним інтелектом для ідентифікації осіб.

Python - це високорівнева мова програмування, яка відома своєю простотою та читабельністю коду. Python широко використовується у багатьох галузях, включаючи розробку веб-додатків, аналіз даних, штучний інтелект та машинне навчання. В моєму проєкті Python був використаний для реалізації основного програмного забезпечення пропускнуої системи, а також для інтеграції з бібліотеками комп'ютерного зору та обробки зображень.

OpenCV (Open Source Computer Vision Library) визнана однією з найвідоміших і широко використовуваних бібліотек у сфері комп'ютерного зору та обробки зображень[10]. Вона може відігравати важливу роль у вашому проєкті створення програмного забезпечення для системи контролю доступу, що базується на штучному інтелекті, пропонуючи ряд ключових функцій.

OpenCV має вбудовані алгоритми для виявлення облич, розпізнавання облич та обробки зображень. У своїй пропускнуї системі я використовував ці функції для ідентифікації осіб на вхідних зображеннях або відео, а також для відокремлення облич від інших об'єктів на зображеннях.

Бібліотека OpenCV може бути застосована для створення систем відеоспостереження, які включають функції, такі як детекція руху та розпізнавання об'єктів у відео. Ці можливості можуть значно підвищити рівень безпеки системи контролю доступу, надаючи змогу спостерігати активність та ідентифікувати несанкціонованих осіб. Використання OpenCV дозволяє автоматизувати певні аспекти вашої системи контролю доступу, зокрема, ідентифікацію автомобілів за допомогою розпізнавання номерних знаків, а також перевірку зображень з камер спостереження на предмет виявлення фальшивих чи недійсних документів доступу. Також ця бібліотека корисна у реалізації функціоналу розпізнавання жестів або емоцій на обличчі користувачів. Це може додати нові можливості та покращити користувацький досвід у вашій майбутній пропускнуї системі. OpenCV має велику кількість інтеграцій з іншими бібліотеками та фреймворками, що дозволяє використовувати його у поєднанні з іншими технологіями для створення повноцінних рішень для пропускнуї системи.

Бібліотека Face recognition є інструментом на базі Python, який забезпечує легкий у використанні інтерфейс для ідентифікації осіб та вирішення різноманітних завдань, пов'язаних з обробкою облич. Вона надає можливість розпізнавати обличчя на фото та відео. Бібліотека підтримує різні алгоритми розпізнавання, в тому числі метод на основі навчання. Бібліотека Face-recognition розпізнає ключові “точки” обличчя такі як ніс, очі, рот, вуха, та інші. Це допомагає у різних задачах, наприклад як розпізнавання емоцій осіб на фото чи відео.

Face recognition оцінює схожість рис між обличчями та може виконати їх порівняння на основі певних характеристик. Це корисно для реалізації функціоналу автентифікації або для виявлення подвійних облікових записів.

Бібліотека підтримує впровадження розпізнавання облич у системи реального часу, такі як відеоспостереження або інтерактивні системи. Це дозволяє використовувати Face recognition для реалізації різних застосувань, включаючи системи безпеки, контроль доступу та інтерфейси користувача.

Сама по собі бібліотека проста у використанні, має комфортний та прости інтерфейс, який допомагає швидко виконувати задачу з розпізнавання облич. Вона підтримується документацією та прикладами, які полегшують використання та розуміння її функціоналу.

RНРMyAdmin є потужним і зручним інструментом для управління базами даних, який може значно полегшити життя розробникам програмного забезпечення. Він дозволяє швидко і ефективно виконувати різноманітні операції з базами даних, що робить його незамінним інструментом у багатьох проектах. Однак, важливо враховувати його обмеження та вживати заходів для забезпечення безпеки та продуктивності системи.

Як для розробки він має інтуїтивно зрозумілий інтерфейс, та дозволив швидко освоїти його як інструмент та ефективно використовувати його для управління базами даних. RНРMyAdmin може бути менш ефективним при роботі з дуже великими базами даних через обмеження веб-інтерфейсу та ресурсів сервера. Окрім того, незважаючи на наявність засобів безпеки, неправильна

конфігурація або відсутність регулярних оновлень можуть зробити систему вразливою до атак.

Але він має підтримку багатьох мов, що робить його більш доступним для розробників з усього світу.

Що ж саме надає цей інструмент.

Можливість створення, редагування, видалення баз даних.

Імпорт та експорт баз даних у різних форматах, таких як SQL, CSV, XML, та інші.

Резервне копіювання та відновлення баз даних.

Створення, зміна структури, та видалення таблиць.

Додавання, редагування, та видалення записів у таблицях.

Підтримка складних типів даних та індексів.

Можливість виконання SQL-запитів вручну з використанням вбудованого редактора.

Збереження та повторне використання часто використовуваних запитів.

Підтримка аутентифікації та авторизації користувачів.

Шифрування з'єднань через SSL/TLS.

Останній на огляді інструмент MySQL. MySQL відомий як ефективний та стабільний інструмент для керування базами даних, який часто застосовують у програмній інженерії. Його широке використання пояснюється легкістю управління, вражаючою швидкістю та широким спектром можливостей. Навіть з урахуванням деяких обмежень, MySQL продовжує бути вибором номер один для різноманітних проектів, завдяки своїй адаптивності, підтримці активної спільноти та обширному набору доступних інструментів та ресурсів.

Основні Функції MySQL.

Архітектура.

Клієнт-серверна архітектура: MySQL використовує модель клієнт-сервер, де сервер управляє базами даних, а клієнти (додатки) взаємодіють з ним через мережу.

Підтримка багатокористувацької роботи: дозволяє одночасний доступ багатьох користувачів до бази даних.

Сумісність та Портативність.

Працює на різних платформах: Windows, Linux, macOS, та інші Unix-подібні системи.

Сумісний з багатьма мовами програмування: PHP, Python, Java, C++, Ruby, та інші.

Продуктивність.

Підтримка індексації, що дозволяє швидко виконувати пошук та сортування даних.

Кешування запитів для покращення продуктивності при частому виконанні однакових запитів.

Безпека.

Підтримка аутентифікації та авторизації користувачів з різними рівнями доступу.

Шифрування даних як на рівні з'єднань, так і на рівні збережених даних.

Реплікація та Висока Доступність.

Підтримка реплікації даних між серверами для забезпечення високої доступності та надійності.

Вбудовані механізми для автоматичного резервного копіювання та відновлення.

Розширюваність.

Підтримка плагінів та розширень, що дозволяють додавати нову функціональність до СУБД.

Вбудована підтримка для збережених процедур, тригерів та подій.

Переваги MySQL для Розробників.

Простота Використання.

Легкість у встановленні та налаштуванні.

Інтуїтивно зрозумілий синтаксис SQL, що дозволяє швидко навчитися працювати з базою даних навіть початківцям.

Добре документована система з великою кількістю ресурсів, включаючи офіційну документацію, форуми та навчальні курси.

Підтримка популярних інструментів розробки, таких як PHPMyAdmin, MySQL Workbench, та інші.

Велика Спільнота та Підтримка.

Активна спільнота користувачів, що постійно розвиває та підтримує систему.

Швидке вирішення проблем завдяки великій кількості доступних ресурсів та експертів.

Хоча MySQL добре працює з малими та середніми базами даних, для дуже великих обсягів даних можуть виникати проблеми з масштабованістю та продуктивністю.

MySQL має як відкриту (GPL), так і комерційну ліцензії, що може бути важливо враховувати при виборі.

Деякі розширені функції можуть бути доступні лише в комерційних версіях або вимагати додаткового налаштування.

РОЗДІЛ 2. ПРОЄКТУВАННЯ, РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1. Проектування системи контролю доступу

Для того щоб створити систему розпізнавання облич на основі конвулюційної нейронної мережі, спочатку я поглибився в теорію. Конвулюційна нейронна мережа, вона ж CNN, це добре відомий метод використання комп'ютерного зору. Зазвичай його використовують в розпізнаванні картинок та відео. Принцип роботи CNN простий, вхідне зображення з камери опрацьовується під час фази згортання а пізніше присвоюється мітці[29;31-33].

```
def preprocess_frame(frame):
    # Зменшення шуму
    frame = cv2.GaussianBlur(frame, (5, 5), 0)

    # Перетворення зображення на чорно-біле
    gray_frame = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
```

```

        # Зміна розміру зображення до розміру, що очікується
        CNN (наприклад, 128x128)
        resized_frame = cv2.resize(gray_frame, (128, 128))

        # Нормалізація зображення
        normalized_frame = resized_frame / 255.0

        # Додавання осі каналу (для чорно-білих зображень ось
        такий формат: (128, 128, 1))
        input_frame = np.expand_dims(normalized_frame, axis=-1)
        input_frame = np.expand_dims(input_frame, axis=0) #
        Додавання batch dimension

        return input_frame

    # Встановлюємо RTSP URL камери
    rtsp_url =
    "rtsp://username:password@ip_address:port/video_stream"

    # Створюємо об'єкт камери за допомогою RTSP потоку
    camera = cv2.VideoCapture(rtsp_url)

    # Перевіряємо, чи вдалося підключитися до камери
    if not camera.isOpened():
        print("Не вдалося підключитися до камери")
        exit()

    # Зчитуємо та обробляємо кадри з камери
    while True:

```

```

ret, frame = camera.read()
if not ret:
    print("Не вдалося отримати кадр з камери")
    break

# Попередня обробка кадру
processed_frame = preprocess_frame(frame)

# Використання моделі для передбачення (розпізнавання
обличч)
predictions = model.predict(processed_frame)

# Постобробка та відображення результатів (це залежить
від специфіки вашої моделі)
# Наприклад, можна відобразити ймовірність наявності
обличчя на зображенні
if predictions[0][0] > 0.5: # Попіг впевненості
    cv2.putText(frame, "Face detected", (10, 30),
cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2)

# Відображення обробленого кадру
cv2.imshow("Камера", frame)

# Вихід з циклу за допомогою клавіші 'q'
if cv2.waitKey(1) & 0xFF == ord('q'):
    break

```

Зображення – це набір пікселів правильно розташовані одне біля одного. Кожен піксель це значення від 0 до 255, ці значення показують інтенсивність

кольору. Враховуючи що у своїй роботі я використовую чорно-білий фільтр для розвантаження системи, інтенсивність чорних і білих кольорів визначається цими значенням, де 0 це білий а 255 це чорний.

Прикладом визначення кольорів на чорний і білий, показано на рис 1.

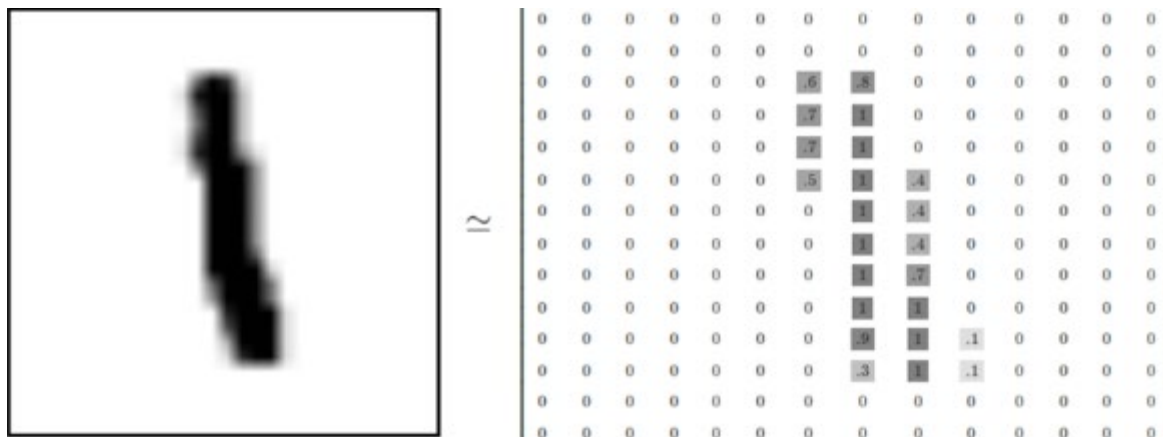


Рис. 2.1. Приклад визначення кольорів на чорний і білий

Як бачимо, звичайна лінія розклалась на пікселі, та визначилась по певним значенням[28].

Модуль на Python для розпізнавання обличчя.

Модуль розроблений мною за допомогою бібліотеки OpenCV також встановлений необхідний шаблон в форматі XML, який уміє розрізняти обличчя від об'єктів, щоб не ловити зайвий раз рухи, предмети на камері та відсіювати лише обличчя. Зі сторони це виглядає наче фільтр для вибору щоб розпізнавати обличчя серед всієї картинки. Також для того щоб розпізнавати обличчя, я підключив камеру Hikvision та підключився в неї за допомогою rtsp потоку.

Ось приклад rtsp посилання: `rtsp://login:password@11.22.33.44:554/live1.sdp`

Код який використовується для підключення до потоку:

```
import cv2
```

Встановлюємо RTSP URL камери

```
rtsp_url =
```

```
"rtsp://username:password@ip_address:port/video_stream"
```

Створюємо об'єкт камери за допомогою RTSP потоку

```
camera = cv2.VideoCapture(rtsp_url)
```

Перевіряємо, чи вдалося підключитися до камери

```

if not camera.isOpened():
    print("Не вдалося підключитися до камери")
    exit()

```

Закриваємо підключення до камери та вікно відображення

```

camera.release()
cv2.destroyAllWindows()

```

Цей модуль буде відповідати за кілька ключових завдань. По-перше, він забезпечуватиме ініціалізацію камери, встановлюючи зв'язок між програмним забезпеченням і апаратним забезпеченням камери. Це включає в себе налаштування параметрів зйомки, таких як роздільна здатність, частота кадрів, баланс білого і експозиція, щоб забезпечити найкращу якість зображення в різних умовах освітлення.

По-друге, модуль буде відповідати за безперервне захоплення кадрів з камери. Використовуючи функції OpenCV, модуль буде зчитувати кадри з камери в режимі реального часу, забезпечуючи постійний потік зображень для подальшої обробки.

```

while True:
    ret, frame = camera.read()
    if not ret:
        print("Не вдалося отримати кадр з камери")
        break
    cv2.imshow("Камера", frame)

```

Вихід з циклу за допомогою клавіші 'q'

```

if cv2.waitKey(1) & 0xFF == ord('q'):
    break

```

Після захоплення, кадри передаватимуться для подальшої обробки, яка включає попередню обробку зображень та розпізнавання облич. Модуль захоплення зображень буде інтегрований з іншими компонентами системи,

такими як модуль обробки зображень і модуль розпізнавання облич, забезпечуючи плавну передачу даних між різними етапами обробки. Ось код який використовується для обробки зображення:

```
def preprocess_frame(frame):
    # Зменшення шуму
    frame = cv2.GaussianBlur(frame, (5, 5), 0)

    # Перетворення зображення на чорно-біле
    frame = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)

    return frame
```

Завдяки використанню OpenCV та високоякісної камери, модуль захоплення зображень забезпечить надійний і ефективний процес збору даних для системи розпізнавання облич, гарантуючи високу точність і швидкість роботи всієї системи контролю доступу.

Для попередньої обробки зображень потрібно створити модуль обробки зображень на Python з використанням OpenCV. Цей модуль виконуватиме декілька ключових завдань. Спершу він перетворюватиме кольорові зображення у відтінки сірого, що зменшить розмір даних і спростить подальшу обробку. Потім здійснюватиметься нормалізація зображень для забезпечення однакової яскравості та контрасту, що покращить якість розпізнавання облич. Масштабування зображень дозволить привести їх до єдиного розміру, що необхідно для коректного порівняння. Видалення шуму з зображень за допомогою фільтрів знизить рівень помилок при розпізнаванні. Нарешті, модуль буде здійснювати виявлення облич на зображеннях, виділяючи області, що містять обличчя.

Для розпізнавання облич потрібно реалізувати окремий модуль з використанням бібліотеки face-recognition. Цей модуль буде використовувати попередньо оброблені зображення, що надаються модулем обробки зображень. Основне завдання модуля розпізнавання облич полягає в ідентифікації облич

користувачів. Модуль аналізуватиме зображення, виділятиме унікальні характеристики обличчя і порівнюватиме їх з даними, що зберігаються в базі даних зареєстрованих користувачів. Результати розпізнавання будуть повертатися у вигляді відповіді, яка вказує, чи знайдено відповідне обличчя в базі даних, і надає інформацію про користувача у випадку успішного розпізнавання.

Для зберігання біометричних даних користувачів потрібно створити базу даних MySQL. Вона буде містити ідентифікатори користувачів, відцифровані зображення облич та метадані, такі як дата і час реєстрації та права доступу. Структура бази даних включатиме таблиці, що зберігають ці дані в зручному для обробки вигляді.

Для управління базою даних буде використовуватися phpMyAdmin, який забезпечить зручний веб-інтерфейс для адміністрування. Це дозволить легко додавати, видаляти та редагувати записи у базі даних. Крім того, phpMyAdmin надає можливість створення резервних копій бази даних для захисту інформації, а також відновлення даних у разі потреби.

Користувачі з відповідними правами доступу зможуть виконувати SQL-запити для отримання, оновлення або видалення даних, що забезпечить гнучкість у роботі з базою даних. Це також дозволить автоматизувати деякі процеси, пов'язані з обробкою даних, що зберігаються в базі даних.

Використання phpMyAdmin спрощує управління базою даних завдяки інтуїтивно зрозумілому інтерфейсу, що робить адміністрування доступним навіть для користувачів з обмеженим досвідом роботи з SQL. Це забезпечує ефективне управління біометричними даними та підтримку безперебійної роботи системи контролю доступу.

Для забезпечення взаємодії користувачів з системою, потрібно створити інтерфейс користувача. Він буде надавати доступ до системи контролю доступу та відображати результати розпізнавання облич, інформацію про користувачів та успішні або невдалі спроби доступу.

Для інтеграції всіх компонентів системи, потрібно налаштувати взаємодію між модулем захоплення зображень, модулем обробки зображень, модулем розпізнавання облич, базою даних MySQL та інтерфейсом користувача. Щоб

забезпечити високу точність та швидкість роботи системи, потрібно використовувати сучасні методи машинного навчання та глибокого навчання, зокрема конволюційні нейронні мережі (CNN) для навчання моделі розпізнавання облич та оптимізацію її параметрів[17;18].

Також для виведення вхідного, обробленого зображення, я використав в своїй системі автоенкодер. Автоенкодер – це інструмент для відтворення введених даних. Його перевага в тому, що вхідні дані кодуються лише мережею, тим самим зосереджуючи увагу лише на важливі функції та разом з цим допомагає зменшити розмірність вихідних даних. Здебільшого він потрібен для приближення введення, зосереджуючись лише на вагомих для розпізнавання елементах. Простіше кажучи, автоенкодер це фільтр який пропускає лише ключові елементи для розпізнавання в картинці, а проміжні, навпаки не пропускає. Знизу зображено типовий автоенкодер, який зменшує якість зображення для виділення основного.



Рис. 2.2. Робота модуля обробки вхідних зображень[30;36]

Для роботи системи розпізнавання облич спочатку потрібно ініціалізувати камеру, підключивши її до системи, та налаштувати параметри зйомки, такі як роздільна здатність, частота кадрів і освітлення. Після цього необхідно підключитися до бази даних MySQL і перевірити наявність таблиць для

зберігання даних користувачів, а також ініціалізувати phpMyAdmin для зручного адміністрування бази даних (рис. 2.3.).

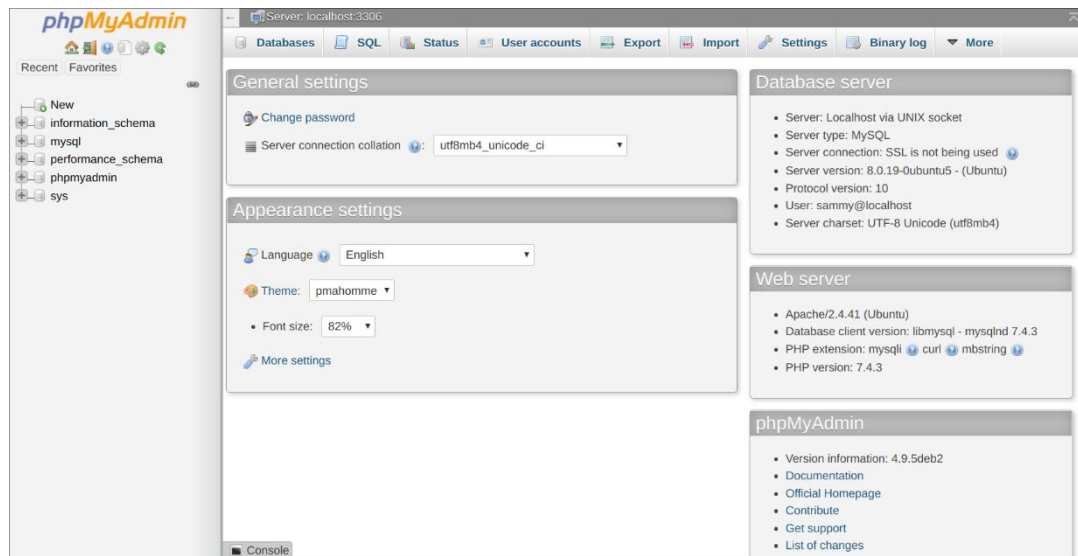


Рис. 2.3. Інтерфейс PhpMyAdmin

Коли система готова до роботи, камера захоплює зображення облич користувачів у реальному часі. Модуль захоплення зображень, реалізований на Python з використанням бібліотеки OpenCV, отримує кадри з камери та передає їх до модуля обробки зображень. Модуль обробки зображень виконує попередню обробку кадрів, включаючи перетворення кольорових зображень у відтінки сірого, нормалізацію, масштабування та видалення шуму. Далі він виявляє обличчя на зображеннях за допомогою алгоритмів OpenCV і передає оброблені зображення до модуля розпізнавання облич.

Модуль розпізнавання облич, реалізований з використанням бібліотеки face-recognition, порівнює виявлені обличчя з даними в базі даних зареєстрованих користувачів. Він використовує попередньо навчені моделі для ідентифікації користувачів. Якщо обличчя знайдене в базі даних, модуль повертає ідентифікатор користувача та інші метадані, такі як ім'я та права доступу. Якщо обличчя не розпізнано, система реєструє спробу доступу як невдалу.

Результати розпізнавання облич відображаються на інтерфейсі користувача, який надає інформацію про користувача, успішні та невдалі спроби доступу. Адміністратори можуть використовувати phpMyAdmin для управління базою даних, додаючи нових користувачів або оновлюючи інформацію про існуючих користувачів.

Система постійно працює в режимі реального часу, захоплюючи нові зображення, обробляючи їх і порівнюючи з базою даних для забезпечення ефективного та безпечного контролю доступу. Для підтримки високої точності та швидкості роботи система використовує сучасні методи машинного навчання та глибокого навчання, зокрема конволюційні нейронні мережі (CNN) для навчання моделі розпізнавання облич і оптимізації її параметрів. Експериментальні дослідження та тестування системи допомагають виявляти та усувати можливі недоліки, а також оптимізувати її продуктивність.

Враховуючи те, що в планах університету є масштабування цієї системи по всій установі, зараз такий термінал пропуску знаходиться лише в одній точці, а саме в корпусі Р на 2 поверсі.

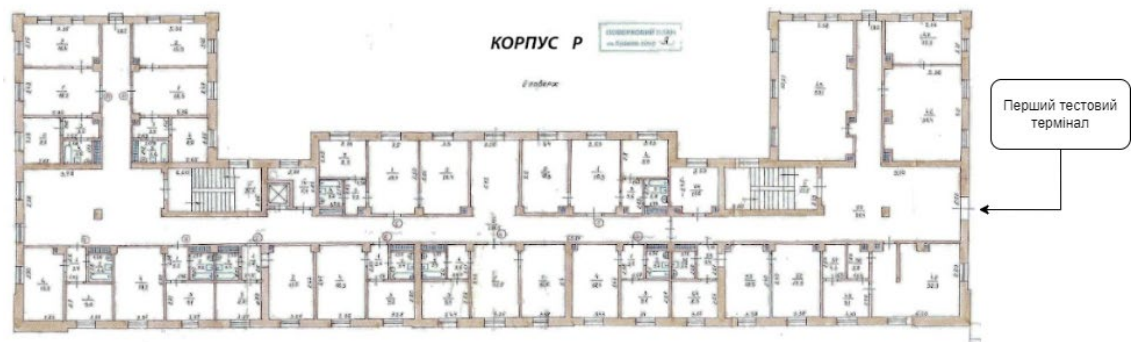


Рис. 2.4. План 2 поверху корпусу Р в ДПУ з розміщенням першого терміналу

В подальшому є плани в розміщенні таких терміналів на основних точках, де є велике скупчення людей. А саме в корпусі В, центральний корпус, та корпус D.

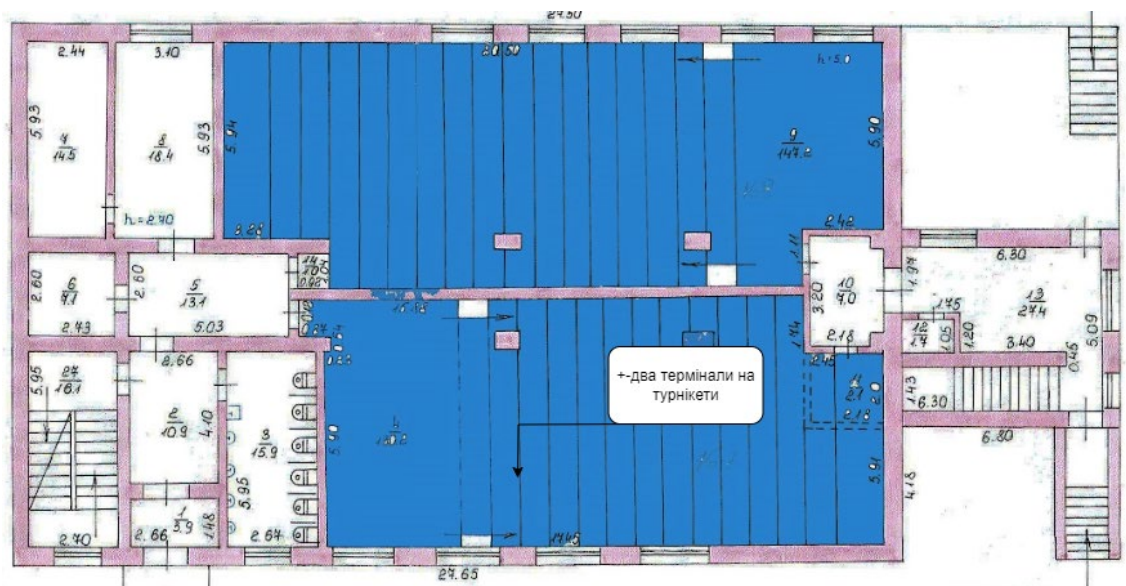


Рис. 2.5. План першого поверху корпусу С

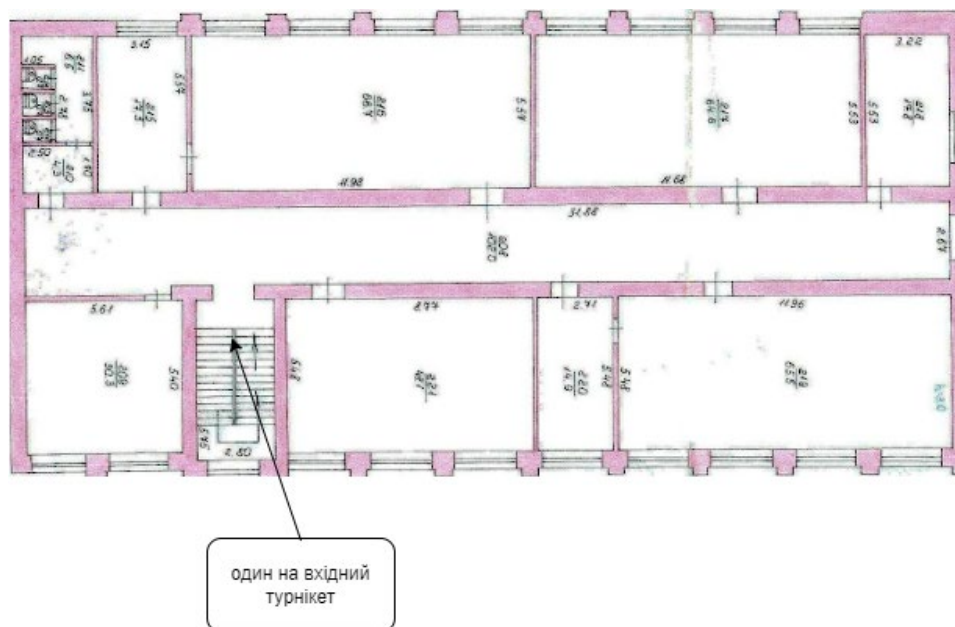


Рис 2.6. План першого поверху корпусу В

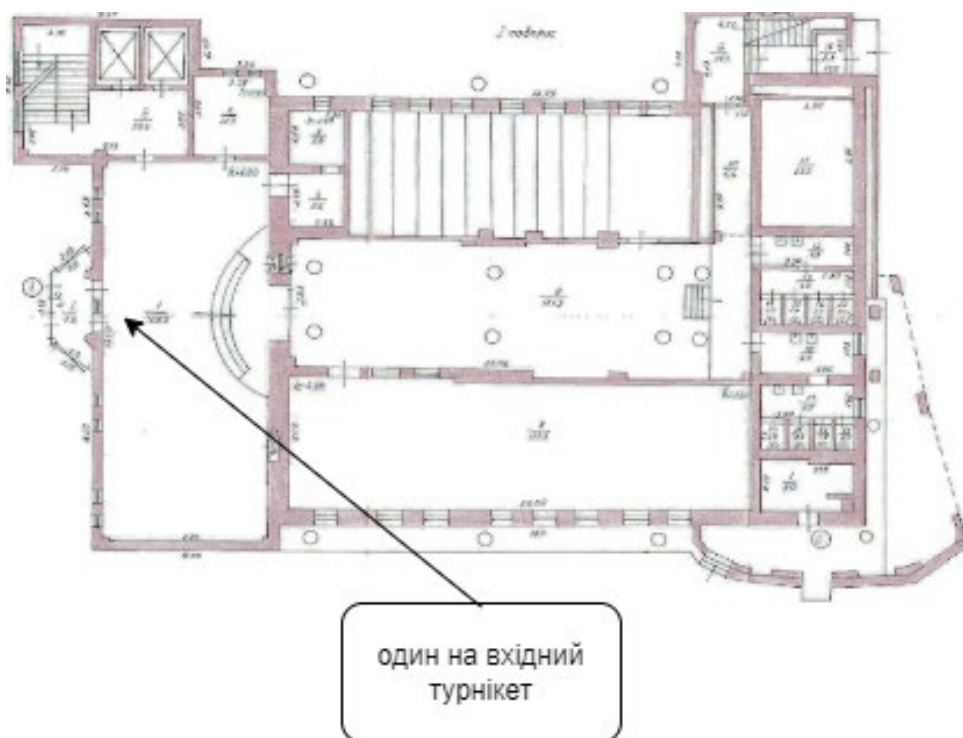


Рис. 2.7. План першого поверху корпусу D

2.2. Компонування системи розпізнавання облич з системою контролю доступу

Для того щоб скомпонувати дві системи в одну, спочатку потрібно розібратись за яким принципом буде працювати вся система. Ось яким чином, я побудував схему роботи загальної системи:

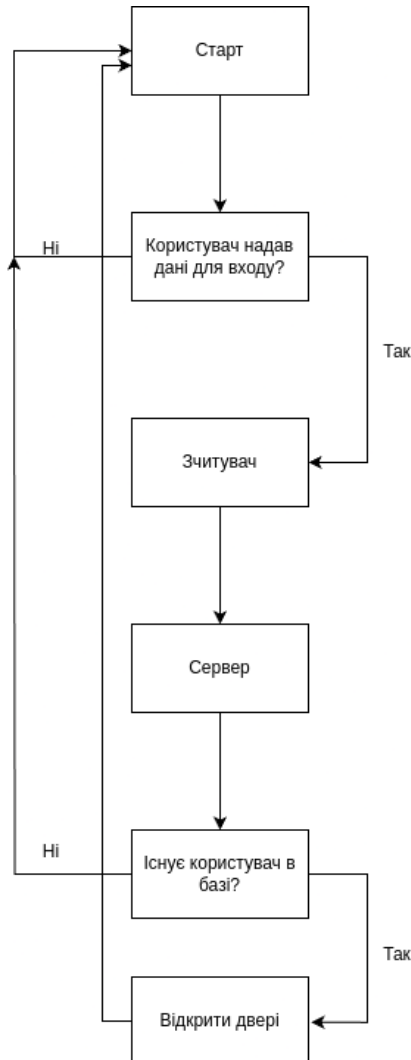


Рис. 2.8. Загальна схема пропуску користувача

В першу чергу користувач подає зчитувачу дані з НФС картки або сам QR код, потім зчитувач подає запит на інформацію до сервера, якщо той відповідає True на те чи існує користувач в базі, сервер посилає сигнал на зчитувач та виводить певний колір індикатора на сканері, а вже потім надсилає сигнал на двері, щоб той відкрив магніт і пропустив користувача до певної території. В іншому випадку, сигнал доходить лише до сервера, надсилає на сканер сигнал False, а зчитувач світиться червоним кольором. Двері не відкриваються.

Далі користувачів реєструють у загальній базі даних через веб-інтерфейс, далі користувачі авторизуються в Telegram-боті, де вже є інформація про них. Під

час реєстрації вони надають необхідні дані, такі як ім'я, фото обличчя та контактну інформацію, необхідну для зв'язки користувача по базі[14]. Після успішної реєстрації користувач отримує унікальні QR-коди, які генеруються з бази даних разом з іншою інформацією про користувача.

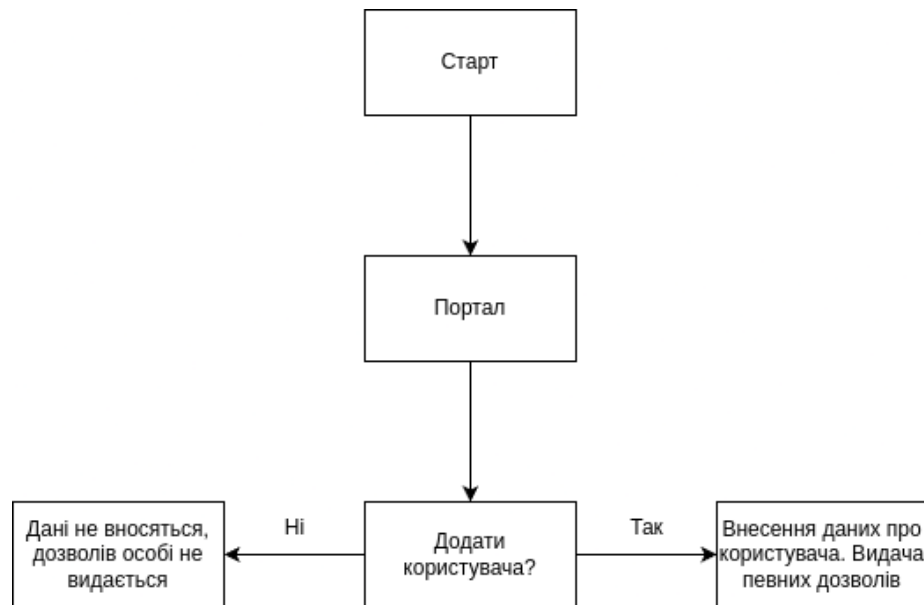


Рис. 2.9. Схема реєстрації користувачів

Коли користувач підходить до точки входу, система починає процес верифікації, який може відбуватися трьома способами: за допомогою QR-коду, картки або розпізнавання обличчя.

Піднесення QR-коду до сканера запускає модуль сканування, який зчитує код і передає його серверу для перевірки. Сервер розшифровує QR-код і порівнює його з записами у базі даних. Якщо код дійсний і відповідає зареєстрованому користувачу, сервер надсилає сигнал про дозвіл доступу до контрольного модуля, який відкриває двері або турнікет. Процес проходить швидко та без затримок, забезпечуючи зручний і ефективний доступ.

Використання картки запускає модуль зчитування, який передає інформацію з картки серверу для перевірки. Сервер порівнює дані картки з базою даних. Якщо картка дійсна і відповідає зареєстрованому користувачу, сервер надсилає сигнал про дозвіл доступу до контрольного модуля, що дозволяє відкрити двері або турнікет, надаючи доступ до приміщення. Верифікація за

допомогою картки забезпечує швидкий і зручний процес входу, що є особливо важливим у місцях з високою прохідністю.

При розпізнаванні облич користувач підходить до камери, яка захоплює зображення обличчя. Модуль обробки зображень обробляє зображення і передає його до модуля розпізнавання облич. Модуль розпізнавання облич порівнює отримане зображення з базою даних зареєстрованих облич. Якщо обличчя розпізнано і відповідає зареєстрованому користувачу, сервер надсилає сигнал про дозвіл доступу до контрольного модуля. Інтеграція з Telegram-ботом забезпечує додатковий рівень зручності для користувачів. Після успішної верифікації через будь-який з методів користувач може отримувати сповіщення у Telegram про кожную спробу входу, а також мати можливість керувати своїм обліковим записом через бот. Telegram-бот також може використовуватися для надсилання тимчасових QR-кодів для гостей або тимчасових користувачів.

Компоненти системи, такі як модуль сканування QR-кодів, зчитувач карток, камера для розпізнавання облич, сервер для обробки запитів та база даних, працюють разом для забезпечення надійного контролю доступу. Всі модулі пов'язані з сервером, який виконує основну логіку верифікації і управління доступом.



Рис. 2.10. Камера та сканер вже вмонтовані в проході

РОЗДІЛ 3. ОЦІНКА ТА ТЕСТУВАННЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1. Тестування системи контролю доступу

Важливим етапом в розробці системи – це тестування. Це дозволяє нам виявити проблемні місця в системі, дефекти коду, або правильну роботу всіх компонентів та їх взаємодію. Тестування охоплює QR-коди, картки, сканери з індикаторами зеленого та червоного світлодіода, а також магнітні двері.

Початковим етапом є генерація та розповсюдження QR-кодів для користувачів через Telegram-бот. Генерація унікальних QR-кодів виконується за допомогою спеціального алгоритму, який створює коди, кожен з яких містить закодовану інформацію про користувача. Ця інформація включає унікальний ідентифікатор користувача та інші дані, необхідні для його ідентифікації в системі.

Після генерації QR-коди розповсюджуються серед користувачів на їх запит, усі згенеровані коди зберігаються у базі даних системи контролю доступу, де вони прив'язуються до відповідних облікових записів користувачів.

Після отримання QR-кодів користувачі можуть використовувати їх для доступу до контрольованих зон. На вході після зчитування, і отримання від серверу сигналу **True**, камера робить фото, та надсилає по зашифрованому ID користувача в базу даних фото, таким чином ведеться наповнення датасету.

Сервер здійснює верифікацію QR-коду, порівнюючи отримані дані з інформацією, що зберігається у базі даних. Якщо код відповідає зареєстрованому користувачу та не викликає підозр, сервер дозволяє доступ і подає сигнал для відкриття дверей або турнікета. У випадку, якщо код не відповідає жодному запису в базі даних або є інші причини для відмови у доступі, сервер блокує спробу та подає відповідний сигнал.

Реєстрація карток доступу для користувачів відбувається через систему Portal, після чого картки асоціюються з відповідними обліковими записами у базі даних. Зчитування карток виконується зчитувачем, який передає дані картки на сервер для перевірки. Сервер верифікує дані картки з базою даних і перевіряє

їхню відповідність зареєстрованому користувачу. Успішні та невдалі спроби доступу також відображаються відповідно.

Сканери з індикаторами зеленого та червоного світлодіода встановлюються та налаштовуються для відображення стану системи. Процес починається з монтажу сканерів у контрольних точках доступу, де вони зможуть ефективно зчитувати дані від користувачів, наприклад, QR-коди або картки. Сканери повинні бути розміщені так, щоб забезпечити легкий доступ користувачів до них. Після встановлення сканерів проводиться їхнє налаштування. Це включає підключення сканерів до системи контролю доступу та налаштування програмного забезпечення для взаємодії з іншими компонентами системи. Важливо переконатися, що сканери коректно передають зчитані дані на сервер для подальшої обробки та верифікації.



Рис. 3.1 Сканер QR-кодів та NFC міток

Одним з ключових аспектів налаштування сканерів є перевірка індикаторів світлодіодів. Зелений та червоний світлодіоди відіграють важливу роль у візуальному інформуванні користувачів про результат верифікації. Налаштування полягає в забезпеченні того, щоб зелений світлодіод сигналізував про успішну верифікацію, тоді як червоний світлодіод попереджав про невдалу спробу доступу. Для перевірки правильного відображення результатів верифікації

проводяться тести з використанням різних сценаріїв доступу. Наприклад, при успішному зчитуванні та верифікації QR-коду або картки зелений світлодіод повинен загорятися, сигналізуючи користувачу про те, що доступ дозволено. Якщо ж дані не відповідають зареєстрованому користувачу або виникають інші помилки, червоний світлодіод повинен засвітитися, попереджаючи про невдалу спробу доступу.

Магнітні двері встановлюються та підключаються до системи з налаштуванням параметрів відкриття та закриття. Процес починається з фізичного монтажу магнітних дверей на відповідних входах та виходах. Після встановлення дверей вони підключаються до центральної системи контролю доступу, що дозволяє керувати ними за допомогою електронних сигналів.

Налаштування параметрів відкриття та закриття включає конфігурацію часу відкриття та автоматичного закриття дверей. Це може бути зроблено через спеціалізоване програмне забезпечення, яке дозволяє задавати конкретні інтервали часу, протягом яких двері залишатимуться відкритими після успішної верифікації користувача. Важливо також налаштувати параметри безпеки, які забезпечують блокування дверей при спробах несанкціонованого доступу.

Механізм дверей перевіряється на коректне відкриття при успішній верифікації через різні засоби аутентифікації, такі як QR-коди, картки або розпізнавання облич. Для цього проводяться тестові сценарії, де користувачі проходять верифікацію за допомогою одного з цих методів. При успішній верифікації система подає сигнал на магнітні двері, що призводить до їх відкриття. Перевіряється, що двері відкриваються без затримок та збоїв.

Крім того, проводиться тестування механізму блокування дверей при невдалій верифікації. У цьому випадку система повинна подати сигнал, який утримує двері заблокованими, запобігаючи доступу неавторизованих осіб. Це перевіряється шляхом спроби доступу з використанням невірної QR-коду, картки або за допомогою обличчя, яке не зареєстроване в системі.

Також тестується функція автоматичного закриття дверей після заданого часу. Це передбачає, що після успішного проходу користувача двері залишаються відкритими протягом певного проміжку часу, а потім автоматично закриваються.

Перевіряється, що ця функція працює коректно, та двері закриваються через встановлений час без збоїв. Це гарантує, що двері залишаються відчиненими лише на необхідний час, забезпечуючи безперервний контроль доступу та безпеку приміщень.

Усі компоненти системи контролю доступу пройшли ретельне функціональне тестування. Було підтверджено, що система верифікації QR-кодів та карток функціонує надійно, сканери правильно відображають результати верифікації, а магнітні двері відкриваються та закриваються відповідно до сценаріїв доступу. Тестування показало, що система здатна забезпечити ефективний та безпечний контроль доступу в умовах реального використання.

3.2. Тестування системи розпізнавання облич

Наступний етап тестування – функціональне тестування розпізнавання облич в системі. На даному етапі система знаходиться на стадії навчання та поповнення датасету облич користувачів.

Для збору зображень, я використав наявну камеру зі сканером QR кодів. Коли користувач сканує код який йому був виданий в боті, він тим самим передає дані на сервер. Сервер в свою чергу робить обробку даних, і якщо користувач який надав QR код існує в базі, він посилає сигнал і на двері щоб ті відкрилися, і на камеру, щоб забрати кадр обличчя користувача який зісканував свій пропуск. Таким чином і користувач має доступ до об'єкту, і система має для себе користь у вигляді +1 обличчя для наповнення датасету.

Далі здійснюється попередня обробка зображень, яка включає нормалізацію, масштабування та інші необхідні перетворення, щоб підготувати дані для ефективного навчання моделі. Після цього алгоритми розпізнавання облич проходять етап навчання з використанням поповненого датасету. Навчання включає налаштування моделей для оптимального розпізнавання облич у різних умовах освітлення та ракурсів.

Після навчання моделі здійснюється тестування на нових зображеннях, які не були включені до тренувального датасету. Це дозволяє оцінити точність та

надійність алгоритмів розпізнавання. Успішні результати тестування означають, що система здатна коректно розпізнавати обличчя зареєстрованих користувачів.

Для інтеграції з основною системою контролю доступу необхідно перевірити взаємодію модуля розпізнавання облич з іншими компонентами системи. Це включає перевірку коректної передачі даних між камерою, модулем обробки зображень та сервером для верифікації користувачів.

Під час тестування системи розпізнавання облич також важливо перевірити її стійкість до можливих атак, таких як використання фотографій або відеозаписів для обману системи. Це включає тестування захисних механізмів та алгоритмів виявлення підроблених спроб доступу.

Усі компоненти системи розпізнавання облич пройшли ретельне функціональне тестування. Було підтверджено, що система здатна ефективно навчатися на нових даних, коректно розпізнавати обличчя користувачів та надійно взаємодіяти з іншими компонентами системи контролю доступу. Тестування показало, що система може забезпечити високий рівень безпеки та точності в умовах реального використання.

3.3. Тестування скомпонованої системи контролю доступу з розпізнаванням облич

На початку здійснюється збір зображень облич користувачів для створення базового датасету. Ці зображення фіксуються з різних ракурсів та в різних умовах освітлення, щоб забезпечити максимальну варіативність для навчання. Поповнення датасету новими зображеннями дозволяє системі адаптуватися до реальних умов експлуатації.

Після збирання достатньої кількості даних розпочинається етап попередньої обробки, яка включає нормалізацію, масштабування та інші необхідні перетворення зображень. Це важливий крок для підготовки даних до ефективного навчання алгоритмів розпізнавання.

На етапі навчання системи використовуються наявні дані для налаштування моделей розпізнавання облич. Моделі навчаються розпізнавати обличчя користувачів у різних умовах, що забезпечує високу точність та надійність

роботи системи. Після завершення навчання проводиться тестування на нових, раніше невідомих зображеннях, щоб оцінити здатність системи до загальної верифікації користувачів.

Для інтеграції з основною системою контролю доступу здійснюється тестування взаємодії модуля розпізнавання облич з іншими компонентами. Це включає перевірку коректного обміну даними між камерою, обробкою зображень та сервером. Така перевірка гарантує, що система зможе надійно функціонувати в комплексі з іншими механізмами контролю доступу.

Особлива увага приділяється тестуванню захисних механізмів проти можливих атак, таких як спроби обману системи за допомогою фотографій або відеозаписів. Важливо переконатися, що система здатна виявляти та блокувати такі підробки, забезпечуючи високий рівень безпеки.

На завершення тестування проводиться перевірка роботи всієї системи в комплексі. Перевіряється коректність верифікації користувачів за допомогою QR-кодів, карток та розпізнавання облич, а також взаємодія зі сканерами з індикаторами та магнітними дверима. Успішні результати функціонального тестування підтверджують, що система здатна забезпечити ефективний та безпечний контроль доступу в умовах реальної експлуатації.

ВИСНОВКИ

У даній кваліфікаційній роботі була проведена розробка системи контролю доступу з використанням штучного інтелекту та застосовано модель ШІ на основі OpenCV в ДПУ. Досліджено існуючі системи контролю доступу, їх переваги та недоліки. Виявлено, що розвиток штучного інтелекту в сфері розпізнавання об'єктів та облич дозволяє створювати більш точні та ефективні системи контролю доступу.

Для розробки програмного забезпечення був проведений огляд технологій, серед яких виявлено, що використання штучного інтелекту та машинного навчання є важливими компонентами у створенні ефективних систем контролю доступу.

Проектування системи контролю доступу передбачає створення інтерфейсу для користувачів, методів автентифікації, таких як розпізнавання облич та використання карток доступу. Моделювання системи розпізнавання облич дозволяє визначити оптимальні параметри для її роботи.

Компонування системи розпізнавання облич з системою контролю доступу дозволило створити єдину систему, яка контролює доступ до об'єкту та виявляє несанкціоновані спроби доступу. Тестування систем підтвердило їх працездатність та відповідність вимогам безпеки.

Отже, розроблена система контролю доступу з використанням штучного інтелекту є актуальною та ефективною і може бути успішно впроваджена в різних сферах, де необхідно забезпечити високий рівень безпеки та контролю доступу.

Оцінка та тестування системи контролю доступу показали, що вона працездатна та відповідає вимогам. Тестування системи розпізнавання облич підтвердило її точність та швидкість роботи. Тестування скомпонованої системи контролю доступу з розпізнаванням облич підтвердило її ефективність у реальних умовах.

Розроблена автором система контролю доступу з використанням штучного інтелекту є актуальною у зв'язку зі зростанням потреб у забезпеченні безпеки об'єктів та контролю доступу до них. Штучний інтелект дозволяє значно

підвищити ефективність системи за рахунок автоматизації процесів розпізнавання та автентифікації осіб, які намагаються отримати доступ.

Ця система може бути успішно використана у різних сферах, таких як бізнес, де важливо контролювати доступ співробітників до приміщень та інформації, або в громадських місцях, де необхідно забезпечити безпеку відвідувачів та персоналу.

Перевагою цієї системи є її ефективність у виявленні несанкціонованого доступу та можливість оперативно реагувати на такі ситуації. Крім того, вона може бути легко інтегрована з існуючими системами безпеки та відеоспостереження для забезпечення ще більшого рівня захисту.

Таким чином, розроблена система контролю доступу з використанням штучного інтелекту є необхідним інструментом для забезпечення безпеки в сучасному світі, де зростає кількість загроз та потреба у надійних засобах захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Принципи побудови нейронних мереж – IT Master - електроніка та програмування. Головна – IT Master - електроніка та програмування.
URL: <https://itmaster.biz.ua/programming/vision/neural-networks-principles.html> (дата звернення 27.05.2024)
2. Учасники проєктів Вікімедіа. Згорткова нейронна мережа – Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Згорткова_нейронна_мережа (дата звернення 27.05.2024)
3. Учасники проєктів Вікімедіа. Система розпізнавання облич – Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Система_розпізнавання_облич (дата звернення 27.05.2024)
4. Учасники проєктів Вікімедіа. Штучна нейронна мережа – Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Штучна_нейронна_мережа (дата звернення 27.05.2024)
5. Учасники проєктів Вікімедіа. Hikvision – Вікіпедія. *Вікіпедія*.
URL: <https://uk.wikipedia.org/wiki/Hikvision> (дата звернення 27.05.2024)
6. Учасники проєктів Вікімедіа. Remote Desktop Protocol – Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Remote_Desktop_Protocol. (дата звернення 27.05.2024)
7. Contributors to Wikimedia projects. AnyDesk - Wikipedia. *Wikipedia, the free encyclopedia*. URL: <https://en.wikipedia.org/wiki/AnyDesk>. (дата звернення 27.05.2024)
8. Contributors to Wikimedia projects. Facial recognition system - Wikipedia. *Wikipedia, the free encyclopedia*.
URL: https://en.wikipedia.org/wiki/Facial_recognition_system. (дата звернення 27.05.2024)

9. Contributors to Wikimedia projects. Near-field communication - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Near-field_communication. (дата звернення 27.05.2024)
10. Contributors to Wikimedia projects. OpenCV - Wikipedia. *Wikipedia, the free encyclopedia*. URL: <https://en.wikipedia.org/wiki/OpenCV> (дата звернення 27.05.2024)
11. Contributors to Wikimedia projects. QR code - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/QR_code. (дата звернення 27.05.2024)
12. Contributors to Wikimedia projects. Tesla Autopilot - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Tesla_Autopilot. (дата звернення 27.05.2024)
13. Contributors to Wikimedia projects. Waymo - Wikipedia. *Wikipedia, the free encyclopedia*. URL: <https://en.wikipedia.org/wiki/Waymo> (дата звернення 27.05.2024)
14. Telegram Bot API. *Telegram APIs*. URL: <https://core.telegram.org/bots/api>. (дата звернення 27.05.2024)
15. Welcome to Python.org. *Python.org*. URL: <https://www.python.org/>. (дата звернення 27.05.2024)
16. What is facial recognition and how does it work?. *Official Site | Norton™ - Antivirus & Anti-Malware Software*. URL: <https://us.norton.com/blog/iot/how-facial-recognition-software-works#:~:text=Facial%20recognition%20uses%20technology%20and,but%20also%20raises%20privacy%20issues>. (дата звернення 27.05.2024)
17. NEURAL NETWORKS URL: <https://www.poznavayka.org/en/science-and-technology/neural-networks/>. (дата звернення 27.05.2024)
18. ML: Нейронні мережі та глибоке навчання URL: <https://evergreens.com.ua/ua/articles/neural-network.html>. (дата звернення 27.05.2024)

19. Розпізнавання обличчя: від теорії до практики URL:
https://wiki.tntu.edu.ua/Розпізнавання_обличчя:_від_теорії_до_практики
 (дата звернення 27.05.2024)

20. Могильний С.Б. Машинне навчання з використанням мікрокомп'ютерів : навч.-метод. посіб. \ за ред. О.В.Лісового та ін. –К., 2019. – 224 с.

21. Kravchenko S. N., Grishkun E. O., Vlasenko O. V. CLASSIFICATION METHODS FOR MACHINE LEARNING USING THE SCIKIT-LEARN LIBRARY. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*. 2020. Vol. 1, no. 3. P. 121–125. URL: <https://doi.org/10.32838/tnu-2663-5941/2020.3-1/19> (date of access: 28.05.2024).

22. Машинне навчання та обробка сигналів в біомедичних електронних системах. : Конспект лекцій. Київ, 2020. 97 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/b1880b6c-1111-4f9f-b6a7-daec958a0a32/content> (дата звернення: 28.05.2024).

23. Tyshchenko V. ANALYSIS OF TRAINING METHODS AND NEURAL NETWORK TOOLS FOR FAKE NEWS DETECTION. *Cybersecurity: Education, Science, Technique*. 2023. Vol. 4, no. 20. P. 20–34. URL: <https://doi.org/10.28925/2663-4023.2023.20.2034> (date of access: 28.05.2024).

24. Волонтир О. Система ідентифікації та класифікації зображень для соціальних мереж : Магістерська дисертація. Київ, 2019. 83 с.

25. Албасова А. І. БАГАТОШАРОВА МАТРИЧНА НЕЙРОННА МЕРЕЖА У ЯКОСТІ АЛЬТЕРНАТИВИ БАГАТОШАРОВОМУ ПЕРЦЕПТРОНУ ДЛЯ ЗАДАЧІ КЛАСИФІКАЦІХ ЗОБРАЖЕНЬ. Харків, 2022. С. 9–10. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/4ee70b10-1377-4f3c-b6e3-9a83885237f2/content>.

26. Акіменко В. В. Штучні нейронні мережі в задачах групування та аналізу інформації / В. В. Акіменко
27. Шестаков М. С. РОЗРОБКА НЕЙРОМЕРЕЖІ ДЛЯ ТЕСТУВАННЯ КОМП'ЮТЕРНИХ ЗАСТОСУНКІВ. 2020. URL: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/download/9715/8171> (дата звернення: 28.05.2024).
28. Mozgoenko A. A., Zinovieva O. G., Hesheva H. V. DEVELOPMENT OF SOFTWARE FOR CLASSIFICATION OF EDUCATIONAL TEXTS OF DISCIPLINES USING NEURAL NETWORKS. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*. 2021. No. 6. P. 103–109. URL: <https://doi.org/10.32838/2663-5941/2021.6/17> (дата звернення 27.05.2024)
29. Бондар І. Б. Обробка відео для розпізнавання та ідентифікації об'єктів / І. Б. Бондар – URL: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/149f6328-278d-4c94-8169-b0db42879ad9/content>. (дата звернення 27.05.2024)
30. Яровий А. А., Кашубін С. Г., Кулик О. О. РОЗПІЗНАВАННЯ МІМІЧНИХ МІКРОВИРАЗІВ ОБЛИЧЧЯ ЛЮДИНИ. С. 76–82. URL: <https://oeipt.vntu.edu.ua/index.php/oeipt/article/download/405/403/403> (дата звернення: 28.05.2024).
31. Гетьман М. С. Розпізнавання обличчя з використанням нейронних мереж / М. С. Гетьман – URL: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/bf59c7e9-ff97-4c1f-b756-f107b76fe9d9/content>. (дата звернення 27.05.2024)
32. Mrak M. FACE RECOGNITION METHODS IN VIDEO SURVEILLANCE SYSTEMS USING MACHINE LEARNING. *Information and communication technologies, electronic engineering*. 2023. Vol. 3, no. 2. P. 33–42. URL: <https://doi.org/10.23939/ictee2023.02.033> (date of access: 28.05.2024).

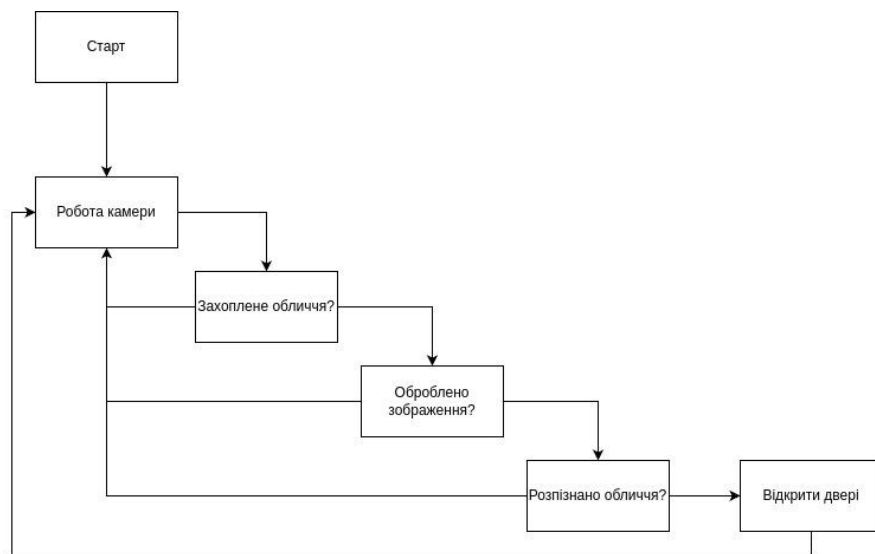
- 33.Доліна К. Методи обробки зображень на основі згорткових нейронних мереж : АТЕСТАЦІЙНА РОБОТА. Харків, 2020. 67 с. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/9723e827-df87-4855-8257-b95e0b6a0155/content> (дата звернення: 28.05.2024).
- 34.Книш Б. П. АНАЛІЗ СЕГМЕНТАЦІЇ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ [Електронний ресурс] / Б. П. Книш – URL: <https://conferences.vntu.edu.ua/index.php/mn/mn2021/paper/viewFile/13042/10966>. (дата звернення 27.05.2024)
- 35.Ковалюк Т. В. Нейромережне розпізнавання об'єктів / Т. В. Ковалюк – URL: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/aa223c43-ee50-4dd3-914b-7ae6eald19ec/content>. (дата звернення 27.05.2024)
- 36.Демішонкова А. О. Огляд та дослідження основних видів нейронних мереж для розпізнавання образів [Електронний ресурс] / А. О. Демішонкова // Сучасні інформаційні технології та програмне забезпечення комп'ютерних систем : Всеукр. наук.-практ. конф. студентів та магістрантів, 27–29 бер. 2013 р., м. Кіровоград : зб. тез доп. / М-во освіти і науки, молоді та спорту України, Кіровоград. нац. техн. ун-т. – Кіровоград, 2013. – С. 29–31. – Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/3946> (дата звернення 27.05.2024)
- 37.Ковальчук А. М. Застосування згорткової нейронної мережі для розпізнавання рукописних символів [Електронний ресурс] / А. М. Ковальчук, Г. В. Марчук, Д. К. Марчук // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки / Тавр. нац. ун-т ім. В. І. Вернадського. – Київ, 2019. – Т. 30, № 4, ч. 1. – С. 68–73. – URL: http://www.tech.vernadskyjournals.in.ua/journals/2019/4_2019/part_1/15.pdf (дата звернення 27.05.2024)

38. Синєглазов В., Чумаченко О. Глибокі Нейронні Мережі для Вирішення Завдань Розпізнавання і Класифікації Зображення. С. 274–277. URL: <https://itcm.comp-sc.if.ua/2017/Sineglazov.pdf>. (дата звернення 27.05.2024)
39. Мозговенко А. А., Зінов'єва О. Г. АНАЛІЗ МЕТОДІВ КОМП'ЮТЕРНОГО ЗОРУ В ЗАДАЧАХ ІДЕНТИФІКАЦІЇ ОСІБ У ВІДЕОПОТОЦІ. *Таврійський науковий вісник. Серія: Технічні науки*. 2022. № 3. С. 56–62. URL: <https://doi.org/10.32851/tnv-tech.2022.3.6> (дата звернення: 27.05.2024).
40. Приставка П. О. Кросплатформенна технологія цифрової обробки потокового відео на основі локальних лінійних операторів / П. О. Приставка, А. В. Ассаул // Вісник Національного авіаційного університету. - 2012. - № 3. - С. 82-86. - Режим доступу: http://nbuv.gov.ua/UJRN/Vnau_2012_3_16. (дата звернення: 27.05.2024).

ДОДАТКИ

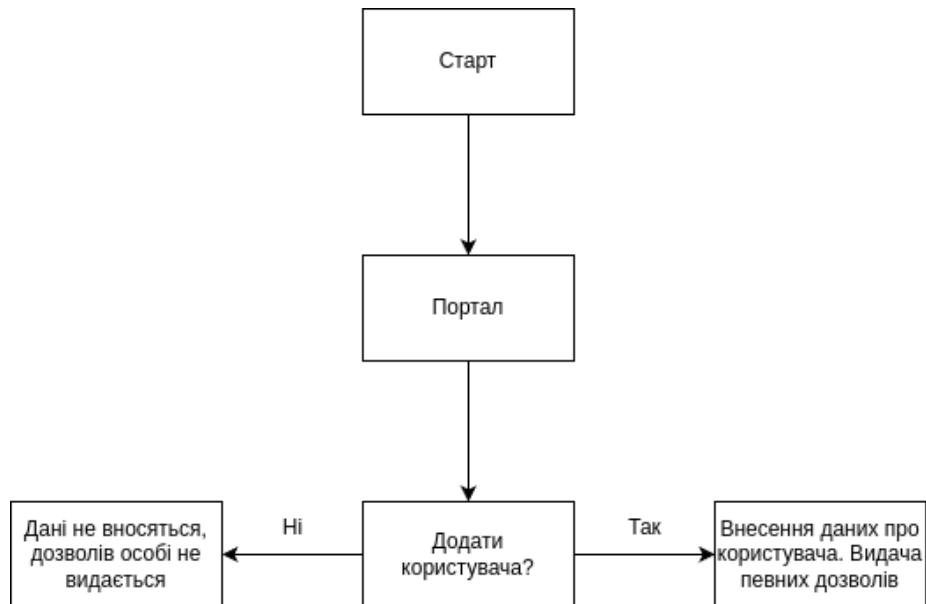
Додаток А

Загальна схема розпізнавання облич



Додаток Б

Схема реєстрації користувачів в порталі ДПУ



Додаток В

Процес обробки даних системою розпізнавання користувачів в ДПУ

