НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет інформаційних технологій

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету інформаційних технологій	**Завідувач кафедри комп'ютерних наук**
_____ Ігор БОЛБОТ_____	_____ Белла ГОЛУБ_
(підпис) (ім'я ПРІЗВИЩЕ)	(підпис) (ім'я ПРІЗВИЩЕ)
"___" _____20_ р.	"___" _____20__ р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему автоматизована система обліку персоналу на основі використання розпізнавання облич

Спеціальність 122 - Комп'ютерні науки
(код і найменування)

Освітня програма Інформаційні управляючі системи та технології
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Гарант освітньої програми

кандидат технічних наук, доцент _____ Белла ГОЛУБ
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Керівник магістерської кваліфікаційної роботи

доктор економічних наук, професор _____ Роман РУДЕНСЬКИЙ
(науковий ступінь та вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

Виконав _____ Олексій НАЗАРЧУК
(підпис) (ім'я ПРІЗВИЩЕ здобувача)

КИЇВ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет інформаційних технологій

ЗАТВЕРДЖУЮ

Завідувач кафедри комп'ютерних наук

к.т.н., доцент _____ Белла ГОЛУБ
(наукоий ступінь, вчене звання) (підпис) (ім'я ПРІЗВИЩЕ)

«____» _____ 2025 року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ

Назарчуку Олексію Васильовичу
(прізвище, ім'я, по батькові)

Спеціальність 122 - Комп'ютерні науки
(код і назва)

Освітня програма Інформаційні управляючі системи та технології
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Тема магістерської кваліфікаційної роботи

Автоматизована система обліку персоналу на основі використання розпізнавання облич

затверджена наказом ректора НУБіП України від "01" листопада 2024 р. № 1964 «С»

Термін подання завершеної роботи на кафедру 01 грудня 2025 року
(рік, місяць, число)

Вихідні дані до магістерської кваліфікаційної роботи пояснювальна записка, презентація до пояснювальної записки, Jupyter Notebooks з порівняннм алгоритмів розпізнавання облич на основі логів (завантаження та підготовка дата-сету, нормалізація даних; експерименти з порівнянням облич методами LBPH, ArcFace та SFace), репозиторій на GitHub, UML та ER-діаграми архітектури, результати тестування

Перелік питань, що підлягають дослідженню:

1. Як організувати ефективне використання бібліотеки OpenCV для детекції та розпізнавання облич?
2. Який алгоритм забезпечує кращу точність і швидкість у системі обліку персоналу: LBPH (OpenCV), ArcFace чи SFace
3. Як інтегрувати модуль розпізнавання облич із базою даних для автоматичного обліку відвідувань?
4. Як визначити рівень точності та надійності розпізнавання облич у різних зонах?

Перелік графічного матеріалу (за потреби) _____

_____

Дата видачі завдання "01" листопада 2024 р.

Керівник магістерської кваліфікаційної роботи _____ Роман РУДЕНСЬКИЙ
(підпис) (ім'я ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Олексій НАЗАРЧУК
(підпис) (ім'я ПРІЗВИЩЕ)

Календарний план

№ з/п	Назва етапів виконання магістерської кваліфікаційної роботи	Строк виконання етапів магістерської кваліфікаційної роботи	Примітка
1	Видача завдання	01.11.2024	
2	Аналіз предметної області	02.11-24.11.2024	
3	Проєктування архітектури системи та сховища даних	25.11-31.12.2024	
4	Розробка програмного забезпечення, бази даних, ETL, аналітичної моделі	01.01-30.04.2025	
5	Проведення експериментів та аналіз результатів	01.05-31.07.2025	
6	Оформлення пояснювальної записки	01.08-10.11.2025	
7	Оформлення постеру за результатами дослідження	05.10-18.10.2025	
8	Написання тез до постеру	19.10-27.10.2025	
9	Постерна сесія	28.10-29.10.2025	
10	Перевірка на плагіат	15.11.2025	
11	Попередній захист	01.12.2025	
12	Захист	05-13.12.2025	

РЕФЕРАТ

Предмет дослідження – алгоритмічні та інженерні рішення для детекції і розпізнавання облич (класичний метод LBPH з бібліотеки OpenCV; глибинні підходи на основі метричного навчання: ArcFace, SFace), архітектура інтеграції з реляційною базою даних, методики оцінювання точності та надійності системи в різних зонах спостереження та умовах експлуатації.

Мета роботи – розробити та експериментально обґрунтувати комплексний підхід до побудови системи контролю доступу з розпізнаванням облич, що забезпечує точний та швидкий облік відвідувань співробітників у реальних виробничих умовах, а також створити аналітичну надбудову для багатовимірного оцінювання ефективності та виявлення проблемних зон.

Методи дослідження. У роботі використано методи комп'ютерного зору для детекції та локалізації облич у відеопотоках; класичні та глибинні підходи машинного навчання для екстракції біометричних ознак та ідентифікації осіб; методи нормалізації зображень та контролю якості кадрів за метриками яскравості, різкості та геометричних характеристик; методи реляційного моделювання даних для проєктування, схеми бази даних з підтримкою транзакційності та індексації; методи OLAP-аналізу та багатовимірної аналітики для побудови KPI та дашбордів у Power BI; експериментальні методи порівняльного тестування алгоритмів з вимірюванням метрик точності та продуктивності; статистичні методи обробки результатів експериментів та стратифікованого аналізу за множинними факторами.

У роботі розроблено повнофункціональний конвеєр розпізнавання облич для системи контролю доступу, який інтегрує етапи детекції, нормалізації, контролю якості, екстракції ознак та прийняття рішень. Проведено систематичне порівняльне дослідження трьох алгоритмів розпізнавання (LBPH, ArcFace, SFace) у контексті специфічних вимог обліку персоналу, що дозволило визначити оптимальний баланс між точністю ідентифікації та швидкістю обробки для виробничого сценарію. Новизну становить комплексний підхід до оцінювання якості розпізнавання через призму множинних факторів впливу –

розроблено методику багатовимірного аналізу, що враховує локацію точки контролю, час доби, метрики якості кадру (яскравість, різкість, розмір обличчя, поза) та дозволяє виявляти зони деградації точності.

Спроєктовано нормалізовану схему реляційної бази даних, що забезпечує ефективне зберігання біометричних еталонів, профілів співробітників, конфігурацій пристроїв, детальних журналів подій розпізнавання з технічними метриками та причинами невдач. Схема підтримує як транзакційну обробку в реальному часі (запис подій доступу, фіксація метрик), так і аналітичні запити для побудови звітності. Розроблено систему індексації, що забезпечує швидке виконання типових запитів з фільтрацією за часовими діапазонами, пристроями, локаціями та співробітниками.

Наукова новизна полягає у систематизації методичних підходів до оцінювання якості біометричних систем контролю доступу в реальних умовах експлуатації з урахуванням варіабельності факторів середовища. Запропоновано методику адаптивного калібрування порогів прийняття рішень на основі стратифікованого аналізу статистики розпізнавання по окремих зонах та часових інтервалах, що дозволяє оптимізувати баланс між зручністю користувачів (мінімізація хибних відхилень) та безпекою (мінімізація хибних прийняттів) індивідуально для кожної локації з урахуванням її специфіки.

Розроблену систему рекомендується впроваджувати поетапно, починаючи з пілотного проєкту на обмеженій кількості точок контролю (2-3 локації з різними умовами освітлення) для калібрування параметрів та накопичення статистики. На основі зібраних результатів необхідно провести тонке налаштування порогів розпізнавання для кожної зони, визначити оптимальні алгоритми для різних сценаріїв (ArcFace для високої точності в контрольованих умовах, LBPH для обмежених обчислювальних ресурсів) та сформувати процедури технічного обслуговування камер і моніторингу метрик якості.

Для забезпечення відповідності нормативним вимогам необхідно реалізувати процедури отримання письмової згоди співробітників на обробку біометричних даних, налаштувати політики строків зберігання різних категорій журналів, впровадити рольову модель доступу до персональних даних та

аналітичних звітів. Рекомендується інтегрувати систему з існуючими корпоративними сервісами.

Для масштабування на велику кількість точок контролю (50+ пристроїв) рекомендується перейти до гібридної архітектури з попередньою обробкою та контролем якості на edge-пристроях і централізованою екстракцією ознак та пошуком по базі еталонів на серверній інфраструктурі. Критично важливо впровадити систему проактивного моніторингу, що відстежує тренди деградації якості та автоматично генерує алерти для технічної підтримки.

Результати роботи мають безпосереднє практичне застосування для підприємств, що впроваджують або модернізують системи контролю доступу та обліку робочого часу. Розроблений програмний прототип демонструє можливість створення ефективної системи розпізнавання облич з використанням відкритих бібліотек та доступного апаратного забезпечення, що значно знижує вартість впровадження порівняно з комерційними рішеннями.

Методика багатовимірного аналізу якості розпізнавання та розроблені аналітичні дашборди можуть використовуватися не лише для систем контролю доступу, але й для інших прикладних сценаріїв біометричної ідентифікації.

ABSTRACT

Subject of research – algorithmic and engineering solutions for face detection and recognition (classical LBPH method from OpenCV library; deep learning approaches based on metric learning: ArcFace, SFace), architecture of integration with relational database, methodologies for evaluating system accuracy and reliability across different surveillance zones and operational conditions.

Purpose of work – to develop and experimentally substantiate a comprehensive approach to building a face recognition access control system that ensures accurate and fast employee attendance tracking in real production environments, as well as to create an analytical framework for multidimensional performance evaluation and identification of problematic areas.

Research methods. The work employs computer vision methods for face detection and localization in video streams; classical and deep learning approaches for biometric feature extraction and person identification; image normalization methods and frame quality control based on brightness, sharpness, and geometric characteristics metrics; relational data modeling methods for database schema design supporting transactionality and indexing; OLAP analysis and multidimensional analytics methods for building KPIs and dashboards in Power BI; experimental methods of comparative algorithm testing with measurement of accuracy and performance metrics; statistical methods for processing experimental results and stratified analysis across multiple factors.

The work developed a fully functional face recognition pipeline for access control system, integrating stages of detection, normalization, quality control, feature extraction, and decision making. A systematic comparative study of three recognition algorithms (LBPH, ArcFace, SFace) was conducted in the context of specific personnel accounting requirements, which allowed determining the optimal balance between identification accuracy and processing speed for production scenarios. The novelty lies in a comprehensive approach to evaluating recognition quality through the lens of multiple influence factors – a multidimensional analysis methodology was developed that accounts for control point location, time of day, frame quality metrics

(brightness, sharpness, face size, pose) and enables identification of accuracy degradation zones.

A normalized relational database schema was designed that ensures efficient storage of biometric templates, employee profiles, device configurations, detailed recognition event logs with technical metrics and failure reasons. The schema supports both real-time transactional processing (access event recording, metrics capture) and analytical queries for reporting. An indexing system was developed that ensures fast execution of typical queries with filtering by time ranges, devices, locations, and employees.

Scientific novelty lies in systematization of methodological approaches to evaluating biometric access control system quality in real operational conditions accounting for environmental factor variability. An adaptive decision threshold calibration methodology based on stratified analysis of recognition statistics for individual zones and time intervals was proposed, which allows optimizing the balance between user convenience (minimizing false rejections) and security (minimizing false acceptances) individually for each location considering its specifics.

The developed system is recommended to be implemented in phases, starting with a pilot project on a limited number of control points (2-3 locations with different lighting conditions) for parameter calibration and statistics accumulation. Based on collected results, fine-tuning of recognition thresholds for each zone should be performed, optimal algorithms for different scenarios determined (ArcFace for high accuracy in controlled conditions, LBPH for limited computational resources), and camera maintenance procedures and quality metrics monitoring established.

To ensure regulatory compliance, procedures for obtaining employees' written consent for biometric data processing must be implemented, retention policies for different log categories configured, and role-based access model to personal data and analytical reports introduced. Integration with existing corporate services is recommended.

For scaling to large numbers of control points (50+ devices), transitioning to hybrid architecture with preprocessing and quality control on edge devices and centralized feature extraction and template database search on server infrastructure is

recommended. Implementing a proactive monitoring system that tracks quality degradation trends and automatically generates alerts for technical support is critically important.

The work results have direct practical application for enterprises implementing or modernizing access control and time tracking systems. The developed software prototype demonstrates the feasibility of creating an effective face recognition system using open-source libraries and accessible hardware, significantly reducing implementation costs compared to commercial solutions.

The multidimensional recognition quality analysis methodology and developed analytical dashboards can be used not only for access control systems but also for other biometric identification application scenarios.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СКД – система контролю доступу: комплекс апаратно-програмних засобів для керування проходами.

БД – база даних: сховище подій, метрик та еталонів (шаблонів).

OpenCV – Open Source Computer Vision Library: бібліотека CV для детекції/обробки зображень.

LBPH – Local Binary Patterns Histograms: гістрограмний варіант LBP для розпізнавання облич.

FaceNe – модель глибинного метричного навчання (triplet-loss) для ембеддингів облич.

ArcFace – модель/втрати з кутовою маржею для підвищення міжкласової відстані.

SFace – сімейство легких глибинних моделей для облич (InsightFace-стек).

PAD – Presentation Attack Detection: виявлення атак представлення («маска», екран тощо).

Embedding (ембеддинг) – вектор ознак, що описує обличчя.

Edge – крайова обробка: обчислення на пристрої/поруч з камерою.

OLTP – Online Transaction Processing.

ETL – Extract-Transform-Load: конвеєр завантаження даних у сховище.

OLAP – On-Line Analytical Processing: багатовимірна аналітика/агрегації.

k-Means – алгоритм кластеризації за відстанню до центрів мас.

PCA – Principal Component Analysis: метод зниження розмірності/візуалізації.

FRVT – Face Recognition Vendor Test: звіти NIST з тестування систем розпізнавання.

ER-модель – Entity-relationship model або Entity-relationship diagram.

SADT – Structured Analysis and Design Technique.

FAR – частота хибного прийняття сторонньої особи.

FRR – частота хибного відхилення авторизованого користувача.

ВСТУП

Системи контролю доступу на основі розпізнавання облич швидко поширюються у корпоративній та державній інфраструктурі. Разом із перевагами безконтактної ідентифікації вони породжують нові виклики: чутливість до умов зйомки (освітлення, розмиття, кут огляду), вибір алгоритму та порогів, пояснення помилок і оперативний моніторинг якості. На практиці значна частина журналів подій лишається невикористаною як джерело знань для підвищення точності. Тому актуальним є створення аналітичного контуру, який з реальних логів (успіхи/невдачі, метрики кадру, причини відмов) виділяє закономірності, порівнює методи, допомагає налаштовувати пороги та умови зйомки. Саме таке дослідження пропонується у роботі.

Об’єктом дослідження виступає процес контролю доступу з використанням технологій розпізнавання облич.

Предмет дослідження – методи та засоби аналітики журналів розпізнавання (метрики якості кадру, причини відмов, параметри алгоритмів) для оцінювання та підвищення успішності розпізнавання.

Метою дослідження є розробка і впровадження підходу до аналітики журналів розпізнавання, що дозволяє:

- порівняти алгоритми (LBPH, ArcFace, SFace) у реальних умовах;
- виявити ключові чинники невдач;
- побудувати інтерпретовані моделі класифікації “High/Low”;
- сформувати практичні рекомендації з налаштування камер і порогів, які підвищують загальну ефективність системи.

Завдання дослідження:

1. Опис бізнес-процесів обліку відвідувань, ролей і вимог безпеки; огляд бібліотек і алгоритмів OpenCV (LBPH, ArcFace, SFace) та способів оцінювання якості.
2. Використання ETL-процесів для наповнення СД.

3. Організувати ефективне використання OpenCV для детекції та розпізнавання облич.

4. Визначити, який алгоритм (LBPH, ArcFace, SFace) забезпечує найкращий баланс точність-швидкість у системі обліку персоналу?

5. Інтегрувати модуль розпізнавання з БД для автоматичного обліку відвідувань (схема, транзакції, індекси, логування невдач)?

6. Визначити як вимірювати точність і надійність розпізнавання у різних зонах та часах доби

7. Спроєктувати модулі та розмежувати сервіси (детекція, порівняння, трекінг, запис у БД, аналітика Power BI).

8. Сформувати пороги, оцінити ефект на тестовому періоді.

9. Зібрати результати у репозиторії GitHub, забезпечити повторюваність експериментів.

Для дослідження використовуються методи інтелектуального аналізу даних і статистики: класифікація алгоритмом наївного Баєса, K-means, PCA; елементи OLAP для агрегування та порівнянь. Засоби реалізації: Microsoft SQL Server, Python (pandas, scikit-learn, matplotlib), Power BI (візуальна аналітика й Python-візуали).

Для реальних журналів створено цілісний аналітичний контур, що поєднує метрики кадру та причини відмов для пояснюваної оцінки трьох методів розпізнавання.

Запропоновано інтерпретований класифікатор High/Low на базі наївного Баєса з декомпозицією за Метод-Локація-Період доби, який надає керовані ймовірності ризику відмов.

Удосконалено підхід до налаштування порогів – рекомендації для налаштування камер з урахуванням періоду доби та метрик якості кадру.

Розроблено кластерну модель (K-means+PCA), яка дозволяє оперативно виявляти деградацію умов зйомки.

Основні результати представлені на постері та усній доповіді [назва конференції/семінару, місто, рік]; підготовлено тези до публікації «Теоретичні та прикладні аспекти розробки комп’ютерних систем» 2025 року.

Структура магістерської роботи:

Розділ 1. Системний аналіз предметної області.

Опис процесів контролю доступу; огляд алгоритмів розпізнавання, огляд рішень із літератури/патентів; постановка задачі.

Розділ 2. Моделювання системи.

Функціональне та об’єктно-орієнтовне моделювання – діаграми прецедентів, послідовності, активності; ER-діаграма БД, СД; вимоги до даних і інтеграцій.

Розділ 3. Розробка системи.

Архітектура модулів (детекція, порівняння, логування, аналітика), алгоритми обробки, конвеєр даних; Jupyter-ноутбук з аналізом алгоритмів LBPH, ArcFace, SFace; інтеграція з SQL Server та Power BI.

Розділ 4. Результати дослідження.

Умови експериментів, апаратні й програмні вимоги; порівняння методів за метриками; теплові карти; класифікація High/Low (наївним Баєсом); кластеризація K-means + PCA; практичні рекомендації та оцінка впливу.

Висновки. Узагальнення результатів та напрями подальших робіт.

Додатки. SQL-скрипти, конфіги, повні таблиці метрик, UML/ER-діаграми, посилання на репозиторій.

РОЗДІЛ 1. СИСТЕМНИЙ АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Опис предметної області

Система контролю доступу з розпізнаванням облич являє собою комплексне технологічне рішення, яке забезпечує безконтактну ідентифікацію співробітників та автоматизований облік відвідувань у режимі реального часу. На відміну від традиційних методів контролю доступу, що базуються на використанні фізичних носіїв (картки, ключі) або введенні PIN-кодів, біометричний підхід на основі розпізнавання облич пропонує зручніший та більш захищений спосіб ідентифікації особи. Така система органічно поєднує сучасні технології комп'ютерного зору, машинного навчання та інформаційної безпеки, створюючи надійний інструмент для управління фізичним доступом до приміщень та контролю робочого часу персоналу [1, 5].Типовий високорівневий конвеєр обробки в системах розпізнавання облич складається з послідовності взаємопов'язаних етапів.

Спочатку відбувається детекція обличчя в потоці відеокадрів, що надходять від камер спостереження. Після успішного виявлення обличчя система виконує нормалізацію зображення, яка включає вирівнювання геометрії обличчя відповідно до еталонної орієнтації та масштабування до стандартного розміру. Наступним кроком є отримання ознакового подання обличчя у вигляді компактного числового вектора (ембеддінгу), що зберігає унікальні характеристики особи. Цей вектор порівнюється з еталонними зразками, що зберігаються в базі даних системи, і на підставі міри подібності та встановленого порогу приймається рішення про ідентифікацію особи [3, 4].

Якість роботи системи суттєво залежить від низки факторів, пов'язаних з умовами зйомки. До них належать характеристики освітленості сцени, різкість зображення, кут повороту та нахилу голови (поза обличчя), а також наявність часткових перекриттів (оклюзій) через аксесуари, такі як окуляри, маски чи інші предмети. Не менш важливими є технічні характеристики обладнання –

роздільна здатність камер, якість оптики об'єктивів, швидкість захоплення кадрів та обчислювальна потужність апаратної платформи.

Окремого значення набувають параметри налаштування алгоритмічної частини системи, зокрема пороги прийняття рішень, які визначають баланс між помилками першого роду (хибне прийняття) та другого роду (хибне відхилення) [3, 4].Для виробничого використання систем розпізнавання облич критично важливими стають питання, що виходять за межі суто технічної точності алгоритмів. По-перше, продуктивність системи та час відгуку (затримка від моменту появи особи до прийняття рішення) безпосередньо впливають на пропускну здатність точок контролю та комфорт користувачів. По-друге, питання приватності та захисту біометричних персональних даних потребують особливої уваги з огляду на регуляторні вимоги та національного законодавства про захист персональних даних. По-третє, система повинна бути стійкою до атак представлення, коли зловмисник намагається обдурити систему, використовуючи фотографії, відео, маски чи інші підроблені біометричні зразки [1, 8].

Ключові бізнес-процеси системи контролю доступу охоплюють повний життєвий цикл роботи з користувачами та подіями. Процес реєстрації користувачів передбачає відбір якісних біометричних еталонів у контрольованих умовах, валідацію їх придатності для подальшого розпізнавання, а також дотримання політик отримання згоди на обробку біометричних даних та забезпечення конфіденційності відповідно до вимог законодавства [1, 8].

Основний робочий режим системи – онлайн-розпізнавання на точках доступу забезпечує ідентифікацію співробітників у момент проходження через контрольовану зону та автоматичне прийняття рішення про надання чи відмову в доступі.

Інтеграція системи з фізичними виконавчими пристроями, такими як турнікети та електронні замки, дозволяє автоматизувати процес контролю проходів без необхідності втручання персоналу охорони. При цьому всі події розпізнавання, як успішні, так і невдалі спроби доступу, детально журналюються

разом з метриками якості кадру та технічними параметрами обробки. Ці дані стають основою для побудови системи аналітики, що надає керівництву та службам безпеки можливість отримувати KPI системи, формувати звіти про відвідуваність та спізнення співробітників, а також проводити аудити використання системи для виявлення аномалій та потенційних інцидентів безпеки.

1.2. Дані, метрики якості та оцінювання

Вхідними даними для системи розпізнавання облич є безперервні відеопотоки або окремі кадри, що надходять від мережі камер, розташованих у точках контролю доступу. Разом з візуальною інформацією система обробляє метадані, що характеризують джерело зображень – ідентифікатори камер, їх фізичне розташування, технічні характеристики та параметри налаштування.

Центральним елементом системи є довідник біометричних еталонів (шаблонів), що містить векторні подання облич зареєстрованих співробітників. У виробничих умовах експлуатації ці базові компоненти доповнюються складною інфраструктурою, яка забезпечує надійність роботи, контроль затримок обробки, керованість налаштувань порогів розпізнавання та дотримання політик інформаційної безпеки.

Для ефективного керування якістю розпізнавання система повинна аналізувати та контролювати базові метрики якості кадру вже на етапі захоплення зображення. До таких метрик належать середня яскравість кадру та розподіл яскравості, що характеризують умови освітлення; контраст зображення, який впливає на розрізнюваність деталей; міра розмиття, що оцінюється через оператори виявлення країв та визначає різкість зображення; а також геометричні характеристики, такі як розмір виявленого обличчя відносно загального розміру кадру та його положення [3, 4].

Ці параметри прямо впливають на стійкість розпізнавання та стабільність біометричних ознак, що екстрагуються нейронною мережею. Низька якість вхідних даних може призводити до деградації точності навіть найсучасніших

алгоритмів, тому превентивний контроль якості кадру є критично важливим етапом конвеєру обробки.

Оцінювання та тестування біометричних систем регламентується міжнародними стандартами, що визначають методологію та метрики для порівняльного аналізу. Стандарти серії ISO/IEC 19795 встановлюють процедури тестування продуктивності біометричних систем, включаючи вимоги до організації експериментів, статистичної обробки результатів та формату звітності [8].

Ці документи визначають такі ключові показники, як – частота хибного прийняття сторонньої особи, частота хибного відхилення авторизованого користувача, та точка, в якій FAR та FRR збігаються, що використовується як інтегральна міра якості системи.

Окремим напрямком стандартизації є протидія атакам представлення, що регламентується серією ISO/IEC 30107. Ці стандарти визначають рамку для оцінювання стійкості біометричних систем до спуфінгу (підробки біометричних даних) та встановлюють вимоги до механізмів виявлення живості [6, 8]. Для систем розпізнавання облич це означає необхідність детектування спроб обдурити систему за допомогою фотографій, відеозаписів, масок чи інших артефактів, що імітують справжнє обличчя.

Еволюція підходів до розпізнавання облич відображає загальний тренд розвитку машинного навчання від ручного конструювання ознак до автоматичного навчання глибоких представлень. Ранні методи базувалися на локальних дескрипторах, таких як Local Binary Patterns та його варіант LBPH, що широко представлений у бібліотеці OpenCV та залишається практичним вибором для обмежених обчислювальних ресурсів [4]. Однак справжній прорив у точності розпізнавання став можливим завдяки появі методів глибинного метричного навчання, де обличчя відображається у високорозмірний векторний простір таким чином, що класи виявляються добре розділеними, а відстань між векторами корелює з подібністю облич.

Серед репрезентативних підходів нового покоління особливе місце займає архітектура FaceNet, запропонована дослідниками Google. Ця система використовує triplet loss функцію втрат для навчання нейронної мережі генерувати 128-вимірні ембеддінги, де евклідова відстань безпосередньо відповідає ступеню подібності облич [2].

Подальшим розвитком цього напрямку став метод ArcFace, що застосовує кутову функцію втрат для покращення міжкласової сепарабельності. ArcFace демонструє особливо високу стабільність на великих наборах даних та стійкість до варіацій у позі, освітленні та віці особи [7].

Для детекції облич сучасні системи майже повсюдно використовують згорткові нейронні мережі. Практичною опорою для розробників прикладних систем служить екосистема InsightFace – відкритий проект, що надає інтеграцію високоякісної детекції та екстракції ембеддінгів у зручному програмному інтерфейсі [9]. Паралельно інструментарій OpenCV залишається незамінним для попередньої обробки зображень, нормалізації, контролю якості та інтеграції з периферійним обладnанням [4].

Процес оцінювання та вибору оптимальних алгоритмів для конкретного прикладного сценарію значною мірою орієнтується на результати масштабних незалежних тестувань, таких як програма FRVT. Ці звіти надають порівняння точності комерційних та академічних алгоритмів на стандартизованих наборах даних, оцінюють стійкість до різних типів варіацій (вік, етнічна приналежність, умови зйомки) та встановлюють узгоджені метрики для об'єктивного порівняння [5]. Результати FRVT у поєднанні з вимогами стандартів ISO/IEC 19795 щодо методології тестування слугують референтною рамкою для прийняття обґрунтованих інженерних рішень при побудові виробничих систем [8].

На практичному рівні конвеєри розпізнавання в промислових системах включають кілька критично важливих компонентів, які виходять за межі базового алгоритму розпізнавання. Попередній контроль якості відфільтровує кадри, непридатні для надійного розпізнавання, економлячи обчислювальні ресурси та зменшуючи кількість помилкових спрацьювань. Етап нормалізації

приводить зображення обличчя до стандартизованого вигляду, компенсуючи варіації в розташуванні, розмірі та поворотах. Процедура зіставлення з еталонами оптимізується через індексні структури для швидкого пошуку в великих базах даних. Нарешті, прийняття рішення здійснюється на основі адаптивних порогів, які враховують специфіку конкретної локації, часу доби та поточних умов зйомки [1, 8].

1.3. Архітектурні патерни впровадження

Архітектурний дизайн системи розпізнавання облич визначає фундаментальний розподіл обчислювальних операцій та даних між периферійними пристроями, центральними серверами та хмарною інфраструктурою. Вибір між edge-орієнтованою, серверною, хмарною або гібридною архітектурою диктується балансом між латентністю системи, обсягом переданих персональних даних, складністю керування розподіленою інфраструктурою та вимогами до масштабованості.

Edge-архітектура (обробка на пристрої) передбачає розміщення всього конвеєру розпізнавання, включаючи детекцію, екстракцію ознак та порівняння з локальною базою еталонів, безпосередньо на периферійному обчислювальному модулі, інтегрованому з камерою або розташованому поблизу неї. Така схема забезпечує мінімальні затримки обробки, оскільки повністю виключає необхідність передачі відеопотоку мережею, що критично важливо для сценаріїв з жорсткими вимогами до часу відгуку. Додатковою перевагою є мінімізація обсягу персональних даних, що передаються мережею та потенційно можуть бути перехоплені - у разі edge-обробки по каналах зв'язку передаються лише результати ідентифікації та метадані події, але не сирі біометричні дані [6, 9].

Водночас edge-підхід висуває суттєві вимоги до локальних обчислювальних ресурсів, оскільки сучасні глибокі нейронні мережі для розпізнавання облич потребують спеціалізованих акселераторів для забезпечення прийнятної продуктивності. Додатковою складністю стає процедура оновлення моделей та еталонної бази на розподілених edge-

пристроях, що потребує продуманої системи, синхронізації та відкату змін у разі виявлення проблем. Для підприємств з десятками чи сотнями точок контролю управління життєвим циклом edge-компонентів може перетворитися на значну операційну складність.

Серверна або хмарна архітектура централізує обчислювальні операції на потужних серверних платформах або в хмарній інфраструктурі. Периферійні камери та термінали виступають пасивними джерелами відеопотоку, що передається на центральну систему для обробки. Такий підхід суттєво спрощує керування моделями розпізнавання, еталонною базою та аналітичними системами - всі оновлення, налаштування та моніторинг виконуються централізовано [1]. Серверна архітектура також дозволяє ефективніше використовувати обчислювальні ресурси через мультиплексування - один потужний сервер може паралельно обслуговувати десятки відеопотоків, тоді як у edge-схемі кожен пристрій потребує власних обчислювальних можливостей.

Проте централізована обробка створює жорсткі вимоги до мережевої інфраструктури, оскільки передача множинних відеопотоків високої роздільності потребує значної пропускної здатності каналів зв'язку. Будь-які проблеми з мережевою доступністю або перевантаженням каналів безпосередньо впливають на роботу всієї системи контролю доступу. Критично важливими стають питання захисту біометричних даних у транзиті (шифрування каналів) та у спокої (захист серверних сховищ), оскільки компрометація центрального сервера означає витік всіх біометричних шаблонів організації [8].

Гібридна архітектура прагне поєднати переваги обох підходів, розподіляючи обчислювальні операції між периферією та центром відповідно до їх характеристик. Типова гібридна схема виконує попередній скринінг якості кадру та перевірку PAD на edge-пристрої, відфільтровуючи непридатні зображення та потенційні атаки вже на етапі захоплення. Лише кадри, що пройшли первинну валідацію, передаються на сервер для точної екстракції ембеддінгів глибокою нейронною мережею та пошуку по великій централізованій галереї еталонів [1, 6, 9]. Така схема зменшує навантаження на

мережу порівняно з повністю серверним підходом, зберігаючи при цьому переваги централізованого керування та доступу до потужніших моделей.

У виробничих системах контролю доступу доцільно проєктувати архітектуру як набір асинхронних конвеєрів обробки, пов'язаних через черги повідомлень або шину подій. Кожен етап може масштабуватися незалежно відповідно до свого профілю навантаження - наприклад, детекція може бути відносно легковагою, тоді як екстракція ознак потребує GPU-прискорення [1].

Асинхронна архітектура на основі черг надає кілька суттєвих переваг. По-перше, вона природним чином підтримує горизонтальне масштабування - для збільшення пропускної здатності достатньо додати додаткові екземпляри обробників критичних етапів. По-друге, черги виступають буферами, що згладжують пікові навантаження та забезпечують graceful degradation у разі тимчасового перевантаження окремих компонентів. По-третє, така архітектура спрощує моніторинг та діагностику, оскільки для кожного етапу можна окремо відстежувати метрики продуктивності та ідентифікувати вузькі місця. По-четверте, асинхронність полегшує відновлення після збоїв - повідомлення в чергах зберігаються до успішної обробки, що забезпечує семантику доставки подій.

Критично важливим компонентом архітектури є система журналювання, що зберігає детальну інформацію про всі події розпізнавання. Доцільно підтримувати окремі логи для успішних ідентифікацій та невдалих спроб, доповнюючи їх технічними метриками кадру (яскравість, різкість, розмір обличчя, поза) та параметрами обробки (час виконання кожного етапу, використаний метод розпізнавання, міра подібності). Таблиці логів повинні бути індексовані за часом події та ідентифікатором пристрою для забезпечення швидкого виконання типових аналітичних запитів. Ці дані стають основою для OLAP-аналізу та побудови інтерактивних дашбордів у BI-інструментах, що дозволяють керівництву відстежувати KPI системи, виявляти тренди та аномалії [10, 12].

Практичні виробничі системи повинні реалізовувати строге версіонування моделей розпізнавання та еталонної бази. Кожна зміна моделі (оновлення ваг нейронної мережі, зміна архітектури) або набору еталонів (додавання нових співробітників, оновлення існуючих шаблонів) супроводжується створенням нової версії з можливістю швидкого відкату до попередньої у разі виявлення деградації якості. Процедура оновлення повинна включати етап тестування на підмножині пристроїв перед повним розгортанням. Пороги подібності для прийняття рішення про ідентифікацію доцільно калібрувати окремо для різних локацій та частин доби, враховуючи специфічні умови зйомки [5, 8].

Система моніторингу повинна відстежувати не лише технічні метрики продуктивності, але й зміни в розподілах якісних характеристик розпізнавання. Систематичний зсув у розподілі яскравості кадрів може сигналізувати про зміну умов освітлення, що вимагає перекалібрування; зростання частки розмитих кадрів може вказувати на необхідність очищення оптики або заміни камери; збільшення середньої відстані в embedding-просторі між зразком та еталоном може свідчити про старіння біометричних шаблонів та необхідність їх оновлення. Проактивний моніторинг цих індикаторів дозволяє тригерувати процедури технічного обслуговування до того, як проблеми призведуть до суттєвої деградації якості обслуговування користувачів.

Біометричні дані відносяться до категорії особливо чутливих персональних даних, що висуває підвищені вимоги до їх захисту. Одним з ключових принципів є мінімізація даних - де це технічно можливо, система повинна зберігати лише компактні числові ембеддінги замість сирих зображень облич, оскільки вектори набагато складніше використати для реконструкції зовнішності особи. Ембеддінги повинні зберігатися в зашифрованому вигляді з використанням сучасних алгоритмів симетричного шифрування (AES-256), а ключі керуватися через спеціалізовані системи управління секретами (key management systems) [8].

Архітектура системи повинна реалізовувати строге розмежування доступів на основі ролей, обмежуючи можливості кожного компонента та користувача

лише необхідним мінімумом привілеїв. Всі операції з персональними даними повинні детально аудитуватися з незмінними логами, що дозволяють простежити хто, коли та до яких даних отримував доступ. Система повинна підтримувати прозорі політики щодо строків зберігання різних категорій даних та автоматизоване видалення даних після закінчення легітимного строку їх збереження або на запит суб'єкта даних відповідно до права на забуття.

Протидія атакам представлення реалізується через підсистему Presentation Attack Detection, що аналізує додаткові ознаки зображення. Сучасні PAD-системи поєднують кілька підходів: аналіз текстурних особливостей (справжня шкіра має характерні мікротекстури, відсутні на фото); детекцію карт глибини, отриманих стереокамерами або сенсорами; виявлення мікрорухів та фізіологічних процесів (пульсація крові, мікровібрації); спектральний аналіз у різних діапазонах (інфрачервоний, ультрафіолетовий), що дозволяє виявити матеріали, відмінні від живої тканини. Комбінація цих методів відповідно до рекомендацій ISO/IEC 30107-1 дозволяє досягти високого рівня захисту від широкого спектру атак, від найпростіших (роздруковане фото) до складних (3D-маски) [6]

1.4. Постановка завдання магістерського дослідження

Метою даного магістерського дослідження є розробка та експериментальне обґрунтування комплексного підходу до побудови системи контролю доступу з розпізнаванням облич та створення аналітичної надбудови для оцінювання її ефективності. Дослідження спрямоване на забезпечення точного та швидкого обліку відвідувань співробітників у реальних умовах експлуатації з урахуванням варіабельності освітлення, кутів зйомки та інших факторів, що впливають на якість розпізнавання в промислових сценаріях.

Об'єктом дослідження виступають процеси детекції та розпізнавання облич у контексті автоматизованої системи обліку персоналу та контролю доступу до приміщень підприємства. Предметом дослідження є алгоритмічні рішення для детекції облич та екстракції біометричних ознак, зокрема

порівняння класичних методів (LBPH з бібліотеки OpenCV) та сучасних підходів на основі глибокого навчання (ArcFace, SFace). Окрему увагу приділено інженерним аспектам інтеграції алгоритмічних компонентів з реляційною базою даних для зберігання подій, еталонів та метрик, а також методикам оцінювання точності й надійності системи в різних зонах спостереження та під час різних періодів доби [2, 7, 9].

Дослідження структуроване навколо чотирьох основних дослідницьких питань, що охоплюють повний цикл проєктування та оцінювання системи. Перше завдання полягає у проєктуванні ефективного конвеєру детекції облич та попередньої обробки зображень. Це включає вибір та налаштування методів детекції (каскади Хаара, глибокі детектори), алгоритмів вирівнювання обличчя за ключовими точками для компенсації варіацій у позі, а також розробку системи контролю якості кадру, що автоматично оцінює придатність зображення для подальшого розпізнавання на основі метрик яскравості, різкості, розміру обличчя та кута повороту [3, 4].

Друге дослідницьке питання фокусується на проведенні контрольованих та відтворюваних експериментів для порівняння альтернативних алгоритмів розпізнавання. Необхідно емпірично встановити, який з розглянутих підходів (LBPH, ArcFace, SFace) забезпечує оптимальний баланс між точністю ідентифікації та швидкістю обробки у специфічному сценарії обліку персоналу. Експерименти повинні включати вимірювання як accuracy-метрик, так і показників продуктивності. Результати мають бути статистично значущими та отриманими на репрезентативному наборі даних, що відображає реальні умови експлуатації [2, 5, 7, 13].

Третє завдання присвячене розробці схеми бази даних та транзакційної логіки для надійного збереження всієї інформації, генерованої системою. Схема БД повинна забезпечувати ефективне зберігання профілів співробітників, біометричних еталонів, конфігурацій пристроїв, а також детальних журналів подій розпізнавання. Особлива увага приділяється проєктуванню структур для логування як успішних ідентифікацій, так і невдалих спроб з фіксацією причин

відмови (низька якість кадру, незареєстроване обличчя, недостатня впевненість). Кожна подія повинна супроводжуватися набором технічних метрик (час обробки, використаний метод, міра подібності, параметри якості кадру), що створює основу для подальшого аналізу. Схема індексації таблиць має забезпечувати швидке виконання типових аналітичних запитів з фільтрацією за часовими діапазонами, пристроями, локаціями та іншими атрибутами [10, 14, 15, 16, 17].

Четверте дослідницьке питання стосується розробки методології вимірювання та порівняльного аналізу якості розпізнавання в різних умовах експлуатації. Необхідно визначити процедури стратифікованого аналізу, що дозволяють виявити залежність точності системи від локації (точки контролю з різними умовами освітлення та кутами зйомки), часу доби (ранок/день/вечір з природним або штучним освітленням), а також метрик якості кадру. На основі зібраних даних необхідно побудувати візуалізації у вигляді теплових карт, розподілів, зрізів по різних вимірах, що дозволять ідентифікувати проблемні зони та умови. Результати аналізу повинні стати основою для розробки рекомендацій щодо калібрування порогів прийняття рішень індивідуально для кожної зони, що дозволить оптимізувати баланс між зручністю користувачів (низький FRR) та безпекою (низький FAR) з урахуванням специфіки локації [5, 8, 12].

РОЗДІЛ 2. МОДЕЛЮВАННЯ СИСТЕМИ

2.1. Функціональний підхід до моделювання

Функціональне моделювання являє собою один з фундаментальних підходів до аналізу та проєктування складних систем, що розглядає досліджуваний об'єкт як організовану мережу взаємопов'язаних процесів або функцій. На відміну від структурного підходу, який акцентує увагу на статичній організації компонентів системи, функціональна модель фокусується на динамічній поведінці - як саме система перетворює вхідні потоки інформації, матеріалів або енергії на вихідні результати за визначеними правилами та алгоритмами [11].

Ключовою ідеєю функціонального моделювання є декомпозиція складної системи на ієрархію простіших функцій з чітко визначеними інтерфейсами. Кожна функція характеризується своїми входами, виходами, механізмами та керуючими впливами. Такий систематичний підхід дозволяє аналітику послідовно деталізувати розуміння системи, рухаючись від загального контексту до конкретних низькорівневих операцій, при цьому зберігаючи цілісне бачення взаємозв'язків між компонентами.

Для систем контролю доступу з розпізнаванням облич функціональне моделювання особливо важливе, оскільки дозволяє явно описати складні потоки обробки даних - від захоплення відеокадру камерою до прийняття рішення про надання доступу та фіксації події в журналі. Акцент у функціональному моделюванні робиться на поведінці процесів та потоках інформації між ними. Аналітик відповідає на питання: які дані споживає кожен процес, які перетворення з ними відбуваються, які проміжні та кінцеві результати генеруються, які зовнішні фактори впливають на виконання процесу, які виключні ситуації можуть виникнути та як система на них реагує. Детальне розуміння цих аспектів критично важливе на етапі проєктування архітектури, оскільки визначає розподіл відповідальності між програмними модулями, вибір

протоколів обміну даними, стратегії обробки помилок та масштабування системи під зростаюче навантаження [11, 14].

2.1.1. Контекстна діаграма

Контекстна діаграма автоматизованої системи обліку персоналу на основі використання розпізнавання облич зображена на Рис.2.1, показує потік даних через розроблювану систему, що дає змогу максимально актуалізувати програмний додаток для користувачів системи.

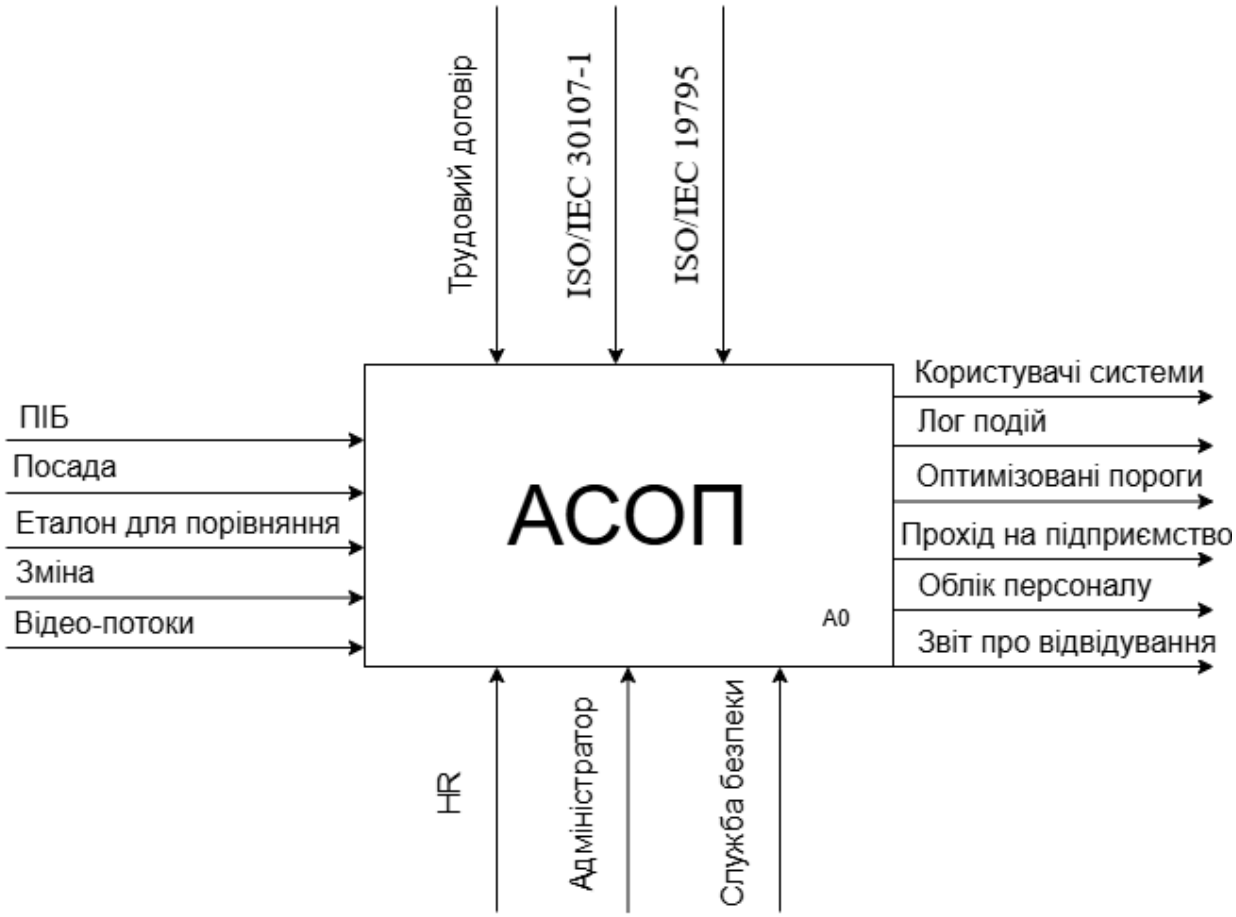


Рис. 2.1 – контекстна діаграма за методологією SADT

2.1.1. SADT діаграма

SADT – технологія структурного аналізу і проектування), заснована на концепції «сутність-зв'язок» (entity-relationship). Являє собою подальший розвиток методології структурного аналізу і проектування.

Методологія SADT розроблена Дугласом Россом. На її основі розроблена, зокрема, відома методологія IDEF0 (Icam DEFinition), яка є основною частиною програми інтеграції комп'ютерних та промислових технологій, що проводиться за ініціативою ВПС США.

Методологія SADT являє собою сукупність методів, правил і процедур, призначених для побудови функціональної моделі об'єкта будь-якої предметної області. Функціональна модель SADT відображає функціональну структуру об'єкта, тобто вироблені їм дії і зв'язку між цими діями [11].

При створенні моделі спочатку необхідно зобразити найвищий рівень – дію контексту. Найменування дії описує систему безпосередньо і, як правило, складається з одного активного дієслова в поєднанні з узагальнюючим іменником, яке роз'яснює мету діяльності з точки зору самого загального погляду на систему.

Кожен блок може мати різні типи пов'язаних з ним стрілок. Стрілки позначають людей, місце, речі, поняття або події. Стрілки пов'язують кордони діаграм з блоками, а також дії (блоки) на діаграмі між собою. У діаграмах IDEF0 є чотири основні типи стрілок.

Вхід блоку представляє матеріал або інформацію, яка повинна бути використана або перетворена блоком, щоб виробити продукцію (випуск). Стрілки входу завжди направляються в ліву сторону блоку. Стрілки входу необов'язкові, так як не всі дії можуть перетворити або змінювати (заміняти) що-небудь.

SADT діаграма 0 рівня автоматизованої системи обліку персоналу на основі використання розпізнавання облич зображена на Рис.2.2

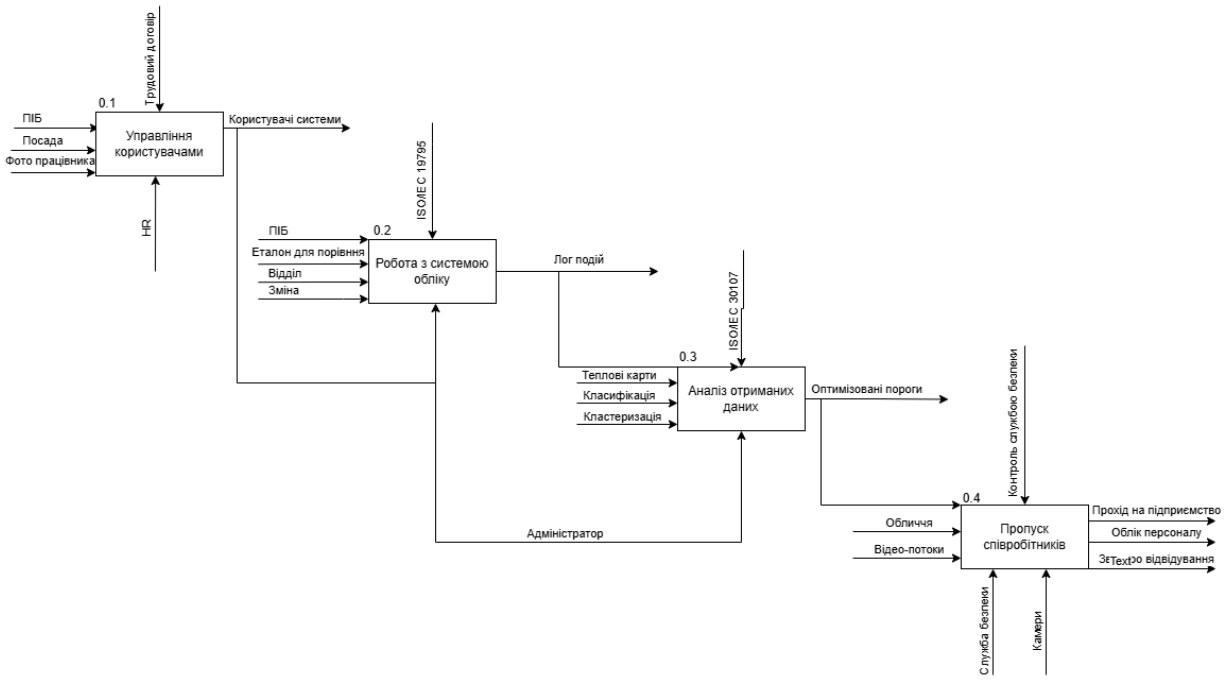


Рис. 2.2 – SADT діаграма 0 рівня

2.2. Об’єктно-орієнтований підхід до моделювання

Об’єктно-орієнтоване моделювання представляє систему як сукупність об’єктів/класів із станами, поведінкою та відповідностями. Наголос робиться на інкапсуляції, контрактах інтерфейсів, зв’язках і композиції компонентів, що забезпечує масштабованість і повторне використання.

2.2.1. Діаграма прецедентів

Діаграма прецедентів відображає основні функціональні можливості системи АСОП та взаємодію між різними акторами і системою. Вона дозволяє візуалізувати функціональність системи, що забезпечується для різних категорій користувачів. Основні актори системи – адміністратор, аналітик, HR та інспектор з безпеки. Кожен із них взаємодіє із системою для виконання своїх задач. Діаграма прецедентів для АСОП зображена на Рис. 2.3.

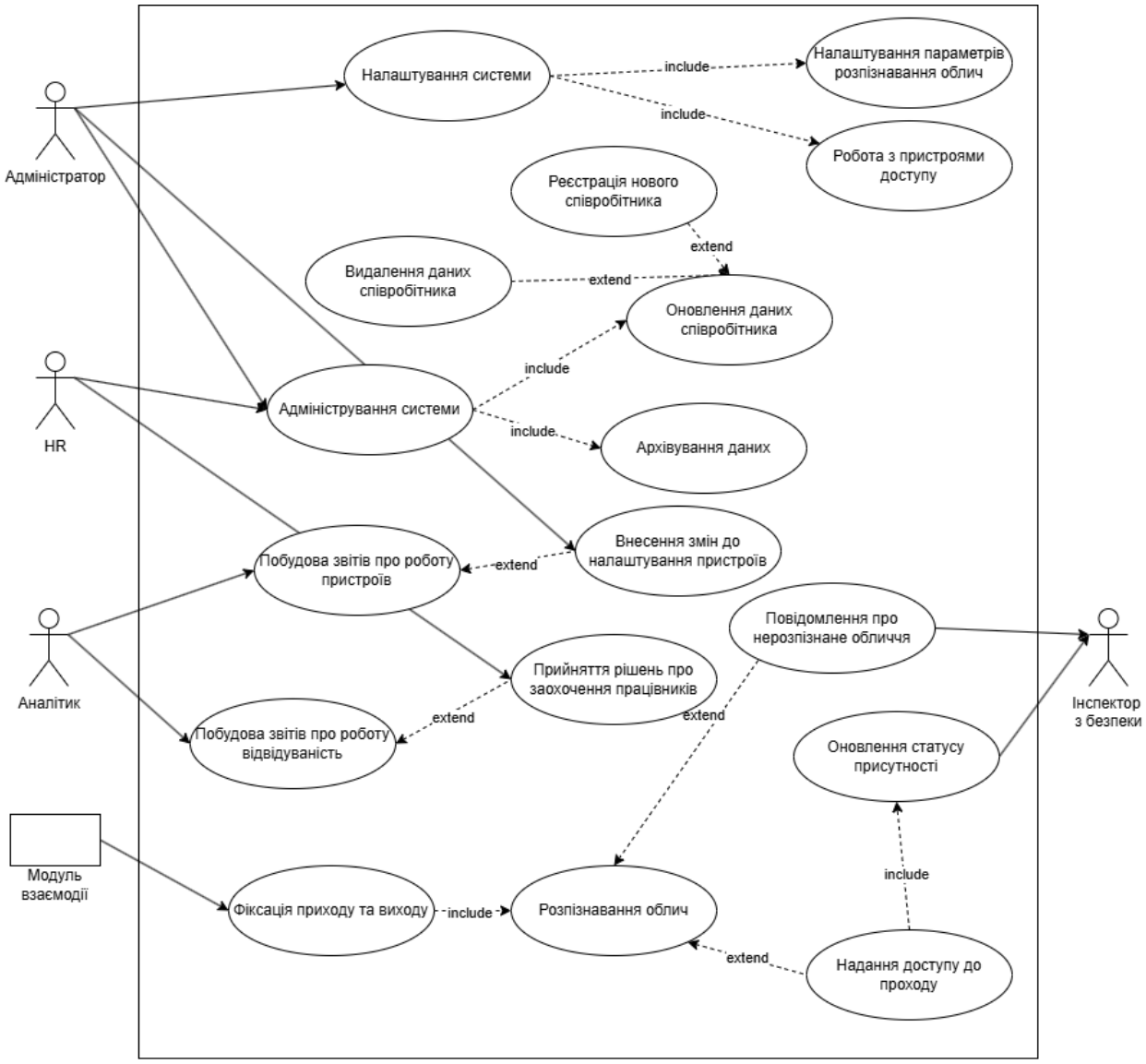


Рис. 2.3 – діаграма прецедентів АСОП

Основні актори:

Адміністратор – відповідає за налаштування і підтримку системи. Виконує адміністрування системи, включаючи оновлення даних співробітників, видалення застарілих даних, архівування даних, роботу з пристроями доступу, а також має можливість налаштовувати параметри розпізнавання облич

Аналітик – відповідає за формування звітів щодо відвідуваності та роботі пристроїв.

HR – використовує дані звітів для прийняття рішень про преміювання чи інших управлінських дій та виконує адміністрування системи. Включаючи реєстрацію, оновлення, архівування та видалення даних.

Інспектор з безпеки – отримує інформацію в реальному часі про спроби входу співробітників .

Опис основних прецедентів:

Адміністрування системи – адміністратор виконує оновлення, архівування або видалення даних співробітників. Додатково, налаштовує параметри розпізнавання облич, взаємодіє з пристроями доступу.

Реєстрація та видалення співробітників – реалізується як розширення прецеденту "Оновлення даних співробітника". Дозволяє реєструвати нового співробітника або видаляти дані існуючого.

Фіксація приходу та виходу – включає прецеденти розпізнавання облич, оновлення статусу присутності та надання доступу до приміщення.

Повідомлення про нерозпізнане обличчя – генерується, якщо система не може ідентифікувати співробітника.

Побудова звітів про відвідуваність – викликається аналітиком на основі даних зі сховища. Звіти можуть використовуватися менеджерами для прийняття рішень.

Побудова звітів про роботу пристроїв – викликається аналітиком на основі даних зі сховища. Звіти можуть використовуватися адміністратором для корегувань роботи пристроїв.

Сповіщення про спробу несанкціонованого доступу – інспектор з безпеки отримує сповіщення в разі виявлення порушень.

Діаграма прецедентів чітко демонструє функціональну архітектуру системи та її інтеграцію з робочими процесами організації. Це забезпечує зручність для подальшого розроблення, тестування та впровадження системи.

2.2.2. Діаграма послідовності

Діаграма послідовності відображає покрокову взаємодію акторів і підсистем під час проходу співробітника через точку контролю. Діаграма послідовності відображена у додатку А.

Учасники – співробітник, камера, детектор облич, фільтр якості, розпізнавач, модуль порогів, журнал подій, контролер доступу, турнікет.

1. Захоплення та детекція – співробітник підходить до точки контролю; Камера передає кадр у детектор облич. Детектор виділяє область обличчя й передає її у фільтр якості.

2. Скринінг якості – фільтр якості оцінює різкість/розмиття, яскравість/контраст, площу обличчя, кут. Якщо показники нижчі за поріг, формується гілка alt: «Якість низька». У Журнал подій записуються метрики кадру й причина відмови, а Контролер доступу отримує команду «Відмова у проході».

3. Виділення ознак і порівняння – за прийнятної якості відбувається вирівнювання обличчя; розпізнавач обчислює векторні ознаки та повертає відсоток/міру відповідності еталону.

4. Прийняття рішення – модуль порогів застосовує актуальні пороги (можуть залежати від локації/частини доби/камери) і формує рішення Дозвіл / Відмова. Подія логується. Журнал подій зберігає статус, оцінку схожості, час обробки, метод і метрики кадру.

5. Виконавча дія – для дозволу контролер доступу надсилає команду турнікету «Відкрити»; у лог додається запис «прохід». Для відмови логується ідентифікатор (якщо відомий) або позначка «нерозпізнано», причина відмови та технічні параметри.

Альтернативні гілки (alt) чітко показані на діаграмі:

- Якість низька – миттєва відмова з фіксацією причин;
- Схожість нижче порогу – відмова, запис «нерозпізнане обличчя»;
- Схожість вище порогу – дозвіл і відкриття турнікета.

Таким чином діаграма демонструє повний цикл виконання проходу працівника, а також місця прийняття альтернативних рішень. Вона слугує основою для подальшого проєктування інтерфейсів між модулями, налаштування та логування, а також для формалізації сценаріїв тестування й аудиту.

2.2.3. Діаграма активності

Діаграма активності моделює потік виконання у процесі. Послідовність дій, розгалуження за умовами, можливі об’єднання гілок, паралельні ділянки та події завершення. Вона добре підходить для опису бізнес-процесів і сценаріїв взаємодії користувача з системою, показуючи хто виконує яку дію, коли приймається рішення та який результат фіксується.

Для події «Реєстрація користувача» діаграма активності зображена на Рис.2.4.

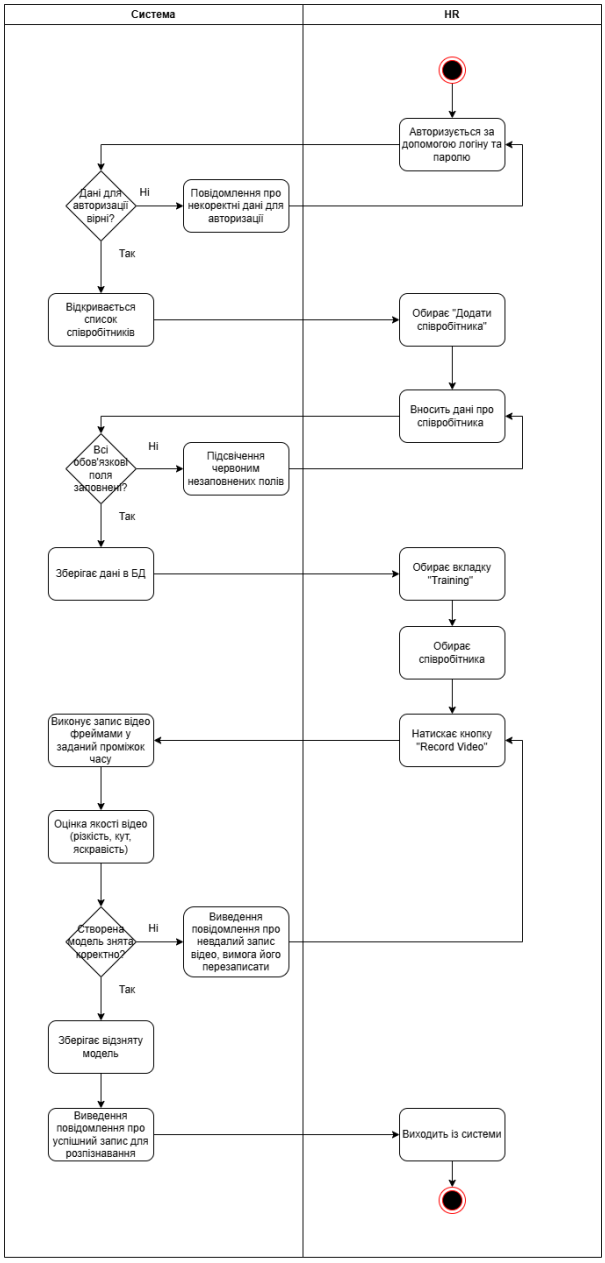


Рис. 2.4 – діаграма активності для події «Прохід через турнікет»

На діаграмі виділено дві доріжки: HR та Система. Процес охоплює повний цикл додавання нового співробітника до довідника та підготовку тренувальних даних для розпізнавання.

Авторизація HR

Користувач вводить логін/пароль. Вузол рішення «Дані для авторизації вірні?»:

Якщо ні – система показує повідомлення про некоректні дані; процес повертається до авторизації.

Якщо так – відкривається список співробітників.

Створення картки співробітника

HR обирає дію «Додати співробітника» й вводить персональні дані. Рішення «Всі обов’язкові поля заповнені?»:

Якщо ні – система підсвічує незаповнені поля.

Якщо так – дані зберігаються в БД.

Підготовка тренувальних даних (зняття відео)

HR переходить на вкладку «Training», обирає потрібного співробітника і натискає «Record Video».

Система виконує запис відео фреймами у заданий проміжок часу та проводить оцінку якості (різкість, кут, яскравість/експозиція).

Контроль якості й побудова моделі

Вузол рішення «Створена модель зняття коректно?»:

Якщо ні – виводиться повідомлення про невдалий запис (низька якість/мало фреймів/некоректний кут) з вимогою перезаписати.

Якщо так – система зберігає відзняту модель (ознаки/ембеддинги, посилання на відео/кадри), і показує повідомлення про успішний запис для розпізнавання.

Завершення сесії

HR виходить із системи; процес завершується кінцевим вузлом.

Для події «Прохід через турнікет» діаграма активності зображена на Рис.2.5.

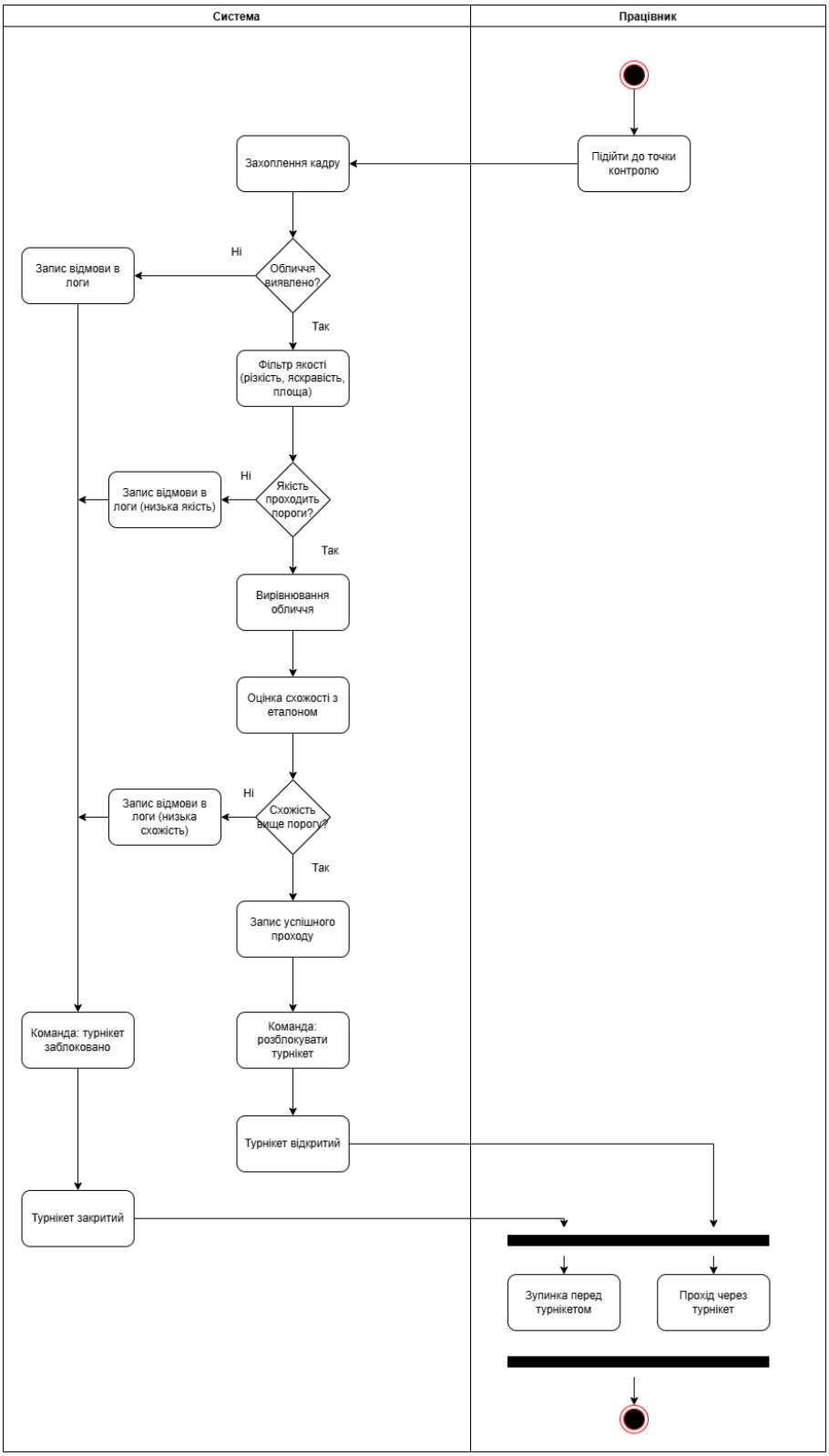


Рис. 2.5 – діаграма активності для події «Прохід через турнікет»

На діаграмі виділено дві доріжки – система та працівник, що показують розподіл відповідальності під час проходу через турнікет.

Старт – співробітник підходить до точки контролю.

Захоплення кадру – камера передає кадри; система бере поточний кадр у роботу.

Виявлення обличчя. Рішення «Обличчя виявлено?».

Ні – фіксується відмова в логах, турнікет залишається заблокованим.

Так – перехід до оцінки якості.

Фільтр якості кадру. Перевіряються різкість, яскравість/експозиція, площа/масштаб обличчя. Рішення «Якість проходить пороги?».

Ні – запис у лог з причиною «низька якість», турнікет не відкривається.

Так – нормалізація/вирівнювання обличчя.

Оцінка схожості з еталоном. Обчислюється відсоток/метрика подібності. Рішення «Схожість вище порогу?».

Ні – запис у лог з причиною: «низька схожість»), турнікет заблокований.

Так – запис успішного проходу.

Керування виконавчим пристроєм. Система надсилає команду «розблокувати турнікет»; стан змінюється на «турнікет відкритий». Після проходу/тайм-ауту турнікет знову закривається.

Фініш. Гілки «Зупинка перед турнікетом» та «Прохід через турнікет» показують можливі завершення взаємодії користувача залежно від рішення системи.

РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ

3.1. Діаграма розгортання

Архітектура системи побудована за модульно-сервісним принципом. На робочих станціях виконуються клієнти для роботи з системою, у вузлі Face-Recognition зосереджено обробку відео та прийняття рішень, а сервер сховища відповідає за транзакційну реєстрацію подій і аналітику. Взаємодія між компонентами відбувається по Ethernet (відео та керування пристроями) і по захищеним HTTPS/SQL каналам (дані та звітність). Узагальнену схему показано на діаграмі розгортання на Рис. 3.1.

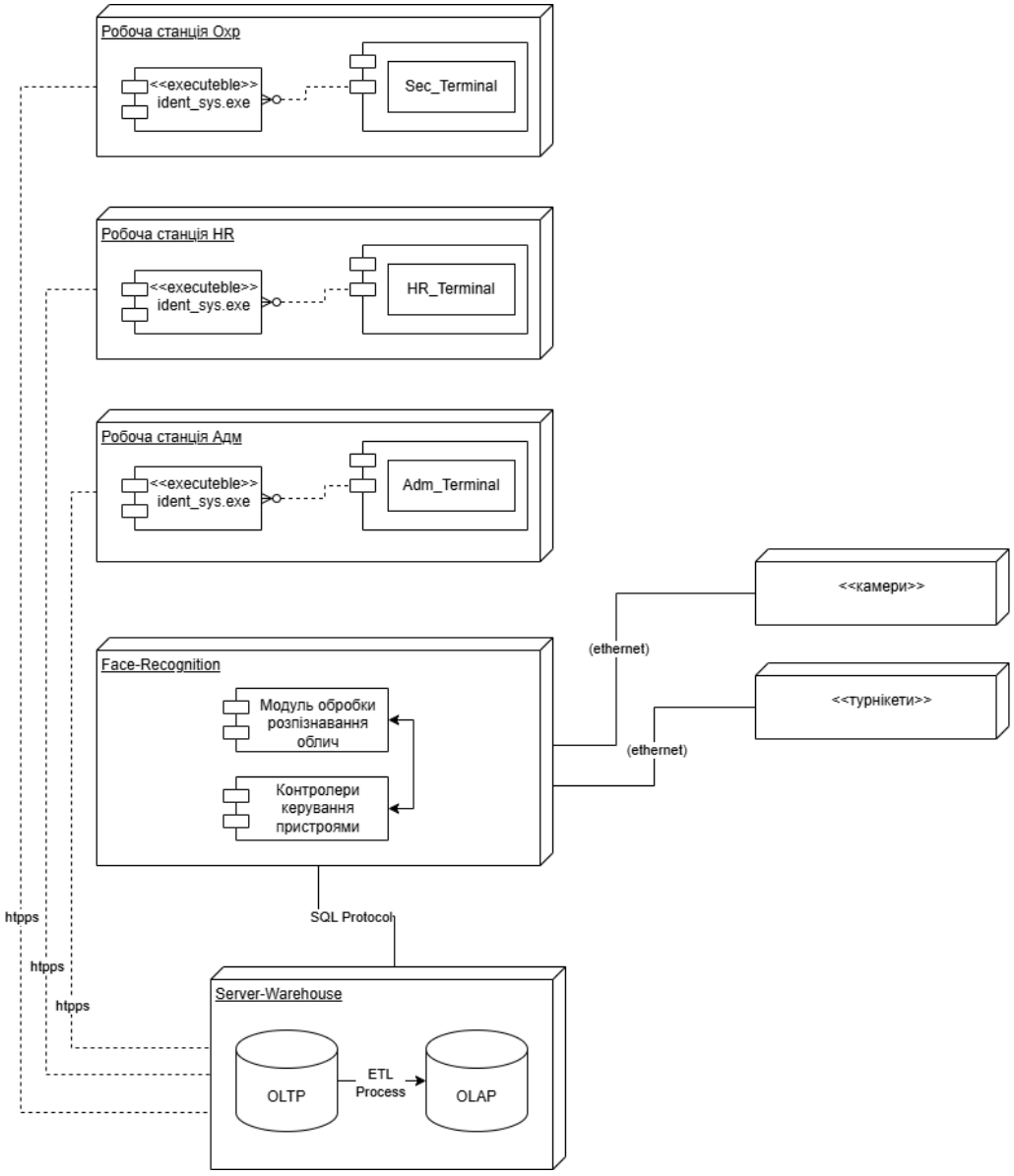


Рис. 3.1 – діаграма розгортання АСОП

Основні компоненти:

- Робоча станція охорони – запускає клієнтський модуль. Призначена перегляду подій у реальному часі, ручне підтвердження/блокування проходів, перегляд сповіщень про інциденти.
- Робоча станція HR – запускає клієнтський модуль. Призначена для реєстрації та оновлення даних співробітників, перегляд відвідуваності, експорт звітів.
- Робоча станція адміністратора – запускає клієнтський модуль. Призначений для конфігурування пристроїв і порогів розпізнавання, керування користувачами, аудит.

Усі термінали обмінюються з бекендом та сховищем через HTTPS (позначено пунктирними лініями).

- Вузол Face-Recognition містить два ключові компоненти:
  - Модуль обробки розпізнавання облич – приймає відео від камер, виконує детекцію, фільтрацію якості/нормалізацію, обчислює ознаки і ухвалює рішення за налаштованими порогами.
  - Контролери керування пристроями – видають команди виконавчим пристроям «розблокувати/блокувати», ведуть локальний журнал технічних подій.

Вузол напряму під’єднаний до камер та турнікетів по Ethernet (прямі лінії на схемі). Для фіксації фактів проходу, причин відмов та технічних метрик Face-Recognition записує дані у транзакційне сховище через SQL-протокол.

- OLTP – операційна БД подій. Саме сюди пише вузол Face-Recognition.
- ETL Process – періодично переносить і агрегує дані з OLTP у аналітичне сховище.
- OLAP – куби для Power BI і звітів терміналів. Термінали звертаються до сервера по HTTPS, отримуючи готові зрізи та дашборди.
- Камери – генерують відеопотік для розпізнавання.

- Турнікети – отримують від контролерів команди «відкрити/закрити»; стан і події повертаються у систему.

3.2. ER діаграма

3.2.1. ER діаграма OLTP

OLTP – це операційна база, яка приймає й зберігає усі поточні транзакції системи – події з камер/турнікетів, результати розпізнавання, логи, зміни довідників. Її головні цілі:

- Швидкий запис і читання невеликих порцій даних у реальному.
- Цілісність і коректність.
- Нормалізована структура для мінімізації дублювання та помилок.
- Джерело істини для всіх бізнес-процесів.
- Витік у сховище через ETL для звітів та аналітики, щоб не гальмувати операційні процеси.

ER діаграма для OLTP зображена у додатку Б.

3.2.2. ER діаграма OLAP

OLAP – аналітичне сховище, куди через ETL потрапляють агреговані та очищені події з OLTP. Воно оптимізоване для запитів і зрізів (звітність, дашборди, порівняння методів, сезонність), а не для транзакцій [10, 17]. Дані зберігаються у формі зірки. Одна факт-таблиця з числовими показниками та два рівні вимірів для зрізів.

ER діаграма для OLAP зображена на Рис. 3.2.

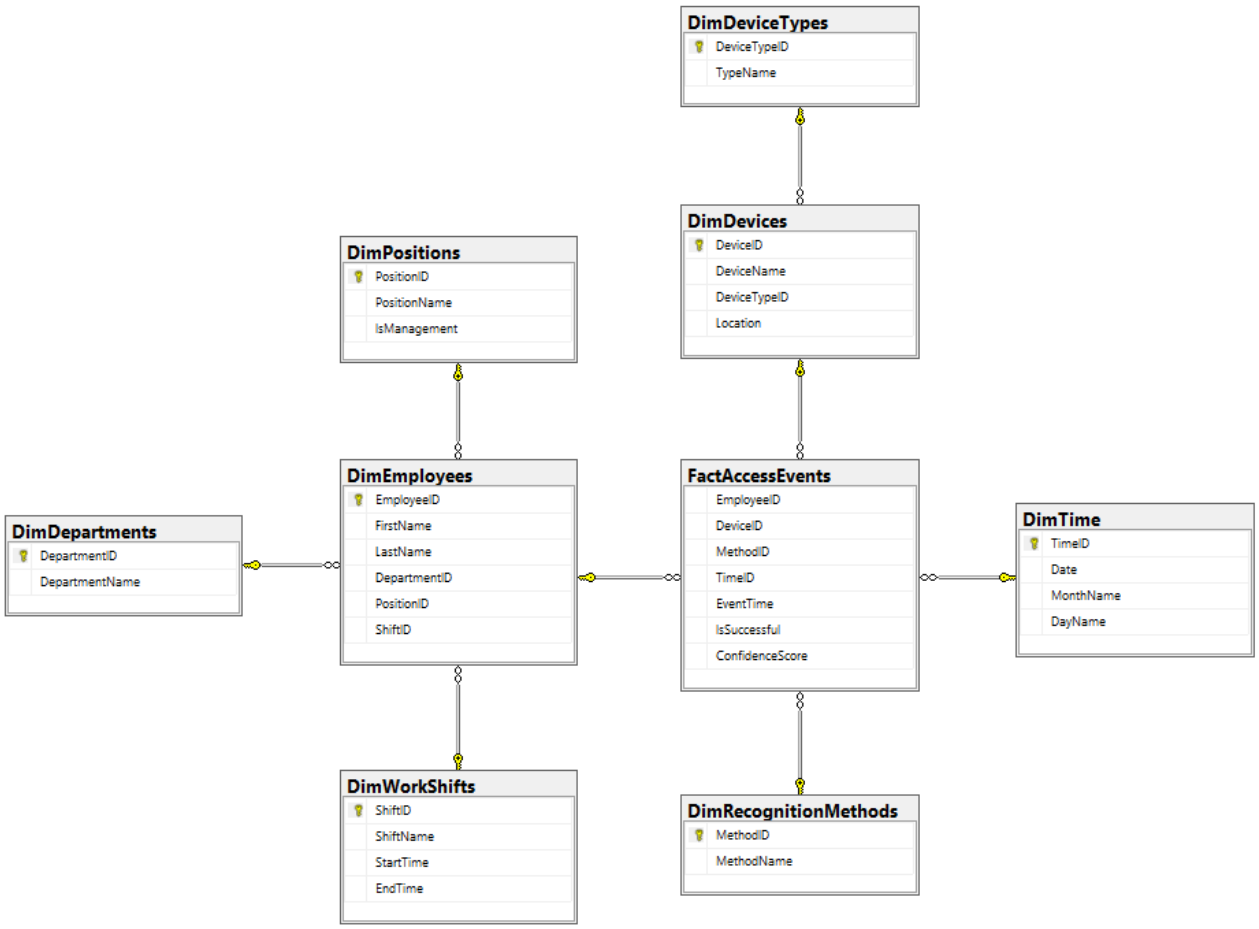


Рис. 3.2 – ER діаграма OLAP для АСОП

3.3. ETL процеси

ETL процеси забезпечують витяг подій та довідників з OLTP. Виконують трансформацію до аналітичної моделі (збагачення часовими атрибутами, нормалізація довідників, очищення, підміна NULL, контроль якості, генерація сурогатних ключів). Як результат – стабільні потоки даних, які Power BI/SSAS агрегують без навантаження OLTP.

Для АСОП загальна схема ETL процесів зображено на Рис 3.3. Наповнення відбувається в 3 етапи. 1 етап – наповнення вимірів 1 рівня. 2 етап – наповнення вимірів 2 рівня. 3 етап – наповнення таблиці фактів.

Рис. 3.3 – загальна схема ETL процесів АСОП

Наповнення вимірів 1 рівня включає в себе наповнення таких таблиць як «DimRecognitionMethods», «DimDepartments», «DimPositions», «DimDeviceTypes», «DimWorkShifts» та виконується наповнення таблиці «DimTime» часовими даними за допомогою SQL скрипта. Наповнення вимірів 1 рівня зображено на Рис. 3.4.

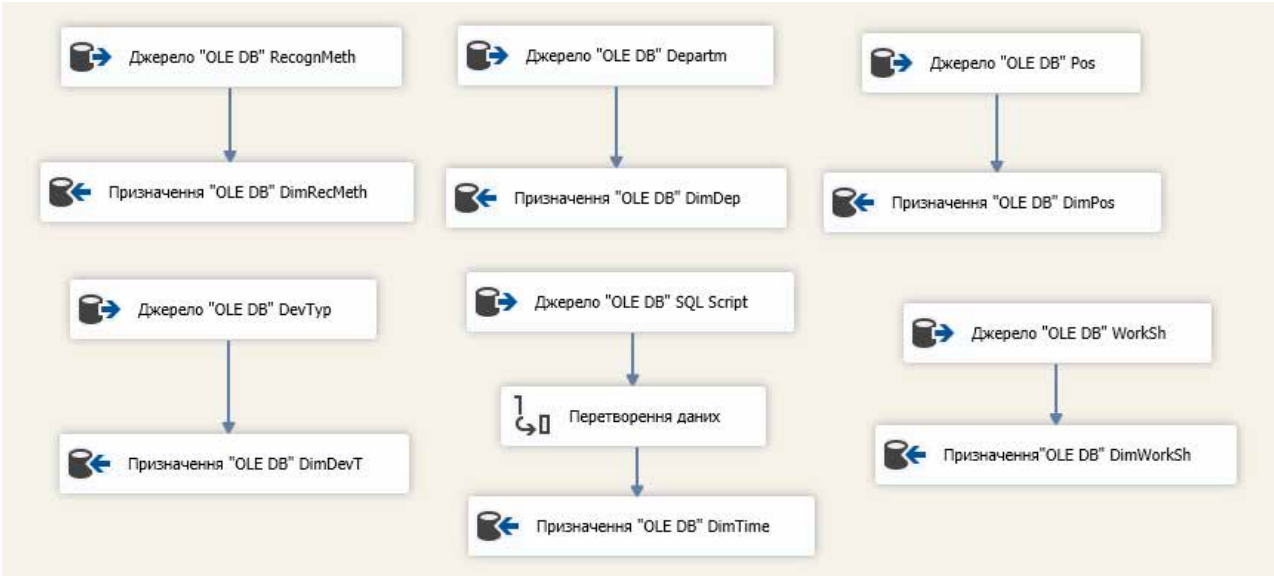


Рис. 3.4 – наповнення вимірів 1 рівня

Після наповнення вимірів 1 рівня відбувається процес наповнення таблиць «DimDevices» та «DimEmployes». Наповнення вимірів 2 рівня зображено на Рис. 3.5.

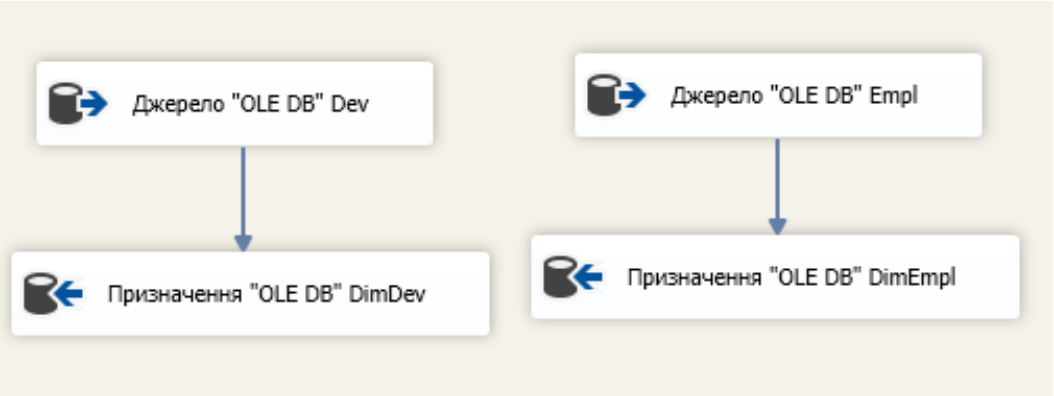


Рис. 3.5 – наповнення вимірів 2 рівня

Наступний етап – наповнення таблиці фактів. Дані беруться з таблиці EventLogs, трансформуються через додаткові стовпчики та уточнюючі запити часу. Процес наповнення таблиці фактів зображено на Рис. 3.6.

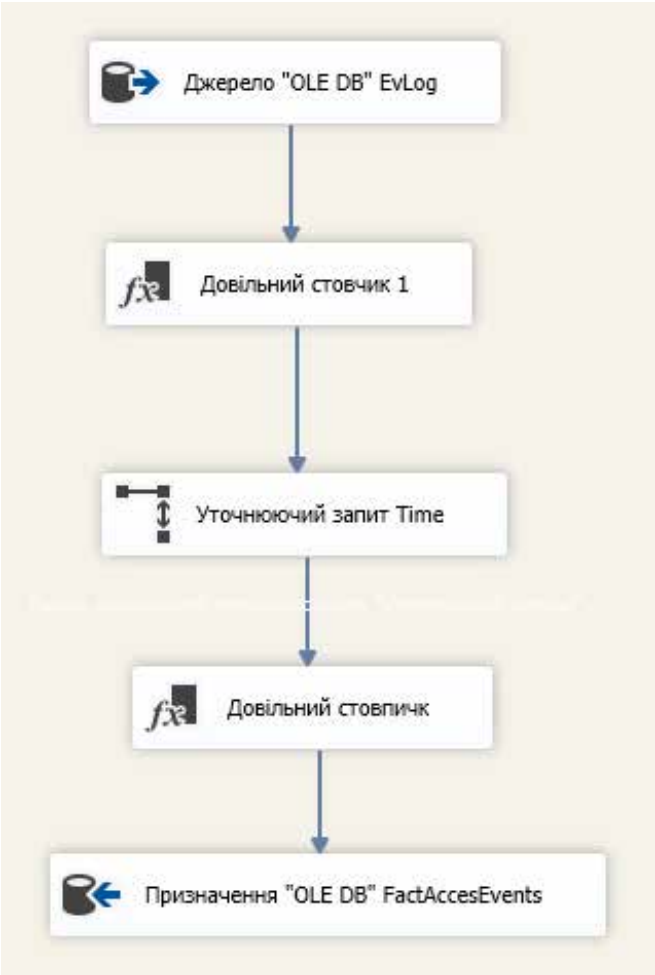


Рис. 3.6 – наповнення таблиці фактів

3.4. Виконання алгоритмів розпізнавання облич

3.4.1. Алгоритм LBPH

LBPH – класичний «нерозумний» метод розпізнавання облич, реалізований у OpenCV. Ідея – перетворити вирівняне ч/б зображення обличчя на набір локальних гістограм шаблонів текстури, а потім порівнювати ці вектори ознак з еталонами за метрикою відстані. Метод стійкий до монотонних змін освітленості, дуже швидкий і потребує мало пам’яті [4]. Алгоритм виконання LBPH зображено у додатку В.

Основні кроки:

- Підготовка. Детекція й вирівнювання обличчя; перетворення в градації сірого.
- LBP-кодування.Для кожного пікселя беруться P сусідів на радіусі R; формується бінарний код за ознакою «сусід ≥ центр». Часто застосовують «uniform LBP», що зменшує розмірність і шум.
- Просторова сітка. обличчя ділять на ґрати G_x x G_y, для кожного блока рахується гістограма LBP-кодів і нормалізується. Гістограми конкатенуються у єдиний вектор ознак.
- Порівняння/класифікація. Для кожного еталону обчислюється відстань. Найменша відстань визначає клас; додатково застосовується поріг «свій/чужий».

Цей алгоритм є досить простим та швидким на CPU. Має малу модель, стійкість до монотонних змін освітлення. Добре підходить для систем реального часу з обмеженими ресурсами. Але з мінусів можна відмітити чутливість до невдалого вирівнювання, виражених поз/оклюзій та різких нерівномірних тіней; зазвичай поступається сучасним глибинним ембеддингам за точністю. [4]

Візуально процес виконання LBPH зображено на Рис. 3.6

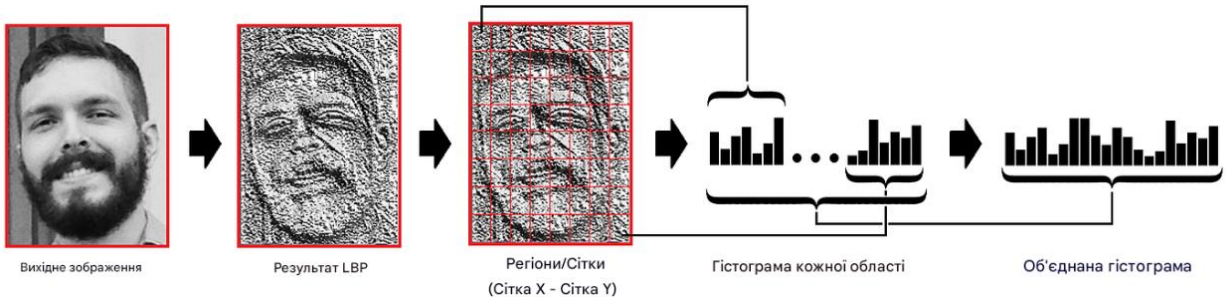


Рис. 3.6 – візуальне відображення процесу роботи LBPH

3.4.2. Алгоритм SFace

SFace – це глибинний метод розпізнавання облич, реалізований в OpenCV як швидкий CNN-ембеддер: на вході – вирівняне обличчя, на виході – компактний вектор ознак (ембеддинг). Розпізнавання зводиться до метричного пошуку: обчислити косинусну подібність між вектором запиту та еталонними векторами з БД і прийняти рішення за порогом «свій/чужий» [4]. Блок-схему алгоритму виконання SFace зображено в додатку Г.

Архітектурно SFace належить до сімейства метричного навчання. Мережа навчається так, щоб вектори одного класу були близько, а різних – далеко; зазвичай це досягається маржинальними функціями втрат. У типовому конвеєрі використовують сучасний детектор і 5-точкове вирівнювання перед ембеддингом [9].

Візуально процес вирівнювання та пошуку векторів у SFace зображено на Рис. 3.7

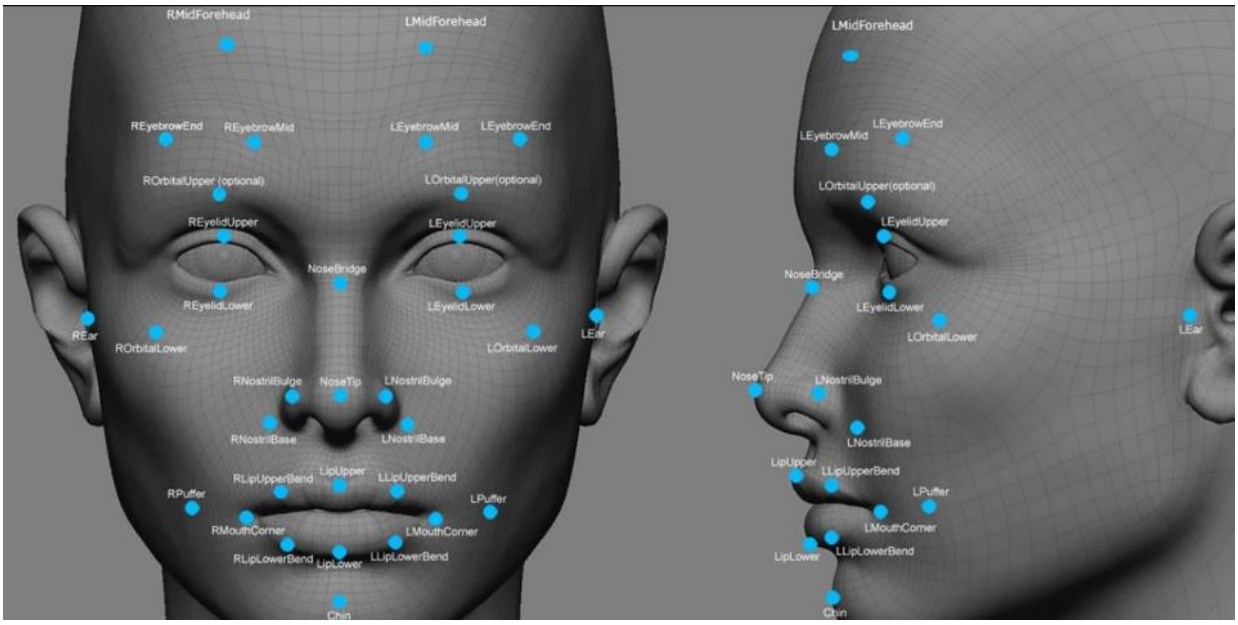


Рис. 3.7 – процес вирівнювання та пошуку векторів алгоритмом SFace

3.4.3. Алгоритм ArcFace

ArcFace – це метод навчання ембеддингів облич на гіперсфері з кутовою маржею. Ідея полягає в тому, щоб після L2-нормалізації векторів ознак x та ваг класів W оптимізувати кут між ембеддингом і центром «свого» класу, штучно збільшуючи цей кут на m для позитивних прикладів. Такий зсув змушує моделі сильніше «розштовхувати» класи і дає кращу міжкласову відстань при збереженні компактності всередині класу, що напряму підвищує точність верифікації та ідентифікації [7]. Проста схема алгоритму виконання методу розпізнавання ArcFace зображено в додатку Ґ.

Нормалізований ембеддинг подається на шар класифікації з нормалізованими вагами W (центрами класів).

Обчислюється косинусна подібність та кут θ між x і кожним центром класу.

Для істинного класу y застосовується кутова маржа

Усі косинуси масштабуються коефіцієнтом s та подаються в Softmax, після чого рахується крос-ентропійна втрата. Це й є ArcFace-loss [7].

На Рис. 3.8 показано й варіант SubCenter-ArcFace. для кожного класу підтримується кілька «підцентрів» (кластерів усередині класу), береться

максимум подібності між ними. Це зменшує чутливість до поз, освітлення та інших внутрішньокласових варіацій.

Під час інференсу (у нашій системі використовується лише ембеддинг і косинусна подібність/відстань до еталонів у БД; Softmax і функція втрат потрібні тільки на етапі тренування.

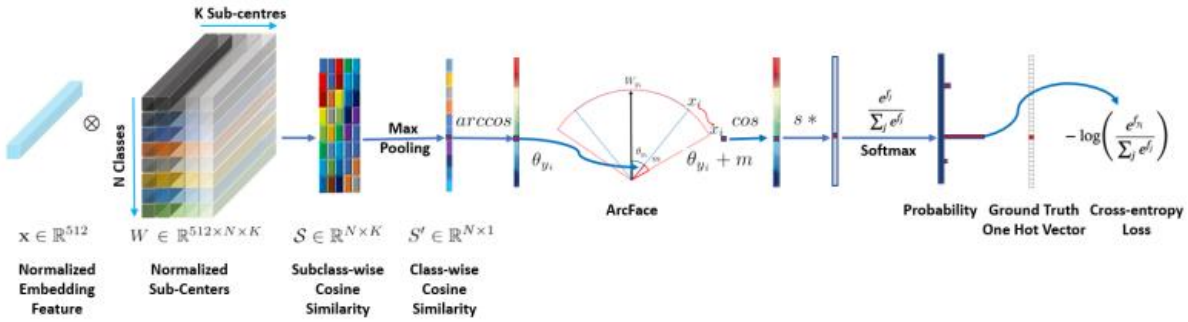


Рис. 3.8 – процес роботи алгоритму ArcFace

Для моєї системи це доречно, тому що нормалізація та кутова маржа роблять рішення стабільним до змін масштабу ознак і дають чіткіший розрив між «своїм» та «чужим» обличчям, що знижує хибні спрацьовування. SubCenter-варіант покращує роботу на реальних потоках, де одна людина може мати кілька стійких підвидів вигляду. Ембеддинги сумісні з пошуком «найближчого сусіда» та зберіганням у БД, що спрощує інтеграцію з OLTP/OLAP [9].

На Рис. 3.9 показано загальну ідею ієрархічного навчання ознак у згорткових нейромережах. На ранніх шарах мережа вчиться виявляти краї, далі – їхні комбінації та частини об’єктів, а на пізніх – цілі моделі облич. Саме так формується вектор ознак (ембеддинг), який ми використовуємо і в ArcFace, і в SFace; різниця між методами полягає не в самому екстракторі ознак, а в способі навчання/нормалізації та функції втрат.

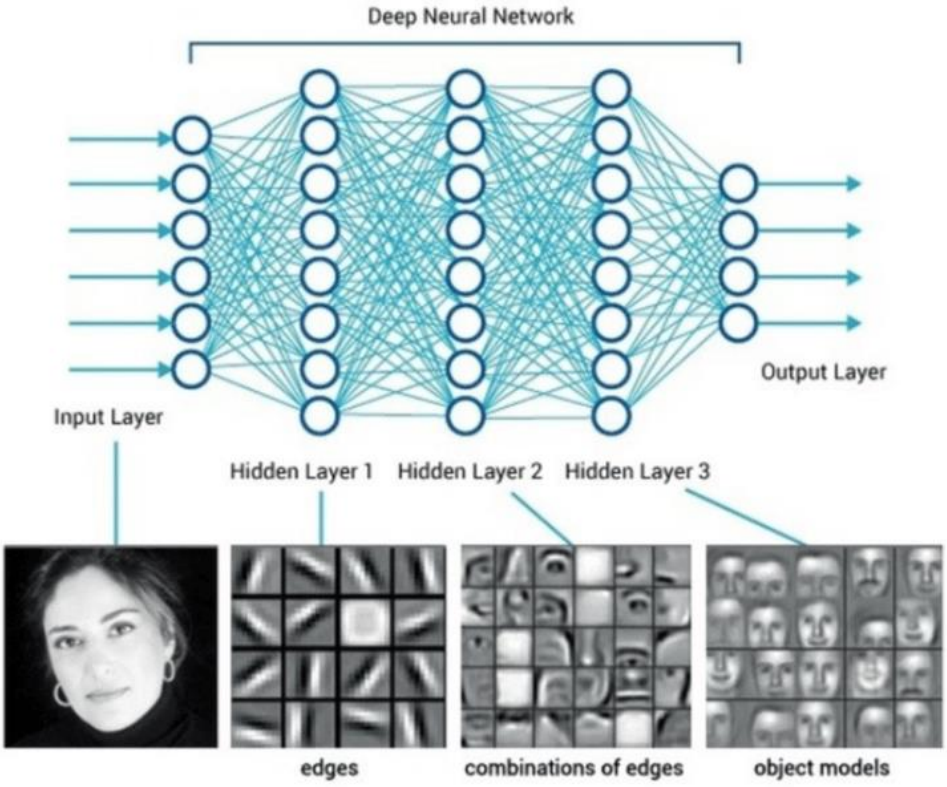


Рис. 3.9 – ієрархічне формування ознак у згорткових нейромережах

3.5. Класифікація за Naïve Bayes

Метод наївного Баєса є одним з фундаментальних алгоритмів машинного навчання, що належить до категорії імовірнісних класифікаторів та ґрунтується на застосуванні теореми Байєса для розрахунку апостеріорної ймовірності належності об'єкта до певного класу на основі спостережуваних ознак. Незважаючи на свою концептуальну простоту та "наївне" припущення про умовну незалежність ознак, цей алгоритм демонструє дивовижно високу ефективність у широкому спектрі практичних задач класифікації - від фільтрації спаму та аналізу тональності тексту до медичної діагностики та рекомендаційних систем [13].

У межах даного дослідження алгоритм наївного Баєса був реалізований за допомогою Python Visual у Power BI – для інтерактивної візуалізації результатів.

Блок-схема в додатку Д демонструє поетапну реалізацію алгоритму. Спочатку обчислюється загальна ймовірність кожного класу (апріорні ймовірності). Далі для кожного значення змінних “Пристрій” та “Локація”

обчислюється умовна ймовірність потрапляння до класу H (висока успішність) або L (низька успішність). На основі добутку апріорних та умовних ймовірностей обчислюється остаточна ймовірність для кожного класу, а об’єкт відноситься до того класу, де ймовірність вища.

3.6. Кластеризація K-means

Кластерний аналіз є фундаментальним напрямком інтелектуального аналізу даних (Data Mining), що належить до категорії методів неконтрольованого навчання (unsupervised learning). На відміну від задач класифікації, де кожен об'єкт навчальної вибірки має відому мітку класу, кластеризація працює з немаркованими даними та має на меті виявити природну внутрішню структуру даних - групи схожих об'єктів, що називаються кластерами [13]. Об'єкти всередині одного кластеру повинні бути максимально подібні один до одного за обраними характеристиками, тоді як об'єкти з різних кластерів мають бути максимально відмінними.

Кластерний аналіз відіграє критично важливу роль у дослідницькому аналізі даних, дозволяючи аналітику отримати перше уявлення про структуру даних без необхідності формулювання апріорних гіпотез. У контексті систем контролю доступу з розпізнаванням облич кластеризація дозволяє виявити природні групи точок контролю або часових періодів зі схожими характеристиками продуктивності, ідентифікувати аномальні режими роботи, сегментувати користувачів за патернами відвідуваності, а також оптимізувати розподіл ресурсів на основі виявлених груп з однорідними вимогами [13, 14].

Алгоритм виконання кластеризації за допомогою K-means зображено у додатку Ґ.

Алгоритм виконується наступним чином:

1. Визначаються початкові центроїди кластерів (випадково або задано).
2. Кожен об’єкт призначається до найближчого центру на основі обчислення евклідової відстані.

3. Для кожного кластеру обчислюється новий центроїд як середнє значення всіх точок, що входять у нього.

4. Кроки 2-3 повторюються доти, доки центри кластерів не перестануть змінюватися (досягнення збіжності).

У межах проєкту було використано Python Visual у Power BI для реалізації алгоритму кластеризації. Було здійснено попередню обробку даних із СД, нормалізацію числових змінних, та кластеризацію з подальшим аналізом груп.

РОЗДІЛ 4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

4.1. Апаратні вимоги

Камери (поблизу турнікета):

- IP-камера класу Hikvision (або сумісна): 2–4 Мп, 25/30 fps, фіксований об’єктив ~4 мм, WDR ≥ 120 dB, IR-підсвітка 20–30 м, PoE; бажано вбудований anti-flicker, можливість виставити shutter/gain.
- Монтаж: висота 1.5–1.7 м, кут до обличчя ≤ 15°, стабільне освітлення 300–500 lux, уникаємо контрового світла.
- Для нічного режиму – додаткова підсвітка.

Сервер розпізнавання:

- CPU 8 ядер (Ryzen 7 / Xeon Silver) або краще, RAM 32 GB, NVMe SSD ≥ 1 TB.

Сервер БД/Сховища:

- CPU 8 ядер, RAM 32–64 GB, NVMe SSD, окремий диск під tempdb.

Контролер доступу / турнікет:

Контролер із релейним виходом, керування по TCP. Інтеграційний сервіс формує команду «відкрити/закрити» за результатом розпізнавання.

Під час тестування використовувались проста веб-камера ноутбука (720p) та IP-камера класу Hikvision, встановлена поряд із турнікетом. Це дозволило порівняти вплив оптики та світла й підтвердило чутливість до якості кадру.

Загальні вимоги для робочих станцій користувачів

- CPU 4 ядра (Intel Core i5 / Ryzen 5) або краще.
- RAM: 8–16 GB (рекомендовано 16 GB для Power BI/великих звітів).
- Диск: SSD 256–512 GB.
- Мережа: 1 GbE або Wi-Fi; доступ до внутрішньої мережі камер/серверів.
- Монітор: Full HD 22–24" (для аналітика бажано 2× монітори).
- Периферія: миша, клавіатура.

Робоча станція HR (додаткові вимоги до обладнання):

- Відео: веб-камера 1080p (для зручного запису еталонів у приміщенні)
- ПЗ: Power BI Desktop, браузер для веб-інтерфейсу, офісний пакет.

Робоча станція адміністратора (додаткові вимоги до обладнання):

- RAM 16 GB, SSD 512 GB (для локальних бекапів/експортів логів)

4.2. Хід виконання дослідження

Насамперед була спроєктована повна архітектура системи: від точок збору даних до серверного модуля розпізнавання, операційної БД та сховища для аналітики. На робочій станції розробника було зібрано конвеєр у Python – детекція облич, нормалізація, виділення ознак трьома методами (LBPH, ArcFace, SFace), зіставлення з еталонами та прийняття рішення за порогом. Паралельно піднятий SQL Server з оперативною для подій проходів і журналів якості кадру та аналітичною – для агрегацій за локаціями, частинами доби, методами тощо. Завантаження між цими шарами реалізовано ETL-пакетами SSIS з окремими кроками наповнення вимірів 1-го, 2-го рівнів та фактів.

Перший цикл тестування і калібрування відбувався в домашніх умовах на веб-камері ноутбука. На цьому етапі ціллю були не високі цифр точності, а важливо було стабілізувати конвеєр і зібрати первинні дані про те, як метрики кадру впливають на поведінку LBPH, ArcFace та SFace. Для кожного методу будували ROC/PR-криві на невеликому, але збалансованому наборі позитивів/негативів, і підбирали стартові пороги подібності. Звідси сформували перші правила контролю якості кадру, які одразу інтегрували в конвеєр як фільтр входу.

Далі система була підключена до виробничої точки. Камера біля турнікетів з передачею кадрів і службових метаданих на сервер. Усі події – як успішні, так і невдалі – зберігались у OLTP разом із метриками кадру, ідентифікатором пристрою, періодом доби та методом розпізнавання. Нічого не відкидалось, навіть відмови потрапляли у журнали з причиною низька якість, недостатня

подібність, відсутність обличчя в кадрі. За розкладом ETL-процеси переносили події, нормалізуючи час, прив’язуючи їх до локації/пристрою та методу.

Коли накопичився достатній масив подій, наступним кроком була аналітика. У Jupyter побудувані теплові карти для кожного з методів розпізнавання зображені на Рис.4.1, Рис. 4.2, Рис.4.3

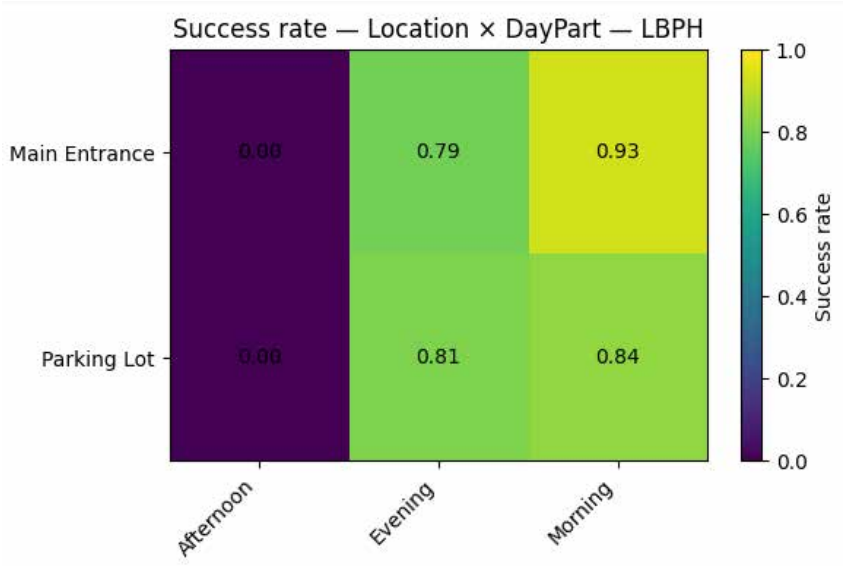


Рис. 4.1 – теплові карти успішності проходу для LBPH

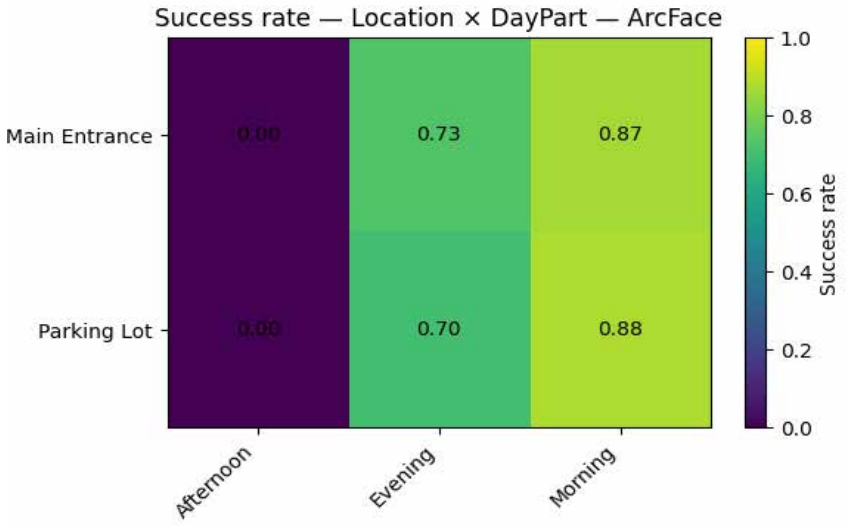


Рис. 4.2 – теплові карти успішності проходу для ArcFace

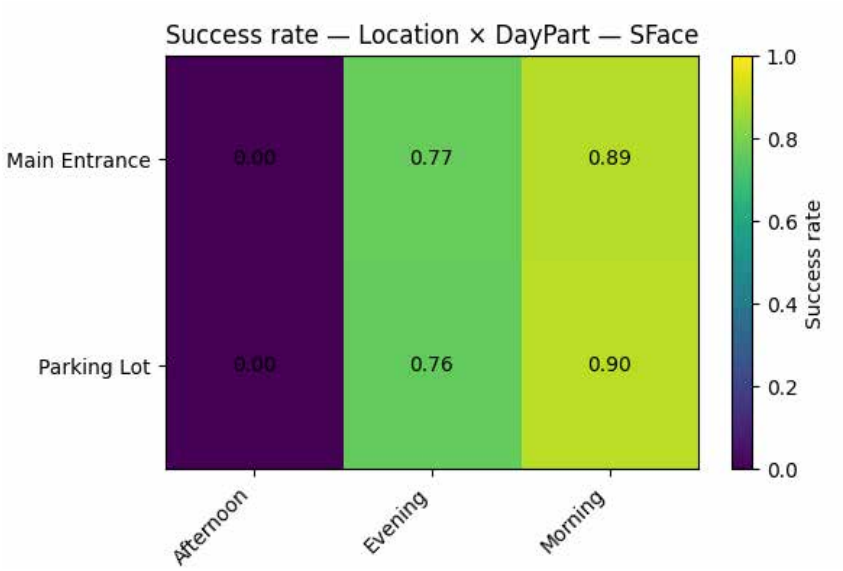


Рис. 4.3 – теплові карти успішності проходу для SFace

Щоб отримати пояснювані висновки, навчений простий класифікатор «High/Low» на базі наївного Баєса, який відображено на Рис. 4.4 та Рис. 4.5, по ознаках якості кадру та контексту – модель показала, які фактори найчастіше тягнуть подію в сторону відмови.

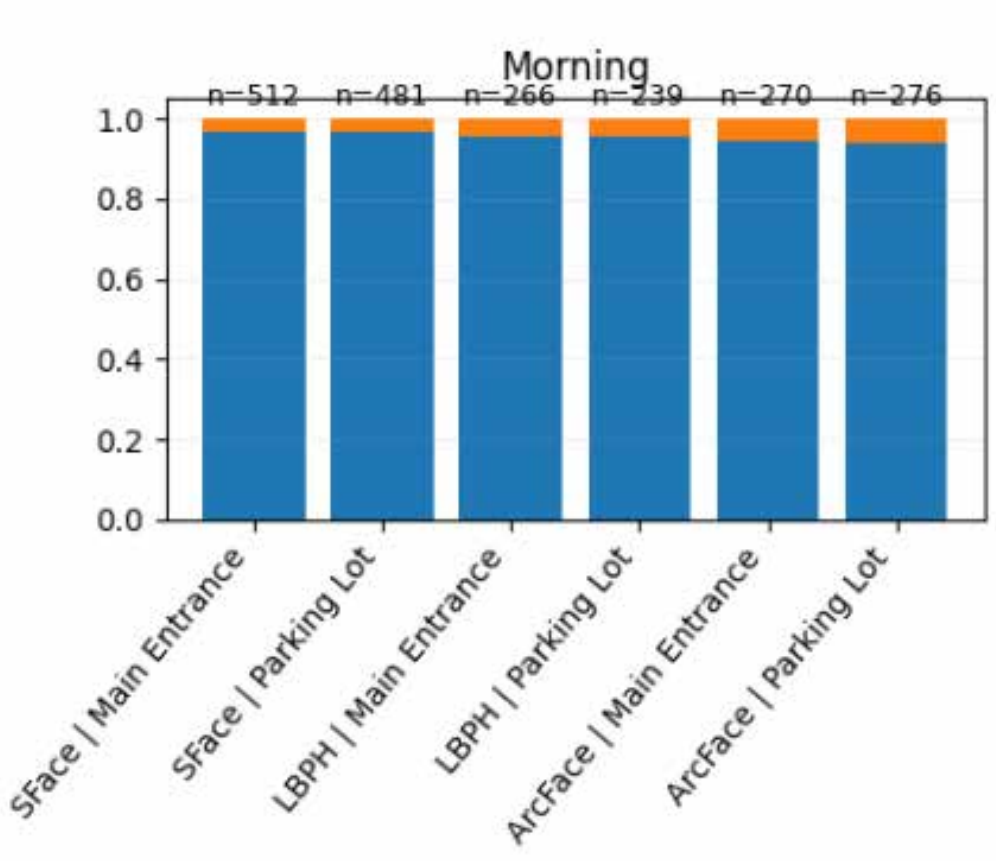


Рис. 4.4 – класифікація Naïve Bayes за методом розпізнавання та локацією в ранню пору доби

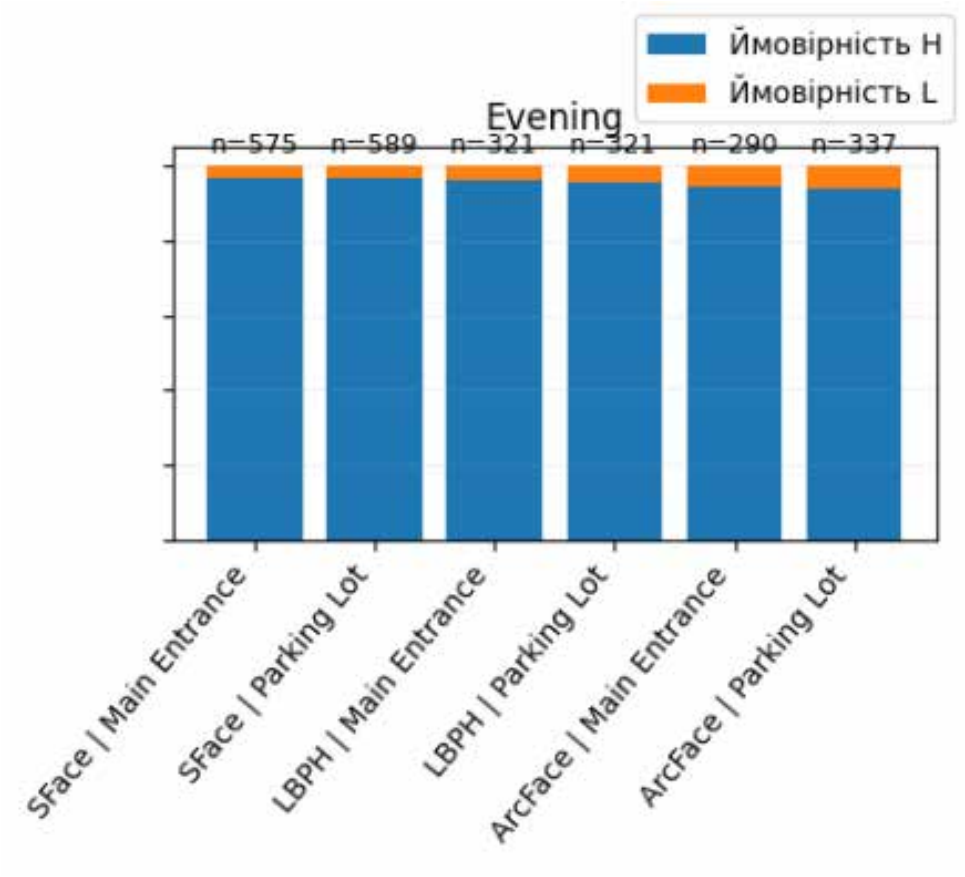


Рис. 4.5 – класифікація Naïve Bayes за методом розпізнавання та локацією в пізню пору доби

Паралельно виконані PCA-проєкція ознак якості та кластеризація K-means, яку зображено на Рис. 4.6 – це дозволило виділити зони якості та швидко виявляти деградацію умов.

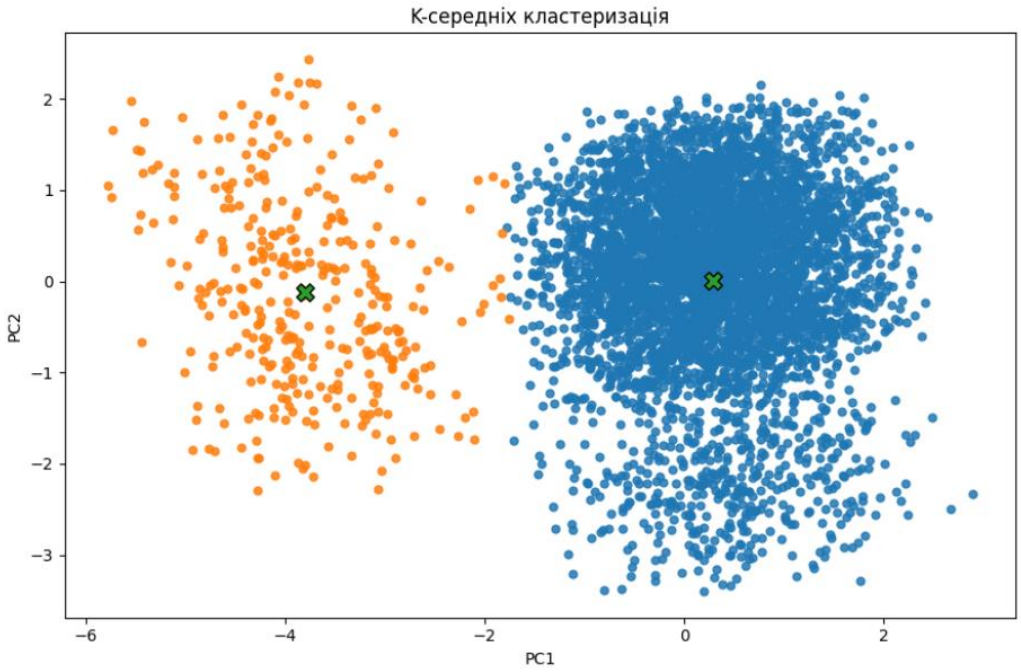


Рис. 4.6 – кластеризація отриманих даних за K-means

На основі цих спостережень були відредаговані пороги. Замість одного глобального значення – адаптивні пороги на рівні. Після повторного прогону зафіксували приріст частки успішних проходів без відчутного збільшення хибних допусків. Усі кроки і результати відображено на дашбордах Power BI. Дашборди дозволяють перевіряти метрики до рівня конкретного пристрою та періоду доби.

4.3. Пошук асоціативних правил

Використання методу асоціативних правил для виявлення прихованих зв'язків між параметрами подій доступу персоналу. Метод дозволяє знаходити повторювані закономірності у вибірках, наприклад, поєднання пристрою, локації, методу розпізнавання та результату доступу.

На блок-схемі зображеній в додатку В, наведено покроковий алгоритм пошуку асоціацій з урахуванням частоти підтримки — мінімального порогу, при якому правило вважається значущим. У Power BI з використанням Python Visual було реалізовано аналіз і візуалізацію отриманих правил.

На діаграмі «Розподіл Lift», яка відображена на Рис. 4.7, зображено гістограму, що відображає частоту появи різних значень показника Lift для

знайдених асоціативних правил. Більшість стовпчиків зосереджені в діапазоні від 1 до 3, що свідчить про переважання правил із помірною силою зв'язку між подіями. Червона пунктирна лінія позначає середнє значення Lift ≈ 2.19 – це означає, що в середньому виявлені залежності приблизно вдвічі сильніші, ніж випадкові збіги. Основна маса правил групується навколо цього середнього, тобто вони мають відносно передбачувану, стабільну поведінку. Разом із тим, поодинокі стовпчики праворуч, які досягають значень 5–8 і вище, відображають рідкісні, але значно сильніші закономірності. Такі правила можуть вказувати на специфічні сценарії у даних – наприклад, певні комбінації пристрою чи робочої зміни, які істотно впливають на успішність подій. Загальна форма діаграми має характерний довгий хвіст праворуч: більшість зв'язків звичайні, але трапляються й окремі, надзвичайно потужні залежності, що заслуговують на глибший аналіз.

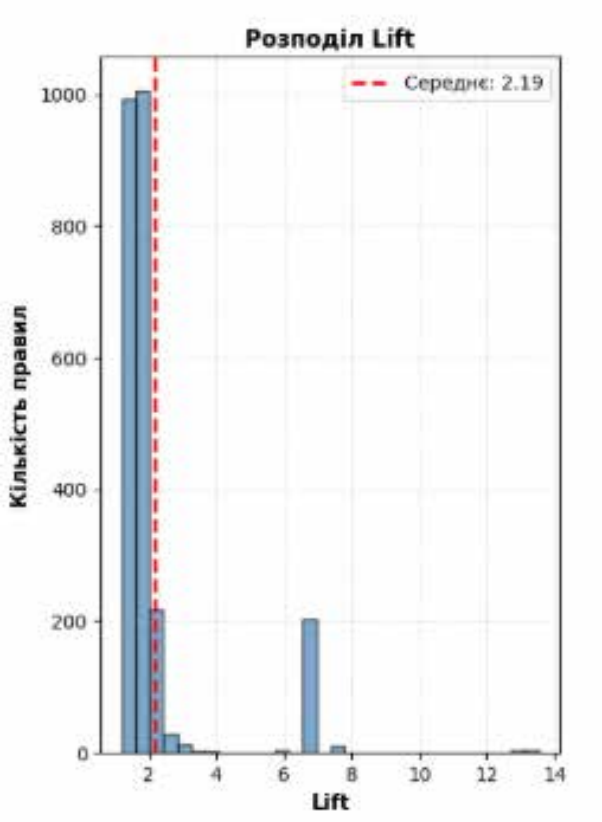


Рис. 4.7 – діаграма Розподіл Lift

На діаграмі «Parallel Coordinates (Топ-10)», яка зображена на Рис.4.8, відображено десять найсильніших асоціативних правил, порівняних за трьома основними метриками – Support, Confidence і Lift. Кожна лінія представляє окреме правило, а осі показують нормалізовані значення цих показників,

приведені до спільного масштабу. Видно, що всі лінії починаються з відносно низьких значень підтримки, оскільки навіть найсильніші правила трапляються рідко у вибірці. Далі показники впевненості зростають, що свідчить про високу точність і передбачуваність правил, а наприкінці спостерігається ще стрімкіше зростання Lift, що демонструє їхню значущість і силу зв'язку. Така форма ліній вказує на те, що найцікавіші правила – це ті, які мають помірну підтримку, але одночасно високу впевненість і дуже високий Lift, тобто зустрічаються нечасто, проте відображають стійкі та вагомі залежності між подіями. Графік дає змогу швидко побачити баланс між частотою, точністю та силою зв'язку для кожного з найкращих правил.

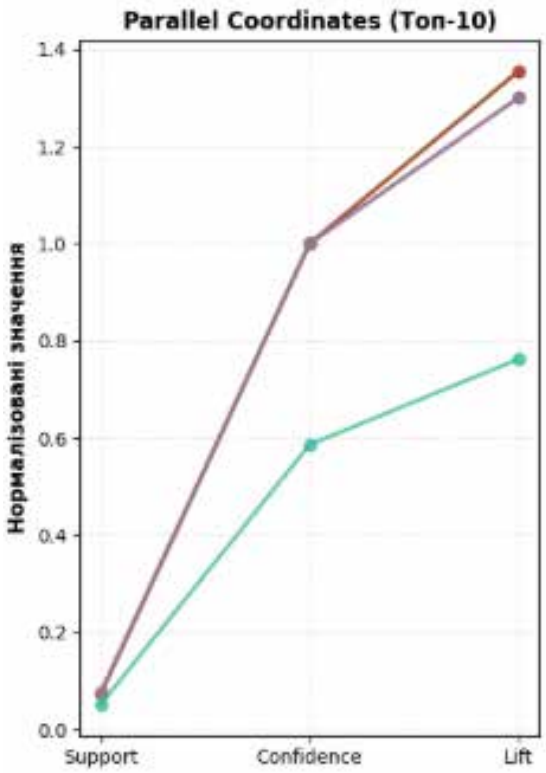


Рис. 4.8 – діаграма Paralel Coordinates

На діаграмі «Топ-15 правил за Lift», яка зображена на Рис. 4.9 представлено п'ятнадцять найсильніших асоціативних правил, відсортованих за показником Lift. Кожен горизонтальний стовпчик відповідає окремому правилу, де ліва частина описує умову, а права – результат події. Довжина стовпчика показує значення Lift, тобто силу зв'язку між елементами правила. Чим довший стовпчик, тим міцніша взаємозалежність. Зверху розташовані правила з

найвищими значеннями Lift – близько 13–14 – вони вказують на винятково сильні закономірності, які суттєво перевищують випадкову ймовірність появи результату. Зі спуском униз значення Lift зменшується, що свідчить про поступове зниження сили зв’язку. Колірна шкала – від насиченого помаранчевого до зеленого візуально підкреслює цю градацію. Теплі кольори означають найпотужніші правила, а холодні – помірні. Загалом діаграма демонструє, що лише невелика частка правил має справді високий Lift, тобто саме вони становлять основний аналітичний інтерес, оскільки відображають стійкі, нетривіальні залежності між параметрами, такими як пристрій, локація, зміна чи успішність розпізнавання.

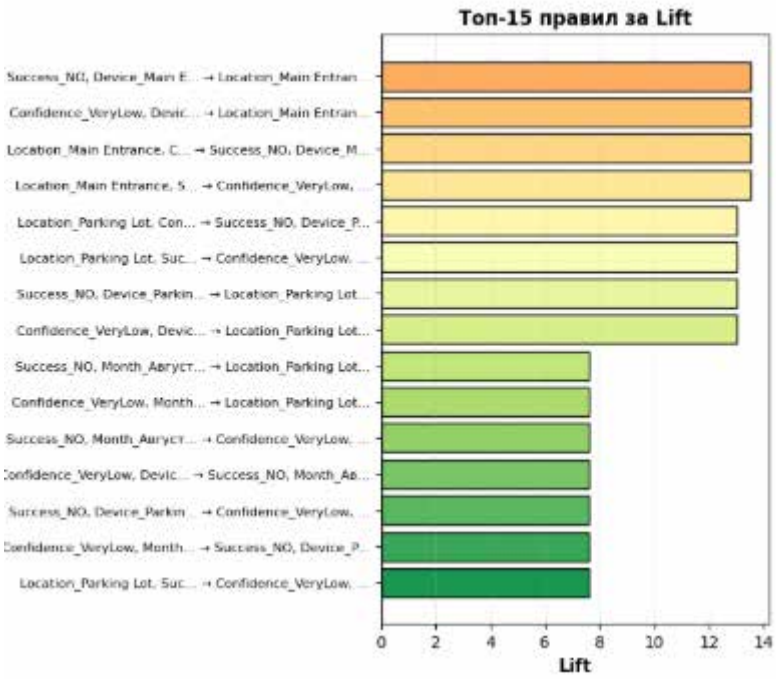


Рис. 4.9 – діаграма топ 15 правил за Lift

4.4. Аналітика в Power BI

Дашборд показує систему розпізнавання в експлуатації. А саме, якість ідентифікації (середня впевненість/подібність), обсяг успішних розпізнавань, розподіл подій за локаціями та денною порою, а також динаміку якості в часі. Дані надходять із факт-подій FactAccessEvents (EventTime, MethodName,

ConfidenceScore, IsSuccessful, Device/Location, ProcessingMs). Виконаний дашборд зображено на Рис. 4.10.

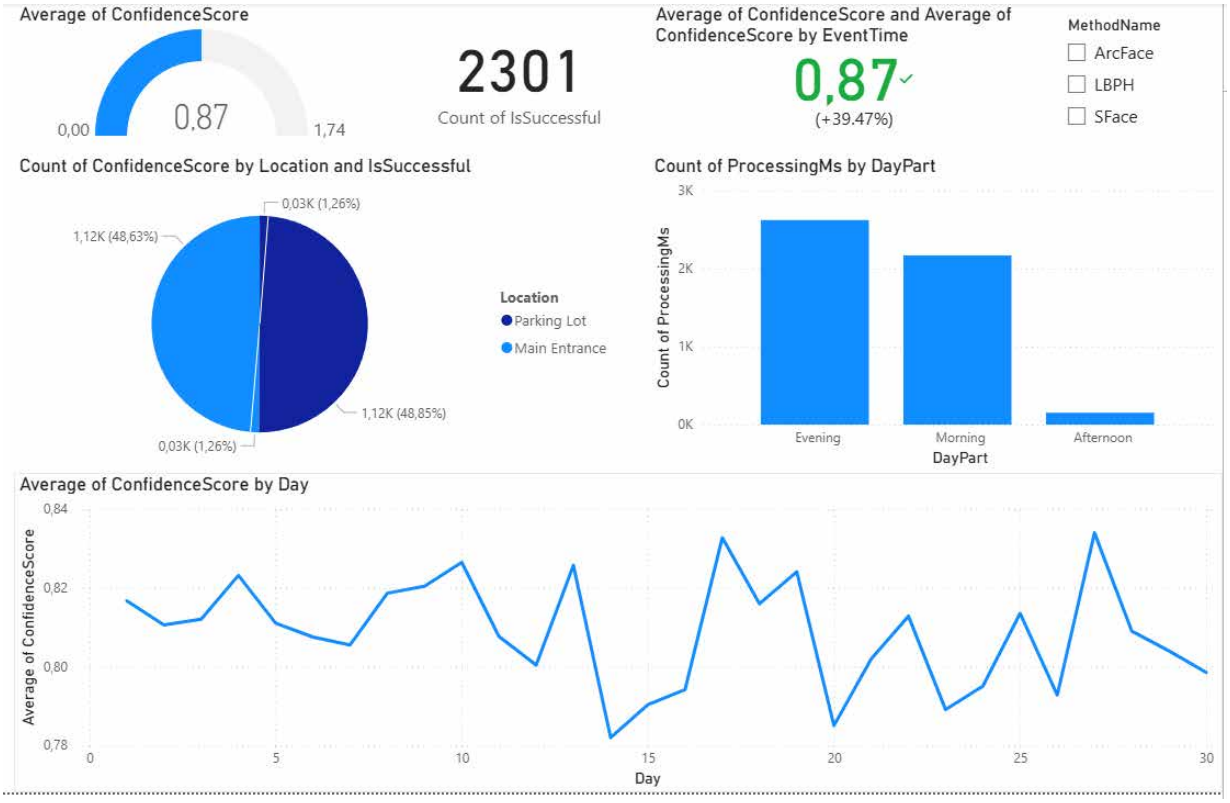


Рис. 4.10 – дашборд аналітика в Power BI для відображення параметрів експлуатації системи

Міра поточного середнього значення ConfidenceScore за обраний період.

KPI “Count of IsSuccessful”. Кількість успішних ідентифікацій. Показує навантаження/пропускну спроможність системи.

KPI “Average of ConfidenceScore by EventTime”. Середній рівень успішності за останній період із дельтою до попереднього (на скрині +33,99%). Праворуч перемикач за методами розпізнавання (ArcFace/LBPH/SFace) для порівняння методів.

Кругова діаграма “Count of ConfidenceScore by Location and IsSuccessful”. Розподіл подій за локаціями з часткою успішних. На прикладі Main Entrance ~50% усіх подій, Parking Lot ~47%, невелика частка відмов (~1–2%). Діаграма допомагає швидко виявити проблемну точку доступу.

Стовпчата діаграма “Count of ProcessingMs by DayPart”. Кількість подій/вимірів затримки за частинами дня. Видно, що основне навантаження

припадає на ранок і вечір; значно менше — пополудні. Корисно для планування обчислювальних ресурсів та охорони.

Лінійна діаграма “Average of ConfidenceScore by Month and Day”. Динаміка середньої впевненості щоденно. Дозволяє побачити сезонність та освітлювальні умови, деградації після змін камер або порогів, а також результат калібрувань (піки/провали).

Перемикач MethodName дає змогу порівняти ArcFace/LBPH/SFace. Різницю в середній якості, стабільності та чутливості до умов.

Якщо певна локація має нижчу успішність розпізнавання або більшу частку відмов – це сигнал перевірити камеру (кут, освітлення, фокус) або пороги якості кадру.

Піковий час доби вказують коли посилювати обчислювальні ресурси чи охорону.

Тренд середньої впевненості допомагає оцінювати ефект від оновлення моделей, зміни порогів, чистки еталонів, технічного обслуговування камер.

Середня впевненість ≈ 0,83 із позитивною динамікою.

Щоденний графік показує помітні коливання – є сенс перевіряти умови освітлення і за потреби мати окремі пороги «День/Ніч».

Такий дашборд закриває потреби оперативного моніторингу, дає швидкий доступ до причин відхилень і слугує основою для прийняття рішень щодо калібрування порогів, обслуговування камер і вибору оптимального методу розпізнавання.

4.5. Отримані результати

Отримані дані показали, що головним важелем якості є не тільки вибір алгоритму, а й умови зйомки: освітленість, різкість та частка обличчя в кадрі. Теплові карти дали цілісну картину. У денний час та в приміщенні всі три методи працюють стабільно; у вечірній час і на відкритих майданчиках успішність знижується синхронно з погіршенням експозиції й різкості. Це важлива

практична знахідка. Вона знімає алгоритмічну полеміку і переводить фокус у площину керування якістю кадру та локальних налаштувань.

Порівняння методів на реальних журналах підтвердило очікувані профілі – SFace найстабільніший за помірних коливань якості, LBPH чутливіший до освітлення, але конкурентний у простих сценах, ArcFace найкраще розділяє свій/чужий за доброї якості, проте вимагає кращої різкості та контрасту. Це дозволяє раціонально розподілити ролі: у чистих внутрішніх точках опори – ArcFace; у змішаних або нестабільних сценах – SFace як більш терпимий; LBPH – як легковажний резерв.

Журнали невдач дали причинно-наслідковий шар. Сслабка освітленість, низький контраст, зміна зовнішності. Ці мітки зійшлися з полями теплових карт і підказали конкретні інтервенції: підсвітка в проблемних коридорах, маркери зони стояння перед камерою, візуальні нагадування «без капюшона/маски/темних окулярів», регулярне чищення оптики. Тобто лог помило» перестав бути архівом інцидентів і став інструментом керування сценою.

Класифікація High/Low (за наївним Баєсом) перевела інсайти у прикладну політику. Модель дає імовірність низької успішності для конкретної події з урахуванням методу, локації, частини доби та якості кадру. Це дозволило підняти точність без глобального послаблення порогів: у складних сценаріях система динамічно підлаштовує робочу точку, тоді як у легких сценаріях утримує більш суворий поріг, стримуючи хибні допуски.

Кластеризація додала радар для моніторингу деградацій. У просторі головних компонент утворюються стійкі хмари сцен. Зсув потоків подій у напрямку поганих кластерів сигналізує про локальну проблему. Це не просто діагностика – це основа для активного обслуговування камер і перевірки місць зростання відмов.

Узгоджений висновок з усіх шарів аналітики такий – найбільший приріст точності забезпечує керування сценою і локальна політика порогів, а не заміна моделі. Дані безпосередньо підказують, де і коли падіння якості неминуче, і

дозволяють там підсилити освітлення, підтягнути фокус, розмістити маркери позиціонування користувача й за потреби перемкнути метод або робочу точку. Дашборди Power BI закріплюють це у щоденній практиці: оператори бачать зони, топ-причини і тренди, а інженери – сигнали про деградацію, перш ніж це стане проблемою безпеки.

Отже, аналіз даних не просто описав поведінку алгоритмів – він перетворив журнали подій на систему прийняття рішень та показав, де покращити сцену, як налаштувати пороги під контекст, коли обслуговувати камери, і який метод обрати для конкретної точки.

ВИСНОВКИ

У ході виконання магістерської роботи було досягнуто мету – розроблено підхід до аналітики журналів розпізнавання облич у системі контролю доступу, який дозволяє не лише порівнювати алгоритми (LBPH, ArcFace, SFace) на реальних даних, а й пояснювати причини невдач, будувати класифікатори успішності та формувати практичні рекомендації з експлуатації.

У рамках роботи:

- проаналізовано предметну область біометричного контролю доступу, оглянуто сучасні алгоритми розпізнавання облич, стандарти тестування та захисту, а також інженерні підходи до побудови надійних ML-систем;
- спроєктовано архітектуру системи з розділенням на OLTP-рівень та OLAP, розроблено ETL-процеси для наповнення сховища;
- реалізовано та протестовано три методи розпізнавання (LBPH – класичний локальний метод; ArcFace та SFace – глибинні методи з ембеддингами), виконано їх порівняння на реальних журналах подій;
- побудовано пояснювані візуалізації, які показали залежність успішності не лише від алгоритму, а й від умов зйомки;
- застосовано методи інтелектуального аналізу даних – класифікацію наївним Баєсом та кластеризацію K-means із подальшою PCA-проекцією для виявлення зон якості кадрів і моніторингу деградацій;

За результатами дослідження встановлено, що найбільший вплив на успішність розпізнавання мають не стільки обрані алгоритми, скільки умови формування зображення: освітленість, різкість, частка обличчя в кадрі. Це підтверджено як тепловими картами, так і журналами невдач.

У сценах усі три методи дають прийнятний результат, але ArcFace показує кращу міжкласову роздільність; при погіршенні якості кадру стабільніше поводиться SFace; LBPH може використовуватися як резервний/легкий варіант у простих умовах або на малопотужних пристроях.

Реєстрація та збереження причин відмов робить систему пояснюваною: за цими полями можна будувати правила очищення даних і рекомендації для користувачів.

Класифікація High/Low успішності дає змогу динамічно налаштовувати пороги під локацію й час доби, не знижуючи загальну безпеку.

Кластеризація та PCA показали, що події природно групуються за якістю сцени; зміщення подій у кластери може використовуватися як сигнал для технічного обслуговування камер або переналаштування точок доступу.

Отримані результати можуть бути використані:

- для впровадження у виробничі СКД як аналітичний модуль «над» існуючими журналами подій;
- для подальших досліджень зі збагаченням датасету ;
- для розробки адаптивних політик порогів і автоматичних рекомендацій по камерах;
- як навчальний приклад інтеграції Python/Jupyter з MS SQL Server і Power BI для задач біометричної безпеки.

Перспективи подальших робіт полягають у розширенні набору алгоритмів, використанні детекції атак представлення у реальному часі, автоматичному підборі порогу для кожної камери окремо, а також у розгортанні системи в контейнеризованому середовищі з віддаленим моніторингом її якості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. P. Santhanam, Eitan Farchi, Victor Pankratius, Engineering Reliable Deep Learning Systems. – Artificial Intelligence in Government and Public Sector, Virginia, USA. 2019.

2. Florian Schroff, Dmitry Kalenichenko, James Philbin FaceNet: A Unified Embedding for Face Recognition and Clustering // Proc. CVPR, 2015.

3. Aparna Vyas, Soohwan Yu, Joonki Paik – Fundamentals of Digital Image Processing – 2017.

4. OpenCV Documentation: Image Quality & Face modules [Електронний ресурс]. – Режим доступу: https://docs.opencv.org/

5. NIST. Face Recognition Vendor Test (FRVT) Reports [Електронний ресурс]. – Режим доступу: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

6. ISO/IEC 30107-1. Information technology – Biometric presentation attack detection (PAD). – ISO, 2023.

7. Jiankang Deng, Jia Guo, Jing Yang, Niannan Xue, Irene Kotsia, Stefanos Zafeiriou ArcFace: Additive Angular Margin Loss for Deep Face Recognition // Proc. CVPR, 2022.

8. ISO/IEC 19795. Biometric performance testing and reporting. – ISO, 2021.

9. InsightFace Project (ретина-детекція, ембеддинги) [Електронний ресурс]. – Режим доступу: https://insightface.ai/

10. Документація служб аналізу SQL Server корпорації Microsoft [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/analysis-services/ssas-overview?view=asallproducts-allversions.

11. The official UML Web site [Електронний ресурс]. — Режим доступу : http://www.uml.org.

12. Microsoft Power BI Documentation [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/power-bi

13. Scikit-learn: Machine Learning in Python [Електронний ресурс]. – Режим доступу: https://scikit-learn.org/stable/

14. Бондаренко, М.Ф. Інформаційні технології в управлінні організаціями / М.Ф. Бондаренко, А.В. Козлов. – Київ: Ліра-К, 2020.

15. Гончарук, В.І. Системи підтримки прийняття – Київ: Вид-во КПІ ім. Ігоря Сікорського, 2019.

16. Документація служб аналізу SQL Server корпорації Microsoft [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/analysis-services/ssas-overview?view=asallproducts-allversions.

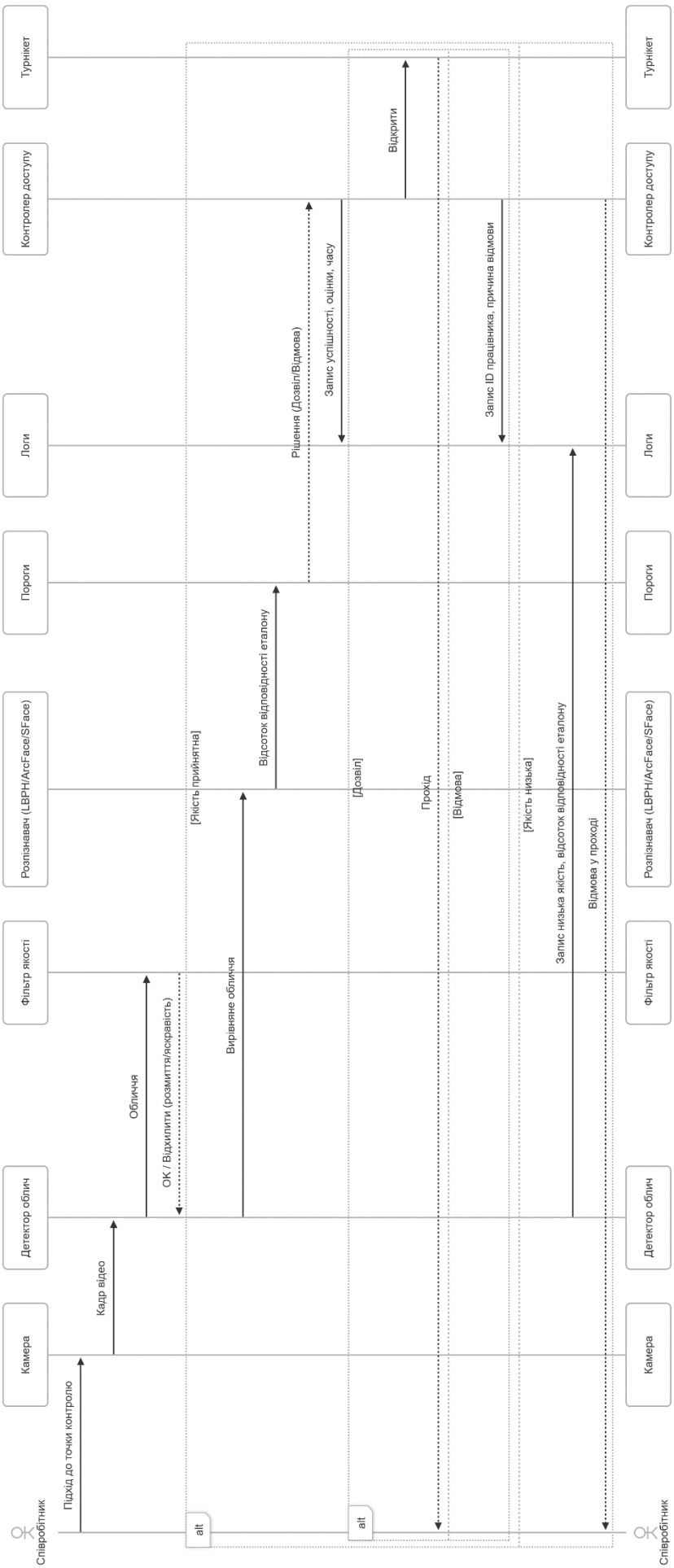
17. Організація сховища даних : навч. посібник / Національний університет біоресурсів і природокористування України. – Київ: НУБіП України, 2018.

ДОДАТОК А

ДІАГРАМА ПОСЛІДОВНОСТІ АСОП

СТОРІНОК – 1

Київ 2025

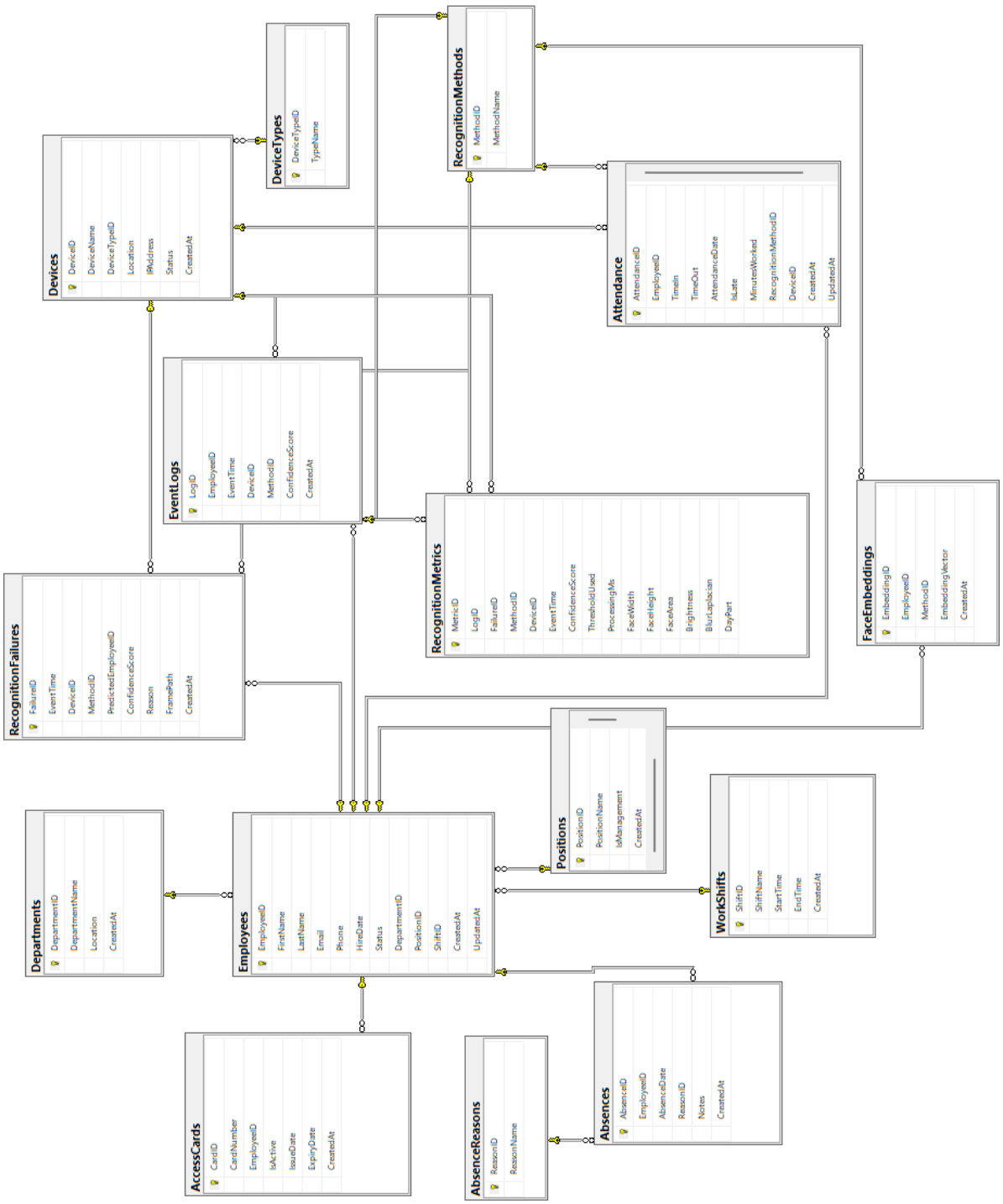

Співробітник
Камера
Детектор облич
Фільтр якості
Розпізнавач (LBPH/ArcFace/SFace)
Пороги
Логи
Контролер доступу
Турнікет
Підхід до точки контролю
Кадр відео
Обличчя
OK / Відхилити (розмиття/яскравість)
[Якість прийнятна]
Вирівняне обличчя
Відсоток відповідності еталону
Рішення (Дозвіл/Відмова)
Запис успішності, оцінки, часу
[Дозвіл]
Відкрити
Прохід
[Відмова]
Запис ID працівника, причина відмови
[Якість низька]
Запис низька якість, відсоток відповідності еталону
Відмова у проході
alt
alt
Турнікет
Контролер доступу
Логи
Пороги
Розпізнавач (LBPH/ArcFace/SFace)
Фільтр якості
Детектор облич
Камера
Співробітник

ДОДАТОК Б

ER ДІАГРАМА OLTP ДЛЯ АСОП

СТОРІНОК – 1

Київ 2025

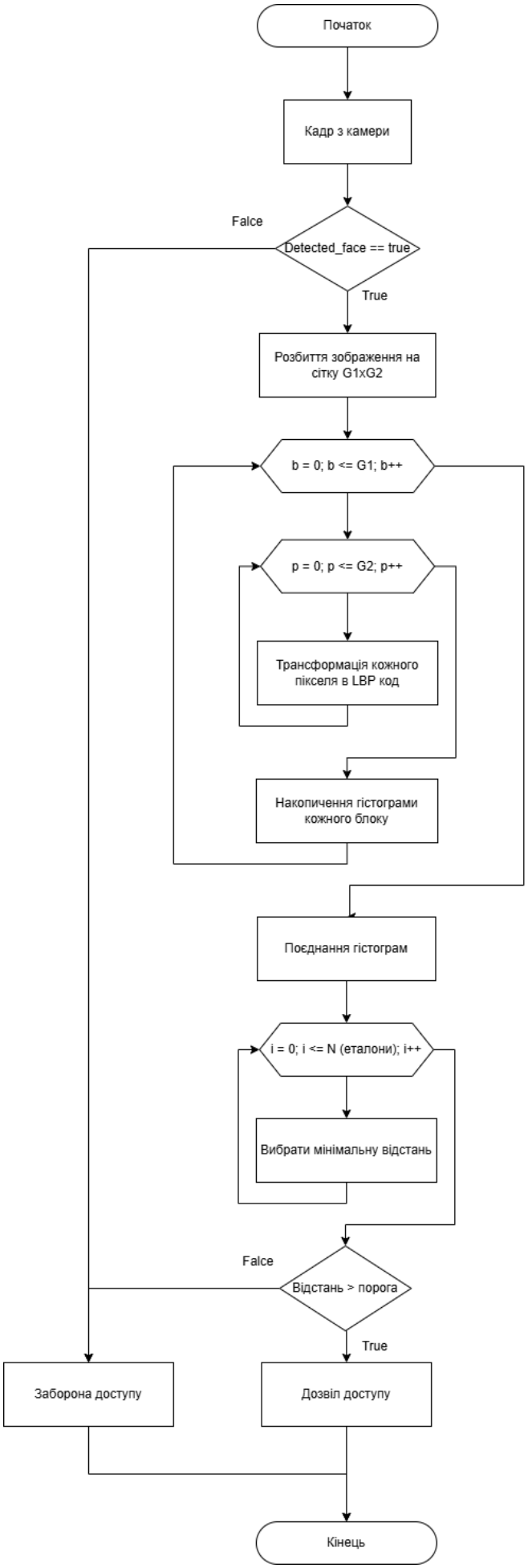

RecognitionMethods
MethodID
MethodName
DeviceTypes
DeviceTypeID
TypeName
Devices
DeviceID
DeviceName
DeviceTypeID
Location
IPAddress
Status
CreatedAt
Attendance
AttendanceID
EmployeeID
TimeIn
TimeOut
AttendanceDate
IsLate
MinutesWorked
RecognitionMethodID
DeviceID
CreatedAt
UpdatedAt
EventLogs
LogID
EmployeeID
EventTime
DeviceID
MethodID
ConfidenceScore
CreatedAt
RecognitionMetrics
MetricID
LogID
FailureID
MethodID
DeviceID
EventTime
ConfidenceScore
ThresholdUsed
ProcessingMs
FaceWidth
FaceHeight
FaceArea
Brightness
BlurLaplacian
DayPart
FaceEmbeddings
EmbeddingID
EmployeeID
MethodID
EmbeddingVector
CreatedAt
RecognitionFailures
FailureID
EventTime
DeviceID
MethodID
PredictedEmployeeID
ConfidenceScore
Reason
FramePath
CreatedAt
Positions
PositionID
PositionName
IsManagement
CreatedAt
Departments
DepartmentID
DepartmentName
Location
CreatedAt
Employees
EmployeeID
FirstName
LastName
Email
Phone
HireDate
Status
DepartmentID
PositionID
ShiftID
CreatedAt
UpdatedAt
WorkShifts
ShiftID
ShiftName
StartTime
EndTime
CreatedAt
AccessCards
CardID
CardNumber
EmployeeID
IsActive
IssueDate
ExpiryDate
CreatedAt
AbsenceReasons
ReasonID
ReasonName
Absences
AbsenceID
EmployeeID
AbsenceDate
ReasonID
Notes
CreatedAt

ДОДАТОК В

БЛОК-СХЕМА АЛГОРИТМУ РОЗПІЗНАВАННЯ LBPH

СТОРІНОК – 1

Київ 2025

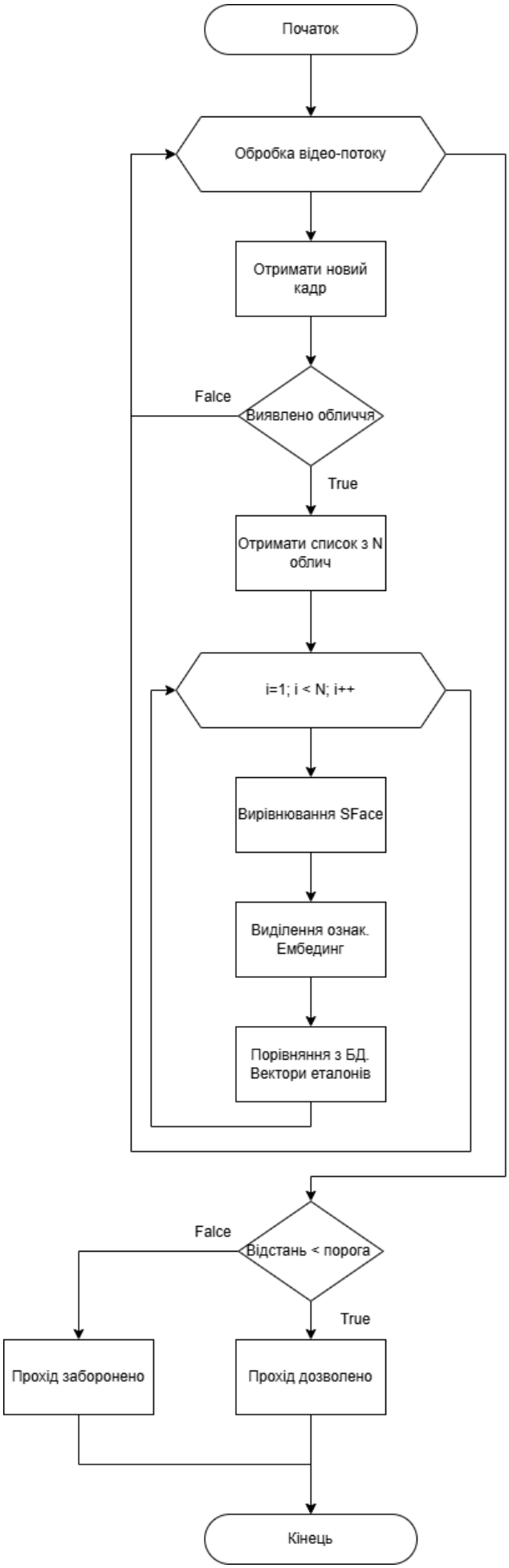

Початок
Кадр з камери
Falce
Detected_face == true
True
Розбиття зображення на сітку G1xG2
b = 0; b <= G1; b++
p = 0; p <= G2; p++
Трансформація кожного пікселя в LBP код
Накопичення гістограми кожного блоку
Поєднання гістограм
i = 0; i <= N (еталони); i++
Вибрати мінімальну відстань
Falce
Відстань > порога
True
Заборона доступу
Дозвіл доступу
Кінець

ДОДАТОК Г

БЛОК-СХЕМА АЛГОРИТМУ РОЗПІЗНАВАННЯ SFACE

СТОРІНОК – 1

Київ 2025

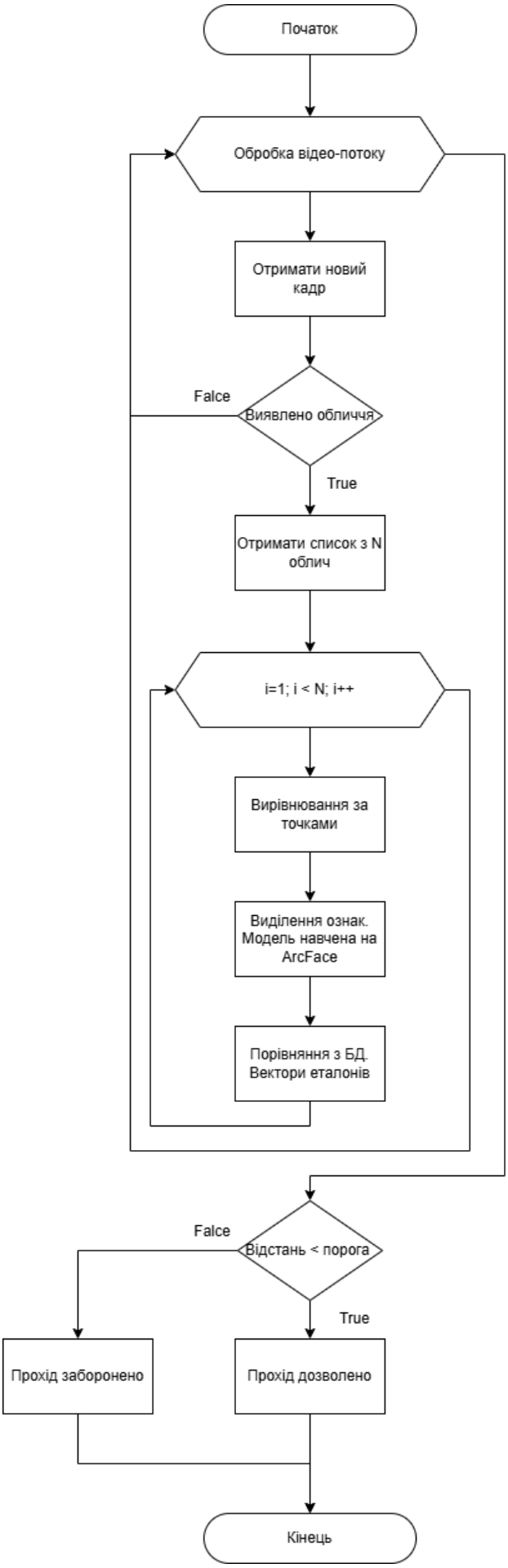

Початок
Обробка відео-потоку
Отримати новий кадр
Falce
Виявлено обличчя
True
Отримати список з N облич
i=1; i < N; i++
Вирівнювання SFace
Виділення ознак. Ембединг
Порівняння з БД. Вектори еталонів
Falce
Відстань < порога
True
Прохід заборонено
Прохід дозволено
Кінець

ДОДАТОК Ґ

БЛОК-СХЕМА АЛГОРИТМУ РОЗПІЗНАВАННЯ ARCFACE

СТОРІНОК – 1

Київ 2025

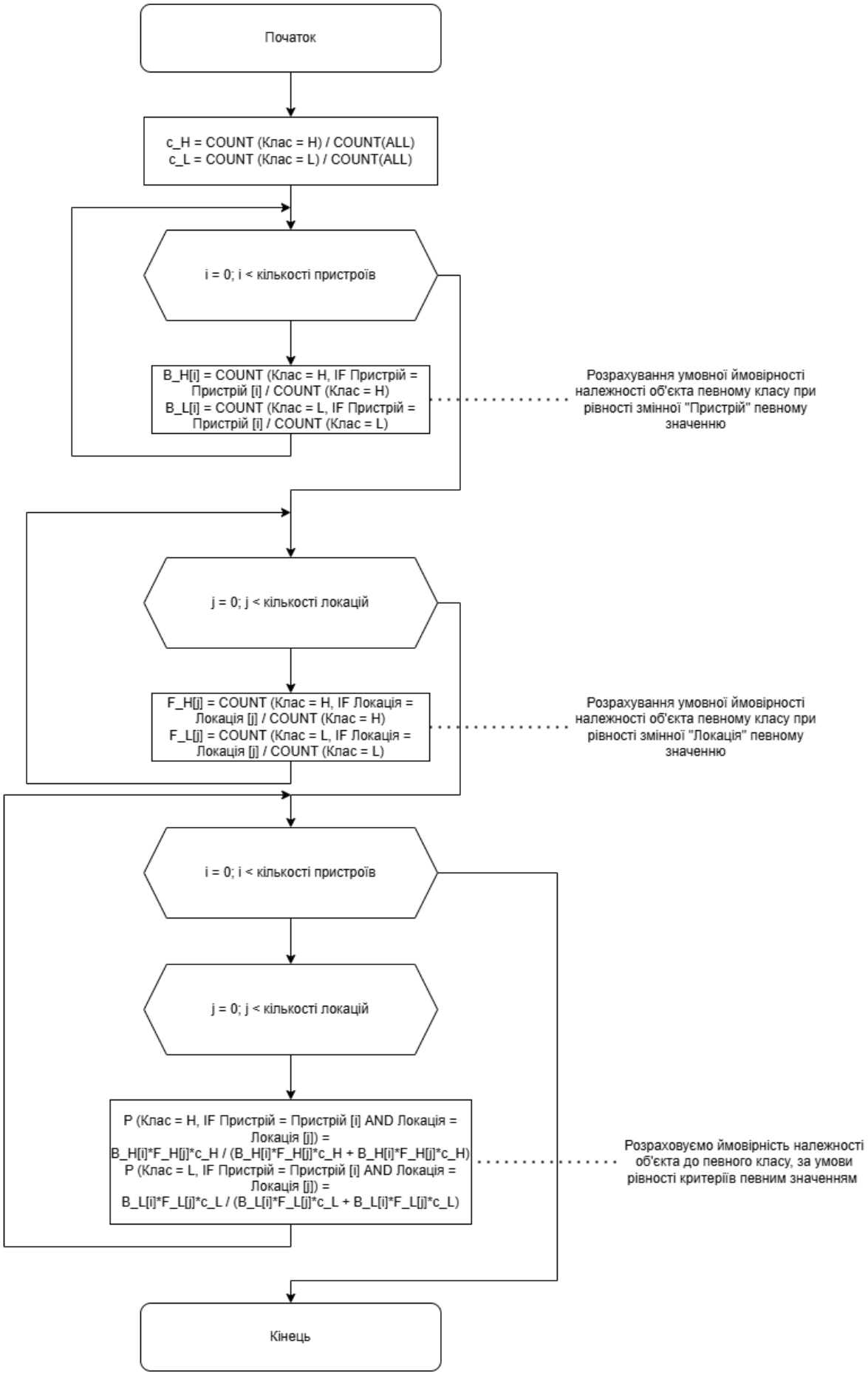

Початок
Обробка відео-потоку
Отримати новий кадр
Falce
Виявлено обличчя
True
Отримати список з N облич
i=1; i < N; i++
Вирівнювання за точками
Виділення ознак. Модель навчена на ArcFace
Порівняння з БД. Вектори еталонів
Falce
Відстань < порога
True
Прохід заборонено
Прохід дозволено
Кінець

ДОДАТОК Д

БЛОК-СХЕМА АЛГОРИТМУ КЛАСИФІКАЦІЇ МЕТОДОМ NAÏVE BAYES

СТОРІНОК – 1

Київ 2025

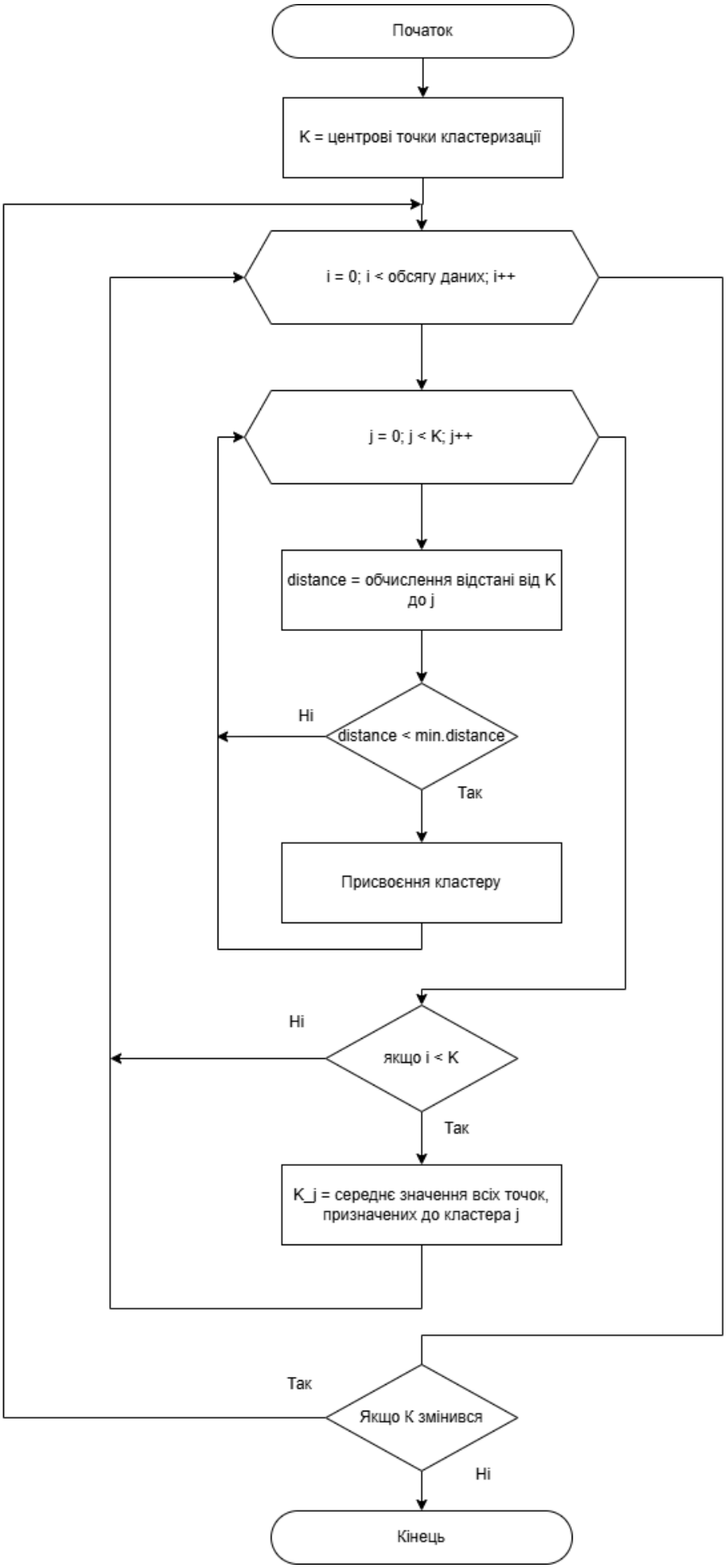

Початок
c_H = COUNT (Клас = H) / COUNT(ALL)
c_L = COUNT (Клас = L) / COUNT(ALL)
i = 0; i < кількості пристроїв
B_H[i] = COUNT (Клас = H, IF Пристрій = Пристрій [i] / COUNT (Клас = H)
B_L[i] = COUNT (Клас = L, IF Пристрій = Пристрій [i] / COUNT (Клас = L)
Розрахування умовної ймовірності належності об'єкта певному класу при рівності змінної "Пристрій" певному значенню
j = 0; j < кількості локацій
F_H[j] = COUNT (Клас = H, IF Локація = Локація [j] / COUNT (Клас = H)
F_L[j] = COUNT (Клас = L, IF Локація = Локація [j] / COUNT (Клас = L)
Розрахування умовної ймовірності належності об'єкта певному класу при рівності змінної "Локація" певному значенню
i = 0; i < кількості пристроїв
j = 0; j < кількості локацій
P (Клас = H, IF Пристрій = Пристрій [i] AND Локація = Локація [j]) =
B_H[i]*F_H[j]*c_H / (B_H[i]*F_H[j]*c_H + B_H[i]*F_H[j]*c_H)
P (Клас = L, IF Пристрій = Пристрій [i] AND Локація = Локація [j]) =
B_L[i]*F_L[j]*c_L / (B_L[i]*F_L[j]*c_L + B_L[i]*F_L[j]*c_L)
Розраховуємо ймовірність належності об'єкта до певного класу, за умови рівності критеріїв певним значенням
Кінець

ДОДАТОК Е

БЛОК-СХЕМА АЛГОРИТМУ КЛАСТЕРИЗАЦІЇ K-MEANS

СТОРІНОК – 1

Київ 2025


Початок
K = центрові точки кластеризації
i = 0; i < обсягу даних; i++
j = 0; j < K; j++
distance = обчислення відстані від K до j
Ні
distance < min.distance
Так
Присвоєння кластеру
Ні
якщо i < K
Так
K_j = середнє значення всіх точок, призначених до кластера j
Так
Якщо K змінився
Ні
Кінець