КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії
(назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему: Біометричні технології в системах безпеки аеропортів

Сивець Богдана Олександрівна

(прізвище, ім'я та по батькові здобувача повністю)

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кафедра кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ

_____

„___" _____2025 року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Біометричні технології в системах безпеки аеропортів

(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Сивець Богдана Олександрівна

(прізвище, ім'я та по батькові повністю)

125 «Кібербезпека та захист інформації»

(спеціальність)

«Безпека інформаційних і комунікаційних систем»

(освітня програма)

Група БІКСм_24

Керівник Шабала Є.Є.

(прізвище та ініціали)

доцент, к.т.н

(вчене звання, науковий ступінь)

Рецензент Гончаренко Т.А.

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій
Кафедра: кібербезпеки та комп'ютерна інженерія
Освітній рівень: магістр
Спеціальність: 125 «Кібербезпека та захист інформації»
ОПП:«Безпека інформаційних і комунікаційних

ЗАТВЕРДЖУЮ

Завідувач кафедри
_____
„___"_____2025 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Сивець Богдана Олександрівна
(прізвище, ім'я та по батькові здобувача)

1. Тема роботи «Біометричні технології в системах безпеки аеропортів» затверджена наказом ректора КНУБА № 165/23.2/25 від «30» вересня 2025 року
2. Керівник роботи Шабала Є.Є. доцент, к.т.н
(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)
3. Термін подання здобувачем роботи до захисту грудень 2025
4. Зміст пояснювальної записки за розділами:
Р. 1. Біометрія та системи безпеки аеропорту _____
Р. 2. Технічна основа та оцінка методів _____
Р. 3. Архітектура біометричної системи для українського аеропорту _____
Р. 4.____
Р. 5.____
5. Графічний матеріал за розділами:
Р. 1._ Схема зонування аеропорту та сучасні біометричні технології_____
Р. 2. Біометричні технології, що використовуються в аеропортах та основні ризики _____
Р. 3. Схема архітектури біометричної системи, рівні, маршрут пасажира, модель загроз і сценарії реагування_____
Р. 4.____
Р. 5.____

6. Консультанти розділів кваліфікаційної випускної роботи

Розділи	Прізвища, ініціали та посади консультанта	Перевірив	
		дата	підпис
Розділ 1. Біометрія та системи безпеки аеропорту			
Розділ 2. Технічна основа та оцінка методів			
Розділ 3. Архітектура біометричної системи для українського аеропорту			

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1. Біометрія та системи безпеки аеропорту	Жовтень 2025
Розділ 2. Технічна основа та оцінка методів	Листопад 2025
Розділ 3. Архітектура біометричної системи для українського аеропорту	Грудень 2025
Остаточне оформлення роботи	Грудень 2025
Направлення роботи на рецензування, перевірку на плагіат	Грудень 2025
Попередній захист роботи на кафедрі	Грудень 2025

8. Дата видачі завдання Вересень 2025

Керівник _____ _____
(підпис) (прізвище та ініціали)

Здобувач _____ _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Сивець Б.О. «Біометричні технології в системах безпеки аеропортів»

Метою кваліфікаційної роботи є аналіз біометричних технологій у системах безпеки аеропортів та розробка біометричної системи для цивільного аеропорту з урахуванням сучасних вимог до безпеки та організації пасажирських процесів. У роботі розглядаються підходи до ідентифікації пасажирів і персоналу, зонування аеропорту, біометричні методи та ризики, пов’язані з їх використанням.

У практичній частині змодельовано архітектуру системи, визначено критичні точки контролю, маршрут пасажира, сценарії реагування на аномальні події та резервний режим роботи.

Ключові слова: біометрія, аеропорт, безпекова система, розпізнавання обличчя, відеоаналітика, ідентифікація, контроль доступу.

SUMMARY

Syvets B.O. "Biometric technologies in airport security systems"

The purpose of the qualification work is to analyze biometric technologies used in airport security systems and to develop a biometric system architecture for a civil airport, taking into account modern security requirements and the organization of passenger processes. The work examines approaches to passenger and staff identification, airport zoning, biometric methods, and the risks associated with their use.

In the practical part, the system architecture is designed, critical control points and passenger routes are defined, and scenarios for responding to abnormal events and backup system operation are developed.

Keywords: biometrics, airport, security system, facial recognition, video analytics, identification, access control.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ *здобувача українською та англійською мовами* *Сивець Богдана Олександрівна* *Syvets Bohdana*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Біометричні технології в системах безпеки аеропортів Biometric technologies in airport security systems		
Освітній ступінь	Магістр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки і комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека та захист інформації		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Шабала Є.Є		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	118	3	19
Розділ 1	Біометрія та системи безпеки аеропорту		
Розділ 2	Технічна основа та оцінка методів		
Розділ 3	Архітектура біометричної системи для українського аеропорту		
Розділ 4			
Розділ 5			
Висновки по роботі			
Ключові слова: Keywords:	біометрія, аеропорт, безпекова система, розпізнавання обличчя, ідентифікація, контроль доступу. biometrics, airport, security system, facial recognition, identification, access control.		

Здобувач _____/ _____

Керівник _____/ _____

ЗМІСТ

ВСТУП

Стрімкий розвиток світового пасажиропотоку щороку збільшує кількість авіаперевезень, а разом з цим зростає і кількість потенційних загроз. Події на початку 2000-х років, коли масштабна терористична атака поставила під загрозу всю світову авіацію, змусила міжнародну спільноту повністю переглянути систему контролю аеропортів та почати шукати надійніші методи ідентифікації пасажирів. Одним із визначальних рішень стало поширення біометричних паспортів, які дозволяють використовувати біометричні параметри для підтвердження особи.

Разом з цим в світових аеропортах почали розвиватися й інші технології, що використовують біометричні ознаки для контролю безпеки та спрощення прикордонних процедур. За останні кілька років ці рішення суттєво модернізувалися і тепер частина перевірок виконується без участі співробітників аеропорту, а автоматично на основі біометричних ознак.

Актуальність обраного напряму роботи: В Україні цивільні аеропорти припинили свою роботу 24 лютого 2022 року, що фактично зупинило їх розвиток. Після відновлення цивільних авіаперевезень вони матимуть потребу швидкої модернізації до сучасних технологічних вимог, а також до підвищених безпекових ризиків.

Метою роботи є формування архітектурної моделі біометричної системи для цивільного аеропорту, яка відповідає сучасним технічним вимогам та адаптована до українських умов після відновлення авіаперевезень.

Завданням роботи є:

- Аналіз розвитку біометричних технологій та їх застосування у світових аеропортах;
- Визначення ризиків, пов’язаних з ідентифікацією пасажирів та персоналу;
- Визначення критичних точок доступу, необхідного обладнання та його характеристики;

- Розробка архітектури системи біометричної безпеки для аеропорту.

Об’єктом дослідження є біометричні технології, що використовуються у безпекових процесах в аеропортах.

Предметом дослідження є архітектура біометричної системи, її компоненти та можливість інтеграції у структуру аеропорту.

Наукова новизна роботи полягає у формуванні моделі біометричної системи, яка поєднує фізіологічну та поведінкову біометрію, автоматизовану перевірку документів та сценарії реагування на інциденти. У роботі запропоновано новий підхід до визначення критичних точок маршруту пасажира та адаптація біометричних процесів під умови вітчизняних аеропортів, які відновлюватимуть роботу після тривалого простою.

Практичне значення: створена модель може слугувати основою для підготовки технічних вимог до модернізації аеропортів після відновлення авіасполучення. Архітектура дозволяє визначити необхідний склад обладнання, логіку обробки даних, а також порядок поетапного впровадження технологій. Запропонований підхід може бути використаний у різних аеропортах України.

Обгрунтування необхідності розробки: біометрія стала базовим інструментом контролю в більшості світових аеропортів. Ці технології швидко розвиваються, сконцентрувавшись на автоматизації процедур перевірки документів, розпізнаванні обличчя та поведінковій аналітиці, які зменшують кількість ручних операцій і підвищують точність ідентифікації.

В українських аеропортах розвиток біометричних технологій фактично зупинився, коли зупинилися цивільні авіаперевезення. Тому виникає потреба у створенні нової моделі, яка визначає, як саме мають бути організовані процеси біометричної ідентифікації, які технології необхідні на кожному етапі маршруту пасажира та персоналу, і яким чином система може працювати в умовах відновлення та поступової модернізації.

Методи дослідження:

- Аналіз нормативних документів та технічних стандартів, зокрема ICAO,

ISO, нормативних документів України та Європейського Союзу, матеріалів IATA, пов’язаних з біометричними технологіями, авіаційною безпекою або прикордонним контролем;

- Порівняльний аналіз рішень, які застосовуються у провідних аеропортах світу;
- Моделювання пасажирського маршруту з визначенням критичних точок, у яких необхідне застосування біометричних методів і автоматизованого контролю;
- Аналіз ризиків, який включав визначення потенційних загроз та побудову сценаріїв реагування;
- Побудова архітектурної моделі, що описує взаємодію сенсорів, модулів обробки даних, резервування;
- Моделювання на прикладі схеми реального аеропорту критичних точок доступу.

РОЗДІЛ 1. БІОМЕТРІЯ ТА СИСТЕМИ БЕЗПЕКИ АЕРОПОРТУ

1.1 Сутність біометричних систем та еволюція авіаційної безпеки

Авіація відіграє важливу роль у світовій економіці. На неї припадає близько 3,5% світового ВВП, щодня виконується понад 120 тисяч рейсів і перевозиться понад 10 мільйонів пасажирів. Це один із секторів, що найшвидше зростають за останні десятиліття, і очікується, що до 2035 року обсяг авіаперевезень подвоїться.

Зі стрімким зростанням обсягів авіаперевезень пропорційно зростають і виклики, пов'язані з безпекою. Аеропорти – це відкриті простори, через які щоденно проходить потік тисяч людей. Такий потік складно контролювати: пасажири постійно переміщуються між різними зонами, поряд працює обслуговуючий персонал, і до цього ще додається багаж і вантажі. Усе це створює середовище, де контроль доступу стає надзвичайно складним завданням. [1]

Ще одна проблема полягає у швидкому зростанні кількості пасажирів. Системи перевірки працюють із дедалі більшим навантаженням, а ресурсів для їхнього розширення часто бракує. До цього також додається й проблема актуалізації обладнання, яке не завжди встигає оновлюватися відповідно до нових вимог і стандартів. Повна модернізація інфраструктури вимагає великих витрат і може призвести до зупинки частини процесів, що для аеропорту означає прямі збитки. У результаті зростає ризик використання застарілих технологій, які поступово втрачають ефективність і не відповідають сучасним підходам до безпеки. [2]

Класичних методів недостатньо, необхідно застосовувати технології, які можуть не тільки підняти рівень безпеки, а й зробити контроль швидшим та стійкішим, аби він відповідав масштабам сучасної авіації.

Для авіації біометрія є особливо важливою. Події 2001 року, а саме теракт 11 вересня, пов'язаний з викраденням літаків, змусив світ сильніше сконцентрувати увагу на авіаційній безпеці, зокрема змінити правило "до гейту може пройти будь-хто, хто має квиток" на багаторівневу систему доступу та перевірки пасажирів, персоналу та багажу, зокрема з застосуванням біометричних даних.

Терористи безперешкодно пройшли стандартні перевірки, використовуючи дійсні, але не свої документи, а також скористалися відсутністю суворого розмежування між зонами доступу в аеропортах. Це дозволило їм сісти на літаки як звичайним пасажирам та, коли літаки вже були в повітрі, захопити управління.

Трагедія показала одразу кілька серйозних прогалин існуючої на той момент системи безпеки:

- Ідентифікація грунтувалася виключно на паперових документах, які можна було підробити або отримати шахрайським чином;
- Контроль на вході до «стерильної зони» був надто поверховим і не враховував всі можливі загрози;
- Персонал аеропортів і екіпаж літаків фактично не був захищений від потенційного втручання сторонніх осіб. [3]

Посвідчення особи можна підробити, натомість відбиток пальця або особливості обличчя майже неможливо. Саме після цих подій біометричні технології почали активно впроваджуватися в аеропортах як доповнення до вже наявних систем безпеки.

Міжнародна організація цивільної авіації (ICAO) ініціювала перехід до біометричних паспортів і інтеграцію біометрії у перевірку особи як одного з найефективніших інструментів підвищення безпеки.

Поширення біометрії стало звичним для аеропортів, її почали активно використовувати на паспортному контролі, у службових зонах та під час посадки на рейси.

Біометрія – це сукупність технологій, які використовують унікальні фізіологічні або поведінкові характеристики людини для її розпізнавання чи підтвердження особи.

Кожна людина має набір ознак, які складно або практично неможливо відтворити штучно. До фізіологічних ознак належать відбитки пальців, геометрія обличчя, малюнок райдужної оболонки ока, форма долоні чи візерунок вен. До поведінкових – голос, його особливості, хода людини, моторика рухів почерк та

навіть звички користування пристроями.

Метою цих процесів є забезпечення надійного контролю доступу до об’єктів та інформації, підтвердження та пошук особи та загальне підвищення рівня безпеки, де традиційні методи (паролі, картки, ключі доступу), які можуть бути втрачені або підроблені, не завжди гарантують достатній рівень захисту.

Біометричні системи використовують унікальні ознаки для двох основних процесів – ідентифікації та автентифікації:

- Ідентифікація – це визначення особи шляхом порівняння отриманих даних із великою базою зразків;
- Автентифікація – підтвердження, що користувач є саме тією особою, за яку себе видає, шляхом співставлення з одним еталонним шаблоном.

Принцип роботи біометричних систем включає кілька етапів. Насамперед у базі даних вже має бути еталонний шаблон користувача, тобто заздалегідь збережене цифрове представлення його біометричної ознаки в базі даних, яке було створено під час первинної реєстрації.

Система за допомогою спеціальних сканерів та камер зчитує біометричний параметр та перетворює його на унікальну математичну модель біометричної ознаки. Після цього проводиться цифрова обробка, яка виділяє ключові характеристики (контури, точки, візерунки). Отримані дані порівнюють з еталоном, збереженим у базі, і, якщо збіг перевищує встановлений поріг подібності (throughput), користувач вважається автентичним і система надає йому доступ. Якщо ж збіг недостатній або об’єкт викликає підозри, запит відхиляється, і потрібна додаткова перевірка. [4]

Сьогодні існує велика кількість біометричних технологій, що використовують різні ознаки людини. Серед них можна виділити ознаки, які найчастіше використовуються у сфері безпеки: сканування геометрії руки, розпізнавання обличчя, аналіз райдужної оболонки та відбитки пальців.

- Розпізнавання обличчя – один із найзручніших способів, який майже не потребує дій від користувача. Камера фіксує зображення, система

обробляє його і порівнює з базою даних чи інформацією в електронному паспорті. Метод швидкий і зручний, але іноді чутливий до освітлення або наявності маски.

- Сканування райдужної оболонки ока відзначається дуже високою точністю. Візерунок райдужки унікальний для кожної людини, тому цей метод часто використовують у зонах із підвищеним рівнем контролю. Значущим недоліком цього методу є дорожче обладнання і дещо повільніша перевірка.
- Геометрія руки – система вимірює форму долоні та пальців. Вона менш точна, проте зручна й стабільна в умовах, коли потрібна проста ідентифікація персоналу без складного обладнання.
- Відбитки пальців – мабуть, найпоширеніший варіант, що залишається популярним через свою простоту, швидкість і точність. Система виділяє унікальні особливості відбитка та порівнює його зі зразком в базі. Недоліком може бути складність зчитування у разі пошкодження або забруднення шкіри чи сенсора.

Сучасні аеропорти постійно розвивають системи контролю: окрім базових методів, вони поступово впроваджують і додаткові біометричні рішення. Сюди належить розпізнавання за ходою, тепловізійне вимірювання температури тіла, аналіз міміки та поведінкових ознак. Також застосовуються комбіновані системи, які поєднують розпізнавання обличчя з перевіркою голосу чи жестів.

Утім, слід зазначити, що біометричні технології варіюються за технічними характеристиками, вартістю та зручністю використання. Їхня ефективність у реальних умовах аеропорту залежить від низки факторів: освітлення, кількості пасажирів, швидкості руху, а також наявності масок. [5]

Нижче, в таблиці 1.1, наведено узагальнене порівняння основних технологій, що використовуються або тестуються в аеропортах, із урахуванням їхніх технічних характеристик, переваг, недоліків.

Таблиця 1.1 Порівняння біометричних технологій

Метод	Точність	Швидкість	Вартість впровадження	Зручність для користувача	Актуальність для аеропорту	Недоліки
Відбитки пальців	Висока	Висока	Низька	Висока	Використовується переважно для персоналу, у пасажирських зонах поступається безконтактним методам	Контактна технологія, потребує регулярної дезінфекції, чутливий до стану шкіри
Розпізнавання обличчя	Середня/ висока	Дуже висока	Середня	Висока	Один із ключових методів у системах eGate	Чутливість до освітлення, кута зйомки, масок, можливі помилки в натовпі
Райдужна оболонка	Дуже висока	Середня	Висока	Середня	Використовується у зонах підвищеної безпеки (персонал, критичні приміщення)	Дороге обладнання, повільніше зчитування, потребує точного позиціонування
Геометрія руки	Середня	Середня	Середня	Середня	Використовується переважно у службових приміщеннях	Менша точність, потребує фізичного контакту, дещо застаріла

Тепловізійне випромінювання та поведінковий аналіз	Середня	Висока	Висока	Висока	Використовується як допоміжний елемент для моніторингу стану пасажирів	Не ідентифікує особу напряму, обмежена точність, високі витрати

Біометричні системи вже стали базовою технологією в транспортній інфраструктурі, їх головними перевагами є швидкість, точність та певний персоналізований підхід до перевірки особи. Для кожної людини формується своєрідний унікальний "ключ" у вигляді біометричних даних, який можна використовувати для контролю доступу до об’єктів з обмеженим входом. Саме тому біометричні системи адаптуються під потреби конкретних об’єктів: від фінансових установ і державних служб до транспортної інфраструктури.

Більшість всіх нововведень, пов’язаних з біометрією, відбулися в період, починаючи з 2015 року. Якщо до 2001 року безпека означала фізичну перевірку багажу, то після появи біометрії в системах аеропортів сталася певна еволюція протоколів до аналітичних моделей управління ризиками.

Еволюція систем захисту та роль біометрії:

- Період до 2001 року: тоді безпека базувалася на ручній перевірці документів та базових металодетекторах. Система була орієнтована на виявлення заборонених предметів, а не на ідентифікацію людини.
- Період 2001-2010 років: після терористичних актів відбувся вимушений стрибок у розвитку технологій, впроваджено тотальний контроль багажу, обмеження рідин, сканери тіла та більш детальна перевірка документів та їх власників. У цей період з’явилися електронні паспорти та розвинулася саме цифрова автентифікація.
- 2020 – дотепер: біометрія перетворилася на базовий елемент всієї архітектури контролю, вона інтегрувалася не лише в пасажирські процеси (реєстрація, посадка), а й у роботу персоналу та аналітику ризиків. ШІ-

системи відеоаналітики дозволяють виявляти аномальні патерни поведінки пасажирів та працівників, формує ризик-профіль та може автоматично направити службу безпеки до підозрілої особи, або взагалі самостійно заблокувати їй доступ.

В цьому контексті буде доцільно розглядати біометричну безпеку аеропорту більше як послідовність дій людини, наприклад, для подорожуючого – це пасажирський маршрут (від входу в термінал і до посадки на борт), а для співробітника – профіль доступу та рух у службових зонах відповідно до його функцій. На кожній критичній точці система фіксує подію, яку можна використати для аналізу, саме тому в роботі для аналізу вибрано модель, що враховує і ідентифікацію особи, і поведінкові фактори одночасно.

1.2. Архітектура системи безпеки аеропорту та біометрія для пасажирів

1.2.1. Безпекове зонування аеропорту

Територія аеропорту, відповідно до міжнародних стандартів безпеки (EU Regulation No 300/2008; ICAO Annex 17), поділяється на кілька зон, кожна з яких має свої правила та умови доступу, і різний рівень контролю:

- Landside (зовнішня зона) – це відкрита частина аеропорту: зона перед терміналом, зали очікування, парковка, стійки реєстрації, каси, багажні стійки. Доступ до цієї зони вільний, але тут використовуються базові заходи нагляду, такі як відеоспостереження, в деяких аеропортах на вході до терміналу встановлені рентгенівські сканери та металодетектори.
- Airside (внутрішня стерильна зона) – це простір після проходження контролю безпеки. Доступ сюди мають лише пасажири з посадковим талоном, які вдало пройшли безпековий контроль, і персонал з перепустками. Доступ суворо контролюється, повернутися у зовнішню зону можна лише через охоронні пункти.
- Security restricted areas (зони обмеженого доступу) – це частини аеропорту, де ризики вищі: ділянки контрольованої зони аеропорту, які

визначені як зони найвищого ризику і в яких поряд з контролем доступу застосовуються інші заходи контролю з метою забезпечення безпеки. Як правило, такими зонами є всі зони, призначені для пасажирів, які користуються послугами комерційної авіації; [6]

- Critical parts of security restricted areas (критичні ділянки з обмеженим доступом) – найбільш захищені місця: перони, злітно-посадкові смуги, технічні приміщення, зони обслуговування літаків. Потрапити сюди можна лише з окремим рівнем доступу після перевірки й обов'язкової перевірки біографічних даних (background check) для всього персоналу, включно з екіпажами повітряних суден. [7]

Розглянемо ці зони детальніше на прикладі аеропорту «Бориспіль». На схемі нижче зображено загальну структуру території: під'їзд з боку траси, транспортні зупинки, термінали, перони та летовище.

Термінал D – головний пасажирський термінал аеропорту, саме через нього проходить основна частина міжнародних рейсів. Простір перед ним є зовнішньою зоною, яка охоплює під'їзні смуги, громадський транспорт, зону стоянки таксі та прилеглі паркінги. І хоча доступ сюди відкритий, проте вже тут працює система відеоспостереження, діє патрулювання, а також, за необхідності, може додатково впроваджуватися контроль при вході в сам термінал (наприклад перевірка через металошукачі, вимірювання температури тіла, або пропуск лише осіб подорожуючих, з забороною пропуску відвідувачів або проводжаючих).

Далі починаються зони із вищим рівнем доступу. На схемі стоянки повітряних суден та прилеглі секції позначені окремо – це перон і технічні ділянки, куди персонал потрапляє лише через контрольовані пункти. Тут діють вимоги щодо перевірки перепусток і фіксації входу/виходу.

На схемі видно, що зони розмежовано так, щоб не перетиналися загальнодоступні маршрути та ділянки, пов'язані з обслуговуванням літаків. Це необхідно для підтримання контролю за переміщенням персоналу і техніки.

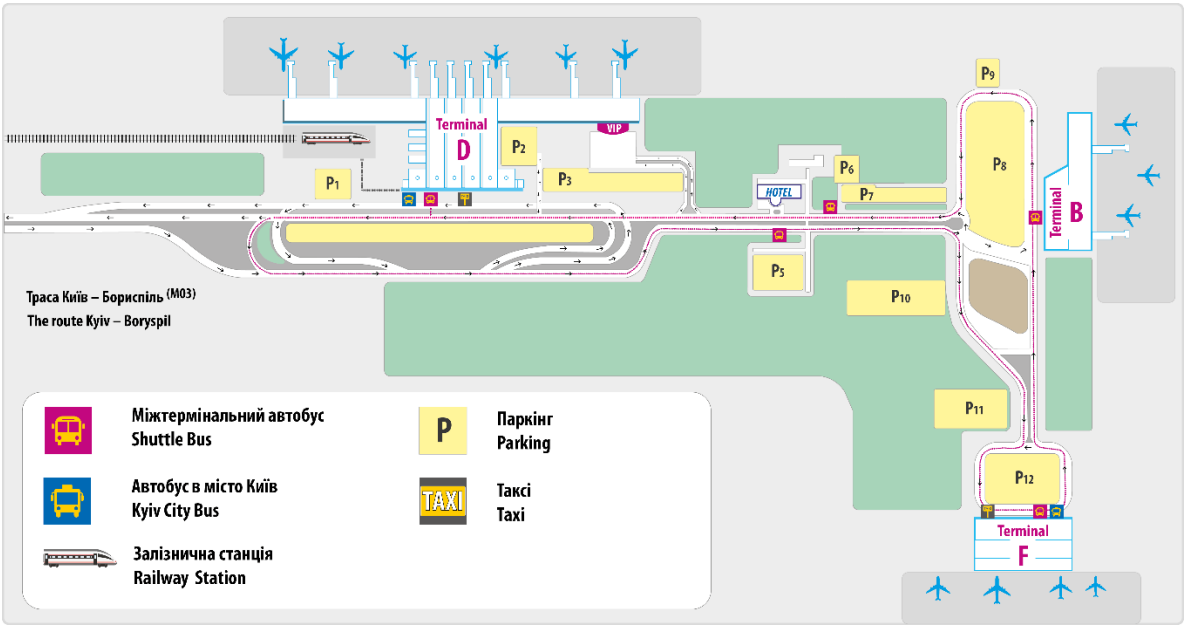


Рис. 1.1 Схема аеропорту «Бориспіль»

Подальше розмежування зон добре видно на прикладі внутрішньої структури терміналу D, який має три рівні, кожен з яких відповідає за свій етап пасажирського потоку. Таким чином, аеропорт чітко розділено на прибуття, міжнародні та внутрішні вильоти.

На рисунку 1.2 зображено перший рівень терміналу, який призначений для міжнародних прибуттів. Тут розташовані зали для пасажирів після прильоту, видача багажу, паспортний і митний контроль. Рух організований так, щоб пасажири, після контролю за видачі багажу, одразу переходили до відкритої зони та не змішувалися з пасажирами, що прибули в аеропорт для вильоту.

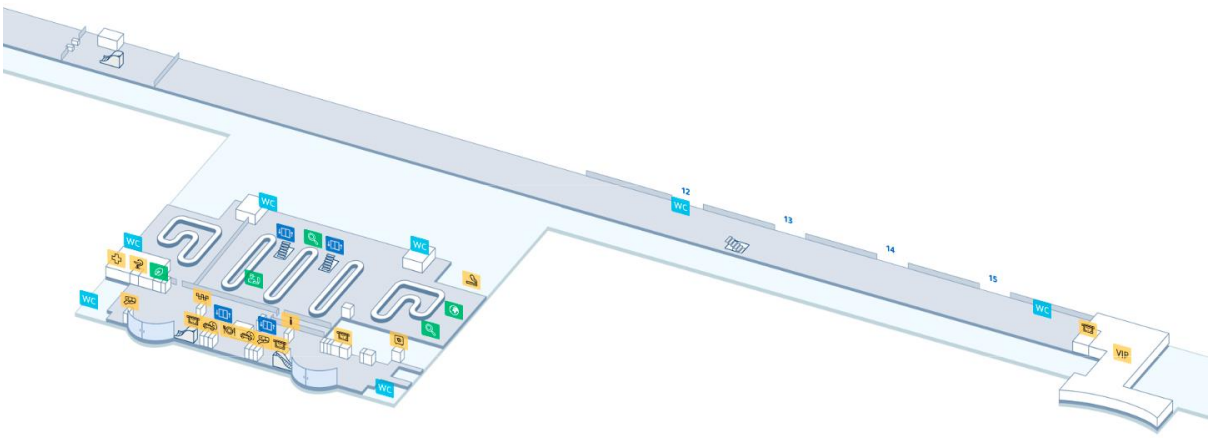


Рис. 1.2 Перший рівень терміналу D

Другий рівень (рис 1.3) використовується для внутрішніх рейсів. На ньому розміщені стійки реєстрації, перевірка документів, а також проходження контролю безпеки. Після проходження контролів пасажир потрапляє до стерильної зони, звідки очікує посадку на рейс Україною. Оскільки для внутрішніх перевезень не застосовуються прикордонні процедури, пасажири проходять маршрут швидше.

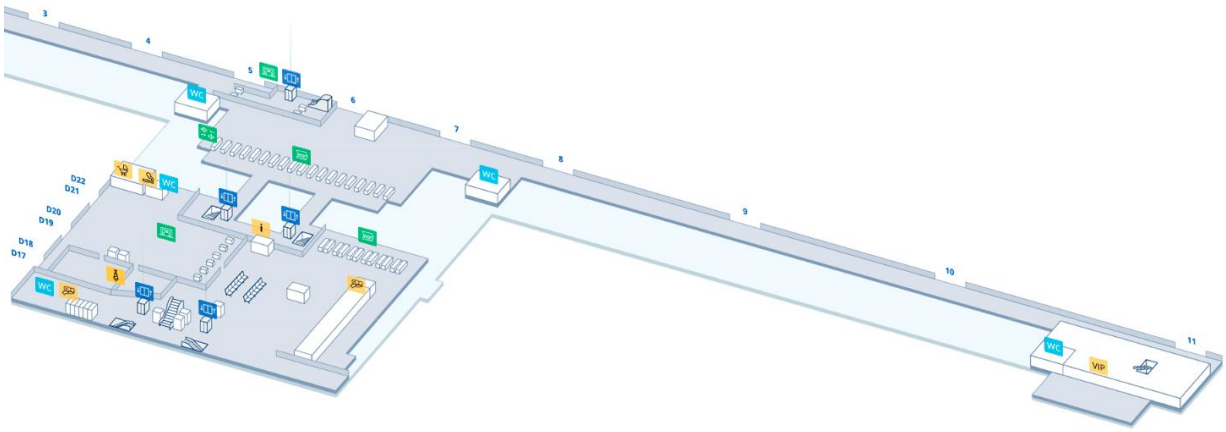


Рис. 1.3 Другий рівень терміналу D

Третій рівень (рис 1.4) обслуговує міжнародні вильоти. Тут знаходяться стійки реєстрації, безпековий контроль, паспортний контроль та подальший прохід у стерильну частину із магазинами, лаунджами та виходами на посадку, без можливості повернення до зовнішніх зон.

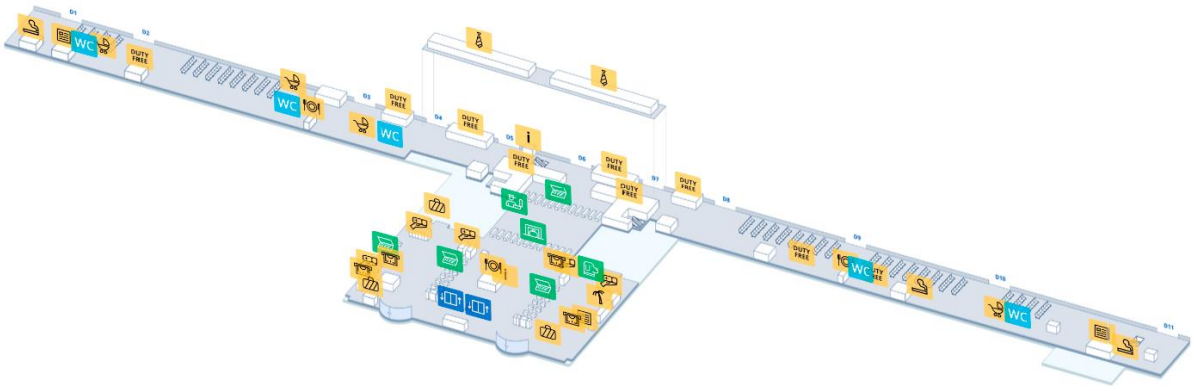


Рис. 1.4 Третій рівень терміналу D

Схеми терміналу D аеропорту «Бориспіль» показують, що після проходження контролю пасажир переходить у внутрішній рівень безпеки, де пересування

обмежується зоною до гейтів. Фактично, в цій зоні в пасажир може рухатися по обмеженому маршруту – від контролю до посадки на борт, залишаючи можливість користуватися внутрішньою пасажирською інфраструктурою (магазини, кафетерії, зали очікування тощо). Перехід між рівнями організований так, щоб рух здійснювався через контрольовані точки, які підтримуються відеонаглядом, перевіркою документів та перевіркою перепусток для персоналу. [8]

1.2.2 Використання біометрії в обслуговуванні пасажирів

До початку 2000-х паспортний і прикордонний контроль в аеропортах здійснювався вручну. Інспектор звіряв фото з документа з людиною перед собою, переглядав паспорт та візу, ставив штам і впускав в країну. Уся процедура трималася на уважності прикордонника, та не виключала можливість зловмисникам використовувати чужі або підроблені документи.

У 2002 році Міжнародна організація цивільної авіації (ICAO) ухвалила стандарт, який став основою впровадження біометричних паспортів.

Біометричний паспорт (електронний паспорт, Е-паспорт) – це закордонний документ, який містить вбудований мікропроцесорний чип, де зберігаються персональні і біометричні дані власника. На відміну від традиційного паспорта, який можна підробити чи використати шахрайським способом, дані з чипа зчитуються автоматично та порівнюються з шаблоном у базі даних. [9]

Стандарт Doc 9303 визначав, які дані мають бути на чипі та в якому форматі вони зберігаються. В біометричних паспортах містяться базові дані з паспортної сторінки: ім’я, дата народження, громадянство, номер документа, а також біометричні параметри. Обов’язковим є цифрове фото обличчя – фронтальне зображення об'єкта з рівномірним освітленням обличчя та нейтральним фоном, а також у багатьох країнах додають відбитки пальців, іноді ще скан райдужної оболонки ока. [10]

Малайзія була першою країною, яка ще в 1998 році видала біометричний паспорт, а до кінця 2006 такі паспорти видавали 60 країн, а до 2020 року їх кількість

зросла до понад 150. В Україні біометричні паспорти запроваджено з 1 січня 2015 року.

Впровадження біометрії в аеропортах не обмежилося паспортним контролем. Поступово вона інтегрувалася в інші процеси, які раніше виконувалися персоналом. Найпомітніші зміни відбулися у процесах реєстрації на рейс, посадки та митному контролі:

- Реєстрація: у багатьох аеропортах з'явилися кіоски самообслуговування. Пасажир може самостійно підтвердити особу через розпізнавання обличчя, після чого система видає посадковий талон і бирку для багажу, якщо в цьому є потреба.
- Посадка: на виходах до літака все частіше працюють автоматизовані ворота. Пасажир просто підходить до зчитувача, камера фіксує його обличчя й порівнює з даними з е-паспорта та квитка. Якщо інформація збігається, то ворота відкриваються, і таким чином відбувається посадка без участі інспектора. Автоматизовані гейти вже діють у Франкфурті, Амстердамі та Сінгапурі. [11]
- Митний контроль: у деяких країнах (наприклад, Австралія та Канада) замість ручної перевірки декларацій пасажир може скористатися спеціальними кіосками. Людина сканує паспорт, система зчитує дані з чипа та звіряє їх із образом на камері. Якщо система не бачить ніяких підозрілих факторів, декларація підтверджується автоматично. [12]

Їхня ефективність вже підтвердилась: за результатами глобального опитування IATA, проведеному у 2023 році, серед 8000 пасажирів зі 140 країн, більшість респондентів зазначили, що найбільше часу вони витрачають саме на прикордонний контроль.

Системи біометричної ідентифікації працюють на основі кількох джерел даних: інформації з паспорта, даних систем реєстрації, результатів розпізнавання обличчя, а також поведінкові ознаки. Ці дані обробляються алгоритмами штучного інтелекту та машинного навчання в режимі реального часу, перевіряють, чи

відповідають дані пасажира зафіксованим раніше в системі. Це дозволяє системі реагувати швидше за людину та оперативно приймати рішення на основі отриманої інформації.

Камери систем відеоспостереження передають інформацію на модуль відеоаналітики, далі алгоритми машинного навчання визначають обличчя, виділяють унікальні біометричні характеристики та звіряють їх з наявними базами даних у режимі реального часу. Також, залежно від можливостей самої системи та її конфігурацій, вона може паралельно звертатися до внутрішньої бази зареєстрованих пасажирів і до глобальних системам розшуку: списків Інтерполу, Європолу або Шенгенської інформаційної системи. В той самий час, на другому рівні обробки інші модулі аналізують поведінкові характеристики: динаміку руху осіб, швидкість пересування, зупинки в нетипових зонах, напрями, реакції, поведінку людей загалом. Якщо система фіксує аномалію, наприклад нетипове скупчення людей, затримку в певних зонах або різку зміну напрямку, вона автоматично формує сигнал до чергових груп, який містить прив'язку до камери, яка це зафіксувала, час, місцезнаходження об'єкта та сам об'єкт.

Ефективність таких систем залежить насамперед від точності алгоритмів розпізнавання та ступеня інтеграції між різними підсистемами. Тобто, чим краще система поєднує біометричну ідентифікацію з поведінковим аналізом, тим вища її здатність виявляти потенційні загрози, менший час обробки та менша кількість помилкових спрацювань. Навіть невелике відхилення між рівнем хибного сприйняття (FAR – False Acceptance Rate) та рівнем хибного відхилення (FRR – False Rejection Rate) у великому потоці пасажирів може створити занадто багато зайвих сповіщень, цим самим перевантаживши систему та службу безпеки, яка, відповідно, має реагувати на ці сповіщення. Щоб цього уникнути, системи встановлюють пороги спрацювання залежно від середовища: в зонах підвищеного ризику цей поріг має бути вищим, у зонах скупчення пасажиропотоку та загальних зонах – нижчий. Часто для цього використовують послідовність перевірки, де

спочатку йде аналіз поведінки, а потім підтвердження підозрюваної особи за біометрією.

Найбільш поширеним прикладом автоматизації стали електронні ворота (eGate). У Великій Британії працює понад 200 таких систем у 13 аеропортах. Вони розміщені на головних контрольних пунктах і складаються з двох частин: стійок для ручної перевірки та автоматизованих воріт. Один офіцер може одночасно наглядати за роботою до десяти eGate. [13]

Принцип роботи eGate поєднує біометрію та електронний паспорт:

1. Пасажир підходить до eGate і прикладає е-паспорт до сканера. Система миттєво зчитує дані з мікрочипа (особиста інформація, біометричне фото, а за потреби, також відбитки пальців або райдужку ока).
2. Одночасно камера використовує технологію розпізнавання обличчя: система зчитує живе зображення пасажира. При цьому фіксується час, ID воріт, і лог події записується в базу.
3. Далі відбувається первинна верифікація:

a) Зіставляється фото з чипа та живе зображення пасажира

b) Перевіряється справжність та цілісність чипа та, відповідно, документа

4. Після успішної первинної перевірки система проводить додаткові автоматичні перевірки ризиків:

a) Шукає дані пасажира в локальних чи національних базах (статуси розшуку, заборони на виїзд тощо)

b) Звіряється з базою авіакомпанії (наявність квитка, статус посадки)

c) Проводить аналіз поведінкових/аномальних тригерів (наприклад, невідповідна поза, неспокій, спроба обману).

5. На основі встановлених порогів збігу і правил ризику система приймає рішення:

d) Якщо всі перевірки успішно пройдені, і ризик оцінено як низький, ворота автоматично відкриваються.

e) Якщо виявлена невелика невпевненість (наприклад, показник збігу трохи

нижчий за поріг), пасажир спрямовується на ручну верифікацію.

f) Якщо ж виникає підозра чи зафіксовано негативний результат (підробка, відсутність збігу), доступ блокується, негайно надсилається сигнал офіцеру, який може проводити додаткову перевірку.

Це робить процес напівавтоматизованим: система обробляє більшість пасажирів самостійно, а людина втручається лише тоді, коли потрібна додаткова перевірка. Фактично, це рішення пришвидшує обслуговування і водночас зміцнює безпеку. [14]

У рамках ініціативи IATA One ID, яка планує оцифрувати весь процес подорожі, технологія biometric bag drop, вже впроваджена у Сінгапурі, Гельсінкі, Мюнхені, у цих аеропортах система реєструє багаж лише після того, як його власник верифікував обличчя та підтвердив свої біометричні дані з паспортними. Ця технологія дозволяє виключити випадки передачі речей іншим особам, а також випадки плутанини багажу. Система спочатку, ще під час здачі пасажиром багажу, сканує його обличчя та підв'язує конкретну багажну бирку до конкретного обличчя, потім вона перевіряє, чи пасажир пройшов всі контрольні точки перед завантажуванням багажу на борт судна. Якщо ж ідентифікація не завершена, вантажний модуль автоматично блокує виліт багажу. Додатково деякі аеропорти, наприклад в Сінгапурі та Дубаї, уже тестують біометричну авторизацію операторів рентгенівського обладнання. [15]

Світова пандемія COVID-19 у 2020 році різко зупинила авіаційний сектор. Більшість аеропортів тимчасово припинили роботу, міжнародні рейси скоротилися до мінімуму, а після часткового відновлення пасажиропотоку з'явилися нові вимоги до безпеки. Завданням стало не лише перевіряти документи, а й мінімізувати фізичний контакт між людьми, щоб зменшити ризик поширення вірусу.

Біометричні технології в цей період отримали потужний і абсолютно новий імпульс розвитку. Якщо раніше вони використовувалися переважно для пришвидшення перевірок і підвищення точності ідентифікації, то під час пандемії

акцент змістився на автоматизацію процесів, безконтактність і санітарну безпеку, а також контроль за пасажирами, що перебували в масках та рукавичках.

Саме тоді з’явився ряд нововведень, які змінили підхід до контролю доступу в аеропортах:

- Тепловізійний контроль: У багатьох аеропортах на вході встановлювали камери з інфрачервоними сенсорами, які автоматично вимірювали температуру пасажирів і сигналізували персоналу про відхилення. Іноді такі системи інтегрували з розпізнаванням обличчя, щоб ідентифікувати конкретного пасажира у разі відхилень.
- Безконтактні технології: Класичні процедури, які вимагали передачі документів в руки прикордонника або дотиків до обладнання замінили повністю безконтактні перевірки, які базувалися на повному використанні біометрії: замість сканування паспорта людина могла пройти перевірку лише за обличчям або відбитками пальців із безконтактних сенсорів. Такі системи з’явилися в Сінгапурі, Гонконзі, Дубаї та низці європейських аеропортів.
- Розпізнавання обличчя в масках: Масковий режим став серйозним викликом для алгоритмів, але саме це й стало стимулом для їх удосконалення. Правильне носіння масок вимагало повністю закривати рот та ніс, таким чином ховаючи половину обличчя пасажира та ускладнюючи роботу систем розпізнавання. У 2020 році, з початком пандемії, точність таких систем впала нижче 50 %, а вже до 2021 року з’явилися алгоритми, які могли ідентифікувати особу навіть у масці з точністю понад 95 %.
- Автоматизація доступу: Через скорочення персоналу аеропорти почали активніше застосовувати електронні ворота та мобільні додатки з біометрією. Пасажир міг зареєструватися, здати багаж і пройти на посадку без контакту з інспектором, використовуючи лише обличчя як «ключ» до всіх цих зон.

Після скасування карантинних обмежень деякі технології виявилася тимчасовими (зокрема, масове використання тепловізорів), але інші стали частиною постійної інфраструктури. Серед них безконтактні біометричні сенсори, покращені алгоритми для розпізнавання обличчя навіть у складних умовах, а також розширене використання eGate.

Таким чином пандемія стала своєрідним каталізатором для додаткового впровадження та удосконалення біометрії в аеропортах. Технології, які раніше розглядалися як «зручність для пасажирів», перетворилися на необхідність для забезпечення як безпеки, так і санітарного захисту. [16]

В аеропортах часто трапляються і ситуації, коли, наприклад, дитина або літня людина губиться серед великої кількості пасажирів, і саме тут знову працює поєднання біометрії з відеоаналітикою. Сучасні системи ідентифікації загублених працюють наступним чином:

1. Служба розшуку подає запит на пошук.
2. Система по відео виконує пошук серед камер та відеозаписів, використовуючи алгоритми розпізнавання обличчя, порівнюються шаблони.
3. Виділяються основні кандидати, на основі схожості.
4. Місцезнаходження людини передається черговій службі разом з часом, камерою та ракурсом зйомки.

Таким чином виконується пошук самої людини і її поточного або останнього місцезнаходження. Тут важливо, щоб система могла правильно виділяти зони пошуку на основі аналітики, переміщення та поведінки особи.

Хоча біометричні системи в аеропортах передусім створені для безпеки, їхній вплив на зручність пасажирів теж не можна недооцінювати. Контроль став простішим, швидшим і менш виснажливим, тепер замість кількох перевірок документів достатньо лише кількох секунд біля сканера.

Біометрія значно зменшила час очікування, відповідно, мінімізувала черги. Пасажиру більше не потрібно постійно діставати паспорт чи посадковий талон, щоб підтвердити свою особу, система все розпізнає автоматично.

Є вигода і для самих працівників аеропорту. Коли частина процесів автоматизована, персонал може зосередитися не на рутині, а на тих випадках, які справді потребують уваги. Це допомагає уникати перевантаження і робить роботу контрольних служб ефективнішою, адже увага приділяється саме підозрілим пасажирам.

Також, варто зазначити, що пасажири сприймають наявність біометричних технологій як ознаку безпеки. У більшості випадків такі системи підвищують довіру до процесів контролю, зокрема й через те, що вони працюють більш стабільно і передбачувано. Сама подорож тепер стає значно легшою: від пасажира вимагається менше дій, тоді як система сама забезпечує чіткий контроль. І, з часом навіть ті, хто не довіряє автоматизованим біометричним технологія, визнають переваги швидшого проходження та зменшення черг, які забезпечує цифровізація.

1.2.3 Практичний досвід впровадження біометрії в аеропортах світу та України

Один з найбільш інноваційних аеропортів світу – це сінгапурський аеропорт Changi, де біометрія інтегрується як частина цифрової екосистеми аеропорту. Там біометрія працює від моменту реєстрації людини (self-check-in), реєстрації багажу та аж до посадки на літак, а також працює як система управління пасажиропотоком, аналізуючи ситуацію та поведінку людей з камер відеоспостереження. Зараз там діють 130 автоматизованих смуг імміграційного оформлення, біометричні дані іноземних подорожуючих автоматично реєструються під час процесу оформлення документів на прибуття, а інформація про їхню реєстрацію міститься в електронній перепустці. [17][18]

В США U.S. Customs and Border Protection вже давно впроваджує системи біометричного в’їзду-виїзду для іноземних громадян, і вже з 26 грудня 2025 року

набуває чинності закон, який розширить застосування технологій розпізнавання обличчя та збору відбитків навіть при виїзді з країни. Метою цього вдосконалення законодавства є зменшення кількості випадків нелегального перебування в країні та осіб, які не мають записи про в'їзд до країни, а також для підвищення точної ідентифікації. Хоча громада й висловлює критику щодо приватності та точності, зокрема серед представників меншин, проте США застосовують моделі, що інтегрують біометричний в'їзд/виїзд як частину антитерористичного контролю та авіаційної безпеки. [19]

У Японії ще з 2007 року функціонує система імміграційного контролю J-BIS, яка збирає відбитки обох вказівних пальців та фото іноземних громадян, які збираються в'їхати в країну. [20]

Під час пандемії COVID-19 в країнах Азії біометричні технології знову активізувалися. Зокрема, в Японії система Face Express, яку запустили в липні 2021 року, де пасажир реєструє своє обличчя та потім може проходити реєстрацію багажу, контроль безпеки та посадку без повторного пред'явлення паспорта та посадкового талона. [21]

В аеропорту Південної Кореї Incheon в період пандемії впровадили комплекс біометрії, автоматизації та штучного інтелекту, а опісля більшість пасажирів самі вже обирали системи з мінімальною фізичною взаємодією.

Пандемія також прискорила впровадження біометричних технологій і в аеропортах Китаю, наприклад Beijing Capital International Airport впровадив понад 600 біометричних точок контролю: 250 автоматичних смуг, 80 кіосків самообслуговування, 30 пунктів самореєстрації багажу. [22]

Європейський Союз 12 жовтня 2025 року запустив систему в'їзду/виїзду EES, яка автоматизує реєстрацію на кордоні для громадян країн, що не входять до ЄС. Якщо особа вперше в'їжджає до Шенгенської зони, прикордонна служба збирає їх відбитки пальців та фото обличчя, які потім зберігаються в базі. Якщо особа вже перетинала кордон, то її дані просто будуть порівняні з даними, які вже збережені

в базі. А власники біометричних паспортів зможуть самостійно зареєструватися, скориставшись кіосками самообслуговування. [23]

В Арабських Еміратах активно застосовуються проєкти «безпаспортного контролю», де пасажир може пройти на посадку без використання паперових документів, а лише за допомогою біометрії. Тут вже діє повна інтеграція біометрії на всьому пасажирському маршруті: онлайн-реєстрація, check-in, реєстрація багажу, eGate, та загалом безперервне сканування.

Усі передові аеропорти рухаються одним маршрутом – вдосконалюють систему аеропорту шляхом її цифровізації, зокрема з серйозним впровадженням біометрії.

З 24 лютого 2022 року робота цивільних аеропортів України була припинена у зв'язку з введенням воєнного стану. Відповідно, за останні чотири роки розвиток пасажирської інфраструктури та інтеграція біометричних систем відстали від міжнародних тенденцій та останніх технологій.

До початку повномасштабного вторгнення українські аеропорти, зокрема Міжнародний аеропорт «Бориспіль» та інші великі хаби, поступово оновлювали інфраструктуру та адаптувалися до оновлень стандартів ICAO і Європейського Союзу. В період пандемії COVID-19 вже використовувалися термокамери для вимірювання температури пасажирів, проводився фото-контроль, використовувалися стандартні камери відеоспостереження, системи контролю доступу за перепустками для працівників та інші методи, які на сьогодні можна вважати вже дещо застарілими. Проте в аеропортах не було систем eGates, відеоаналітика обмежувалася звичайними функціями фіксації руху, контроль переміщення персоналу здійснювався без аналізу маршрутів, створення типового профілю співробітника та журналювання відхилень від робочого маршруту.

Деякі технології варто модернізувати, аби вони відповідали поточним вимогам безпеки та рівню автоматизації, який зараз використовується у світових аеропортах. Також, варто загадати, що після відновлення роботи аеропорти мають працювати в умовах підвищених ризиків. Зокрема це стосується фізичних ризиків,

загроз, пов’язаних із доступом у контрольовані зони, інсайдерських загроз, саботажу, спроби теракту та обману системи ідентифікації і спроби незаконного виїзду з країни.

Для відновлення роботи цивільних аеропортів та піднесення її до рівня міжнародних стандартів необхідно буде:

- Інтегрувати оновленні біометричні рішення, систему eGate та інші рішення, які спрощують пересування аеропортом пасажирів, але, при цьому, важливо, впровадити суворі вимоги для перевірки та контролю за пасажирськими аномаліями.
- Інтегрувати біометричні системи контролю доступу до контрольованих зон аеропорту, зокрема мультифакторні технології, збільшити захист від кібер- та терористичних атак, саботажу.
- Налаштувати систему так, щоб у разі надзвичайних ситуацій, вона могла працювати автономно, система має передбачати резервні канали зв’язку, захищені від атак, а також аварійні протоколи.
- Забезпечити сумісність з європейськими й міжнародними системами перевірки документів та пасажирських даних, щоб підготувати аеропорт до відновлення міжнародних рейсів, які вимагають співпраці з прикордонними службами інших країн.
- Визначити ризики та процедури моніторингу для персоналу, оскільки вони отримають доступ до контрольованих зон набагато раніше за пасажирів.
- Модернізувати систему відеоаналітики так, щоб вона фіксувала події в ключових точках, а також могла реагувати на загальні потоки пасажирів та персоналу в усіх зонах аеропорту, підтримувала пошук осіб у натовпі та могла реагувати на аномалії і автоматично надсилати сповіщення службі безпеки.

Загалом, за останнє десятиліття біометричні технології в аеропортах суттєво еволюціонували. Моделі розпізнавання стали точнішими завдяки глибокому

навчанню та перевірці на «живість». Паралельно посилилася загальна автоматизація процесів, зокрема біометрія інтегрувалася з мобільними додатками аеропортів, з'явилися кіоски самостійного біометричного контролю, реєстрації та eGates.

1.3. Біометричний контроль персоналу та протидія внутрішнім загрозам

Якщо для пасажирів біометрія переважно спрощує процес пересування аеропортом, то для персоналу вона є інструментом безпеки. В цьому випадку біометричні технології доповнюють перевірки, передбачені політиками безпеки персоналу, які мають на меті мінімізацію ймовірності того, що співробітники стануть загрозою безпеці, зменшення ризику інсайдерської діяльності та захист активів організації.

Відповідно до регламенту (документ про безпеку персоналу) ICAO - Insider Threat Toolkit усі співробітники, яким потрібен несупроводжуваний доступ до зони контролю та зон обмеженого доступу, а також особи, які мають доступ до конфіденційної інформації безпеки, повинні пройти перевірку біографічних даних, яка включає перевірку посвідчення особи, рекомендацій, кримінального минулого, історії зайнятості та освіти.

Правила вимагають проводити постійну перевірку та оновлювати дані персоналу, зокрема, щоразу, коли потрібно поновлювати дозволи на посвідчення особи в аеропорту.

Політика та процедури повинні бути чіткими та включати такі дії:

- деактивувати ідентифікаційні бейджи співробітників, які звільнилися з організації;
- обмежити права доступу до обмежених зон для власників перепусток на основі суворих операційних потреб;
- належним чином захистити периметр та точки контролю доступу, щоб гарантувати, що перевірку безпеки персоналу неможливо буде обійти;
- впровадити протоколи нагляду та ширше використання системи

відеоспостереження для операційної діяльності, де це доречно.

Аеропорт має складну структуру з чітким розмежуванням зон, де кожен рівень доступу регулюється окремо. До зон з обмеженим доступом (службових і технічних зон) належать приміщення, де розташоване обладнання для обслуговування літаків, системи зв'язку та навігації, пункти енергопостачання, диспетчерські кабіни, ангари, склади пального, серверні кімнати, а також офіси авіаційної безпеки. Ці території мають обмежений доступ, і потрапити туди можуть лише уповноважені співробітники з відповідним рівнем допуску.

Відповідно до Регламенту ЄС № 300/2008, контрольовані зони мають бути організовані так, щоб запобігти проникненню сторонніх осіб або транспортних засобів:

- Доступ до контрольованої зони має бути обмежений, щоб запобігти проникненню сторонніх осіб та транспортних засобів у ці зони.
- Доступ до зон обмеженого доступу має контролюватися, щоб забезпечити недопущення до цих зон сторонніх осіб та транспортних засобів.
- Особам та транспортним засобам може бути надано доступ до контрольованої зони та зон обмеженого доступу лише за умови, що вони відповідають необхідним умовам безпеки.
- Особи, включаючи членів екіпажу, повинні успішно пройти перевірку біографічних даних, перш ніж їм буде видано посвідчення екіпажу або посвідчення в аеропорту, що дозволяє доступ без супроводу до зон обмеженого доступу. [7]

Таким чином, зважаючи на перераховане вище, система безпеки в аеропортах для персоналу працює як Система контролю та управління доступом, де чітко розділяються зони доступу та категорії осіб, які можуть в кожну з цих зон потрапити.

Система контролю і управління доступом (скорочено СКУД або СКД) – це комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу/виходу та переміщень людей чи транспортних об'єктів на територіях, які

знаходяться під охороною, для адміністративного моніторингу та попереджень несанкціонованого проникнення. [24][25]

За допомогою системи контролю доступу також досягається:

- ідентифікація осіб, що мають право доступу;
- розмежування доступу до різних приміщень;
- керування автоматичними режимами;
- реєстрація часу перебування особи на об’єкті;
- обробка інформації та ведення статистики.

Тобто, робітник контрольованої зони не зможе потрапити в зону з обмеженим доступом, якщо його допуск на це не поширюється. Таке розмежування гарантує, що кожен працівник перебуває в зоні своєї відповідальності.

СКУД дійсно допомагає створити певну ієрархію доступу, а біометрія робить її персоніфікованою – жодна перепустка не спрацює без підтвердження конкретної особи. Саме тому аеропорти застосовують багаторівневі системи ідентифікації, які поєднують фізичні перепустки, персональні коди та біометричні дані.

Перепустка – документ, що видається особам, які працюють в аеропортах, або особам, яким з інших обґрунтованих причин необхідний санкціонований доступ в аеропорт, контрольовану зону, стерильні зони або зони обмеженого доступу, що охороняються. Такий документ дає змогу ідентифікувати особу та встановлені для неї зони доступу. Для подібних цілей видаються і використовуються перепустки на транспортні засоби.

Мультифакторна автентифікація (багатофакторна автентифікація) – це метод, за якого для доступу до зони з підвищеними вимогами потрібно надати декілька незалежних факторів. Зазвичай ці фактори комбінують:

- Щось, що людина знає: пароль або код доступу.
- Щось, що людина має: картка та електронна картка, пропуск, ключ.
- Щось, що є частиною: біометричні характеристики, такі як обличчя, відбиток пальця чи райдужна оболонка. [26]

Найпоширенішим поєднанням мультифакторної ідентифікації є картка співробітника і біометрична перевірка, наприклад за обличчям. Система не дозволяє пройти, якщо не підтверджено обидва типи автентифікації, наприклад, навіть при наявності перепустки вхід без сканування обличчя неможливий. Лише після збігу обох факторів відкривається доступ. Окрім цього, кожна спроба, вдала та невдала, фіксується в журналі системи, що дає змогу формувати поведінкові профілі персоналу. Система автоматично аналізує відхилення: час, доступ до нетипових зон, результати спроб входу, а також повторювані короткі входи та виходи. В разі нетипової поведінки працівника, система автоматично фіксує аномалію, особу працівника та надсилає сповіщення про ризик службі безпеки, а також може превентивно заблокувати доступ працівнику до критичних зон, до моменту ручної перевірки службою безпеки.

У більшості сучасних СКУД реалізовано механізм контролю щільності проходу через турнікет або шлюз. Якщо система фіксує спробу проходу двох осіб за однією перепусткою, вона самостійно блокує двері, скидає сесію доступу та надсилає сигнал тривоги. Такі алгоритми працюють разом з відеоаналітикою, що розпізнає кількість осіб у кадрі, а також траєкторію їх руху.

В деяких захищених установах, зокрема аеропортах, перепуски співробітників інтегровані з їхніми графіками і забороняють доступ персоналу в захищені зони.

Контроль доступу ефективно застосовується разом із моніторингом переміщення співробітників в реальному часі. Система фіксує не лише факт доступу, а й подальший маршрут працівника та його поточне місцеперебування. Біометрія в цьому контексті працює і для виявлення конкретного співробітника на основі його рис обличчя, і для виявлення підозрілої або нетипової поведінки працівника.

На основі звичної поведінки персоналу профілюються можливі ризики, що дозволить виявити підозрілі інциденти ще на ранніх етапах та ефективно їх ліквідувати. Спочатку система вивчає типові дії працівників, відповідно до їх

обов’язків та зон відповідальності, аналізує дані про пересування, час входів, дії біля критичних об’єктів та інші специфічні фактори. На основі цих спостережень формується профіль поведінки кожного співробітника.

Коли камери фіксують нетипову поведінку, працівник відхиляється від звичних маршрутів, намагається потрапити в зону, яка не входить до його рівня допуску, перебуває в приміщені поза графіком, система сприймає це як потенційну загрозу та автоматично реагує, відповідно до встановлених протоколів, наприклад, надсилає сповіщення службі безпеки. Якщо відхилення підтверджуються фахівцем служби безпеки, інформація повертається в систему як приклад реальної загрози.

У деяких організаціях дані про працівників можна знайти в журналах різних програмних застосунків, які фіксують дії працівників.

- журнали фізичного входу/виходу, з головним акцентом на час та доступ до фізичних просторів;
- записи про вхід/вихід із системи, з акцентом на зіставлення облікових даних за часом та користувачами;
- журнали програм електронної пошти;
- журнали програм бази даних.

Загалом, головна перевага біометрії полягає в тому, що біометричний ідентифікатор не можна позичити, загубити або передати. Якщо традиційна картка доступу може бути використана іншою особою, то біометрична верифікація лише підтверджує, що пропуск належить саме тому, хто його використовує. Це повністю виключає передачу доступу співробітників третім особам.

Також, на відміну від фотографії на посвідчення, яке зберігається в системі як звичайне зображення, біометричний шаблон зберігається у вигляді числового коду, який сформовано з унікальних фізіологічних ознак особи. Сам код захищений від копіювання і підробки, а використання технології перевірки на «живість» ефективно запобігає спробам використати муляжі, фото та відео. Наприклад, системи розпізнавання обличчя аналізують мікрорухи очей, глибину обличчя (3D-сканування, щоб впевнитися, що зразок перед ним не двовимірний) та температуру

об’єкта, щоб переконатися, що перед сканером знаходиться жива людина, а не її копія. Завдяки цьому ризики зловживання службовими перепустками значно зменшилися.

Крім того, біометрія зменшує кількість помилкових спрацювань і спрощує процедури доступу для співробітників, а також унеможливлює відділене втручання в процес ідентифікації. Навіть у разі компрометації бази даних, доступ до реальних біометричних характеристик залишиться неможливим.

1.4. Нормативно-правова база та етичні аспекти впровадження біометрії

Використання біометричних технологій у цивільній авіації має бути чітко узгоджене з міжнародними нормами. Їх використання регулюється міжнародними документами, внутрішніми законодавствами держав, а також вимогами до обробки та захисту персональних даних.

Основні вимоги до використання біометричних технологій у цивільній авіації визначає Міжнародна організація цивільної авіації (ICAO), яка створює базові стандарти для всіх країн-учасниць (сьогодні до її складу входять 193 держави – майже всі країни світу, які мають свій авіаційний простір і здійснюють міжнародні перевезення).

Документ ICAO Doc 9303 визначає технічні вимоги для машинозчитуючих документів та електронних паспортів. У ньому описана структура зберігання біометричних даних, процедури та алгоритми перевірки автентичності мікрочипа та формат даних, який використовують для міжнародного обміну даними. Саме цей стандарт став основою для впровадження біометричних паспортів у більшості країн світу. [10]

Наступний важливий *документ ICAO – Annex 17*, він визначає стандарти для організації авіаційної безпеки. Тут визначено порядок контролю доступу до зон обмеженого доступу та процедури перевірки персоналу. В цьому документі біометрія визначається як один з рекомендованих інструментів, які дозволять

посилити рівень контролю, зменшити вплив людського фактора та запобігти використанню чужих перепусток . [27]

Aviation Security Global Risk Context Statement (GRCS) ICAO подає загальну оцінку ризиків у сфері авіаційної безпеки . У ньому підкреслюється роль біометрії у захисті від інсайдерських загроз та закцентовано увагу на потребі інтеграції біометрії в систему контролю доступу в аеропортах і для пасажирів, і для персоналу. [28]

Практичні рекомендації щодо захисту від внутрішніх загроз викладено в *Insider Threat Toolkit*. Цей документ регулює вимоги до перевірки персоналу, процедури прийому на роботу, моніторингу поведінки співробітників протягом часу їх роботи та яким чином має здійснюватися захист даних співробітників від внутрішніх загроз. [29]

Європейське законодавство доповнює стандарти ICAO через *Регламент ЕС №300/2008*, який визначає загальні вимоги до авіаційної безпеки в межах ЄС. Документ регламентує порядок доступу до контрольованих і обмежених зон, вимоги до перевірки осіб та загальні принципи захисту персональних даних. [7]

Ще один важливий для ЄС документ – це регламент *General Data Protection Regulation No 2016/679* про захист фізичних осіб стосовно обробки персональних даних та про передачу цих даних. Цей документ визначає біометричні дані як «особливі» (чутливі) персональні дані: «**біометричні дані**» – персональні дані, отримані в результаті спеціальної технічної обробки, що стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи, наприклад зображення обличчя або дактилоскопічні дані (відбитки пальців).

Регламент (ЄС) 2019/817 Європейського парламенту про створення рамок для взаємодії між інформаційними системами ЄС у сфері кордонів та віз. Він створює єдину технічну базу для обміну біометричними та персональними даними між усіма важливими системами ЄС:

- EES (Entry/Exit System) – реєстрація в системі дати в’їзду та виїзду

громадян третіх країн.

- VIS (Visa Information System) – зберігання біометрії осіб, які подають візи;
- ETIAS (European Travel Information and Authorisation System) – електронна авторизація для безвізових поїздок.
- SIS (Schengen Information System) – інформаційна система про розшук та заборони на в'їзд.
- Також в цьому документі передбачено створення Common Identity Repository (CIR) – спільної бази, яка містить основні ідентифікаційні дані (ім'я, дату народження, громадянство) та біометричні дані (відбитки пальців і зображення обличчя). Ця база дозволяє прикордонним службам швидше встановлювати особу навіть у разі втрати чи підробки документів.
- Також документ передбачає створення системи Multiple-Identity Detector (MID), яка допомагає виявляти випадки, коли одна людина намагається використовувати кілька особистостей у різних системах. [30]

Також варто згадати Міжнародну асоціацію повітряного транспорту (IATA), яка хоч і не є регуляторним органом, але має значний вплив на формування стандартів у галузі авіаційних перевезень. Її рекомендації не є обов'язковими, проте широко застосовуються авіакомпаніями та аеропортами по всьому світу.

IATA розробила ініціативу One ID, яка має на меті стандартизацію використання єдиного біометричного ідентифікатора для проходження всіх етапів подорожі. В межах цієї ініціативи прописані вимоги щодо безпечного обміну біометричними даними між аеропортами, авіакомпаніями та державними структурами. При цьому система не повинна передбачати централізованого зберігання чутливої інформації, біометричні дані використовуються лише локально, для конкретного рейсу, наприклад, після чого підлягають видаленню або шифруванню. [15]

В Україні загальні принципи обробки біометричних даних визначає Закон України «Про захист персональних даних». В цьому законі біометричні дані

відносяться до категорії персональних даних, які мають особливі вимоги для обробки, яка можлива лише за умови згоди особи або в межах визначених законом повноважень державних органів. Закон вимагає, щоб такі дані збиралися лише для конкретної мети, зберігалися у захищеному вигляді та не передавалися третім сторонам без правових підстав. [31]

У сфері прикордонного контролю біометрія застосовується відповідно до Закону України «Про державну прикордонну службу» та Закону «Про правовий статус іноземців та осіб без громадянства». Ці документи регулюють використання біометричних даних під час перетину державного кордону, а також створення єдиних баз даних осіб, які в'їжджають або виїжджають з країни. Останнє викладено в постанові Кабінету Міністрів «Про затвердження Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства». Постанова визначає біометричні дані (параметри) як відцифровані відбитки пальців рук, відцифроване зображення обличчя та уточнює, які саме дані можуть міститися в електронних наборах, що передаються між суб'єктами національної системи біометричної верифікації: [32][33]

- прізвище, ім'я, по батькові (за наявності);
- дату народження;
- стать;
- місце народження;
- паспортний документ та його електронний вигляд;
- біометричні дані (параметри);
- перетин державного кордону;
- інші відомості.

Для авіаційної галузі основні положення викладені у Повітряному кодексі України та нормативних актах Державної авіаційної служби. У них визначено, що заходи з авіаційної безпеки мають відповідати стандартам і рекомендованим практикам Міжнародної організації цивільної авіації (ІСАО). Та Закон «Про Державну програму авіаційної безпеки цивільної авіації», яка визначає комплекс

заходів, спрямованих на захист цивільної авіації від актів незаконного втручання, та встановлює вимоги до організації системи контролю доступу, перевірки персоналу, пасажирів і багажу. [34][35]

Загалом, Україна ще з 1970 року є членом ІСАО (як правонаступниця СРСР, який вступив в ІСАО 10 листопада 1970 року), саме тому всі національні норми, які регулюють використання біометрії, формуються з урахуванням вимог ІСАО, Європейського Союзу та рекомендацій інших міжнародних структур.

Нормативні документи, як міжнародні, так і національні, досить чітко регламентують використання біометричних технологій в авіаційній галузі. Проте навіть за наявності детальних правил залишається питання, що стосується ризиків, обробки даних і етичних меж застосування таких систем.

Біометричні дані належать до найчутливішої категорії інформації, витік або підробка таких даних може мати серйозні наслідки, тому системи, які їх зберігають та обробляють, мають забезпечити багаторівневий захист: шифрування шаблонів, обмеження доступів, контроль дій операторів та заборона на копіювання та несанкціоноване використання цих даних.

Але, окрім технічного захисту, важливо враховувати й етичний аспект використання біометричних технологій. Рівень довіри населення до використання біометрії залишається досить неоднозначним з кількох причин. По-перше, сама ідея збору фізіологічних і поведінкових маркерів викликає етичні сумніви, адже не кожен готовий прийняти, що його обличчя, відбитки пальців, голос чи хода зберігається в базі даних, до якої людина не має жодного доступу, ще й можуть бути використані проти неї.

По-друге, занепокоєння викликає і масштаб зберігання такої інформації. Біометричні системи обробляють дані мільйонів людей, і будь-який збій або кібератака можуть призвести до компрометації унікальних ідентифікаторів, які неможливо замінити чи «перевипустити».

Ця вимога актуальна для будь-якої установи, де використовуються персональні біометричні дані, але саме для аеропортів вона стає ще більш

значущою. Тут обробляються дані пасажирів і працівників із різних країн, чиє законодавство про конфіденційність та порядок використання персональних даних може відрізнятися. Таким чином, служби безпеки та оператори систем мають забезпечувати універсальні стандарти захисту, незалежно від громадянства пасажира. У таких умовах навіть незначне несанкціоноване втручання в персональні дані пасажира може мати міжнародні наслідки.

Подібний інцидент стався у США у 2019 році, коли через неналежний захист даних субпідрядником Perceptics – американською компанією, яка спеціалізується на технологіях розпізнавання номерних знаків і зображень транспортних засобів, було скомпрометовано понад 184 000 зображень, з яких близько 100 000 належали реальним подорожуючим, що проходили прикордонний контроль у межах біометричного пілотного проєкту технології розпізнавання облич Vehicle Face System. Витік став наслідком того, що субпідрядник зберіг копії бази на власному сервері, який не мав належного шифрування. Цей випадок викликав велике обурення серед громадськості, адже лише через одну технічну недбалість дані сотні тисяч людей опинилися в відкритому доступі. А у медіа вкотре заговорили, чи виправдано збирати настільки чутливі дані, якщо навіть державні системи не можуть гарантувати їх безпеку. [36][37]

Щоб уникнути подібних випадків, системи, які працюють з біометрією, мають дотримуватися суворих принципів зберігання та обробки даних. В ідеальній системі все має бути прозоро та повністю контролюватися на всіх етапах. Усі зібрані шаблони повинні зберігатися в зашифрованому вигляді, без можливості прямого доступу до оригінального зображення чи відбитка. Передача інформації між системами має відбуватися тільки через захищені канали зв’язку, із застосуванням цифрових сертифікатів і протоколів автентифікації, із фіксацією кожного запиту та його джерела. А самі дані повинні використовуватися лише для визначеної мети – ідентифікації або верифікації, без передачі і копіювання в інші бази та без передачі їх будь-яким третім сторонам, доступ до бази має бути обмежений.

Після закінчення терміну зберігання, біометричні дані мають бути видалені, це одна з вимог міжнародних стандартів, довготривале зберігання або повторне використання цих даних підвищує ризик їх витоку. Крім того, власник даних має знати коли, де і як обробляються його дані.

Проте, варто враховувати, що в подібних установах частина біометричних даних збирається пасивно, наприклад за допомогою камер відеоспостереження, які фіксують обличчя та поведінкові ознаки без прямої взаємодії з людиною.

Перевагою пасивного збору є можливість прогнозування – коли системи навчаються на повторюваних патернах минулих подій, наприклад, за серією крадіжок або підготовчих діях перед терактом, розпізнає відповідні «дзвіночки» і завчасно попереджає службу безпеки. Завдяки цьому формується превентивна аналітика, коли система розпізнає характерну послідовність дій і видає попередження до того, як ситуація переросте в реальний інцидент.

Важливо, щоб система не тільки спостерігала, а могла аналізувати і миттєво перевіряти підозрілу особу за зовнішніми списками, а потім, в разі потреби, повідомити правоохоронні служби. Ефективність таких систем безпосередньо залежить від доступу до зовнішніх баз розшуку. У більшості країн вони інтегруються зі списками Інтерполу, Європолу та Шенгенською інформаційною системою, що дозволяє верифікувати особу в режимі реального часу. Якщо людина знаходиться в списку підозрюваних, переслідуваних або осіб з обмеженням на виїзд, система автоматично передає дані до служб безпеки або правоохоронних служб.

Відповідно до офіційних даних Інтерполу, процес біометричної верифікації здійснюється шляхом завантаження в систему зображення обличчя (пробного зображення), воно автоматично кодується алгоритмами та порівнюється з шаблонами зображень обличчя, які вже зберігаються в системі. В результаті створюється список «кандидатів» з найбільш схожим обличчям. [38]

Основна складність технології полягає в змінності людського обличчя. На відміну від відбитків пальців та ДНК, які не змінюються протягом життя,

розпізнавання облич вимагає враховувати наступні фактори: старіння, пластичну хірургію, використання косметики, наслідки зловживання наркотиками, алкоголем та куріння, а також роздільну здатність камери, освітлення, позу об'єкта зйомки, ракурс.

У структурі Інтерполу діє біометричний центр – це сучасна система для ідентифікації злочинців, яка забезпечує обробку даних країн-членів у спільному середовищі, він поєднує бази даних відбитків пальців і зображень облич, використовує потужне програмне забезпечення для порівняння зображень з даними для виявлення потенційних збігів, що дозволяє правоохоронним органам швидко ідентифікувати осіб, підозрюваних у міжнародних злочинах. З технічної точки зору це хороший приклад централізованої моделі, де пріоритетною є саме швидкість обробки запитів, співставлення та надання «відповіді». [39]

Європейський Союз, на відміну від Інтерполу, створює не окрему систему, а мережу взаємопов'язаних систем. Regulation (EU) 2019/817 чітко визначає технічну модель сумісності, яка інтегрує у спільну аналітичну систему наступні бази: Європейський пошуковий портал (ESP), спільну службу біометричного зіставлення (спільну BMS), спільне сховище ідентифікаційних даних (CIR) та детектор множинних ідентифікаційних даних (MID). Разом всі ці бази утворюють багаторівневу систему, яка здатна не тільки підтверджувати особу, а й виявляти спроби використання різних ідентичностей однією особою чи аномальні збіги між базами^

«Забезпечуючи можливість одночасного запиту до всіх відповідних інформаційних систем ЄС, даних Європолу та баз даних Інтерполу, Європейський пошуковий портал (ESP) має діяти як єдине вікно або «посередник повідомлень» для пошуку в різних центральних системах і отримання необхідної інформації без затримок та з повним дотриманням правил контролю доступу і захисту даних, установлених у цих системах». [30]

З аналітичної точки зору, є велика різниця між цими підходами у реагуванні на загрозу: система Інтерполу переважно шукає вже розшукуваних осіб на основі

відомих даних, тоді як Європейська модель, завдяки перехресним перевіркам, дозволяє виявляти невідповідності та повтори даних у різних системах.

Ще одна проблема, яка пов’язана з етичністю використання біометричних технологій – це своєрідне упередження самих алгоритмів розпізнавання. Національний інститут стандартів та технологій США провів дослідження різних комерційних систем розпізнавання обличчя і виявив, що найбільша похибка розпізнавання спостерігалася серед осіб із Західної та Східної Африки, а також Східної Азії, а найнижча похибка була серед осіб зі Східної Європи. Алгоритми частіше помилялися при ідентифікації жінок, дітей та людей похилого віку, а також людей з темнішим кольором шкіри. [40]

Якщо система не спрацює належним чином та не зможе здійснити ідентифікацію, це призведе до затримок, повторної перевірки або навіть хибного спрацювання, яке, в свою чергу, може спричинити додатковий контроль чи тимчасову відмову в доступі людині, яка нічого протизаконного не зробила. Для персоналу некоректна робота системи загрожує ризиком блокування доступу, перепустки, або навпаки, надання неналежного доступу. Саме тому система безпеки аеропортів не може покладатися виключно на технології, навіть якщо йдеться про найсучасніші біометричні розробки. Вона має працювати за принципом «людина + машина», технології спрощують та пришвидшують, але людина досі контролює процес та може самостійно реагувати на помилки та неточності алгоритмів.

Щоб система працювала стабільно, важливо, щоб вона була вдало інтегрована в існуючу інфраструктуру аеропорту. Біометричні технології не можуть функціонувати окремо, вони мають поєднуватися з системою контролю доступу, реєстрації пасажирів, базами прикордонного контролю та системою виявлення аномалій, це узгоджує роботу всієї системи та виключає дублювання дій між різними службами.

Як вже в роботі раніше зазначалося, повний перезапуск системи аеропорту вимагає значних ресурсів і часу, саме тому під час оновлення безпеки застосовують

модульний підхід. Всі оновлення, зокрема біометричні технології, впроваджують поступово, спочатку в контролі персоналу, і тільки потім в зони обслуговування пасажирів, включно з eGate та кіосками самообслуговування. Також важливо, щоб технологія злагоджено працювала з уже існуючими системами контролю та управління доступом (СКУД), базами даних реєстрації пасажирів, прикордонними службами та міжнародними базами розшуку.

Крім того, система має бути масштабованою та здатною обробляти великі обсяги інформації, здійснювати одночасну ідентифікацію тисяч осіб без витрати швидкості та точності. Система має рости разом із самим аеропортом, чим більше пасажирів, маршрутів і перевірок, тим важливіше, щоб вона функціонувала стабільно, а біометрія залишалася швидкою і точною.

Успішне впровадження біометрії в аеропортах неможливе без одночасного урахування вимог безпеки та комфорту самих пасажирів. Необхідно посилити контроль, але при цьому не створювати зайвих бар'єрів, зробити пересування через аеропорт швидшим та зрозумілішим. Біометрія дозволяє впровадити ризик-орієнтований підхід, коли ступінь контролю залежить від рівня довіри до конкретного пасажира. Тобто, ті, хто пройшов вже попередню перевірку, наприклад PreCheck, проходять процедури швидше, а ресурси служби безпеки зосереджуються на тих, хто становить потенційний ризик.

Певним чином, зручність стає частиною безпеки: чим швидше проходить ідентифікація, тим менше черг і скупчень у контрольованих зонах, а це автоматично знижує ймовірність інцидентів. У підсумку аеропорт перетворюється на злагоджену систему.

Висновок до першого розділу

У цьому розділі було розглянуто загальну структуру цивільного аеропорту, основні принципи зонування та різні рівні безпеки для хабів подібних масштабів. А також розвиток біометричних технологій та причини, через які авіаційна галузь перейшла до їх активного використання. Проаналізовано, як змінилися підходи до

ідентифікації пасажирів та контролю доступу після головних авіаційних інцидентів, які, власне, стали початком масштабного перегляду процедур безпеки та вимог для перевірки осіб.

Розглянуто основні біометричні методи, їх переваги та недоліки, а також умови, за яких ці методи працюють найбільш стабільно. Окремо описано, які технології вже використовуються в пасажирському маршруті, зокрема автоматизовані системи реєстрації, оформлення багажу та посадки. Кожна з цих систем використовує біометрія як основний засіб підтвердження особи пасажира. А також розглянуто систему контролю управління доступом для персоналу, і загальну систему відеоаналітики, що реагує на поведінкові патерни як пасажирів, так і співробітників.

Також розглянуто нормативну базу, що регулює використання біометричних технологій в авіаційні галузі: ICAO Doc 9303, Annex 17, регламенти ЄС та стандарти ISO. А також українські документи, що визначають порядок обробки біометричних даних, вимоги до прикордонного контролю та Закон України «Про Державну програму авіаційної безпеки цивільної авіації».

У цьому розділі також були розглянуті етичні аспекти використання біометрії, включно з пасивними методами спостереження та питання конфіденційності. Такі технології мають певні обмеження, однак, попри це, реальний досвід сучасних аеропортів показав, що користь від біометричних технологій значно переважає можливі ризики і поступово вони стають стандартом для авіаційної галузі. Тому, після відновлення роботи, українські аеропорти також мають продовжити впровадження біометрії на рівні з іншими світовими авіаційними хабами.

РОЗДІЛ 2. ТЕХНІЧНА ОСНОВА ТА ОЦІНКА МЕТОДІВ

Підрозділ 1. Математичні та алгоритмічні основи біометрії

Практична точність біометричних систем визначається значеннями помилкового прийняття (False Acceptance Rate – FAR) та помилкового відхилення (False Rejection Rate – FRR). [41]

Помилкове прийняття (FAR) – це ймовірність того, що система неправильно прийме несанкціоновану особу як авторизовану. У біометричних системах його зазвичай розраховують за наступною формулою:

$$FAR = \frac{\textit{кількість помилкових спрацювань}}{\textit{загальна кількість спроб несанкціонованого доступу}} \times 100\% \quad (2.1)$$

Розширена формула FAR, яка використовується в технічних звітах, наведена нижче:

$$FAR(\tau) = FMR(\tau) \times (1 - FTA) \quad (2.2)$$

Де:

FMR – коефіцієнт помилкових збігів, що виникають унаслідок помилки алгоритму під час порівняння одного шаблону з іншим:

$$FMR = \frac{\textit{кількість помилкових збігів}}{\textit{загальна кількість спроб міжособових порівнянь}} \quad (2.3)$$

FTA – частка спроб верифікації або ідентифікації, під час яких біометрична система не змогла отримати зразок або зафіксувати зображення чи сигнал достатньої якості.

Помилкове відхилення (FRR) – це ймовірність того, що система неправильно відхилить автентичного користувача. Проста формула наступна:

$$FRR = \frac{\textit{кількість помилкових відхилень}}{\textit{загальна кількість спроб санкціонованого доступу}} \times 100\% \quad (2.4)$$

Якщо транзакція верифікації складається з однієї спроби, частка помилкових відхилень наведена в наступній формулі:

$$FRR(\tau) = FTA + FNMR(\tau) \times (1 - FTA) \quad (2.5)$$

Де:

FNMR – частота неправильних негативних результатів, коли алгоритм не розпізнає збіг під час одиночного порівняння шаблонів:

$$FNMR = \frac{\textit{кількість неправильних негативних результатів}}{\textit{загальна кількість внутрішніх порівнювань}} \quad (2.6)$$

Загальна помилка (Total Error Rate - TER) – це точка, де зрівнюються значення FAR і FRR, тобто момент, коли система має однаковий рівень помилок обох типів. У багатьох дослідженнях TER використовується як єдиний показник, який дозволяє порівняти різні способи ідентифікації в реальних умовах. [42]

$$TER = FAR + FRR \quad (2.7)$$

Ще одне важливе для біометричної системи значення – показник рівних помилок (**Equal Error Rate, EER)** – це значення, яке використовують для оцінки ефективності даних систем під час ідентифікації користувачів. Значення EER визначає точку, у якій показники FAR та FRR є однаковими, тобто, поріг, за якого система з однаковою ймовірністю може прийняти стороннього користувача і відхилити легітимного. [43]

$$EER = FAR = FRR \quad (2.8)$$

Окрім значень помилкового прийняття та відхилення, для аналізу ефективності системи окремо ще оцінюють пропускну здатність та затримку.

Пропускна здатність (Throughput) – показник кількості людей, яких система може коректно опрацювати за годину.

Оцінку пропускної здатності можна представити наступною формулою:

$$\text{Пропускна здатність} = \frac{3600\ c}{\textit{середній час обробки одного пасажира}} \quad (2.9)$$

Затримка (Latency) – це проміжок часу від сканування біометричного зразка до відповіді системи (дозвіл або відмова доступу).

Адекватне проєктування системи має враховувати, що затримка прямо впливає на показники пропускної спроможності, відповідно і на якість обслуговування, адже, чим менший показник затримки, тим менша вірогідність утворення черг.

Метрики для відеоаналітики та пасивної біометрії

Окрім базових біометричних розрахунків, у системах аеропортів важливо враховувати точність роботи відеоаналітики. Для оцінки таких систем використовуються окремі розрахунки, що описують здатність детектора знаходити та класифікувати об’єкти. [44]

Для цих метрик використовуються базові показники:

- TP (True Positives) – правильно класифіковані позитивні випадки;
- FN (False Negatives) – позитивні випадки, які були класифіковані як негативні;
- FP (False Positives) – негативні випадки, які були класифіковані як позитивні;
- TN (True Negatives) – правильно класифіковані негативні випадки.

Рівень виявлення (Detection Rate - DR або Recall або True Positive Rate - TPR) – це частка фактичних позитивних випадків, які були правильно виявлені:

$$DR = \frac{TP}{TP + FN} \tag{2.10}$$

Рівень хибно позитивних спрацювань (False Positive Rate - FPR) – частка негативних випадків, які були неправильно класифіковані як позитивні:

$$\text{FPR} = \frac{FP}{FP + TN} \tag{2.11}$$

Рівень хибно негативних спрацювань (False Negative Rate - FNR) – частка негативних випадків, які були неправильно класифіковані як негативні:

$$\text{FPR} = \frac{FN}{TP + FN} \tag{2.12}$$

Рівень істинно негативних спрацювань (True Negative Rate - TNR) – частка негативних випадків, які були правильно класифіковані як негативні:

$$\text{TNR} = \frac{TN}{TN + FP} \tag{2.13}$$

Precision – частка всіх виявлень, які насправді є правильними:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{2.14}$$

2.2. Аналіз технологій та обґрунтування вибору

Face Recognition

В контексті аеропортів логічно виходити не з теоретичних порівнянь біометричних методів, а з того, які технології вже інтегровані в систему, документи, нормативну базу та реальні пасажирські процеси. В даному випадку саме обличчя стало базовою біометрією, зокрема через те, його зображення є обов'язковим біометричним ідентифікатором в е-паспорті відповідно до ICAO Doc 9303. [10]

У структурі паспортного чипа біометричні дані поділяються на групи:

- DG2 для зображення обличчя (обов'язковий);
- DG3 для відбитків пальців (необов'язковий);
- DG4 для райдужки ока (необов'язковий).

У таблиці 2.1 наведено порівняння біометричних методів та доцільність їх використання в аеропортах України.

Таблиця 2.1. Порівняння біометричних методів

Метод	**Точність**	**Швидкість**	**Масштабування на великий потік**	**Сумісність з е-паспортами ICAO 9303**	**Доцільність впровадження**
Обличчя	Середня/висока	Дуже висока	Добре – безконтактна технологія	DG2 — обов'язковий	Найоптимальніший метод. Підходить для потоків 300–450 пас/год, не потребує додаткових дій від пасажира
Відбитки пальців	Висока	Середня	Середнє – контактний сенсор	DG3 — не обов'язковий	Доцільно лише для прикордонного контролю
Райдужка ока	Дуже висока	Низька/середня	Погано масштабується	DG4 — не обов'язковий	Не доцільно – дорогі сенсори, пасажири не знайомі з технологією

Комбінована (Обличчя + відбитки)	Дуже висока	Середня	Залежить від організації процесу	Часткова потреба	Підходить, якщо треба підтвердити особу з підвищеним рівнем ризику

Тобто, у будь-якого пасажира еталонне фото вже є в чипі паспорта, і система не потребує створення нового шаблону.

В Україні прикордонні системи зчитують обличчя з 2018 року з біометричних паспортів та повністю відповідають стандарту ICAO 9303. Тому проєктована система повинна базуватися на удосконаленні наявної біометричної інфраструктури так, щоб вона відповідала сучасним технологічним вимогам.

З практичної точки зору це означає:

- Технології eGates працюватимуть на моделі 1:1, де обличчя пасажира зіскановується з DG2;
- СКУД мають працювати у режимі 1:N, що дозволить ідентифікувати працівника незалежно від картки доступу або перепустки;
- Розпізнавання обличчя зменшує кількість необхідних контактних сенсорів;
- Біометрія обличчя працює як пасивний чинник безпеки, де системи відеоаналітики здатні виявити й ідентифікувати особу у натовпі без додаткових дій з її боку.

У більшості міжнародних аеропортів системи eGates використовують різні топології роботи, залежить від того, як саме поєднано перевірку документа та біометрію обличчя. На рисунку 2.1. наведено три основні топології, які застосовуються для ідентифікації людини через eGates: [45]

a) Однокрокова модель – паспорт і обличчя перевіряються одночасно в одному модулі.
b) Інтегрована двокрокова модель, де спочатку зчитується документ, потім виконується біометрична верифікація.

c) Розділена двокрокова модель – паспорт і обличчя зчитуються в окремих модулях, фізично розташованих один від одного.

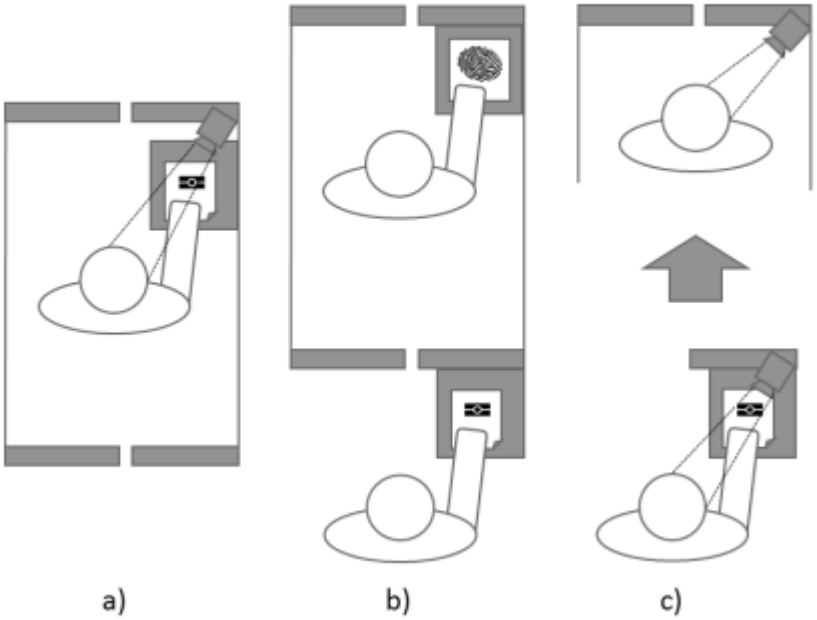


Рис. 2.1. Три топології eGates

Важливо зазначити, що інші модальності, хоча й можуть бути точнішими, проте не можуть масштабуватися на потоки у 15-20 тис. пасажирів на добу, потребують більш дорогого обладнання, не є обов'язковими для е-паспортів і просто можуть бути відсутні в громадян інших країн. Тому їхнє застосування не буде доцільним в системах біометричної безпеки аеропортів України.

Liveness

У проєктованій системі модуль розпізнавання обличчя обов'язково має працювати разом з технологією розпізнавання «живості» та виконувати вимоги IATA та ISO/IEC 30107.

Для аеропорту активний метод розпізнавання, який вимагає від користувача дій, не підходить, тому одразу варто орієнтуватися на обладнання та архітектуру, що реалізовуватиме пасивний метод: аналіз текстури шкіри, інфрачервоний спектр, визначення глиби сцени.

Алгоритм працює наступним чином (рис. 2.1):

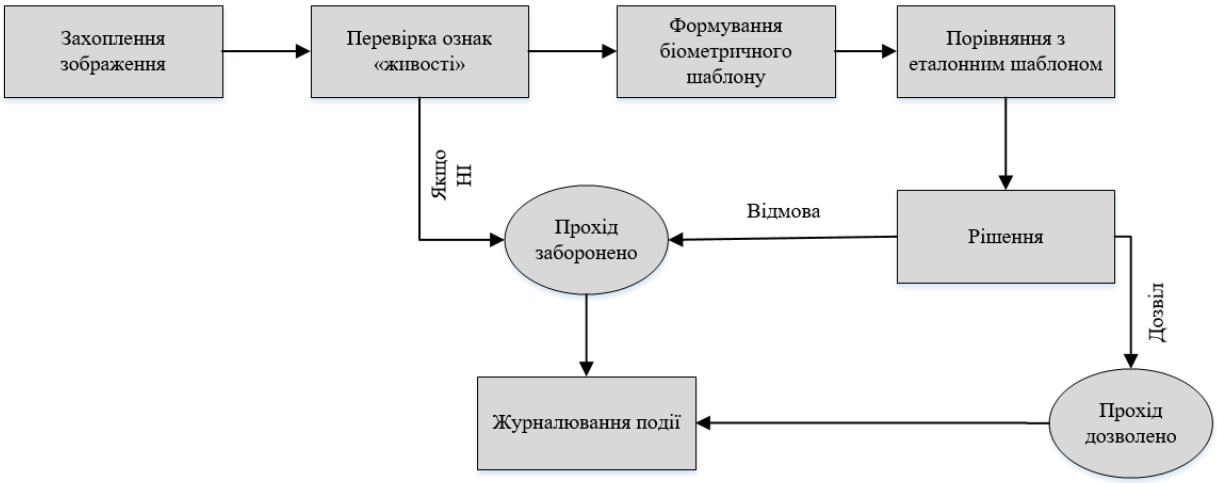


Рис. 2.2. Схема ідентифікації за обличчям

Фактично, перевірка на «живість» визначає реальний показник FAR, який без неї значно зростає.

СКУД та багатофакторна автентифікація для персоналу

В оновленій системі безпеки для українських аеропортів контроль персоналу має будуватися на багатофакторній автентифікації. Детальний процес ідентифікації зображено на схемі (рис. 2.2)

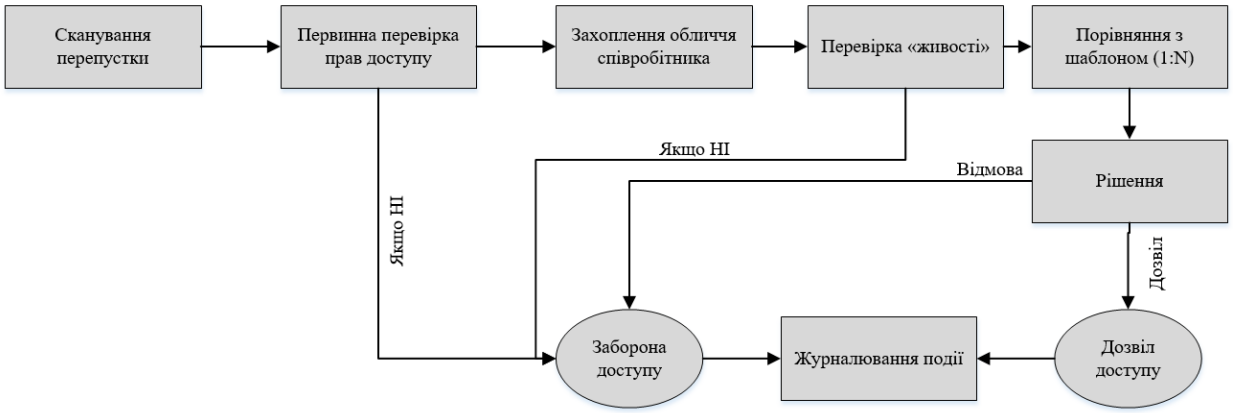


Рис. 2.3. СКУД для персоналу

Система має передбачувати та усувати різні спроби компрометації внутрішнього доступу, зокрема сценарії, які наведено в таблиці (таб. 2.2) нижче.

Таблиця 2.2. Загрози та сценарії реалізації

Тип загрози	Сценарій реалізації загрози	Технічний механізм протидії	Принцип роботи
Передача картки іншій особі	Передача картки іншій особі	Порівняння обличчя, перевірка на «живість»	Система перевіряє відповідність обличчя особи та її біометричного шаблона, а також чи ця особа «жива»
Прохід кількох осіб	Вхід за одним дозволом доступу кількох людей	Сенсори підрахунку осіб та відеоаналітика	Камера розпізнає кількість осіб у кадрі та блокує доступ при >1
Підробка обличчя	Використання фото, відео, масок або гриму	Пасивна та активна (в разі потреби) перевірка на «живість»	Визначення глибини сцени, аналіз структури шкіри, реакція на мікрожести та інфрачервоний аналіз
Нетипова активність	Вхід поза робочим часом, вхід в нетипову зону	Поєднання даних СКУД, розкладу змін, списку співробітників, профілю поведінки	Система перевіряє чи відповідає спроба входу типовій поведінці співробітника
Компрометований доступ	Використання перепустки співробітника, що вже не працює	Інтеграція СКУД зі списком співробітників, кадровими даними та операційною базою даних аеропорту	Перевірка статусу співробітника перед дозволом на вхід
Спроба умисного обходу системи безпеки	Вхід у нетипову зону або зону з вищим рівнем доступу	Порівняння маршруту руху співробітника з його типовим рухом	Відхилення від стандартного маршруту фіксується як аномалія

У такому вигляді СКУД і мультифакторна автентифікація одночасно перевіряє особу та формує систему аудиту.

Інтеграція з іншими системами аеропорту

Система має будуватися як єдина операційна платформа, яка поєднує систему управління відльотами, базою операційних подій аеропорту eGates та

системою прикордонної служби. У більшості українських аеропортів до 2022 року ці системи працювали скоріше паралельно, а не об’єднано, що створювало певні затримки інформації, що передавалася між модулями.

Ця інтеграція має забезпечити зручне пересування пасажира та контроль всіх етапів його пересування (рис. 2.3):

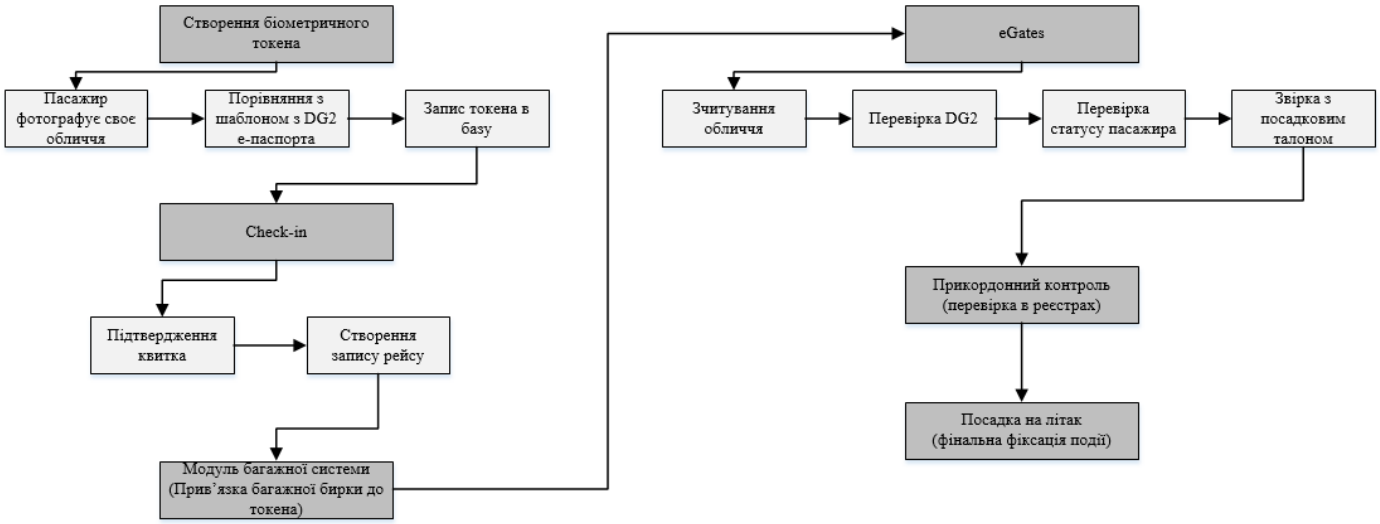


Рис. 2.4. Схема інтеграції пасажирського маршруту

Попередня схема показує послідовність дій на рівні маршруту пасажира. Щоб коректно виконати перевірку, eGate має доступ до кількох службових модулів і працює наступним чином:

1. Спочатку система зчитує через спеціальний ридер дані е-паспорта і фіксує зображення обличчя для первинного зіставлення.
2. Біометричні дані та інформація з документів передається на сервер, де виконується виділення ознак, побудова біометричного шаблону та перевірка цілісності документа.
3. Потім сервер надсилає запит до національних та міжнародних систем на пошук особи, отримує відповідь щодо достовірності документів та збігом їх з пасажиром.
4. Після успішного проходження всіх попередніх етапів система виводить

результат: дозвіл, заборону або запит на додаткову ручну перевірку. [45]

Схема на рисунку 2.4 відображає структуру підключення eGate до цих компонентів.

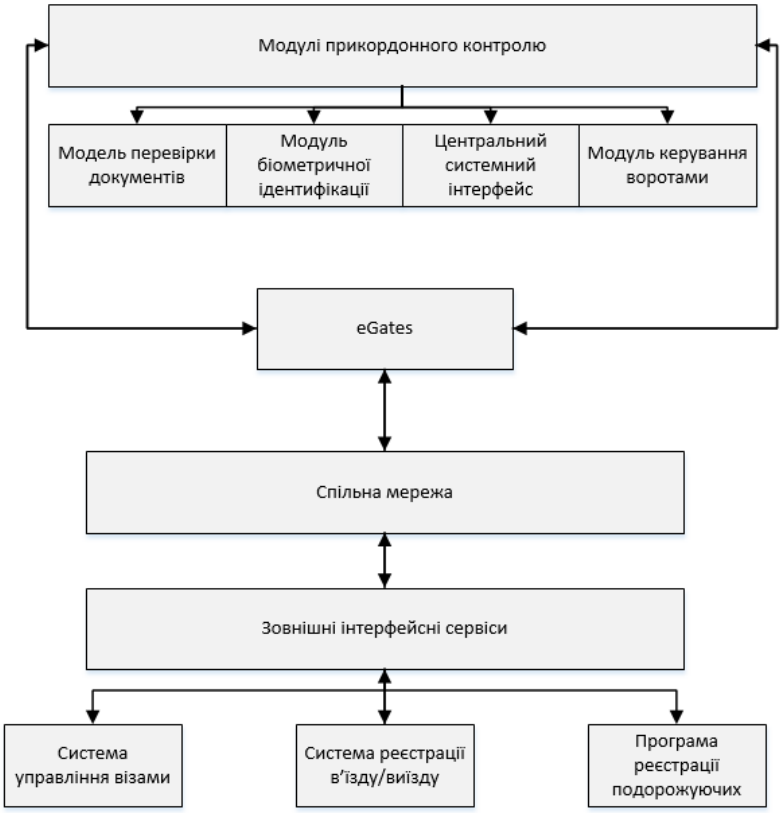


Рис. 2.5. Архітектура взаємодії eGates з зовнішніми системами

Запровадження такої архітектури дає можливість одразу будувати систему на рівні з сучасними світовими аеропортами, таким чином Україна одразу може вийти на потрібний рівень. У таблиці 3.2 наведено оцінку запропонованих технологій, їх статус для України, переваги та очікувані результати:

Таблиця 2.3. Оцінка технологій

Технологія	Статус	Переваги	Очікуваний результат для аеропорту після відновлення роботи
Face Recognition для пасажирів (1:1)	Потрібна модернізація,	Швидка, безконтактна	Мінімальні черги, швидке проходження,

	втановлення eGates/біометричних кіосків	ідентифікація, підвищення пропускної здатності	автоматизація, зменшення потреби в ручній обробці, стабільність
Мультифакторна ідентифікація + СКУД для персоналу	Має бути переглянута та по новому впроваджена при відновленні аеропорту	Захист від компрометації перепусток, стороннього входу, контроль доступу, аудит	Значне зниження ризику саботажу та неправомірного доступу
Перевірка на «живість»	Вимагає підтримки при закупівлі сенсорів/камер	Захист від підробки біометричного зразку, підвищення надійності біометрії	Зменшення FAR, збільшення надійності системи
Інтеграція з іншими системами аеропорту	Потрібне програмне проєктування + налаштування протоколів	Створюється єдиний «пасажирський маршрут», синхронізація даних між базами, автоматичний запис процесів	Об’єднана система, мінімум ручного втручання, полегшення аудиту осіб, оперативність роботи
Повна міжнародна сумісність	При відновленні потрібно передбачити сумісні модулі	Відповідність міжнародним вимогам	Аеропорт одразу буде готовий до глобальних стандартів

Системи відеоаналітики

У великих аеропортах системи відеоаналітики працюють як пасивний біометричний сенсор, який доповнює систему розпізнавання обличчя та контролю доступу, забезпечує постійний моніторинг у режимі реального часу. Фактично, це окремий модуль, який аналізує сам рух людей, їхню поведінку, скупчення, залишені предмети, спроби обійти контрольовані зони тощо.

Для стабільної роботи в аеропорту система відеоаналітики використовує чіткий алгоритм, який наведено на рисунку 2.5, де кожен етап виконує задачу, а результат передається до модулів поведінкової аналітики та журналу подій.

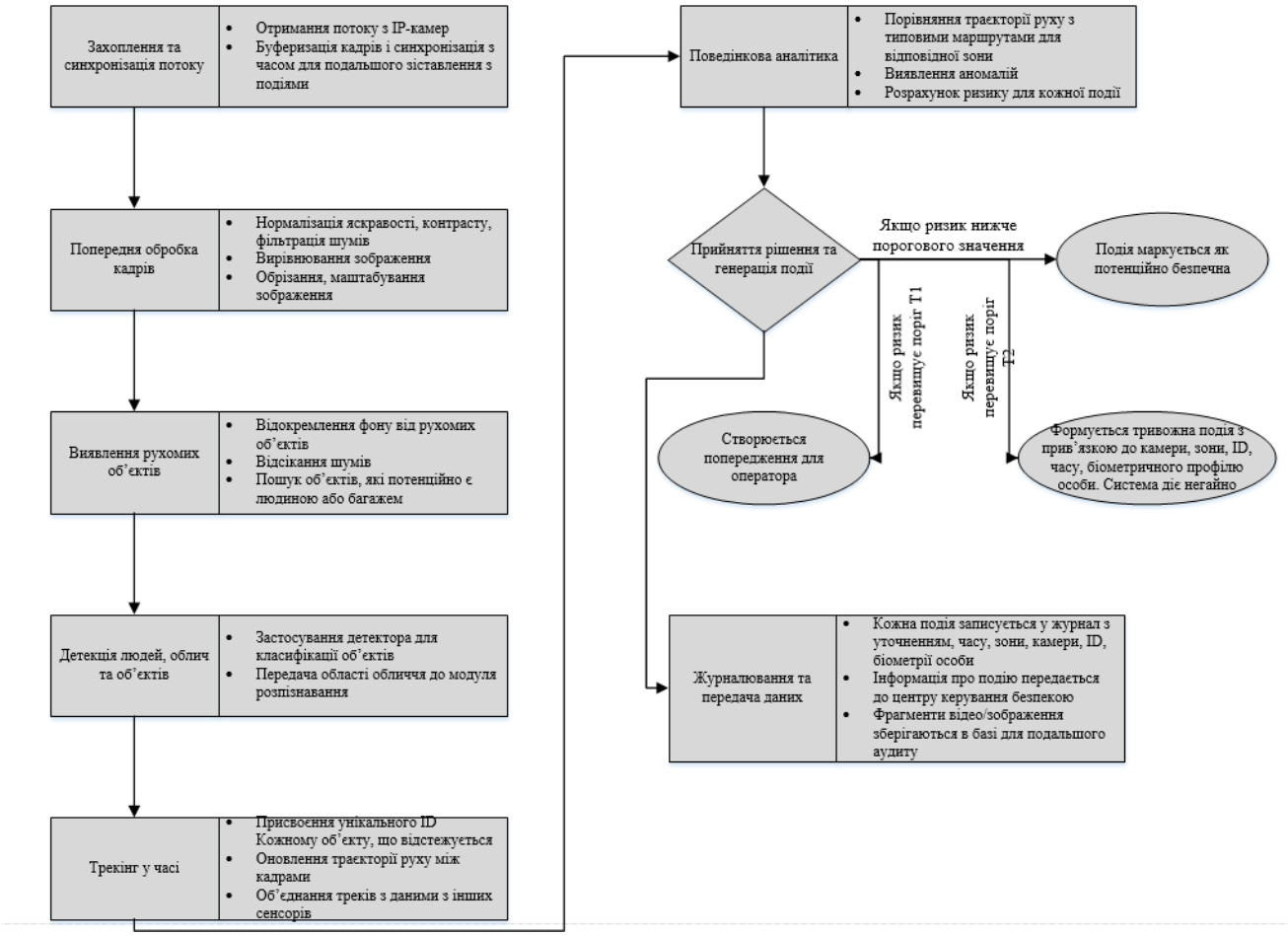


Рис. 2.6. Алгоритм роботи відеоаналітики

На схемі наведені значення інтегрального показника ризику R для кожної події. Він відображає наскільки поточна поведінка особи відхиляється від типової для даної зони.

Практичний показник ризику розраховується за формулою:

$$R = w_1 \times f_1 + w_2 \times f_2 + \cdots w_n \times f_n \qquad (2.15)$$

Де:

f_i – нормоване значення у діапазоні від 0 до 1 (де 1 — максимальне відхилення від норми).

w_i – ваги з урахуванням критичності зони та поточного рівня безпеки.

У системі зазвичай задаються два пороги:

- Поріг попередження T_1 – якщо $R \geq T_1$, подія визначається як підозріла, система надсилає оператору сигнал, проте сама не діє.
- Поріг тривоги T_2 – Якщо $R \geq T_2$, система формує інцидент з високим пріоритетом, фіксує його в журналі та може самостійно приймати дії.

Якість роботи такого алгоритму оцінюється за метриками, наведеними в підрозділі 1 (DR, FPR, Precision тощо), де окремо аналізуються хибні спрацьовування та пропущені події для різних типів зон аеропорту.

2.3. Ризики та загрози

Якщо дивитися на архітектуру безпекової системи аеропорту з точки зору функцій, її можна умовно розділити на дві підсистеми: пасажирську та підсистему контролю персоналу. В першому випадку мета біометричної системи безпеки в пропускній здатності та мінімальному FRR, друга підсистема виконує функцію жорсткого керування доступом.

Ризики варто розглядати в контексті реальних сценаріїв використання біометрії в аеропорту, де одночасно присутнє пасажирське навантаження, багаторівневий доступ персоналу та складна IT-інфраструктура.

Першою групою загроз є фальсифікація документів та біометричного зразка. Для перевірки достовірності документа система спочатку звіряє його структуру та електронний вміст з вимогами ICAO Doc 9303, перевіряється цілісність машиночитаної зони, підпис сертифіката, а також відповідність даних на чипі інформації.

Друга група ризиків пов’язана з внутрішніми загрозами. ICAO зазначає, що найбільш поширені інциденти в авіації часто були пов’язані з персоналом. [46]

Третя група – кіберзагрози до IT-інфраструктури, на якій, безпосередньо, працює біометрія. Системи зазвичай вразливі до SQL-ін’єкцій, DoS-атак на сервери автентифікації та replay-атак на канали зв’язку.

Звідси можна виділити ще одну групу ризиків, які не залежать напряму від об’єкта або системи, а залежить від навколишніх умов: освітлення, рух пасажирів, часткове прикриття обличчя, зміни зовнішності особи, що призводить до зростання FRR та, відповідно, погіршення точності, порівняно з реальними лабораторними можливостями біометричної системи.

Щоб оцінити ці ризики, варто використовувати просту модель:

$$R(\text{оцінка ризику}) = A \times B \tag{2.16}$$

Де:

A – ступінь впливу події,

B – імовірність її виникнення.

Оцінка ймовірних для аеропорту ризиків подана в таблиці 2.4, де для кожного ризику визначено рівень його впливу та ймовірність виникнення.

Таблиця 2.4. Оцінка ризиків

Ризик	Вплив (A)	Ймовірність (B)	A×B	Пояснення
Підробка біометрії обличчя (якщо немає перевірки «живості», УФ та ІЧ сканерів)	5	4	20	Ймовірність проходу сторонньої особи замість легітимної
Втрата або передача перепустки (за відсутності біометрії в СКУД)	5	4	20	Несанкціонований доступ до службових зон
Помилкове відхилення (FRR)	3	5	15	Створює черги, потребує ручної перевірки
Помилкове прийняття (FAR)	5	2	10	Ймовірність проходу сторонньої особи замість легітимної
Відеоаналітика не виявляє аномалії в натовпі	4	3	12	Підозрілий об’єкт або поведінка не виявляються
Неправильне зчитування е-паспорта	3	3	9	Вимагає повторної спроби/ремонту

				зчитувача, але не загрожує безпеці напряму
Затримка передачі інформації між модулями	2	3	6	Затримує проходження пасажирів
Відсутність синхронізації про багаж	3	2	6	Ймовірність блокування багажу на відправку/завантаження на борт
Помилки СКУД при великому потоці персоналу	4	2	8	Тимчасово блокує прохід до службових зон
Технічний збій сенсора	3	3	9	Тимчасове зниження якості розпізнавання/необхідний ремонт
Вплив зовнішніх чинників на зчитувачі (освітлення, бруд тощо)	2	3	6	Тимчасове зниження якості розпізнавання, вимагає повторної спроби
Хибні спрацювання відеоаналітики (FP)	1	3	3	Створює зайві події для перевірки

Таблицю оцінки ризиків варто одразу розглядати з чітким ранжуванням ризиків, яке подане в таблиці 2.5. Відповідно до неї, червоним кольором позначені найбільш критичні значення (рівень ризику 20-25) – це події, які одночасно мають високий вплив та високу ймовірність, відповідно, вони становлять найбільшу загрозу для роботи аеропорту.

Таблиця 2.5. Ранжування ризиків

A↓ B→	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

На основі таблиць 2.4 і 2.5 можна зробити висновок, що найвищий рівень критичності мають два ризики:

- Підробка біометрії обличчя;
- Втрата або передача перепустки.

Обидва ризики напряму впливають на доступ до контрольованих зон, тому їх доцільно розглянути окремо. Для цього нижче наведено схеми ризиків (рис. 2.7 і 2.8) які визначають основні причини виникнення загрози та її наслідки.

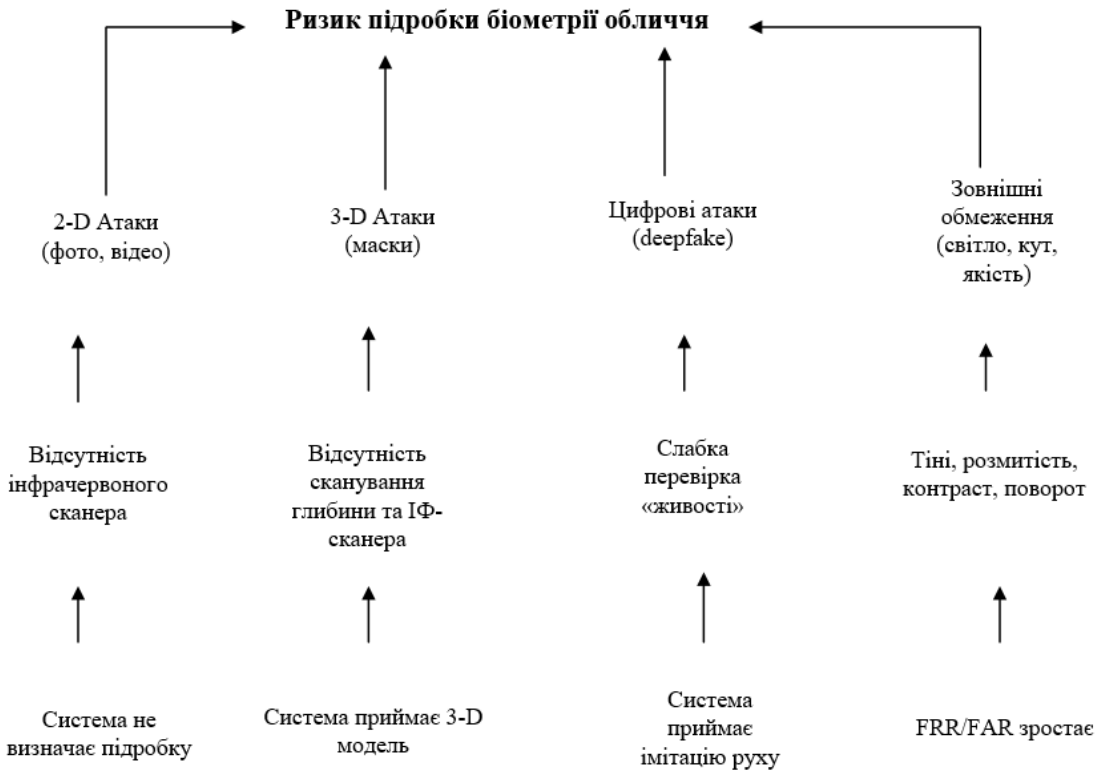


Рис.2.7 Дерево ризиків підробки біометрії обличчя

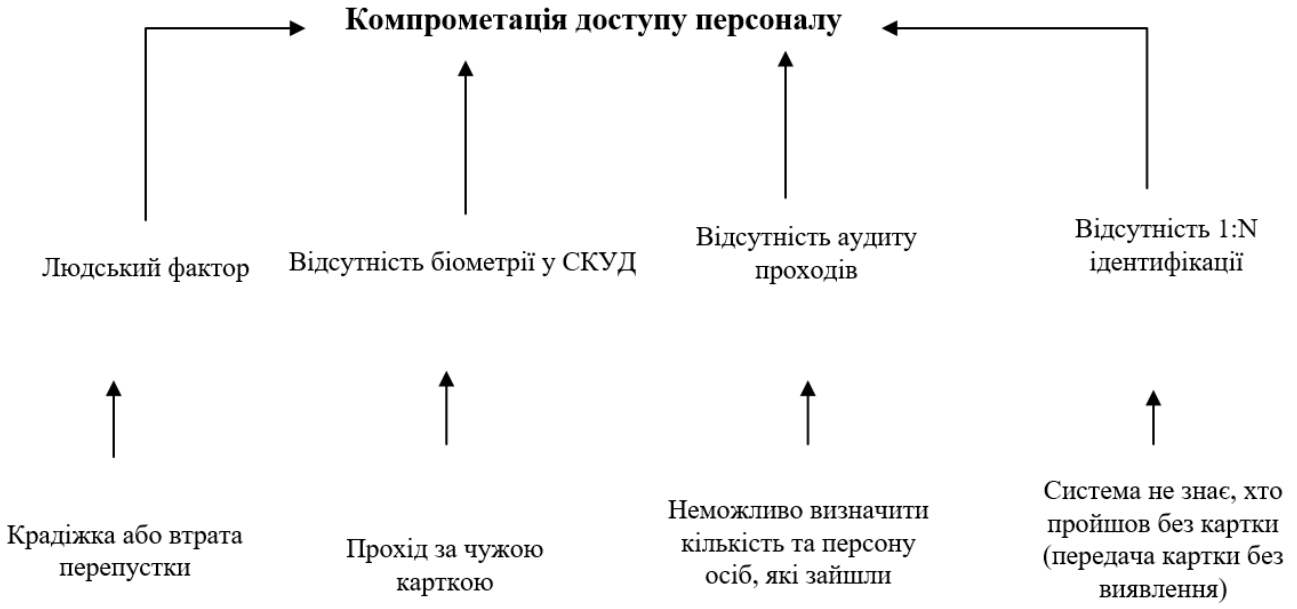


Рис.2.8 Дерево ризиків компрометації доступу персоналу

Усі описані ризики мають безпосередньо враховуватися на рівні вимог до побудови цієї системи. Кожен канал даних (СКУД, відеоаналітика, біометричні технології ідентифікації, тепловізійний контроль, журнали доступу персоналу) мають передавати подію з чіткою фіксацією часу, типом загрози та пов'язаною особою. Саме це дозволить надалі оцінити, наскільки система коректно виявляє аномалії, який відсоток з них є інцидентами і як часто потрібне ручне втручання.

Висновок до розділу 2

У цьому розділі було проаналізовано біометричні методи, математичні основи їх побудови та практичні обмеження, що впливають на пропускну здатність системи. Аналіз та порівняння доступних технологій показало, що саме обличчя є базовою та найбільш доцільною біометричною технологією для українських аеропортів. Зокрема через відповідність стандартам ICAO 9303, наявність еталонного зображення в паспортному чипі, може масштабуватися на великий пасажиропотік та не потребує контактних сенсорів. Для персоналу найоптимальнішим рішенням є впровадження багатофакторної ідентифікації в

систему СКУД, що унеможливлює передачу або компрометацію службових перепусток.

Структурні схеми eGate, алгоритм відеоаналітики та моделі взаємодії між модулями також показали, як біометрія інтегрується в операційну інфраструктуру та які технічні вимоги визначають їхню ефективність в реальних умовах.

Окремо проаналізовано ризики, характерні для біометричних систем аеропортів. Ранжування загроз показало, що найбільший вплив мають підробка біометрії обличчя та можливість використання чужої перепустки. Ці два сценарії визначають технічні вимоги до перевірки «живості», параметрів сенсорів, а також логіку роботи СКУД і системи поведінкової аналітики.

Загалом, отримані результати аналітичного розділу формують основу для подальшого проєктування архітектури біометричної системи. Саме ці дані визначають вимоги до обладнання, алгоритмів роботи та принципів інтеграції в інфраструктуру аеропорту, що відновлюватиме роботу після простою.

РОЗДІЛ 3. АРХІТЕКТУРА БІОМЕТРИЧНОЇ СИСТЕМИ ДЛЯ УКРАЇНСЬКОГО АЕРОПОРТУ

3.1. Аналіз результатів дослідження та доцільність впровадження біометричних технологій в Україні

На основі розглянутих в попередніх розділах ризиків можна зробити висновок, що біометрія працює як технологія, безпосередньо пов’язана з основними загрозами авіаційній безпеці: помилкове прийняття зловмисника (FAR), помилкове відхилення легітимної особи (FRR) та ризики, пов’язані з людським фактором. Ці параметри визначають, наскільки система здатна балансувати між пропускною здатністю та забезпеченням захисту.

Біометричні технології дозволяють перейти від ручного контролю документів та квитків, до автоматизованого, безпосереднього, контролю самої людини. У контексті аеропорту біометрія забезпечує два рівні контролю: відповідність документів міжнародним стандартам та зіставлення біометричного зразка із захищеними шаблонами.

Ручний контроль не здатен повноцінно та безпомилково забезпечити перевірку через людський фактор, тоді як біометричні системи з глибинним навчанням навпаки – стабільні в повторюваних перевірках та ефективніше реагують на нетипові для систем дії. Це особливо актуально для вітчизняних аеропортів, які відновлюють роботу після певного неактивного періоду, зокрема під час воєнних дій та введення режиму закритого повітряного простору для цивільної авіації, в цьому контексті пропускна здатність буде строго обмежена, а ризики помилкового пропуску зростуть через специфіку воєнної інфраструктури.

Для України питання впровадження новітніх біометричних технологій відрізняється інакшими умовами, ніж у країн, які продовжували нормальну роботу цивільних авіаційних перельотів. Закриття українських аеропортів 24 лютого 2022 року фактично зупинило розвиток технологічної інфраструктури, усі плани, проєкти та модернізації були поставлені на паузу. Тим часом світ пережив серйозний стрибок розвитку біометричних та безконтактних технологій, який був

зумовлений пандемією 2020-2022 років. У період простою вітчизняних аеропортів в світі розвинулися технології One ID, масово почали впроваджувати біометричну посадку, все більше аеропортів відмовилося від використання паперових документів на певних етапах маршруту, вдосконалилися системи відеоаналітики та антитерористичні механізми, а також вдосконалилися самі системи зчитування, розпізнавання та зіставлення біометричних параметрів.

Таким чином, українські аеропорти опинилися в унікальній ситуації одночасного відставання та можливості модернізувати систему одразу відповідно до новітніх технологічних рішень.

Це стосується практично всіх процесів, пов'язаних з пасажирами та персоналом: впровадження eGate, реєстрація пасажира на рейс та реєстрація багажу, відстеження осіб в натовпі, СКУД для персоналу та контроль доступу до службових зон.

Важливо також враховувати воєнні ризики: сценарії диверсій, компрометації інсайдерів, спроби несанкціонованого доступу, підроблені документи, використання чужих перепусток та підозріла поведінка персоналу та пасажирів. Все перераховане є реальними загрозами для об'єкта, що може піддаватися ударам безпілотних систем, кібератакам, спробам проникнення через наземні зони, спробам прямого теракту та загрозам повітряної тривоги. В даному випадку біометрія має закрити слабкі місця попередніх методів, які не враховували специфічні фактори.

В українському контексті модернізація біометричної інфраструктури аеропортів є фактично базовою вимогою для повернення до міжнародного та вітчизняного авіасполучення. Доцільніше буде не просто оновити систему у відповідність до світових практик, а врахувати специфіку українських умов і одразу адаптувати її під реальні ризики та потреби.

Варто також розглянути питання економічної доцільності біометричних систем. Модернізація вимагатиме значних інвестицій, але саме вона забезпечить скорочення операційних витрат та зростання пропускної здатності.

У розрахунках, які наводилися в попередньому розділі, видно, що ручний паспортний контроль обробляє приблизно 150-200 пасажирів на годину, тоді як автоматизовані системи здатні за цей самий час обробити 300-500 осіб, тобто більше в два рази. Якщо розглядати це в масштабах найбільшого аеропорту України – «Бориспіль», який в 2019 році обробив 15260000 пасажирів за рік. Такий рівень навантаження на пункт пропуску добре демонструє потребу у впроваджені автоматизованої обробки. Один правильно налаштований біометричний шлюз може замінити роботу двох постів контролю документів без втрати якості пропуску та ідентифікації осіб, а також з мінімальним залученням персоналу. В результаті, таке впровадження призведе до суттєвої економії: зменшаться витрати на оплату праці, скоротиться час обслуговування, а також автоматизовані системи краще пристосовані працювати з нерівномірним навантаженням. Також варто згадати навчання персоналу, кількість якого серйозно скоротиться в порівнянні з довоєнним періодом, такі системи не потрібно «вчити спочатку», відповідно, економляться ресурси на навчання. [47]

Окрім того, біометрія знижує вартість інцидентів. У післявоєнних умовах кожен інцидент проникнення у службові зони нестиме одночасно фінансові, репутаційні та наслідки, які прямо загрожують державній та громадській безпеці, і саме тому розвинена біометрична система знижує FAR і фактично виступає як інвестиція у стабільність і безпеку.

Економічна модель змінюється також завдяки гнучкості, систему можна поступово змінювати, додавати нові модулі, розширювати можливості, впровадити ШІ-аналітику, і таким чином зробити модернізацію поетапною, а витрати більш передбачуваними. Тобто, замість повної реконструкції аеропорт може удосконалюватися поступово, в залежності від нагальних потреб та можливостей.

3.2. Проєкт архітектури біометричної системи українського аеропорту після відновлення роботи

3.2.1. Визначення пріоритетних зон впровадження

Будь-яка модернізація системи авіаційної безпеки потребує чіткого визначення послідовності впровадження технологій. У випадку України, де фактично йдеться про побудову нової інфраструктури, черговість впровадження є критичним чинником. Тому потрібно починати з найбільш вразливих сегментів, вони визначаються залежно від ризику для безпеки та ступеня залежності від міжнародних вимог.

Перший пріоритет – доступ персоналу

Часто саме внутрішні загрози стають причиною авіаційних інцидентів, тому біометрація системи має починатися з персоналу, який має доступ до льотного поля, службових зон та зон підвищеного ризику. Окрім цього, персонал повертається до аеропорту першим, саме він братиме безпосередню участь у фізичному відновленні аеропорту. Тому на етапі запуску аеропорту саме вони становлять найбільший ризик несанкціонованого доступу та саботажу.

Другий пріоритет – прикордонний контроль

Наступним етапом є прикордонний контроль, який напряму пов’язаний з виконанням Україною міжнародних нормативів. Система має гарантувати узгоджену роботу з європейськими інформаційними платформами, зокрема:

- ESS, що фіксує усі перетини кордону громадянами третіх країн;
- ETIAS, який аналізує ризики та перевіряє особу в різних базах;
- SIS, VIS, EURODAC, Інтерпол, Європол, до яких Україні потрібно коректно передавати дані про перетин кордону особами.

Третій пріоритет – пасажирський маршрут

Пасажирська частина впроваджується в останню чергу. Ефективність усіх процесів, пов’язаних з біометрією пасажирів напряму залежить від того, наскільки захищена всередині вся система доступу, контролю, відстеження осіб та аналіз відхилень.

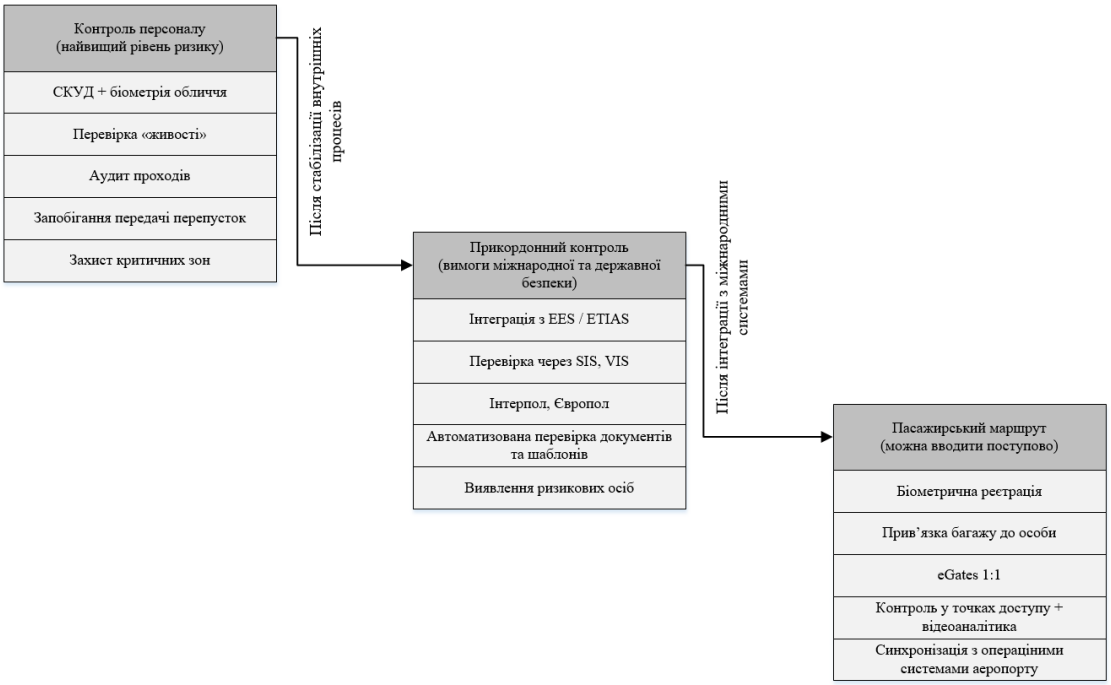


Рис. 3.1. Схема послідовності впровадження біометричних технологій

3.2.2. Архітектура біометричної системи

Архітектура біометричної системи складається з шести рівнів, кожен з яких виконує окрему частину обробки. Загальну структуру запропонованої системи наведено на рисунку 3.2. Вона показує порядок взаємодії рівнів та їх основні компоненти.

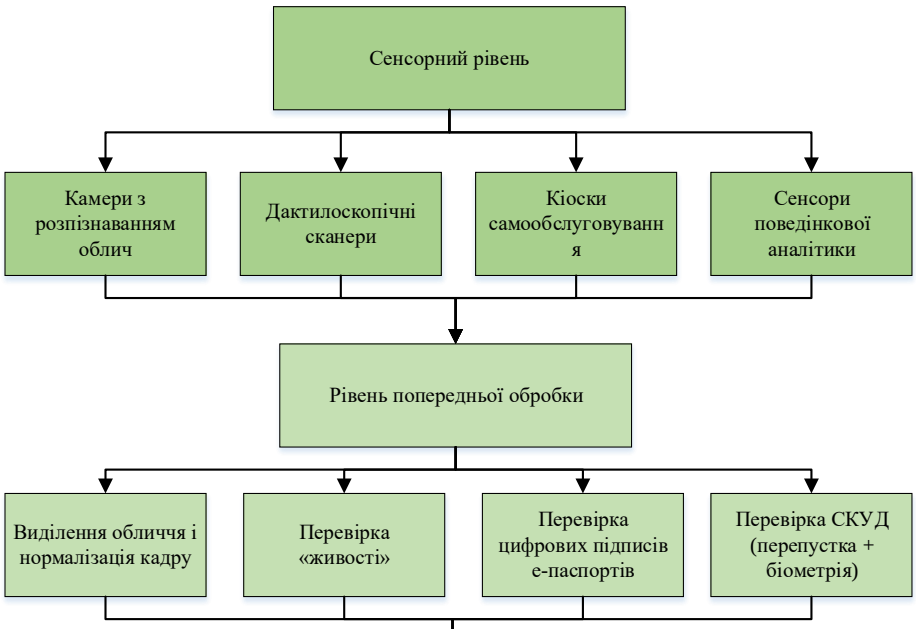
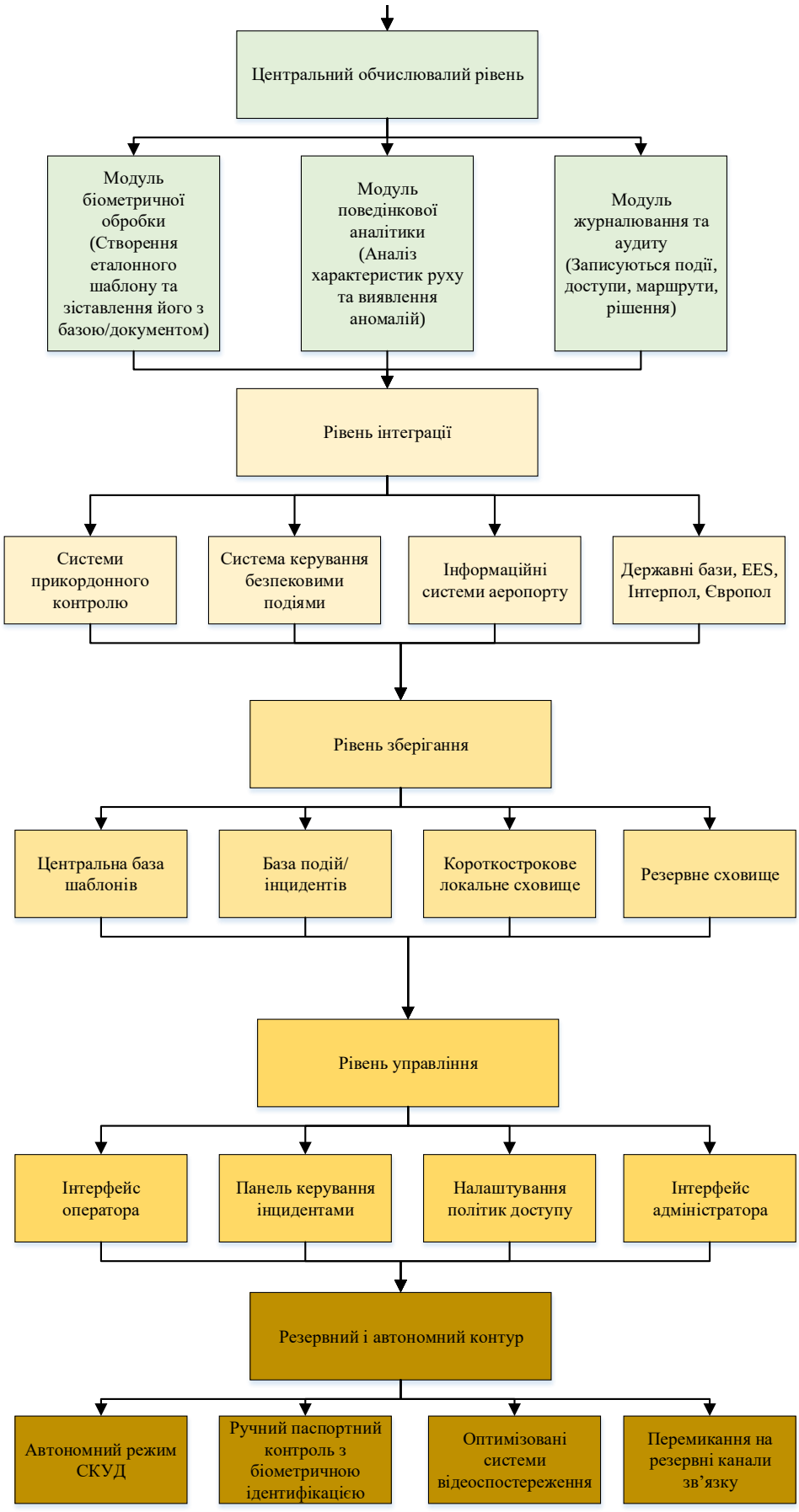


Рис 3.2 Архітектура біометричної системи



Продовження рис. 3.2.

Сенсорний рівень

Сенсорний рівень – це набір апаратних засобів, які зчитують інформацію про людину або подію і передають її на подальшу обробку. У випадку аеропорту він охоплює всі важливі точки: камери, що розпізнають обличчя, сканери для зчитування відбитків (як додатковий метод ідентифікації), термінали самообслуговування, сенсори, що аналізують поведінкову біометрію.

Камери для розпізнавання обличчя мають стабільно працювати в умовах різного освітлення, дистанції, руху осіб, а також вміти ідентифікувати особу попри макіяж та сторонні предмети на обличчі (маски, окуляри, головні убори). В більшості аеропортів застосовуються мережеві камери, наприклад розробки Axis, Bosch, Hanwha, спеціалізовані камери з локально обробкою. [48][49]

Для гейтів та зон обмеженого доступу камери мають виконувати наступні функції:

- Мінімум 25-30 fps;
- Роздільна здатність від 1080;
- Вбудований інфрачервоний сканер;
- Вбудована детекція обличчя в самій камері.

Дактилоскопічні сканери використовуються як доповнення до системи, побудованої на скануванні обличчя. Основними параметрами для цих сканерів є сертифікація FBI PIV/FIPS 201, висока роздільна здатність, здатність працювати в умовах швидкого потоку та з низьким відхиленням.

Кіоски самообслуговування працюють одночасно з камерою, сканером документа, аналізатором «живості» та інтеграцією з іншими системами аеропорту, тому варто передбачити відповідне обладнання: зчитувач документів, камера, модуль порівняння фото з базою/документом, механізм видачі посадкового талона, передача даних про пасажира в загальну систему.

Сенсори поведінкової аналітики, які включають і камери відеоспостереження, і систему контрою доступу, ідентифікацію багажу, сканери залишених предметів, що виявляють аномалії і передають їх у систему для

подальшої оцінки ризиків. Більшу частину становлять IP-камери та сервери відеоаналітики, які автоматично визначають підозрілу поведінку, ідентифікують обличчя особи або заборонені предмети, фіксують спроби несанкціонованого доступу, відхилення від маршруту. Інші сканери зазвичай працюють як записники до журналу подій, з якого система вже фіксує можливу аномалію та створює профіль ризику.

Всі перераховані сканери фактично формують перший рівень системи, який передає дані на модулі попередньої обробки. Детальна структура сенсорного рівня наведена на рисунку 3.3.

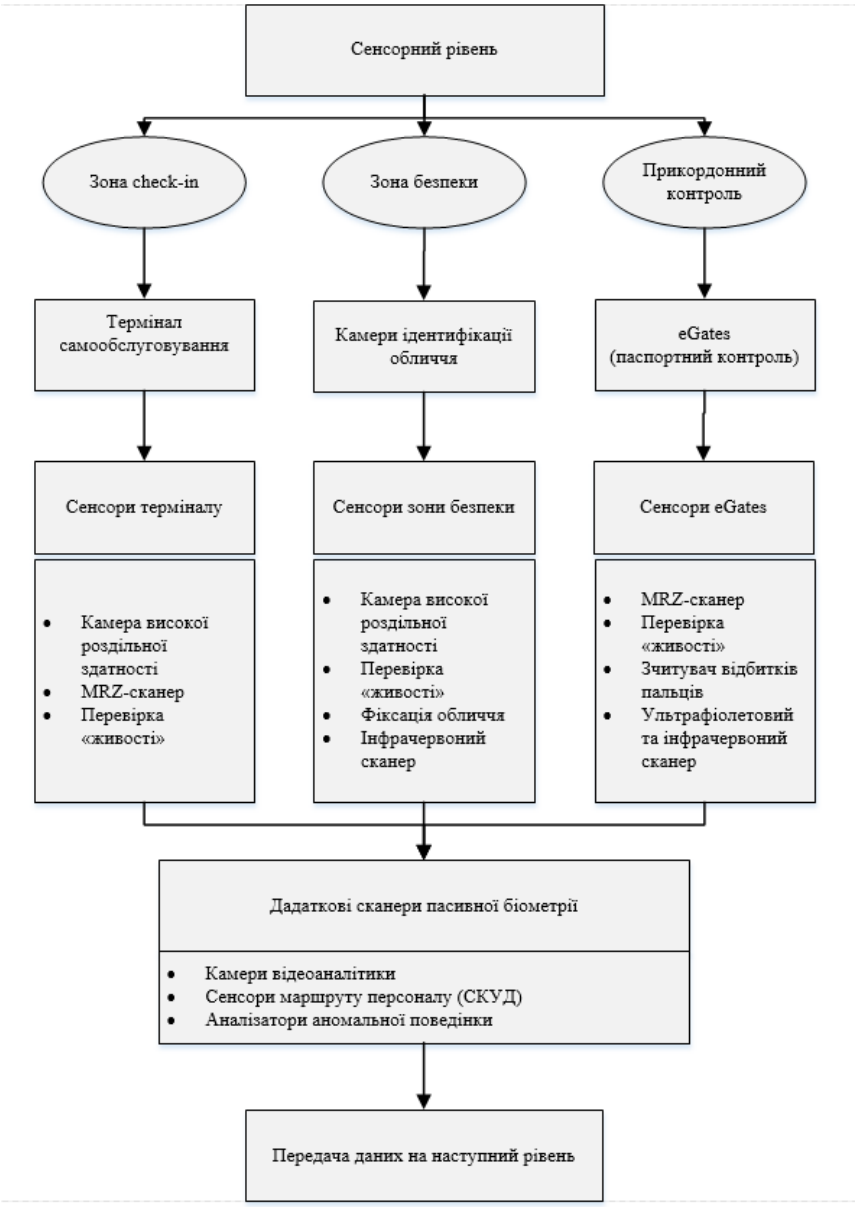


Рис. 3.3. Схема сенсорного рівня

Рівень попередньої обробки

Основне завдання цього рівня – одразу при зчитуванні виконати базову обробку, фільтрацію та підготовку даних для подальшої їх обробки.

Деякі сучасні камери самостійно локально обробляють кадр: визначають обличчя, формують зображення, формують первинний біометричний вектор і вже опісля передають його на центральний обчислювальний модуль без сирого зображення/відео. На цьому ж рівні працюють криптографічні модулі, які перевіряють цифрові підписи на документах та звіряють відповідність DG2.

СКУД також виконує миттєву перевірку доступу, і, якщо відповідність «картка + біометрія» не підтверджується, система видає «відхилення» доступу та прохід особі не дозволяється, тобто ще до того, як подія потрапить до центрального модуля.

Тобто, рівень попередньої обробки виконує первинну фільтрацію та нормалізацію даних, що надходять від сенсорів аеропорту. Схема (рис.3.4) ілюструє три паралельні процеси: обробку відеопотоку, локальну перевірку перепусток та біометрії, а також зчитування й перевірку е-паспортів. В результаті, вихідні дані з рівня попередньої обробки – це біометричний шаблон обличчя, статус документа та статус перевірки СКУД, які передаються до центрального обчислювального рівня для подальшого аналізу.

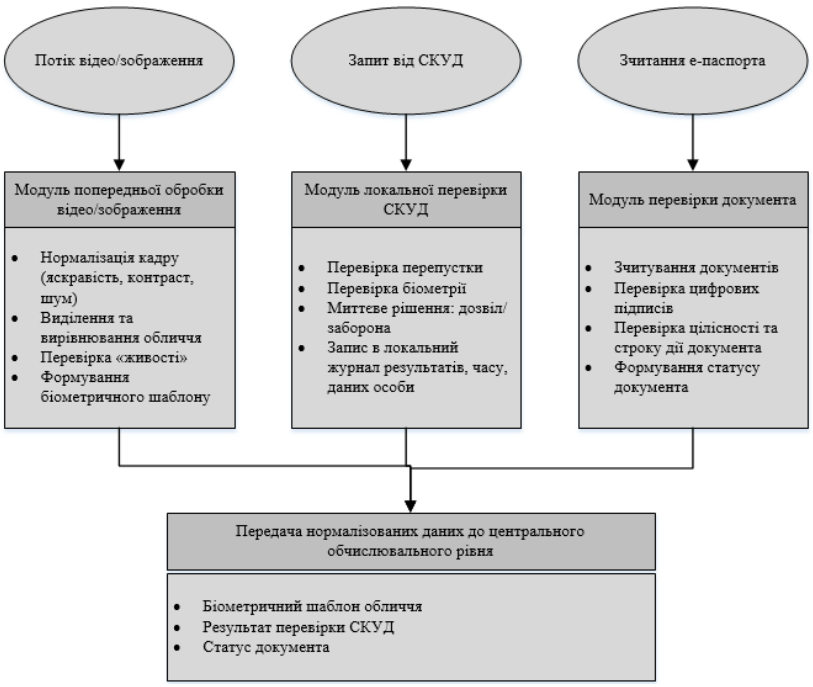


Рис. 3.4. Схема рівня попередньої обробки

Центральний обчислювальний рівень

Це фактично ядро системи, де відбувається ідентифікація, створюються дозволи, фіксуються події та реакція на них.

Модуль біометричної обробки та зіставлення шаблонів має коректно виконувати нормалізацію кадру або відбитку, формувати біометричний шаблон, порівнювати його з еталонним та повертати результат з оцінкою схожості. На цьому рівні також проводиться **остаточне зіставлення документа** особи з її біометрією.

Центральний обчислювальний рівень також обробляє **розпізнавання поведінкових аномалій**. Він працює на основі алгоритмів, що аналізують відхилення від типових маршрутів, підозрілу поведінку, потенційно небезпечні патерни тощо.

Модуль журналювання та аудиту записує всю хронологію подій із точним часом, точкою, конкретною особою та її біометрією/документом, також він формує журнали служб безпеки, прикордонної служби, зберігає історію змін політик, прав доступу, конфігурацій.

На рисунку 3.5 зображено деталізовану схему центрального обчислювального рівня. Тут показано три паралельні процеси (біометрична обробка, поведінковий аналіз і журналювання) та яким чином відбувається фінальне прийняття рішень на основі всіх зібраних даних.

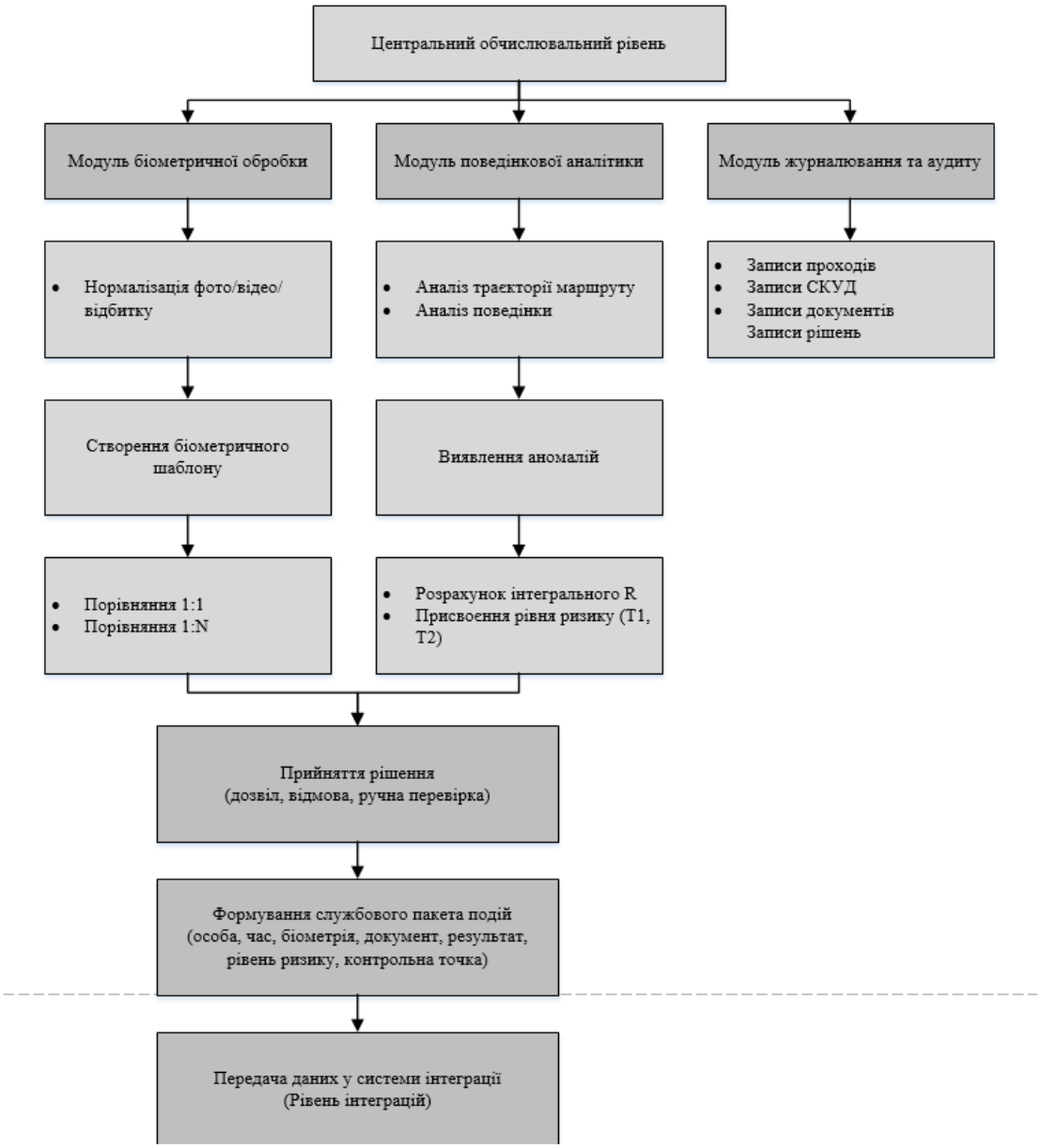


Рис. 3.4. Схема центрального обчислювального рівня

Рівень інтеграції

На цьому рівні біометрична система взаємодії з іншими ключовими компонентами інфраструктури аеропорту, прикордонної служби і безпекової системи.

На рівні інтеграції біометричні модулі мають коректно та своєчасно отримувати і передавати інформацію про «пасажирський шлях». Тут працює й модуль, що відповідає за роботу з даними прикордонного контролю, він передає

інформацію про проходження особи через контрольні точки, перевіряє особу через прикордонні бази, та фіксує перетин кордону.

Також біометрична система інтегрується з центром керування безпековими подіями, де зберігається журнал подій, дані відеоаналітики, події з біометричних модулів, аналіз поведінкової аналітики та сигнали про відхилення.

У попередньому розділі вже описувалася логіка взаємодії біометричних модулів з іншими системами аеропорту, проте на практичному рівні система працює як частина інфраструктури, що постійно обмінюється даними з декількома незалежними платформами. Загалом, рівень інтеграції забезпечує зв’язок між біометричним ядром та основними системами аеропорту, а також зовнішніми базами прикордонного контролю. Схема (рис. 3.5) ілюструє повний цикл інтеграції:

- Біометричне ядро отримує службові дані від зовнішніх систем
- Виконує аналіз (зіставлення, оцінку ризику, перевірку документів)
- Формує результат
- Передає його на рівень зберігання, управління та резервний контур

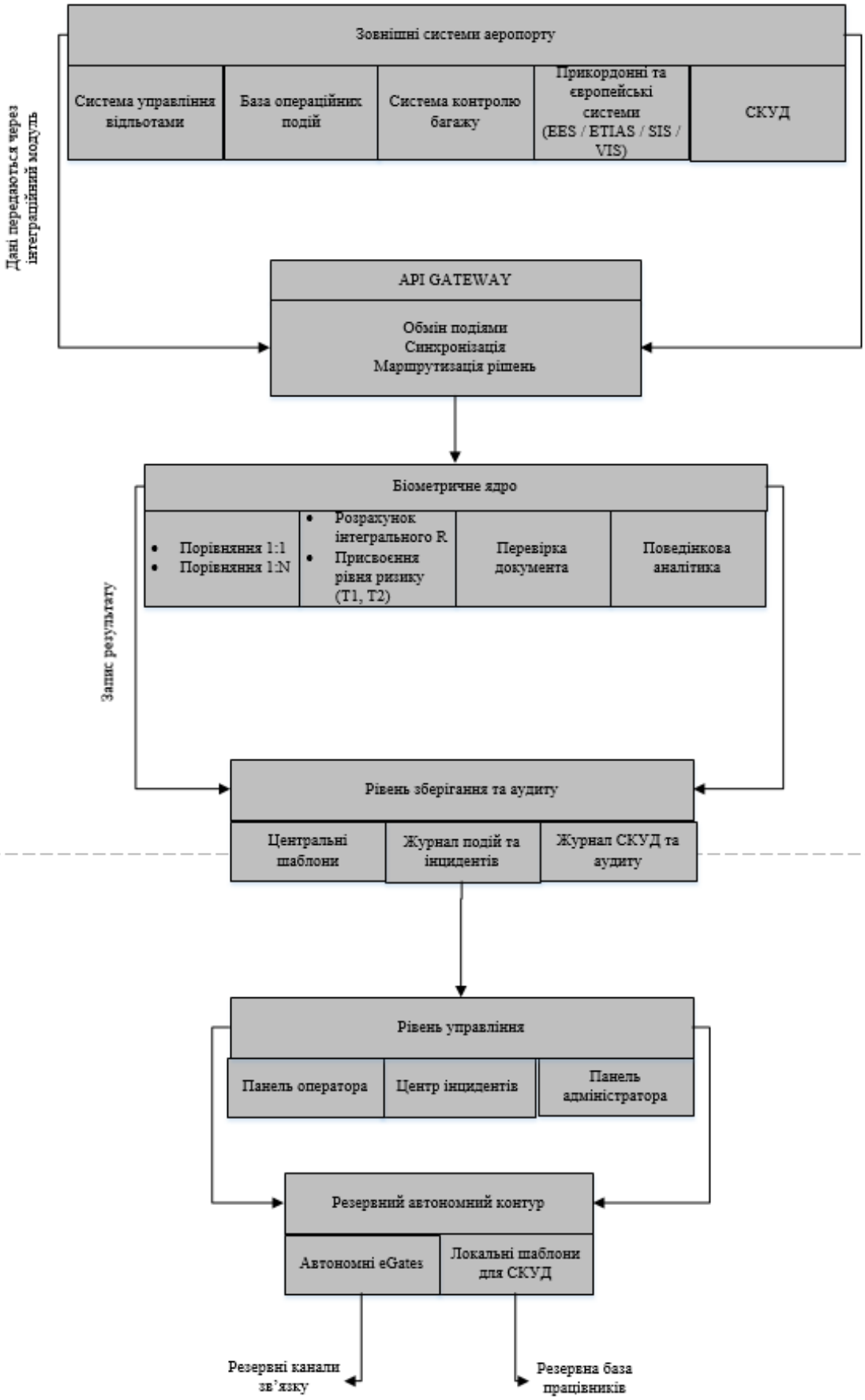


Рис. 3.6. Детальна схема інтеграційного рівня

Рівень зберігання

На рівні зберігання фіксуються біометричні шаблони, службові журнали, інциденти, рішення модулів і всі операції, необхідні для відтворення і аналізу подій. Його можна розділити на :

- Локальне короткострокове сховище тимчасово зберігає біометричні шаблони (відповідно до політик безпеки), проміжні результати верифікації, локальні журнали подій, службові метадані тощо.
- Центральна база біометричних шаблонів – це сховище, де зберігаються зашифровані еталонні шаблони облич або інших біометричних даних.
- Резервне зберігання – окрема, відділена від основної інфраструктури база, яка створена саме для забезпечення безперебійної роботи системи.

На цьому рівні також знаходиться база системних подій, доступів, рішень модулів, спрацювань відеоаналітики, записів про взаємодії систем, тобто всього, що потрібно для формування звітів.

Таблиця 3.1 ілюструє, які саме типи інформації зберігаються на цьому рівні, у якому вигляді та з якими обмеженнями.

Таблиця 3.1. Рівень зберігання

Тип даних	Джерело	Зберігання	Термін зберігання	Формат зберігання	Потреба в резервуванні
Еталонний біометричний шаблон	Центральний модуль	Центральна база шаблонів	До закриття доступу/ відповідно до політики безпеки	Зашифрований вектор ознак	Так
Тимчасовий шаблон	Сенсорний/попередня обробка	Локальне короткострокове сховище	До завершення операції/події	Зашифрований вектор ознак	Ні
Записи СКУД	СКУД	База подій	1-3 роки (залежить від політики)	Структуровані записи	Так

Події відеоаналітики	Аналітичний модуль	База подій	Від 30 днів до 1 року (залежить від політики)	Метадані без зображень, посилання на вихідний фрагмент	Так
Фото/відео кадри	Камери-зчитувачі	Не зберігаються (використовуються лише для формування шаблону)		Одноразова обробка	Ні
Записи прикордонних перевірок	eGate, MRZ, паспортний контроль	База інцидентів та журналів	Залежить від політики	Хешовані записи + службові метадані	Так
Політики доступу, конфігурації, адміністративна інформація	Панель адміністратора	Центр керування	До моменту оновлення	Файл конфігурації	Так

Рівень управління

Це інтерфейс, через який оператори, служба безпеки та адміністратори працюють із системою в режимі реального часу. Сюди входить система централізованого управління, яка має фіксувати поточний стан усієї системи: події зі всіх сенсорів, статуси доступів і проходів, стан пристроїв, журнали, аномальності, сигнали про тривоги, які може відслідковувати оператор.

Також на управлінському рівні знаходиться модуль налаштування політик доступу, який визначає дозволи проходу в контрольовані зони, які методи часові вікна доступу, рівні персоналу та політики для тимчасових дозволів. Панель керування інцидентами, яка визначає реакцію на самі інциденти, їх рівень загрози, пріоритетність, статуси, прив’язувати інцидент до конкретної зони, співробітника або точки, та формувати службові звіти про інцидент.

Найвищим рівнем керування системою має бути інтерфейс адміністратора. Він дозволяє керувати ролями, контролювати права доступу до функцій системи та

до контрольованих зон, керувати конфігураціями фізичних пристроїв та баз, мати повний доступ до журналу аудиту та керувати сценаріями реагування на інцидент.

Резервний і автономний контур

Українські цивільні аеропорти працюватимуть в умовах підвищених ризиків, тому біометрична система повинна мати можливість функціонувати автономно та у режимі мінімального функціоналу.

Функції, які обов'язково мають залишатися в роботі:

- Біометричний контроль доступу до контрольованих зон;
- Біометрична паспортна перевірка;
- Система відеоспостереження;
- Фіксація подій в журналі.

Тобто, у кризовому режимі система не намагатиметься підтримувати повний функціонал, а одразу буде адаптовуватися до ситуації та запускати відповідні протоколи.

Нижче наведена схема (рис. 3.7) резервного контуру, де зображено технології, поділені на рівні критичності. Тобто, найближчий до центру модуль – ядро, яке повинно працювати завжди, наступні рівні йдуть у порядку від найбільш потрібного, до найменш критичного елементу біометричної системи.

Рівень 0 (не вимикається, ядро біометричної системи безпеки аеропорту)	Рівень 1 (критичні модулі, працюють спрощено)	Рівень 2 (знижена функціональність)	Рівень 3 (необов'язкові модулі, вимикаються першими)
• Біометрія на паспортному контролі • СКУД • Журналювання подій	• Відеоспостереження • Сканування і перевірка документів (MRZ) • Локальні шаблони в контролерах	• Спрощена система eGates • Моніторинг стану обладнання • Базова поведінкова аналітика	• Кіоски самообслуговування • Глибинна відеоаналітика • Некритичні інтеграції • Розширена поведінкова аналітика

Рис. 3.7. Схема резервного контуру

3.2.3. Технічні вимоги і параметри

Для коректної роботи системи ідентифікації важливо враховувати характеристики камер, вони мають забезпечити стабільне зчитування облич за різних умов (в потоці людей, при навантаженні, за різного освітлення тощо),

оптимальна конфігурація має поєднувати RGB-канал з інфрачервоним і глибинним сенсором, щоб забезпечити роботу камер навіть за змінного освітлення і перевіряти об’єкт перед ними на наявність «живості». Детальні значення для системи наведено у таблиці 3.3.

Таблиця 3.2. Вимоги до камер біометричної ідентифікації

Параметр	**Мінімальна вимога**	**Оптимальна вимога**	**Обгрунтування**
Тип сенсора	RGB	RGB + Infrared + Depth	Інфрачервоний датчик допомагає при слабкому світлі та розпізнавання «живості», Depth для антиспуфінгу
Роздільна здатність	1080p	4K	Чим вище РЗ, тим точніші шаблони та робота на відстані
Частота кадрів	25 fps	30-50 fps	Знижується значення FRR та мінімізуються помилки при русі об’єкта
Фокусна відстань для звичайних зон	2,8-4 мм	2,8-4 мм	Тут працює загальна відеоаналітика
Фокусна відстань для зон підвищеного ризику	2,8-4 мм	4-6 мм	Більша відстань – менший кут огляду
Фокусна відстань для паспортного контролю	1,8-3 мм	2,8 мм	Менша відстань – більший кут огляду
Підтримка антиспуфінгу	Базова	Infrared + Depth + розпізнавання	Захист від масок, гриму,

		«живості»	фото/відео

Для роботи паспортного контролю необхідно, щоб сенсори коректно зчитували інформацію з документів, а також біометричні дані. Тобто, система має вміти працювати з е-паспортами відповідно до ICAO 9303, тому MRZ-зчитувачі повинні стабільно розпізнавати дані та перевіряти криптографічний захист документа. А сканер документів має забезпечувати якісне оптичне зчитування документів одразу з перевіркою міток в інфрачервоному та ультрафіолетовому спектрах, аби виявити підробки або модифікації паспортів. Детальніше наведено в таблиці 3.4.

Таблиця 3.3. Вимоги для сенсорів паспортного контролю

Сенсор	**Вимога**
MRZ-зчитувачі для е-паспортів	Відповідність ICAO 9303
Сканер відбитків пальців	500 dpi
Сканер документів	Оптичне розпізнавання тексту + інфрачервоний + ультрафіолетовий сканер
Камера кіосків самообслуговування	2К + технологія розпізнавання «живості»

Серверна частина визначає швидкість потоків і стабільність роботи усієї біометричної системи. Наприклад, обчислювальні процеси повинні забезпечувати паралельну роботу алгоритмів та обробку фото і відео у режимі реального часу, тому тут важлива продуктивність процесорів. Оперативної пам’яті має вистачати для виконання одночасно кількох задач, а також кешування проміжних результатів.

Загалом, кількість потоків, які система здатна обробляти залежить від масштабів аеропорту та структури розміщення камер, проте вона має залишатися достатньою, щоб забезпечувати стабільну роботу під час інтенсивного

пасажиропотоку. Затримка обробки повинна залишатися в межах, які дозволяють отримувати результат практично в режимі реального часу. Більш детальні технічні параметри наведено в таблиці нижче (таб. 3.4).

Таблиця 3.4. Сервери обробки

Сенсор	**Вимога**	**Оптимальне значення**
Центральний процесор	8-16	24-32
Оперативна пам’ять	32-64 GB	128 GB
Кількість одночасних потоків	100-200	500+
Затримка обробки	≤300 мс	100-150 мс
Тип відеоспостереження	Edge-сервер + центральний кластер	Гібридне розміщення

Під час роботи з біометричними даним система, відповідно до вимог ICAO, повинна зберігати лише шаблони без сирих фотографій, а доступ до шаблонів пасажирів та співробітників надається виключно за наявності відповідного повноваження.. Це має зменшити ризики у разі прямого доступу до сховища, але, окрім сирих фото, під час передавання та зберігання біометричні дані шифруються алгоритмами AES-128/192/256 та ECC. Усі операції з шаблонами, спроби доступу до них і видалення чітко фіксуються в журналах доступу, зазначаючи час, особу і тип виконаної дії. Також необхідно одразу передбачити резервне дублювання даних у разі збою системи або надзвичайної ситуації, а сховище біометричних шаблонів поділяється на зони, аби можна було чітко відокремлювати записи про персонал, пасажирів і службові записи.

Для коректної роботи системи eGates важливо забезпечити стабільний час проходу та верифікації, аби уникнути затримок, а також забезпечити належну пропускну здатність шлюзу, зменшивши час верифікації до мінімально можливого, дотримуючись при цьому безпекових вимог. Система має швидко реагувати на

запити і обробляти дані без помітних затримок, зокрема і на рівні серверів. Детальні значення наведені у таблиці 3.5.

Таблиця 3.5. Вимоги пропускної здатності для eGates

Параметр	**Вимога**
Час проходу однієї особи	6-12 с.
Пропускна здатність шлюзу	300-450 осіб/год
Час верифікації	≤ 1 с.
Затримка відповіді системи	≤ 200 мс.

Система контролю доступу для персоналу повинна працювати без затримок і навіть у випадку перебоїв зв'язку, залишатися повністю функціональною, від цього напряму залежить неможливість несанкціонованого доступу. Час реакції контролера та швидкість обробки подій має залишатися стабільно швидкою, оскільки це напряму впливає на доступність до самої службової зони. Загалом, система СКУД повинна, за потреби, працювати повністю автономно, тобто вона має підтримувати локальні шаблони, що забезпечать її роботу у випадку втрати зв'язку з кадровою системою або загальними робочими списками.

Детальні вимоги наведено в таблиці нижче (таб. 3.6)

Таблиця 3.6. Вимоги для СКУД для персоналу

Параметр	**Вимога**
Максимальна затримка від моменту сканування	≤ 300 мс
Швидкість роботи edge-контролера	1-2 с. на рішення
Пік навантаження	50-200 проходів/хв
Відмовостійкість	99%
Наявність локальних шаблонів	Обов'язкова наявність локальних

	шаблонів
Синхронізація з базами	Графік роботи + кадровий відділ + база доступу на основі ролей

3.2.4 Модернізована модель маршруту пасажира та зонування біометричних технологій в аеропорту (на прикладі Терміналу D аеропорту “Бориспіль”)

Після впровадження біометричних технологій пасажирський маршрут перетворюється на так званий послідовний «коридор», де особа підтверджується один раз – на початку, а далі система просто перевіряє пасажира, який вже знаходиться в базі аеропорту, разом зі своїм поточним зображенням, посадковим талоном, міткою про багаж та документами. Таким чином, біометрична система буде його «супроводжувати» до самого моменту посадки, поки не позначить пасажира як «відбувшого» та не видалить з часом його конфіденційні дані з бази. З точки зору інфраструктури, це прибирає дублювання процедур, потребу в постійному пред’явленні паперових документів та значно пришвидшує загальний маршрут пасажира.

У точці реєстрації автоматизація починається з того, що пасажир сканує документ у терміналі, система одразу перевіряє його, звіряє фото з біометрією та передає підтвердження до системи, що керує авіаційними відправленнями. Біометричний bag drop працює подібно: система приймає багаж та підтверджує, що багаж відправляє саме та особа, яка зареєструвалася. Це мінімізує ризик передачі багажу третім особам, відповідно, зменшує ризик терористичних дій, пов’язаних з небезпечними предметами, схованими в багажі або особистих речах пасажирів.

На всіх інших точках система автоматично звірятиме біометричний шаблон, який зберігся в системі з моменту реєстрації, а також дані з посадкового талона пасажира, контролюючи його маршрут. Загалом, саме біометрія дозволяє знизити

час проходу до 6-12 секунд на особу і стабілізувати потік пасажирів в пікові години або на великі рейси.

Важливо, що тут біометрія працює не лише на користь пасажиру, а й дозволяє аеропорту повністю контролювати рух пасажира на кожному етапі. Система може обробляти кожного пасажира і якщо він не пройшов вчасно певну точку, надсилати сигнал до відповідної служби, визначити його місцезнаходження серед потоку та оцінити, чи встигне пасажир на свій рейс без додаткового втручання з боку працівників аеропорту. Так адміністрація аеропорту бачить реальний стан пасажирського потоку, має можливість відстежувати пропуски, затримки, відповідно, швидше реагувати на нестандартні випадки.

Описаний вище пасажирський маршрут складається з набору критичних точок, які обов'язково має пройти пасажир до моменту посадки на борт, узагальнена структура цих точок подана в таблиці 3.7. Вона показує, яку функцію виконує кожна зона та які технології там застосовуються.

Таблиця 3.7. Структура контрольних точок

	Критична точка	Функція	Технологія	Вимоги	Результат
0	Зона перед аеропортом	Попередній поведінковий аналіз	Загальне відеоспостереження, базова поведінкова аналітика	Камери з широким кутом та стабільною роботою у потоці	Попереднє виявлення аномалій ще до входу в термінал
1	Вхід у термінал	Попередній поведінковий аналіз, початок фіксації маршруту	Відеоаналітика (виявлення облич і руху)	Камери 1080p+, 25–30 fps, корекція освітлення	Початкова подія маршруту, прив'язка до часової мітки
2	Зона реєстрації	Попередній поведінковий	Відеоаналітика	Камера 1080p+, кут покриття	Виявлення підозрілих дій

		аналіз, контроль черг		всієї черги	
3	Стійка реєстрації	Перевірка документа та біометрії	MRZ-сканер, ідентифікація пасажира (1:1), пасивна перевірка «живості»	Камера 2K, ІЧ сканер + глибина, перевірка DG2; коректне зчитування MRZ	Створення біометричного токена, підтвердження «паспорт-особа», видача посадкового талона
4	Реєстрація багажу	Підтвердження, що багаж здає саме власник документів	Ідентифікація обличчя (1:1), зчитувач документів	Камера з малою затримкою	Прив’язка багажної бирки до особи пасажира
5	Зона перевірки	Поведінковий аналіз, контроль черг	Відеоаналітика	Камера 1080p+, кут покриття всієї черги	Виявлення підозрілих дій, нервування особи, залишення речей
6	Безпековий контроль	Контроль поведінки та фіксація підозрілих дій під час перевірки	Відеоаналітика, сенсори залишених предметів	Стабільна передача, достатній FPS	Розпізнавання аномалій, журналювання подій
7	Паспортний контроль / eGates	Остаточна ідентифікація людини	MRZ, ідентифікація обличчя (1:1), перевірка «живості», перевірка в міжнародних	Затримка ≤1 с; коректне зчитування DG1/DG2	Допуск/відмова/ перенаправлення на ручну перевірку

			пошукових базах (1:N),		
8	Стерильна зона	Пасивний контроль переміщення	Відеоаналітика	Неперервне покриття камер, що охоплює всю територію, аналітика траєкторій	Виявлення відхилень маршруту, аномальної поведінки тощо
9	Посадка / гейт	Перевірка особи та посадкового талона на поточний рейс	Ідентифікація обличчя (1:1), інтеграція з базою вильотів	Камера з швидким захватом	Допуск на посадку, фіксація події в журнал як остання точка пасажира
10	Службові входи	Контроль доступу персоналу	Ідентифікація обличчя (1:N), СКУД	Локальні шаблони, час відповіді ≤300 мс	Доступ лише для авторизованих працівників
11	Критичні технічні зони	Захист внутрішньої інфраструктури	Ідентифікація обличчя (1:N), СКУД	Резервні шаблони, журналювання	Запобігання несанкціонованому втручанню

Саме на основі структури, наведеної в таблиці 3.7, надалі створено схему розміщення біометричних технологій для Терміналу D аеропорту «Бориспіль».

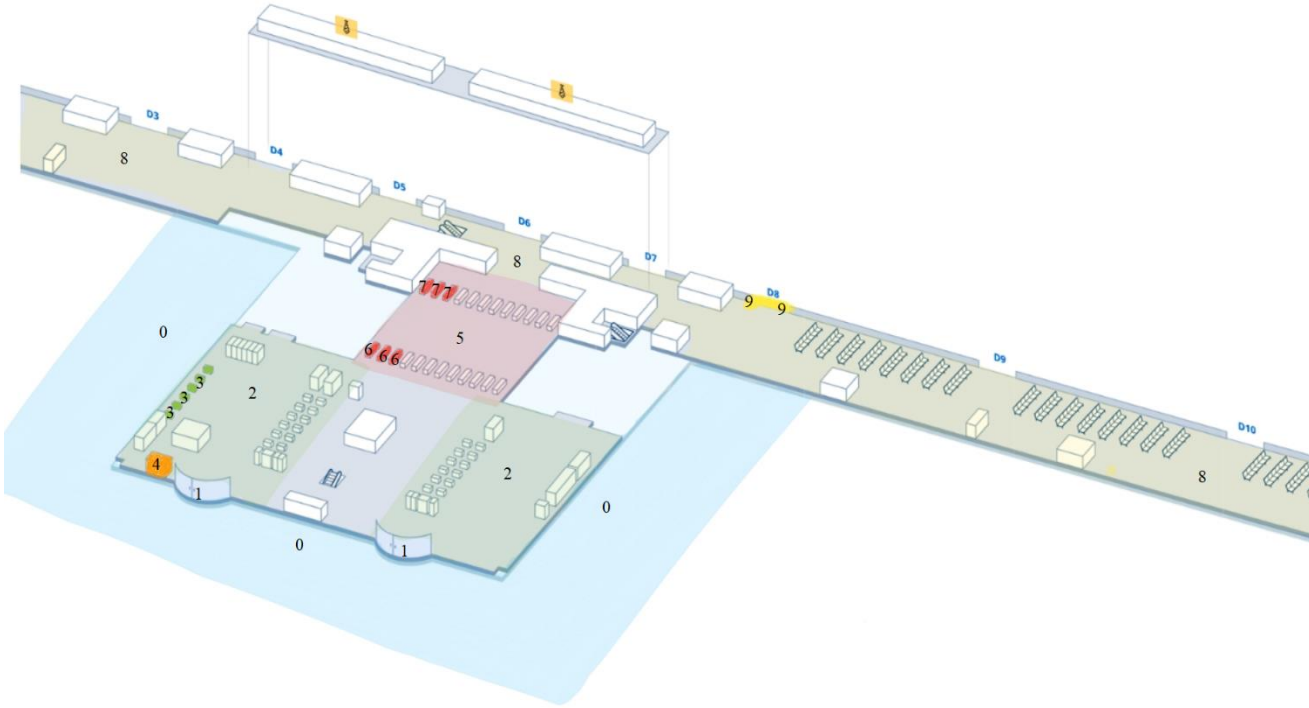


Рис. 3.8. Розташування критичних біометричних точок в терміналі D

На рисунку зображено третій рівень (міжнародні вильоти) терміналу D міжнародного аеропорту «Бориспіль» та позначено критичні точки та зони:

0 – зона перед терміналом, де працює базова відеоаналітика;

1 – вхід до терміналу;

2 – зона реєстрації;

3 – кіоски біометричного самообслуговування;

4 – автоматизована реєстрація багажу;

5 – безпекова зона;

6 – автоматизований безпековий контроль;

7 – eGates, автоматизовані паспортні столи;

8 – Стерильна зона, діє глибока відеоаналітика;

9 – точка посадки на борт, автоматизований гейт.

Ця схема відображає, як аеропорт може впровадити автоматизовані біометричні технології у вже наявну інфраструктуру. На схемі кольором виділено

основні функціональні зони терміналу (зона перед терміналом, зона реєстрації, безпекова і стерильна), у всіх цих зонах знаходиться розширена мережа відеокамер, яка здатна аналізувати пасажиропотік та, в залежності від зони, ідентифікувати конкретну особу, визначати підозрілу поведінку, надсилати сигнал оператору або самостійно реагувати на інцидент.

Наступний рисунок (рис. 3.9) ілюструє оновлений маршрут пасажира за автоматизованими біометричними точками. Нумерація (позначки фіолетового кольору) позначає реальний порядок руху пасажира. Деякі зони, зокрема 2 і 5, не мають окремого номера в пасажирському маршруті, оскільки вони працюють у фоновому режимі та підтримують роботу інших етапів.

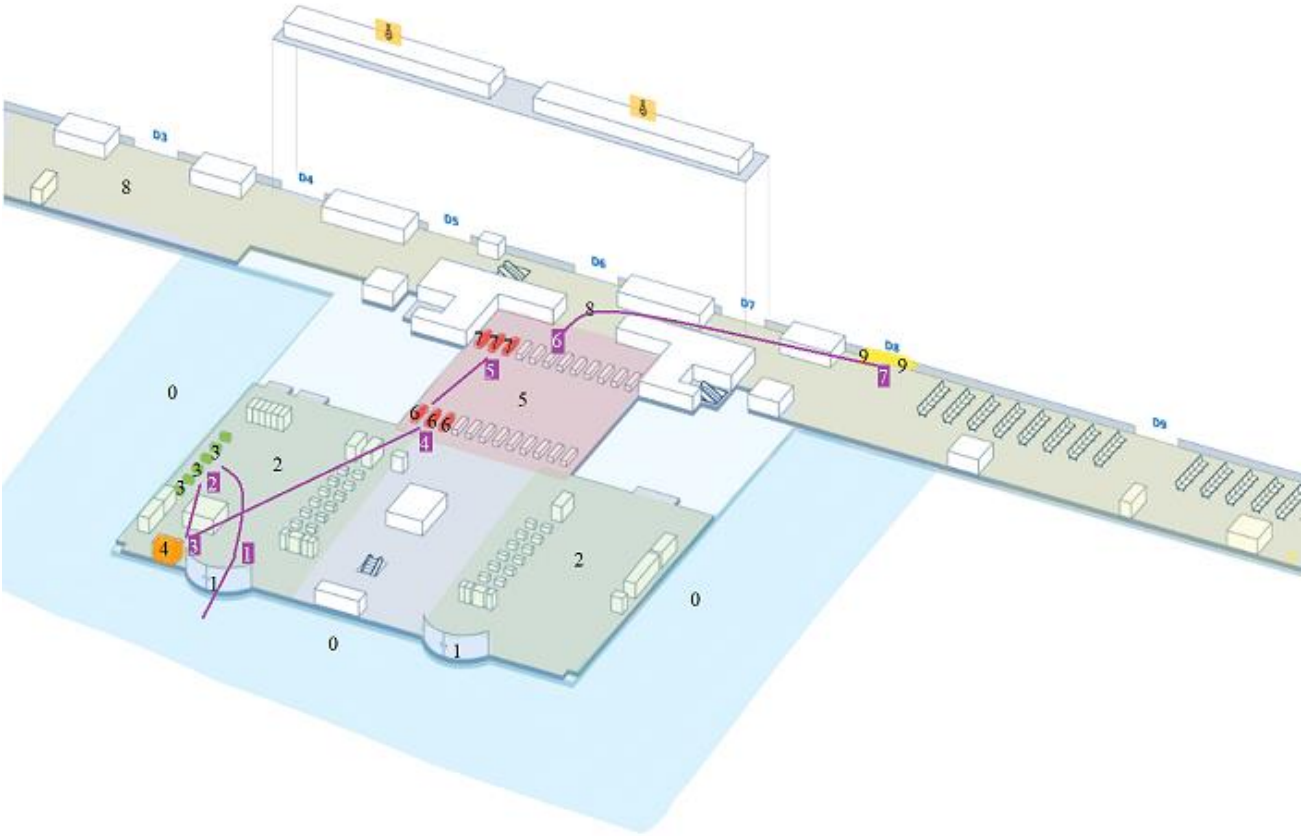


Рис. 3.9. Схема пасажирського маршруту

Представлені схеми показують, як окремі технологічні модулі інтегруються у послідовний маршрут пасажира, а також дозволяють оцінити практичну

придатність розробленої архітектури: система формує узгоджений процес ідентифікації, у якому кожен етап підтверджує або уточнює дані, які було надано на попередньому кроці.

Також схема «Розташування критичних біометричних точок в терміналі D» дозволяє оцінити місця розміщення технологій на основі реального українського аеропорту, та визначити, які саме точки потребують технічної модернізації або повної реорганізації. Вона також показує, що впровадження автоматизованої біометрії може бути поступовим: аеропорт може почати з окремих точок, або обмеженої кількості різних технологій.

З точки зору міжнародного іміджу, використання автоматизованих біометричних технологій, які вже стали стандартом у провідних світових аеропортах, для України означатимуть, що аеропорти одразу повертаються до роботи на відповідному міжнародному рівні.

Окремо варто підкреслити, що для України процес впровадження таких технологій може бути навіть простішим, ніж у багатьох державах, адже цифрові сервіси вже стали нормою повсякдення і для громадян не буде новизною реєстрація через Face ID для підтвердження своєї особистості, зважаючи на те, що подібні технології верифікації використовують державні сервіси і банкінги. Тому впровадження біометричної ідентифікації в аеропортах в «пасажирський маршрут» не вимагатиме особливої адаптації і створює передумови для можливого використання державних цифрових інструментів для підтвердження особи в аеропорту, якщо це буде технічно і нормативно можливо.

3.3. Практична модель загроз та сценарії реагування

Біометрична система контролю повинна виявляти відхилення від звичної поведінки і як персоналу, так і пасажирів. Проте ризики для цих двох груп різні, відповідно пороги реагування теж мають відрізнятися. Система аналізує маршрути, час перебування в зоні, рухи, ходу, напрямок погляду, повторюваність певних дій і після цього визначає, чи є поведінка особи аномальною, і чи потрібне втручання

служби безпеки. Нижче наведені деякі основні ситуації, які потребують окремих сценаріїв реагування, з урахуванням особливостей роботи українських аеропортів після відновлення.

Можна виділити три групи ризиків: перша стосується внутрішніх загроз, зокрема зловмисних дій персоналу, друга пов'язана з поведінкою пасажирів і третя група охоплює технічні загрози, зокрема фізичне пошкодження камер і сенсорів, виведення з ладу обладнання і кіберзагрози біометричній системі. Детальніше описано в таблиці 3.8.

Таблиця 3.8. Ризики і сценарії реагування системи

Фотографування та відеозйомка в зонах обмеженого доступу (для персоналу)	
Службові приміщення, кімнати операторів, периметр, зони з критичним обладнанням, зони обмеженого доступу	Камери відеоаналітики фіксують рухи працівника і в разі виявлення стороннього пристрою, аналізують положення рук, самого інструменту, особу працівника. Подія позначається як критична, одразу надсилається сигнал до служби безпеки, дублюється відео з камер безпеки, надсилається його особа і точне місцезнаходження, а доступ до суміжних критичних зон блокується.
Фотографування та відеозйомка в зонах обмеженого доступу (для пасажирів)	
Публічні та стерильні зони, гейти, Duty-Free, зони відпочинку	Визначаються звичні зони для пасажирського контенту (фото/відео, які пасажир робить без мети зашкодити аеропорту). Система оцінює не лише факт зйомки, а його повторюваність, специфічність об'єктів зйомки та поєднання з іншими поведінковими маркерами, які можуть вказувати на те, що дана особа нервує і поводиться нетипово.
Підозріле використання персоналом особистих пристроїв	

Технічні та службові приміщення, зони обмеженого доступу	Система фіксує як порушення кожен випадок використання особистих пристроїв, а в разі повторів або появи додаткових маркерів повідомляє службу безпеки. В особливо критичних зонах цю дію можна одразу оцінювати як інцидент.
Аномальні траєкторії руху та поведінка персоналу	
Робочі маршрути, переходи, службові точки доступу	Система порівнює фактичний маршрут із профілем, який сформувався на основі звичайних робочих переміщень. Якщо співробітник відхиляється від робочого маршруту, виконує часті входи/виходи, відвідує незвичні для себе зони, система вважатиме подібну поведінку відхиленням. У таких випадках прохід до наступних технічних приміщень може бути автоматично заблоковано, а відповідна служба отримає сповіщення з даними і місцезнаходженням співробітника.
Аномальна поведінка пасажира	
Черги, контрольні точки, стерильна зона	Тут оцінюється поєднання кількох факторів: напрямок руху, затримка в певних зонах, ознаки нервозності та підвищена температура тіла. Якщо пасажир здається системі підозрілим, вона надсилає службі безпеки відповідний сигнал. Якщо це відбувається під час проходження контрольної точки, пасажир автоматично направляється на додатковий ручний огляд або коротку перевірку співробітниками безпеки.
Спроби проходу за іншою особою	

СКУД, службові входи, переходи між зонами	Якщо двері доступу вже відкриті, а в зону намагається зайти друга особа, прохід автоматично блокується, службі безпеки надсилається відповідне повідомлення з вказівкою точки проходу, часу та відповідним фрагментом з камер відеоспостереження.
Спроби виведення з ладу камер або сенсорів	
Контрольні точки та зони з контрольованим доступом	Система визначає неполадку як технічну аномалію і збій, та автоматично блокує сам датчик і під'єднану до нього точку доступу. На місце інциденту відправляється технічна служба для перевірки. Одночасно, разом з записом про інцидент, додається запис з камер для визначення особи, що перебувала біля обладнання і може потенційно бути задіяна в інциденті.
Спроби обійти біометричний контроль	
СКУД, eGate, точки посадки, паспортний контроль	Система блокує прохід, якщо перевірка на «живість» була невдалою або біометричні дані не відповідають документам. Особу автоматично направляють на ручний контроль, а невдала спроба проходу фіксується у журналі як інцидент. Це стосується і працівників, і пасажирів.
Невірне зчитування паспорта або MRZ	
Реєстрація, eGate, паспортний контроль	Система запитує повторну спробу. Якщо зчитування знову невдале/некоректне, пасажир направляється на ручний контроль. Подія фіксується як технічний збій.
Втрата синхронізації між багажем і пасажиром	
Точка реєстрації багажу	У разі втрати відповідності між багажною етикеткою та особою система блокує багаж до

	уточнення. Далі виконується повторне співставлення даних, а подія заноситься до журналу як інцидент.
Відмова центрального сервера	
Всі автоматизовані технології	Автоматизовані технології переходять у ручний режим, а події зберігаються локально і надсилаються вже після відновлення зв'язку.
Нетипове скупчення людей у контрольованій зоні	
Вся контрольована зона	Система фіксує перевищення щільності руху та позначає зону як таку, що потребує втручання. Оператор перевіряє ситуацію за допомогою камер і, в разі необхідності, перенаправляє потік пасажирів.

3.4. Відповідність запропонованої системи міжнародним вимогам та очікування від неї

Запропонована модель біометричної системи охоплює всі важливі вимоги міжнародних організацій, що регулюють ідентифікацію, прикордонний контроль, обробку біометричних даних та безпеку цивільної авіаційної галузі. Структура системи, в першу чергу, базується на документах ICAO, ISO та нормативних актах ЄС, які визначають формат документів, їх зчитування, збереження шаблонів, їх передавання та параметри біометрії та загальні вимоги до інформаційної безпеки.

Перший документ, якому має відповідати система – ICAO Doc 9303. У ньому визначені вимоги до структури та перевірки електронних документів, MRZ-зони та криптографічного захисту чипа. У запропонованій архітектурі ці вимоги реалізує модуль попередньої обробки, який виконує перевірку цифрових підписів, зчитує електронні документи та виявляє їх підробки.

Другий документ – ISO/IEC 19794 та ISO/IEC 30107, вимогам яких відповідають використання технологій виявлення «живості», глибини сенсорів та алгоритми протидії обходу біометричного контрою.

Також, окрім конкретних нормативних документів, важливо, щоб запропонована система відповідала ініціативі IATA One ID, оскільки саме вона визначає, як виглядатиме майбутній біометричний маршрут в аеропортах. У розробленій системі присутні всі необхідні для повноцінної інтеграції One ID елементи: безконтактний маршрут, самостійна біометрична реєстрація, автоматизований контроль документів.

Щодо українських документів, система коректно співвідноситься з вимогами до КСЗІ, а також правилами обробки персональних даних. Усі елементи архітектури передбачають розмежування доступів, надійне шифрування, повний аудит дій кожного користувача, зокрема пасажирів, персоналу, та операторів біометричної системи. Це не потребує додаткового адаптування, окрім створення інструкцій та навчання персоналу вже після впровадження.

Окремо ще варто розглянути, наскільки дана система готова працювати в умовах післявоєнної України. Тут важлива наявність резервної архітектури, що дозволяє підтримувати базові процеси, а також забезпечити повну роботу біометричних безпекових технологій. А також українські аеропорти відкриватимуться поетапно та з обмеженою кількістю рейсів, відповідно, тому система має бути готовою працювати при невеликих потоках пасажирів та уміти розширюватися відповідно до вимог.

Загалом, запропонована модель дозволяє оцінити, як може бути організована повноцінна біометрична безпекова система в українських аеропортах після відновлення авіасполучення. В даному випадку, очікування від системи визначаються не лише міжнародними вимогами та тенденціями, а й фактичним станом інфраструктури, яка не працює з 24 лютого 2022 року.

Очікується, що проєктована система зможе забезпечити стабільну ідентифікацію та мінімізує ризики, пов’язані з помилковими прийняттями, відхиленнями та людським фактором. З практичної точки зору, це означає ще й менший час проходження контролю, менше черг, стабільну роботу і зменшення ролі ручних операцій.

Повернення українських аеропортів до роботи відбуватиметься за умов підвищеного рівня контролю. Це стосується доступу до службових зон, перевірки персоналу, нестачі кадрів та необхідності швидко адаптуватися до вимог міжнародних систем. Тому система має підтримувати поетапне впровадження.

Економічні очікування – автоматизовані системи здатні обробити значно більше пасажирів, ніж ручний контроль, відповідно, великі аеропорти матимуть можливість скоротити операційні витрати, а також зменшити ризик інцидентів та збитки, які вони нанесуть. Це стосується і фінансових, і безпекових наслідків.

Система має бути гнучкою, щоб дозволити поетапно впроваджувати нові, більш нагальні технології без зупинки роботи аеропорту і перебудови всієї інфраструктури.

Тобто, якщо підсумувати, очікується, що система:

- забезпечить однакову якість ідентифікації у всіх ключових точках;
- стабілізує роботу аеропорту на етапі відновлення;
- зменшить навантаження на персонал;
- підвищить точність контролю та зменшить кількість інцидентів;
- дозволить гнучко розширювати інфраструктуру;
- підготує основу для роботи з One ID, EES, ETIAS та іншими міжнародними системами.

Враховуючи досить високий рівень цифровізації населення та широке використання електронних послуг в Україні, впровадження біометричних технологій не вимагатиме тривалого перехідного періоду. Більше того, ця система легко адаптується до специфічних вимог воєнного та післявоєнного часу, включаючи посилений контроль у зонах обмеженого доступу, ретельну фіксацію підозрілих дій персоналу та пасажирів, а також можливість оперативного аналізу аномалій та реагування на них. Тобто, таким чином, запропонована архітектура одночасно відповідає і міжнародним стандартам, і повністю враховує унікальні умови, в яких відбуватиметься відновлення української авіаційної інфраструктури.

Висновки до третього розділу

Результатом роботи в третьому розділі є створення оптимальної біометричної системи для вітчизняних аеропортів, яка поєднує технології розпізнавання обличчя, машинне читання документів, поведінкову аналітику та засоби автоматизованої верифікації особи під час «пасажирського маршруту». Вона враховує специфіку українських аеропортів, зокрема період відновлення після «простою», відновлення інфраструктури та цивільної авіації на території України.

Архітектура системи побудована таким чином, щоб забезпечити послідовний зв'язок сенсорів, зчитувачів, підсистем попередньої обробки, біометричної верифікації та контуру резервування. Це забезпечує системі безперервність роботи навіть за умов часткових відмов або втрати каналів зв'язку.

Відповідно до міжнародних стандартів ICAO, ISO, вимог ЄС та підходів IATA One ID визначено технічні та нормативні умови, у яких система має працювати. Також описано маршрут пасажира через технічні точки та визначено конкретні вимоги для камер, характеристики сенсорів, алгоритми розпізнавання та логіку обробки даних.

Окрім цього, на прикладі реального аеропорту – терміналу «D» МА «Бориспіль», представлено схему зонування, яка показує розташування біометричних технологій, у просторі аеропорту. Це дозволяє на прикладі зрозуміти схему розташування контрольних точок та оцінити, які саме сенсори потрібні в різних зонах.

Також сформовано модель загроз, оцінено ризики, та створено практичні сценарії реагування на них автоматизованою системою. Для кожного сценарію визначено, які модулі реагують на подію, як система фіксує порушення, коли подія передається оператору та які дії виконуються в ручному режимі.

Описана структура може бути використана під час планування модернізації українських аеропортів, вона дає можливість оцінити необхідний склад обладнання, логіку обробки даних та розташування контрольних точок. Також

дозволяє зрозуміти, як окремі технології впливають на пропускну здатність, навантаження на персонал і швидкість обслуговування.

ВИСНОВОК

У роботі було розглянуто підходи до біометричної ідентифікації, досвід їх практичного застосування в аеропортах різних країн та можливості їх подальшої інтеграції в інфраструктуру українських аеропортів. Проаналізовано причини переходу до біометричних паспортів та методів ідентифікації. Вивчено розмежування зон аеропорту на прикладі АМ «Бориспіль», а також доступів в кожну зону.

Проаналізовано основні методи біометрії, які використовуються для проходу пасажирів між зонами, ідентифікації за документами та шаблонами з баз, а також як вплинула автоматизація процесів на пасажирський маршрут, зокрема, пришвидшила сам процес ідентифікації та проходження всіх критичних точок, спростила процедуру перевірки та посадки на рейс, мінімізувала потребу в перд'явленні фізичних документів.

Також розглядалося використання біометричної ідентифікації для персоналу аеропорту, зокрема використання мультифакторного доступу в СКУД. Процедури відеоаналітики та контролю натовпу, розпізнавання підозрілих патернів пасажирів та співробітників, а також реагування на аномалії.

У роботі також проаналізовано вимоги ICAO, ISO та нормативних документів, які визначають порядок зчитування електронних документів, роботу з біометричними даними, їх передачу та збереження, параметри сенсорів та вимоги до інформаційної безпеки. На основі цих документів визначено, які технічні особливості необхідні для роботи системи в аеропорту та які обмеження потрібно враховувати під час реалізації біометричних рішень. Сформовано модель функціонування біометричної системи в аеропорту, визначено роль кожного модуля, описано критичні точки маршруту, де система повинна забезпечувати ідентифікацію та автоматичне реагування на аномальні події або інциденти.

У практичній частині роботи створено архітектуру біометричної системи з урахуванням специфіки українських вимог. Також побудовано схему розташування контрольних точок та маршрут пасажира з позначенням зон, де

працюють різні типи сенсорів. Визначено вимоги до обладнання, параметри камер, логіку передавання й обробки даних.

Окремо сформовано модель загроз та сценаріїв реагування. Для кожного потенційного випадку описано дію системи, зокрема інциденти з боку персоналу, підозрілі дії пасажирів, спроби обходу контролю, технічні збої.

Загалом, запропонована модель показує, як може виглядати біометрична система аеропорту та як її можна адаптувати до українських реалій. Вона демонструє, які технологічні рішення доцільно використовувати та які обмеження варто враховувати при відновленні аеропортів та модернізації біометричної інфраструктури. Модель дозволяє оцінити можливості поетапного впровадження технологій, визначити критичні зони та процеси, які найбільше впливають на точність ідентифікації та безпеку в цілому.

Подальші дослідження можуть бути спрямовані на практичне тестування окремих компонентів системи та моделювання їх роботи в умовах реального пасажиропотоку, щоб перевірити, як змодельована система поводиться під час пікових навантажень або часткових відмов.

Основні положення кваліфікаційної роботи були апробовані під час участі у наукових конференціях. У межах конференцій «БУД МАЙСТЕР КЛАС 2025» та «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» було підготовлено тези доповідей за напрямом дослідження.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Passenger Analysis: звіт / International Air Transport Association. – December 2018. – 80 с

2. Pająk J. Air Terrorism as a Threat to the Safety of Air Transport. Safety & Defense. 2020. Vol. 6, no. 2. P. 123–130. URL:https://doi.org/10.37105/sd.90

3. REAL ID: Fact Sheet / Center for American Progress. – Washington, DC: CAP, 2008. URL:https://cdn.americanprogress.org/wp-content/uploads/issues/2008/06/pdf/realid_fact_sheet.pdf

4. Handbook of Biometrics / ed. by A. K. Jain, P. Flynn, A. A. Ross. Boston, MA: Springer US, 2008. URL:https://doi.org/10.1007/978-0-387-71041-9

5. Biometrics Technology | Transportation Security Administration. U.S. Department of Homeland Security. URL:https://www.tsa.gov/biometrics-technology

6. Про Державну програму авіаційної безпеки цивільної авіації : Закон України від 21.03.2017 № 1965-VIII : станом на 15 листоп. 2024 р.

7. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 : Регламент ЄС // Official Journal of the European Union. – 2008. – L 97.

8. Інтерактивна мапа аеропорту – Аеропорт Бориспіль. Аеропорт Бориспіль. URL:https://kbp.aero/airport/map/

9. Про затвердження зразка бланка, технічного опису та Порядку оформлення, видачі, обміну, пересилання, вилучення, повернення державі, визнання недійсним та знищення паспорта громадянина України для виїзду за кордон: Постанова Каб. Міністрів України від 07.05.2014 № 152: станом на 1 січ. 2025 р.

10. Doc 9303. Machine Readable Travel Documents: Part 1. Machine Readable Passports / International Civil Aviation Organization (ICAO). – 8th ed. – Montréal: ICAO, 2021.

11. Patel V. Airport Passenger Processing Technology: A Biometric Airport Journey: doctoral dissertation / Vishra Patel. – 2018.

12. Traveller Modernization: New tools and technologies for a faster, better and safe experience at the border. Canada Border Services Agency | Agence des services frontaliers du Canada. URL:https://www.cbsa-asfc.gc.ca/services/border-tech-frontiere/modern-eng.html#a2

13. Planning Border Controls at UK Airports: Quantitative Studies into Operational Decisions and Their Impact on Passengers: doctoral thesis. URL:https://etheses.whiterose.ac.uk/id/eprint/33806/

14. Thales FlyGate // Thales Group. – URL:https://www.thalesgroup.com/en/solutions-catalogue/public-security/civil-identity/thales-fly-gate

15. One ID // International Air Transport Association. – URL:https://www.iata.org/en/programs/passenger/one-id/

16. The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic - PMC. URL:https://pmc.ncbi.nlm.nih.gov/articles/PMC7337876/

17. Readiness A. T. Changi Airport – AI & Digital Transformation Case Study // AI Transformation Readiness Institute. – URL:https://www.aitransformationreadiness.org/post/changi-airport-digital-transformation

18. Visiting Singapore // Immigration & Checkpoints Authority (ICA), Singapore. – URL: https://www.ica.gov.sg/public-education/visiting-singapore

19. Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States // *Federal Register*. – 2025. – Doc. № 2025-19655. URL:https://www.federalregister.gov/documents/2025/10/27/2025-19655/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states

20. J-BIS - Wikipedia. URL: https://en.wikipedia.org/wiki/J-BIS

21. Promoting seamless travel at Narita International Airport with Face Express (One ID) // *International Airport Review*. 2022.

URL:https://www.internationalairportreview.com/article/184418/promoting-seamless-travel-at-narita-international-airport-with-face-express-one-id/

22. Major biometric deployment goes live at Beijing Capital Airport. Future Travel Experience. 2020. URL:https://www.futuretravelexperience.com/2020/08/major-biometric-deployment-goes-live-beijing-capital-airport

23. Entry/Exit System (EES) // Council of the European Union. URL:https://www.consilium.europa.eu/en/policies/entryexit-system

24. Wilson Y., Hingnikar A. Solving Identity Management in Modern Applications: Demystifying OAuth 2, OpenID Connect, and SAML 2. – 2nd ed. – New York : Apress, 2023. – 143 p.

25. Система контролю і управління доступом // *Вікіпедія*. URL:https://uk.wikipedia.org/wiki/Система_контролю_і_управління_доступом

26. Back to Basics: Multi-Factor Authentication / National Institute of Standards and Technology (NIST). – Gaithersburg, MD : NIST, 2021

27. Annex 17: Security: Додаток до Конвенції про міжнародну цивільну авіацію / International Civil Aviation Organization (ICAO). – 12th ed. – Montréal: ICAO, 2020.

28. Risk Content Statement ICAO // International Civil Aviation Organization (ICAO). – Montréal : ICAO, 2016. URL:https://www.icao.int/sites/default/files/WACAF/MeetingDocs/AFI-Week/AFI-Week-3/Security-Symposium/Risk-Content-Statement-June-2016.pdf

29. Insider Threat Toolkit / International Civil Aviation Organization (ICAO). – Montréal : ICAO. URL:https://www.icao.int/sites/default/files/Security/Security-Culture/Documents/Insider-Threat-Toolkit.EN.pdf

30. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability... // Official Journal of the European Union. – 2019. – L 135.

31. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р.

32. Про правовий статус іноземців та осіб без громадянства : Закон України від 22.09.2011 № 3773-VI : станом на 5 серп. 2025 р.

33. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV : станом на 28 серп. 2025 р.

34. Повітряний кодекс України : Кодекс України від 19.05.2011 № 3393-VI : станом на 31 жовт. 2025 р.

35. Про Державну програму авіаційної безпеки цивільної авіації : Закон України від 21.03.2017 № 1965-VIII : станом на 15 листоп. 2024 р.

36. CBP Needs to Fully Implement a Biometric Entry/Exit System at Airports / U.S. Department of Homeland Security, Office of Inspector General (DHS OIG). – Washington, D.C.: DHS OIG, 2020. – (Report No. OIG-20-71). URL:https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf

37. CBP Traveler Photo Data Breach // uSceure Blog. URL:https://blog.usecure.io/cbp-traveler-photo-data-breach

38. Facial Recognition / International Criminal Police Organization (INTERPOL). URL:https://www.interpol.int/How-we-work/Forensics/Facial-Recognition

39. Biometric Hub / International Criminal Police Organization (INTERPOL). URL:https://www.interpol.int/How-we-work/Forensics/Biometric-Hub

40. Grother P. Face Recognition Vendor Test Part 3: Demographic Effects : NIST Interagency/Internal Report 8280 / Patrick J. Grother, Mei L. Ngan, Kayee K. Hanaoka ; National Institute of Standards and Technology (NIST). – Gaithersburg, MD: NIST, 2019. – 81 p.

41. What is the False Acceptance Rate (FAR) in Facial Recognition? // Facia.ai Knowledgebase. URL:https://facia.ai/knowledgebase/what-is-the-false-acceptance-rate-far-in-facial-recognition/

42. Kittler, J. Evaluation of Biometric Systems – 2013. URL:https://www.researchgate.net/publication/257365353_Evaluation_of_Biometric_Systems

43. Equal Error Rate (EER) // Innovatrics Glossary. URL:https://www.innovatrics.com/glossary/equal-error-rate-eer/

44. Godil A. Performance Metrics for Evaluating Object and Human Detection and Tracking Systems / A. Godil. – Gaithersburg, MD: National Institute of Standards and Technology, 2014. – (NIST Interagency/Internal Report (NISTIR); 7972).

45. Donida Labati R. Advanced design of Automated Border Control gates: Biometric system techniques and research trends // R. Donida Labati// 2015 IEEE International Symposium on Systems Engineering (ISSE), 28–30 September 2015, Rome, Italy. – New York: IEEE, 2015. – P. 412–419.

46. Butterfly Training. Unveiling the Veiled: A Comprehensive Analysis of the Hidden Insider Threat to Aviation Security / Butterfly Training. URL:https://www.butterfly-training.co.uk/insider-threat

47. Бориспіль (аеропорт) // *Вікіпедія*. URL:https://uk.wikipedia.org/wiki/Бориспіль_(аеропорт)

48. Airport Solutions for Ensuring Security & Safety / Bosch Security Systems. – [Germany] : Bosch Sicherheitssysteme GmbH, 2012. – 16 p.

49. Axis Communications AB. Perimeter protection for airports with intelligent video surveillance / Axis Communications AB. – [Lund, Sweden] : Axis Communications AB, 2024.

ДОДАТОК

Інформаційні слайди

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ
Факультет автоматизації і інформаційних технологій
Кафедра кібербезпеки та комп'ютерної інженерії

Кваліфікаційна робота на тему:
«Біометричні технології в системах безпеки аеропортів»

Виконала Сивець Богдана Олександрівна
Група БІКСм_24
Керівник доцент, к.т.н Шабала Є.Є.

Метою роботи є формування архітектурної моделі біометричної системи для цивільного аеропорту, які відповідає сучасним технічним вимогам та адаптована до українських умов після відновлення авіаперевезень.

Актуальність обраного напряму роботу: В Україні цивільні аеропорти припинили свою роботу 24 лютого 2022 року, що фактично зупинило їх розвиток. Після відновлення цивільних авіаперевезень вони матимуть потребу швидкої модернізації до сучасних технологічних вимог, а також до підвищених безпекових ризиків.

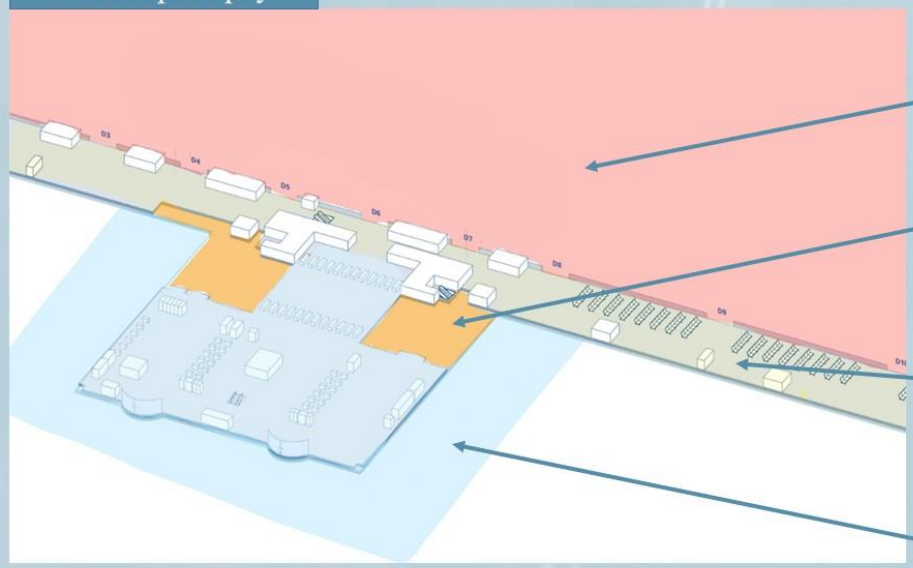
Наукова новизна роботи полягає у формуванні моделі біометричної системи, яка поєднує фізіологічну та поведінкову біометрію, автоматизовану перевірку документів та сценарії реагування на інциденти. У роботі запропоновано новий підхід до визначення критичних точок маршруту пасажира та адаптація біометричних процесів під умови вітчизняних аеропортів, які відновлюватимуть роботу після тривалого простою.

Об'єктом дослідження є біометричні технології, що використовуються в безпекових процесах в аеропортах.

Предметом дослідження є архітектура біометричної системи, її компоненти та можливість інтеграції у структуру аеропорту.

Завдання роботи	Методи, які використовувалися для виконання завдання
Аналіз розвитку біометричних технологій та їх застосування в цивільних аеропортах	Дослідження історії впровадження біометрії в системи аеропортів, аналіз нормативних документів ICAO, ISO та ЄС
Визначення ризиків, пов'язаних з ідентифікацією пасажирів та персоналу	Аналіз загроз і побудова сценаріїв реагування на загрози, оцінка точності біометричних методів
Визначення критичних точок доступу та обладнання для них	Моделювання пасажирського маршруту з визначенням критичних точок, у яких необхідне застосування біометричних методів і автоматизованого контролю
Розробка архітектури системи біометричної безпеки для аеропорту	Моделювання на прикладі схеми реального аеропорту критичних точок доступу

Зони аеропорту



Критичні ділянки з обмеженим доступом

Найбільш захищені зони аеропорту, доступ тільки за дозволом

Зони обмеженого доступу

Ділянки з підвищеними вимогами до доступу

Внутрішня стерильна зона

Зона після контролю безпеки, доступна лише пасажирам, що вдало пройшли контроль і персоналу з перепусткою

Зовнішня зона

Відкрита частина аеропорту до контролю безпеки

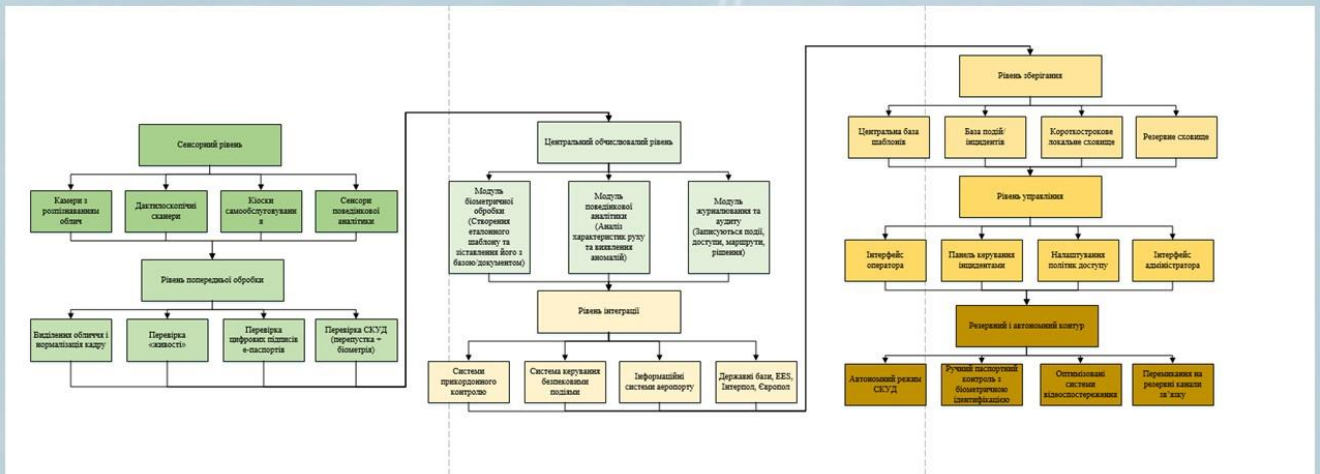
Сучасні біометричні технології в аеропортах

- Електронні паспортні ворота (eGate)
- Кіоски самообслуговування (self check-in)
- Автоматизована здача багажу (self bag drop)
- Біометрична посадка (face-based boarding)
- Мультифакторна СКУД для персоналу
- Система відеоаналітики (пасивний метод біометрії)

Основні методи біометрії

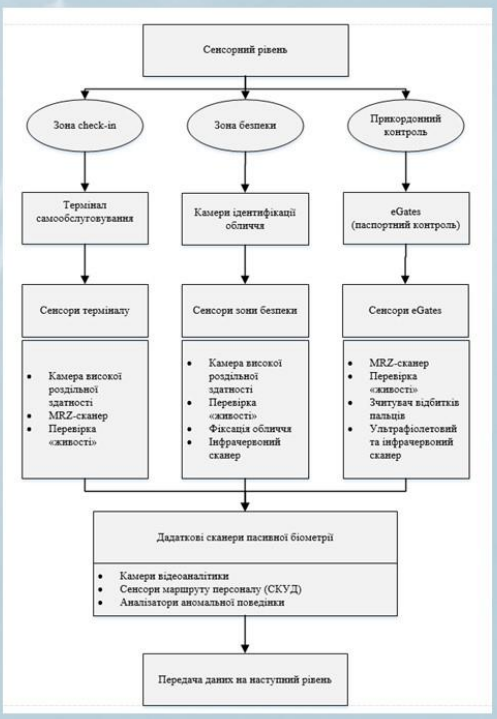
Метод	Характеристика	Доцільність
Обличчя	Безконтактне зчитування, висока швидкість	Базовий метод у e-Gates та при посадці
Відбитки пальців	Висока точність, контактний сенсор	Використовується переважно в прикордонному контролі
Райдужна оболонка ока	Дуже висока точність, проте низька швидкість	Рідко застосовується через складність та високу вартість
Комбіновані	Підвищена надійність	Доцільні для зон із підвищеним рівнем ризику

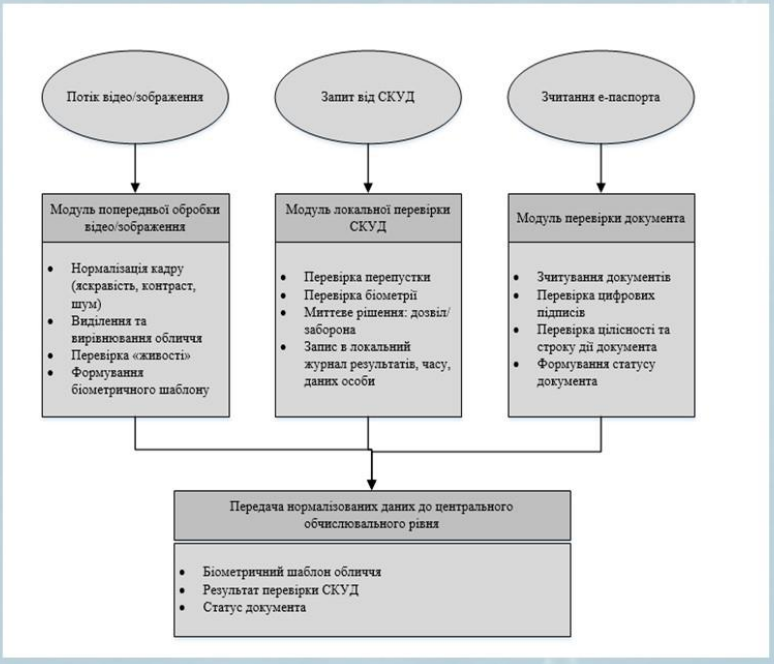
Архітектурна модель біометричної системи безпеки



Сенсорний рівень

Набір апаратних засобів, які зчитують інформацію про людину або подію і передають її на подальшу обробку



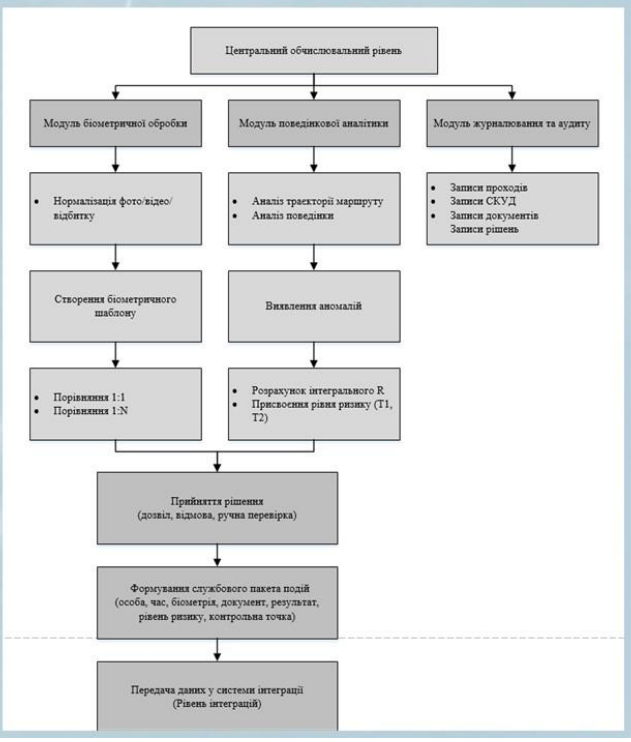


Рівень попередньої обробки

На цьому рівні виконується первинна перевірка даних з сенсорів та їх нормалізація.

Центральний обчислюваний рівень

На цьому рівні відбувається обробка біометрії, аналіз поведінки та остаточне прийняття рішення.

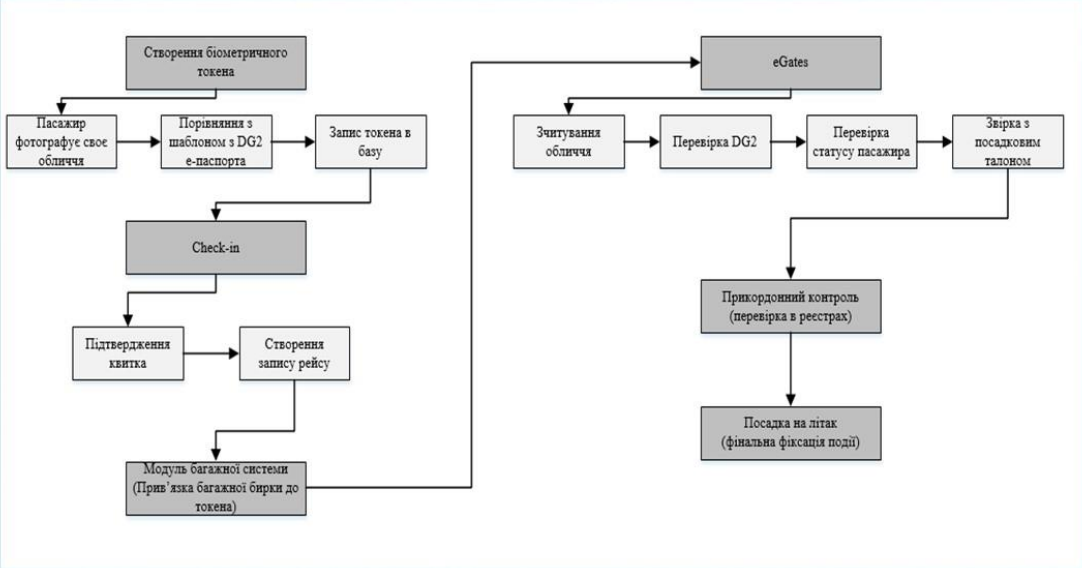


Резервний та автономний контур

У разі збоїв або у кризових ситуаціях, біометрична система аеропорту повинна переходити в режим автономного або резервного функціонування. Зберігаються лише необхідні модулі, решта функцій вимикаються за рівнями критичності.

Рівень 0 (не вимикається, ядро біометричної системи безпеки аеропорту)	Рівень 1 (критичні модулі, працюють спрощено)	Рівень 2 (знижена функціональність)	Рівень 3 (необов'язкові модулі, вимикаються першими)
• Біометрія на паспортному контролі • СКУД • Журналювання подій	• Відеоспостереження • Сканування і перевірка документів (MRZ) • Локальні шаблони в контролерах	• Спрощена система eGates • Моніторинг стану обладнання • Базова поведінкова аналітика	• Кіоски самообслуговування • Глибинна відеоаналітика • Некритичні інтеграції • Розширена поведінкова аналітика

Маршрут пасажира



Маршрут пасажира на прикладі аеропорту «Бориспіль»

1 - вхід до терміналу
(відеоаналітика)

2 – реєстрація
(кіоски самообслуговування self check-in)

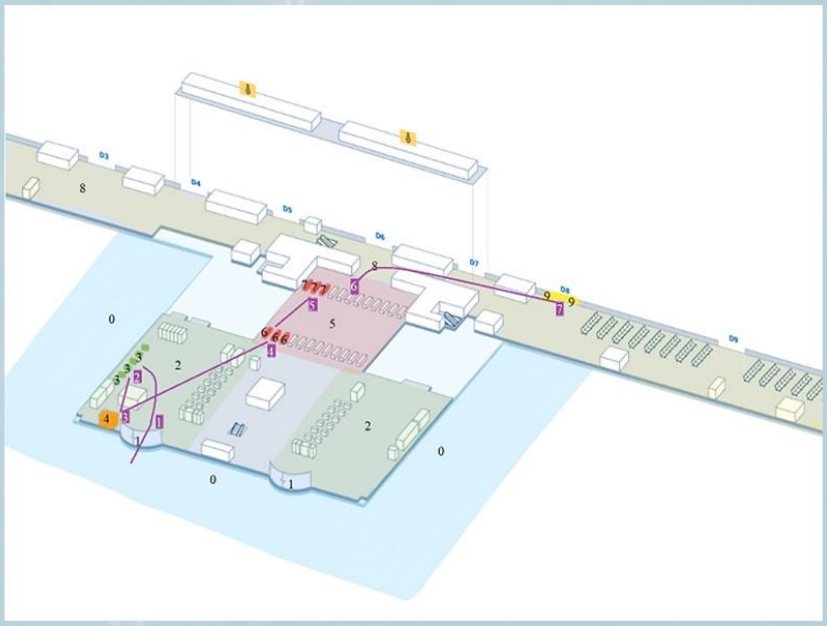
3 – здача багажу
(автоматизована здача багажу self bag drop)

4 – безпековий контроль
(відеоаналітика і сенсори)

5 – паспортний контроль
(електронні паспортні ворота eGate)

6 – вхід в стерильну зону
(відеоаналітика)

7 – посадка на борт
(біометрична посадка face-based boarding)



Модель загроз і сценарії реагування

Ризик	Сценарій реагування
Фотографування/зйомка в критичних зонах (персонал)	Відеоаналітика визначає сторону руху, фіксує пристрій, блокує доступ у суміжні зони, надсилає сповіщення
Фотографування/зйомка пасажирами критичних об'єктів	Відеоаналітика визначає поведінку пасажира, кут, частоту і об'єкт зйомки, у разі аномалії формує інцидент і передає оператору
Підозріле використання персоналом особистих пристроїв	Автоматична реєстрація події, підвищення рівня ризику при повторенні, сигнал службі безпеки
Аномальні траєкторії руху та поведінка персоналу	Аналіз треєкторій, блокування входу в невідповідні приміщення, сповіщення оператора
Аномальна поведінка пасажира	Призначення рівня ризику, перенаправлення на додатковий огляд або ручну перевірку
Спроби проходу за іншою особою	Автоматичне блокування дверей, фіксація інциденту, надсилання запису про подію
Спроби виведення з ладу камер або сенсорів	Виявлення технічної аномалії, блокування точки доступу

Висновки

У роботі проаналізовано біометричні технології, їх практичне застосування в аеропортах та можливість інтеграції в інфраструктуру українських летовищ. Досліджено критичні зони аеропорту, вимоги нормативних документів, принципи роботи технологій і окремих сенсорів, систем безпеки. На основі цього сформовано архітектуру біометричної системи для аеропорту, визначено критичні точки та логіку роботи модулів.

- Розроблено архітектуру біометричної системи з урахуванням специфіки українських аеропортів
- Сформовано модель загроз та сценаріїв реагування
- Побудовано автоматизований маршрут пасажира на основі контрольних точок
- Визначено параметри до обладнання та логіку обробки даних
- Створено модель резервного та автономного режиму роботи системи у разі критичних випадків

Загалом, запропонована модель показує, як може виглядати біометрична система аеропорту та як її можна адаптувати до українських реалій. Вона демонструє, які технологічні рішення доцільно використовувати та які обмеження варто враховувати при відновленні аеропортів та модернізації біометричної інфраструктури. Модель дозволяє оцінити можливості поетапного впровадження технологій, визначити критичні зони та процеси, які найбільше впливають на точність ідентифікації та безпеку в цілому.

Подальші дослідження можуть бути спрямовані на практичне тестування окремих компонентів системи та моделювання їх роботи в умовах реального пасажиропотоку, щоб перевірити, як змодельована система поводиться під час пікових навантажень або часткових відмов.

Публікації

- Участь у конференції «БУД МАЙСТЕР КЛАС 2025»
- Участь у конференції "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (випуск 103)"

Дякую за увагу