МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА імені О. М. БЕКЕТОВА
Навчально-науковий Інститут енергетичної, інформаційної та транспортної інфраструктури
Кафедра автоматизації та комп'ютерно-інтегрованих технологій

РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНА ЗАПИСКА ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ БАКАЛАВРА

на тему: Комп'ютерно-інтегрована система технічного зору для задач автентифікації в електронних платіжних системах

Виконав: здобувач вищої освіти
4 курсу, групи Сінж-2022-1
напряму підготовки (спеціальності)
151 «Автоматизація та комп'ютерно-інтегровані технології»
Борзенко Кирило Сергійович
(прізвище та ініціали)

Керівник Білецький І.В., проф. каф. АКІТ
(прізвище та ініціали, наук. ступ., вч. звання)

Рецензент Ківіренко О.Б., начальник виробництва ТОВ «Альфа-Композіт»
(прізвище та ініціали, наук. ступ., вч. звання)

Харків – 2026

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА ІМЕНІ О. М. БЕКЕТОВА

Навчально-науковий Інститут енергетичної, інформаційної та транспортної інфраструктури

Кафедра автоматизації та комп'ютерно-інтегрованих технологій
Освітньо-кваліфікаційний рівень – бакалавр
Галузь знань 15 «Автоматизація та приладобудування»
Спеціальність 151 «Автоматизація та комп'ютерно-інтегровані технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри АКІТ
_____ БАРАНОВ О.О.
« 19 » червня 2026 року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Борзенко Кирило Сергійович

1.Тема роботи Комп'ютерно-інтегрована система технічного зору для задач автентифікації в електронних платіжних системах
Затверджена наказом університету від « 22 » травня 2026 року № 440-03
Керівник роботи Білецький Ігор Васильович, доктор економічних наук, професор, професор кафедри АКІТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
2. Строк подання роботи здобувачем вищої освіти «__15__» _червня_ 2026 р.
3. Вихідні дані до роботи Система технічного зору для задач автентифікації в електронних платіжних системах
4. Зміст розрахунково пояснювальної записки (перелік питань, які потрібно розробити): Вступ. Аналіз сучасних методів автентифікації та технологій технічного зору. Проєктування комп'ютерно-інтегрованої системи технічного зору. Програмна реалізація комп'ютерно-інтегрованої системи технічного зору.. Охорона праці, висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація.

6. Консультанти розділів проєкту (роботи)

Розділ	Консультант	Підпис, дата	
		завдання видав	завдання прийняв
Аналіз проблеми	Білецький І.В.	11.05.2026	21.05.2026
Основна частина	Білецький І.В.	**22.05.2026**	31.05.2026
Спеціальний розділ	Білецький І.В.	01.06.2026	14.06.2026
Охорона праці	Малишева В.В.	08.06.2026	14.06.2026

7. Дата видачі завдання «_11_» __травня_2026_р.

Керівник _____ Білецький І.В.
(підпис)

Завдання прийняв до виконання _____Борзенко К. С.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання розділів	Примітка
1	Розробка 1го розділу бакалаврської роботи	11.05.2026 - 21.05.2026	
2	Розробка 2го розділу бакалаврської роботи	22.05.2026 - 31.05.2026	
3	Розробка 3го розділу бакалаврської роботи	01.06.2026 - 14.06.2026	
4	Розробка розділу з охорони праці	08.06.2026 - 14.06.2026	
5	Рецензування бакалаврської роботи	15.06.2026	Ківіренко О.Б.
6	Захист на ДЕК	24.06.2026	

Здобувача вищої освіти _____Борзенко К. С.
(підпис)

Керівник _____Білецький І.В.
(підпис)

РЕФЕРАТ

Комп’ютерно-інтегрована система технічного зору для задач автентифікації в електронних платіжних системах – Борзенко Кирило Сергійович, бакалаврська робота, Харків, Харківський національний університет міського господарства імені О.М. Бекетова, кількість сторінок 114, кількість таблиць 34, кількість рисунків 16, кількість літературних джерел 16.

Актуальність теми бакалаврської роботи зумовлена стрімким зростанням обсягів електронних платіжних операцій та підвищеними вимогами до їх безпеки, що потребує впровадження надійних і автоматизованих методів автентифікації користувачів. Використання комп’ютерно-інтегрованих систем технічного зору дає змогу підвищити рівень захисту платіжних систем, зменшити ризики шахрайства та забезпечити ефективну інтеграцію процесів автентифікації в сучасні інформаційно-технологічні середовища.

Метою бакалаврської роботи є розробка та дослідження комп’ютерно-інтегрованої системи технічного зору для автоматизованої автентифікації користувачів в електронних платіжних системах з метою підвищення рівня безпеки та надійності платіжних операцій.

Об’єктом дослідження є процеси автоматизованої автентифікації користувачів у електронних платіжних системах.

Предметом дослідження є методи, алгоритми та програмно-апаратні засоби технічного зору, що використовуються у складі комп’ютерно-інтегрованої системи для автентифікації користувачів електронних платіжних систем.

Для досягнення поставленої мети в роботі необхідно розв’язати такі задачі:

- Проаналізувати сучасні методи та засоби автентифікації користувачів в електронних платіжних системах.

- Дослідити принципи побудови комп’ютерно-інтегрованих систем технічного зору та можливості їх застосування для задач автентифікації.
- Розробити структурну та функціональну схеми комп’ютерно-інтегрованої системи технічного зору.
- Обґрунтувати вибір алгоритмів оброблення зображень і розпізнавання облич для автентифікації користувачів.
- Реалізувати програмну модель комп’ютерно-інтегрованої системи та забезпечити її інтеграцію з електронною платіжною системою.

У процесі виконання бакалаврської роботи використано такі методи дослідження, як аналіз і узагальнення науково-технічної літератури та нормативних джерел у галузі електронних платіжних систем і біометричної автентифікації; системний аналіз для визначення структури та функціональних зв’язків комп’ютерно-інтегрованої системи технічного зору; методи математичного та алгоритмічного моделювання для розробки алгоритмів оброблення зображень і розпізнавання обличь; програмне моделювання розробленої системи.

КЛЮЧОВІ СЛОВА: комп’ютерно-інтегрована система, електронні платіжні системи, біометрична автентифікація.

ABSTRACT

Computer-integrated vision system for authentication tasks in electronic payment systems – Borzenko Kyrylo Serhiyovych, bachelor's thesis, Kharkiv, O. M. Beketov National University of Urban Economy in Kharkiv, number of pages 114, number of tables 34, number of figures 16, number of literature sources 16.

The relevance of the topic of the bachelor's thesis is due to the rapid growth in the volume of electronic payment transactions and high requirements for their security, which requires the implementation of reliable and automated methods of user authentication. The use of a computer-integrated vision system allows you to increase the level of protection of payment systems, reduce the risks of fraud and ensure effective integration of authentication processes in a modern information and technological environment.

The purpose of the bachelor's thesis is to develop and research a computer-integrated vision system for automated user authentication in electronic payment systems in order to increase the level of security and reliability of payment transactions.

The object of the study is the processes of automated user authentication in electronic payment systems.

The subject of the study is the methods, algorithms and software and hardware of technical vision used as part of a computer-integrated system for authenticating users of electronic payment systems.

To achieve the goal of the work, it is necessary to solve the following tasks:

- Analyze modern methods and means of user authentication in electronic payment systems.

- Investigate the principles of building computer-integrated vision systems and the possibilities of their application for authentication tasks.

- Develop a structural and functional diagram of a computer-integrated vision system.

- Justify the choice of image processing and face recognition algorithms for user authentication.

- Implement a software model of a computer-integrated system and ensure its integration with an electronic payment system.

In the process of completing the bachelor's thesis, the following research methods were used: analysis and generalization of scientific and technical literature and regulatory sources in the field of electronic payment systems and biometric authentication; system analysis to determine the structure and functional relationships of a computer-integrated vision system; methods of mathematical and algorithmic modeling to develop image processing and face recognition algorithms; software modeling of the developed system.

KEYWORDS: computer-integrated system, electronic payment systems, biometric authentication.

ЗМІСТ

ВСТУП 10
РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ ТА ТЕХНОЛОГІЙ ТЕХНІЧНОГО ЗОРУ 13
1.1 Особливості функціонування електронних платіжних систем 13
1.2 Сучасні методи автентифікації користувачів 17
1.3 Біометрична автентифікація на основі розпізнавання обличь 21
1.4 Аналіз існуючих систем технічного зору 25
1.5 Формування вимог до комп'ютерно-інтегрованої системи автентифікації 29
Висновок до розділу 1. 33
РОЗДІЛ 2. ПРОЄКТУВАННЯ КОМП'ЮТЕРНО-ІНТЕГРОВАНОЇ СИСТЕМИ ТЕХНІЧНОГО ЗОРУ 35
2.1 Загальна архітектура комп'ютерно-інтегрованої системи 35
2.2 Структурна схема системи та опис її модулів 42
2.3 Інформаційні потоки та інтеграційні зв'язки 47
2.4 Моделювання процесу автентифікації 52
Висновок до розділу 2. 57
РОЗДІЛ 3. ПРОГРАМНА РЕАЛІЗАЦІЯ КОМП'ЮТЕРНО-ІНТЕГРОВАНОЇ СИСТЕМИ ТЕХНІЧНОГО ЗОРУ 58
3.1 Опис програмної реалізації системи технічного зору 58
3.2 Реалізація алгоритмів розпізнавання облич 60
3.3 Програмна реалізація комп'ютерно-інтегрованої системи технічного зору для задач автентифікації 62
Висновок до розділу 3. 72
РОЗДІЛ 4. ОХОРОНА ПРАЦІ 74
4.1. Організаційно-правові основи забезпечення безпеки праці 74
4.2 Характеристика об'єкта та виявлення потенційних небезпек 75
4.3 Дослідження ризику реалізації потенційних небезпек на об'єкті проєктування та розробка заходів щодо їх попередження 78
Висновок до розділу 4. 83
ЗАГАЛЬНІ ВИСНОВКИ 85
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 87
Додаток А 89
Додаток В 99

Перелік умовних позначень, скорочень і термінів

ЕПС – електронна платіжна система

MFA – Multi-Factor Authentication

FAR – False Acceptance Rate

FRR – False Rejection Rate

EER – Equal Error Rate

КІС – комп’ютерно-інтегрованої системи

СТЗ – Системи технічного зору

ВСТУП

Актуальність теми бакалаврської роботи обумовлена інтенсивним розвитком електронних платіжних систем і зростанням кількості дистанційних фінансових операцій, що супроводжується підвищенням ризиків несанкціонованого доступу та шахрайства. Традиційні методи автентифікації, такі як паролі або PIN-коди, дедалі частіше виявляються недостатньо надійними та зручними для користувачів. У цьому контексті впровадження комп’ютерно-інтегрованих систем технічного зору, здатних автоматично ідентифікувати користувачів за біометричними ознаками, є перспективним напрямом підвищення рівня безпеки платіжних операцій. Застосування таких систем також забезпечує ефективну інтеграцію процесів автентифікації з існуючими інформаційними та керуючими підсистемами, що відповідає сучасним вимогам автоматизації та цифровізації.

Метою бакалаврської роботи є розробка, програмна реалізація та дослідження комп’ютерно-інтегрованої системи технічного зору для автоматизованої автентифікації користувачів в електронних платіжних системах, спрямованої на підвищення рівня інформаційної безпеки, надійності та ефективності виконання платіжних операцій. Досягнення поставленої мети передбачає побудову структурної та функціональної архітектури системи, обґрунтування вибору методів оброблення зображень і алгоритмів розпізнавання, а також інтеграцію розробленого рішення у середовище електронної платіжної інфраструктури.

Об’єктом дослідження є процеси автоматизованої автентифікації користувачів у електронних платіжних системах, що реалізуються із застосуванням сучасних інформаційних технологій та засобів комп’ютерного зору в умовах підвищених вимог до безпеки та швидкодії оброблення даних.

Предметом дослідження є методи, алгоритми та програмно-апаратні засоби технічного зору, а також принципи їх інтеграції у структуру комп’ютерно-інтегрованої системи, що забезпечує розпізнавання та

верифікацію особи користувача під час здійснення електронних платіжних операцій.

Для досягнення поставленої мети в роботі необхідно розв’язати такі задачі:

- Провести аналіз сучасних підходів і технологічних засобів автентифікації користувачів, що застосовуються в електронних платіжних системах.
- Дослідити теоретичні засади побудови комп’ютерно-інтегрованих систем технічного зору та оцінити можливості їх використання для вирішення задач автентифікації.
- Сформувати та розробити структурну і функціональну моделі комп’ютерно-інтегрованої системи технічного зору.
- Здійснити обґрунтований вибір методів і алгоритмів оброблення зображень та розпізнавання облич для забезпечення надійної ідентифікації користувачів.
- Виконати програмну реалізацію моделі системи та забезпечити її інтеграцію до складу електронної платіжної інфраструктури.

У процесі виконання бакалаврської кваліфікаційної роботи застосовано комплекс взаємопов’язаних методів дослідження, вибір яких зумовлений специфікою теми та вимогами до побудови комп’ютерно-інтегрованих систем. Метод аналізу й узагальнення науково-технічної літератури та нормативних джерел у галузі електронних платіжних систем і біометричної автентифікації застосовано з метою визначення сучасного стану проблеми, виявлення переваг і недоліків існуючих підходів, а також формування обґрунтованих вимог до розроблюваної системи, що дозволило спиратися на актуальні технологічні рішення та стандарти інформаційної безпеки. Системний аналіз використано для дослідження структури комп’ютерно-інтегрованої системи технічного зору, визначення її функціональних модулів, інформаційних потоків і взаємозв’язків із платіжною інфраструктурою. Застосування цього методу забезпечило цілісне бачення об’єкта дослідження як складної багаторівневої

системи та дало змогу обґрунтувати її архітектуру відповідно до принципів інтеграції та автоматизації. Методи математичного та алгоритмічного моделювання застосовано для розробки й формалізації алгоритмів оброблення зображень і розпізнавання обличчя, що дозволило описати процеси виділення ознак, порівняння біометричних параметрів та прийняття рішення про автентифікацію у формалізованому вигляді, забезпечуючи можливість подальшої оптимізації та оцінювання точності роботи системи. Програмне моделювання розробленої системи використано для практичної реалізації запропонованих алгоритмів і перевірки їх працездатності в умовах, наближених до реальних.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ ТА ТЕХНОЛОГІЙ ТЕХНІЧНОГО ЗОРУ

1.1 Особливості функціонування електронних платіжних систем

Електронні платіжні системи є складовою сучасної фінансової інфраструктури та забезпечують виконання безготівкових розрахунків між користувачами в режимі реального часу. Їх функціонування базується на використанні інформаційно-телекомунікаційних технологій, програмного забезпечення, криптографічних механізмів захисту та розподілених баз даних. Основним завданням таких систем є забезпечення швидкого, надійного та безпечного переказу коштів між учасниками платіжного процесу.

Типова структура електронної платіжної системи включає користувача (платника), отримувача коштів, платіжний шлюз, процесинговий центр, банк-емітент і банк-еквайр (див. табл. 1.1).

Таблиця 1.1 – Основні компоненти електронної платіжної системи

№	Компонент	Функціональне призначення
1	Користувач (платник)	Ініціює платіжну операцію
2	Отримувач коштів	Приймає оплату
3	Платіжний шлюз	Забезпечує передачу даних транзакції
4	Процесинговий центр	Обробляє запит, виконує перевірку та маршрутизацію
5	Банк-емітент	Перевіряє рахунок платника та авторизує операцію
6	Банк-еквайр	Забезпечує зарахування коштів отримувачу

У процесі здійснення операції відбувається передавання даних через кілька взаємопов’язаних підсистем, що працюють у єдиному інформаційному

середовищі. Важливою особливістю є багаторівнева обробка транзакції: перевірка коректності введених даних, автентифікація користувача, авторизація операції, підтвердження та фіксація результату в облікових системах.

Функціонування електронних платіжних систем характеризується високими вимогами до швидкодії, масштабованості та безвідмовності роботи. Системи повинні обробляти значні обсяги транзакцій у режимі реального часу з мінімальними затримками. Крім того, вони повинні відповідати міжнародним стандартам інформаційної безпеки та забезпечувати захист персональних і фінансових даних користувачів. Платіжна транзакція проходить кілька послідовних етапів оброблення (див. рис.1.1).

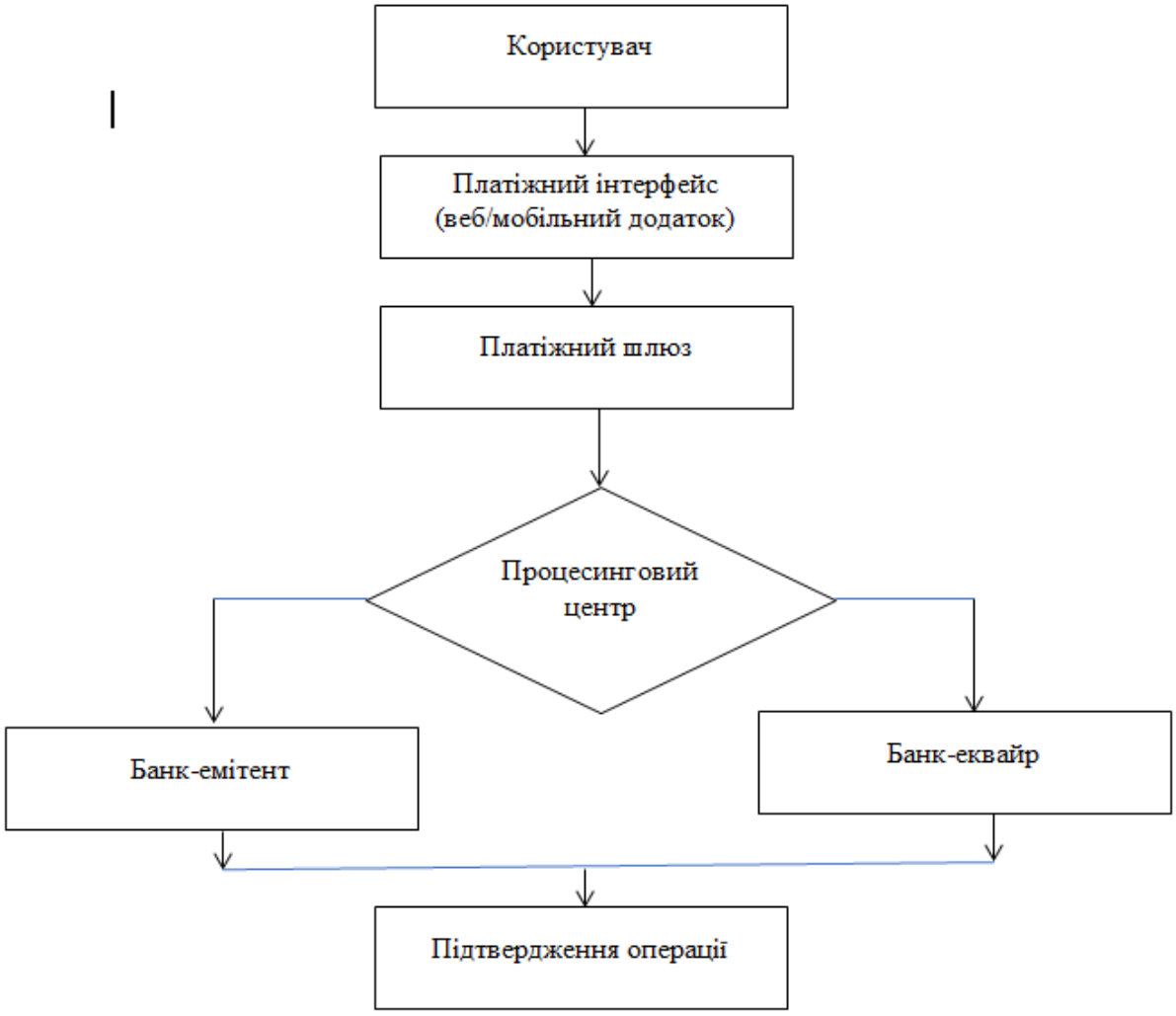


Рисунок 1.1 – Схема проходження платіжної транзакції

Електронні платіжні системи характеризуються низкою технічних та функціональних вимог (див. табл 1.2).

Таблиця 1.2 – Ключові вимоги до електронних платіжних систем

Характеристика	Опис
Швидкодія	Обробка транзакцій у режимі реального часу
Надійність	Безперервність роботи та відмовостійкість
Масштабованість	Можливість обробки великої кількості операцій
Захищеність	Криптографічний захист даних і контроль доступу
Інтегрованість	Взаємодія з банківськими та зовнішніми сервісами

Однією з ключових особливостей електронних платіжних систем (ЕПС) є необхідність надійної автентифікації користувачів перед підтвердженням операції. Зважаючи на віддалений характер здійснення більшості операцій, система не має прямого фізичного контакту з клієнтом, що підвищує ризик шахрайських дій. Тому в сучасних умовах широко застосовуються багатофакторні механізми автентифікації, які поєднують знання (паролі), володіння (токени, смартфони) та біометричні характеристики користувача.

Таблиця 1.3 – Порівняння методів автентифікації

Метод	Переваги	Недоліки
Пароль	Простота реалізації	Низька стійкість до атак
SMS-код	Додатковий рівень захисту	Можливість перехоплення
Токен	Висока безпека	Потребує додаткового пристрою
Біометрія (обличчя)	Висока зручність і надійність	Потребує технічного забезпечення

У сучасних умовах модуль автентифікації інтегрується у загальну архітектуру платіжної системи.

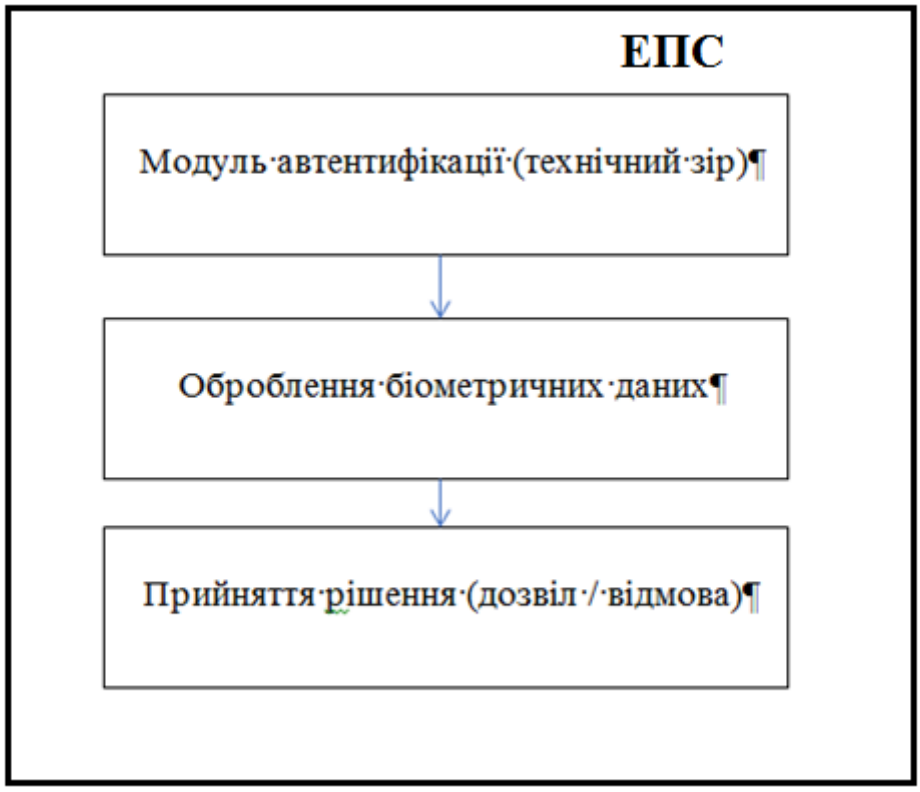


Рисунок 1.2 – Інтеграція системи автентифікації в ЕПС

Важливою особливістю є інтеграція електронних платіжних систем із зовнішніми інформаційними сервісами, мобільними застосунками, банківськими системами та хмарними платформами. Така інтеграція забезпечує гнучкість і розширення функціональних можливостей, однак водночас ускладнює архітектуру системи та висуває додаткові вимоги до узгодженості протоколів обміну даними, захисту інформаційних потоків і контролю доступу.

Електронні платіжні системи є складними комп’ютерно-інтегрованими структурами з розгалуженими інформаційними зв’язками, для яких характерні високі вимоги до безпеки, надійності та швидкодії. Саме ці особливості обумовлюють необхідність удосконалення механізмів автентифікації

користувачів, зокрема шляхом впровадження систем технічного зору як елемента підвищення рівня захисту фінансових операцій.

1.2 Сучасні методи автентифікації користувачів

Забезпечення надійної автентифікації користувачів є ключовим елементом безпеки електронних платіжних систем. Автентифікація – це процес підтвердження особи користувача перед наданням доступу до інформаційних ресурсів або фінансових операцій. У сучасних електронних платіжних сервісах застосовуються різні методи автентифікації, які умовно можна поділити на парольні, багатофакторні та біометричні. У таблиці 1.4 наведено порівняльну характеристику основних методів автентифікації користувачів.

Таблиця 1.4 – Порівняння методів автентифікації користувачів

Критерій порівняння	Парольна автентифікація	Багатофакторна автентифікація (MFA)	Біометрична автентифікація
Принцип роботи	Перевірка знання користувачем секретного пароля або PIN-коду	Комбінація двох або більше факторів: знання (пароль), володіння (токен, телефон), властивість (біометрія)	Перевірка унікальних фізіологічних або поведінкових характеристик (обличчя, відбиток пальця, райдужка ока)
Рівень безпеки	Низький або середній	Високий	Високий
Стійкість до атак	Вразлива до	Значно підвищена	Висока, але можлива

Критерій порівняння	Парольна автентифікація	Багатофакторна автентифікація (MFA)	Біометрична автентифікація
	фішингу, brute-force, перехоплення	за рахунок декількох факторів	підробка (spoofing) без додаткового захисту
Зручність використання	Висока, проста реалізація	Середня (потребує додаткових дій користувача)	Висока (швидке розпізнавання без запам’ятовування паролів)
Необхідність додаткового обладнання	Ні	Можливе (смартфон, токен, смарт-карта)	Так (камера, сканер відбитків, сенсори)
Вартість впровадження	Низька	Середня	Вища (потрібне спеціалізоване обладнання та ПЗ)
Масштабованість	Висока	Висока	Середня (залежить від обчислювальних ресурсів)
Ризик компрометації	Високий (може бути викрадений або переданий)	Низький	Низький (біометричні дані складно передати третім особам)
Можливість відновлення доступу	Легке відновлення через зміну пароля	Можливе через резервні механізми	Ускладнене (біометричні дані незмінні)
Доцільність	Для базового	Для фінансових	Для швидкої та

Критерій порівняння	Парольна автентифікація	Багатофакторна автентифікація (MFA)	Біометрична автентифікація
застосування в платіжних системах	рівня доступу	операцій середнього та високого ризику	безпечної автентифікації в мобільному банкінгу та терміналах

Парольна автентифікація є найпоширенішим і найпростішим способом підтвердження особи. Вона базується на принципі «те, що користувач знає». До таких методів належать текстові паролі, PIN-коди та графічні ключі. Основною перевагою парольних методів є простота реалізації та відсутність необхідності у додатковому обладнанні. Водночас вони мають суттєві недоліки: користувачі часто створюють слабкі паролі, повторно використовують їх у різних системах або зберігають у незахищеному вигляді. Крім того, парольні системи є вразливими до фішингових атак, перехоплення даних та методів соціальної інженерії. У сучасних електронних платіжних системах парольна автентифікація рідко використовується як єдиний механізм захисту, оскільки її рівень безпеки не відповідає актуальним вимогам до фінансових операцій.

Багатофакторна автентифікація (MFA – Multi-Factor Authentication) передбачає використання двох або більше незалежних факторів підтвердження особи. Вона базується на поєднанні трьох основних категорій факторів: знання – те, що користувач знає (пароль, PIN-код); володіння – те, що користувач має (смартфон, токен, банківська картка); біометрія – те, ким користувач є (відбиток пальця, обличчя, голос). Найбільш поширеним прикладом є поєднання пароля та одноразового коду, що надсилається на мобільний телефон або генерується спеціальним додатком. Такий підхід значно підвищує рівень захисту, оскільки навіть у разі компрометації одного фактора зловмисник не зможе завершити автентифікацію без другого. Однак

багатофакторна автентифікація має певні недоліки: залежність від мобільного зв’язку, можливість перехоплення SMS-повідомлень, а також додаткові часові витрати для користувача. У контексті електронних платіжних систем важливо знайти баланс між рівнем безпеки та зручністю використання. Біометрична автентифікація базується на використанні унікальних фізіологічних або поведінкових характеристик людини. До фізіологічних ознак належать відбитки пальців, зображення обличчя, райдужна оболонка ока, геометрія руки; до поведінкових – голос, динаміка набору тексту, характер рухів.

Перевагою біометричних методів є їх висока унікальність і складність підробки. Крім того, вони забезпечують зручність для користувача, оскільки не потребують запам’ятовування паролів або використання додаткових пристроїв. Особливого поширення в електронних платіжних системах набуло розпізнавання облич, що реалізується за допомогою технологій комп’ютерного зору та нейронних мереж. Водночас впровадження біометрії потребує надійного захисту персональних даних, а також врахування можливих похибок розпізнавання. Для оцінювання ефективності біометричних систем застосовують показники точності, зокрема коефіцієнти помилкового прийняття (FAR – False Acceptance Rate) та помилкового відхилення (FRR – False Rejection Rate).

З наведеного аналізу можна зробити висновок, що найбільш перспективним напрямом розвитку систем автентифікації є поєднання біометричних методів із комп’ютерно-інтегрованими технологіями. Застосування технічного зору дозволяє автоматизувати процес розпізнавання особи та інтегрувати його у структуру електронної платіжної системи, що забезпечує підвищення рівня захисту фінансових операцій без ускладнення користувацького досвіду.

Сучасні електронні платіжні системи переходять від традиційних парольних методів до багатофакторних та біометричних рішень, серед яких особливе місце займають технології розпізнавання облич на основі

комп’ютерного зору. Саме це обґрунтовує доцільність розробки комп’ютерно-інтегрованої системи технічного зору для задач автентифікації.

1.3 Біометрична автентифікація на основі розпізнавання обличь

Біометрична автентифікація на основі розпізнавання облич є одним із найперспективніших напрямів розвитку систем захисту інформації в електронних платіжних системах. Її принцип ґрунтується на використанні унікальних анатомічних характеристик обличчя людини для підтвердження особи користувача. Технологія базується на методах комп’ютерного зору, цифрової обробки зображень та машинного навчання, що відповідає сучасним підходам до побудови комп’ютерно-інтегрованих систем.

Опишемо загальну структуру процесу розпізнавання облич. Процес автентифікації складається з послідовних етапів, що забезпечують отримання, оброблення та аналіз зображення.

1 етап – Захоплення зображення здійснюється за допомогою камери, вбудованої у смартфон, банкомат або термінал самообслуговування, з якої отримується цифрове зображення або відеопотік обличчя користувача.

На 2 етапі – Виявлення обличчя, алгоритм визначає на зображенні область, що містить обличчя. Застосовуються класичні методи (Haar-каскади, HOG) або сучасні глибокі нейронні мережі.

3 етап – Попередня обробка зображення передбачає нормалізацію яскравості, масштабування, вирівнювання обличчя відносно очей, усунення шумів, що підвищує точність подальшого розпізнавання.

На 4 етапі – Виділення ознак**,** формується вектор ознак, який відтворює собою компактне числове представлення унікальних характеристик обличчя. У сучасних системах використовуються згорткові нейронні мережі (CNN), які автоматично виділяють інформативні ознаки.

На 5 етапі – Порівняння з еталоном, отриманий вектор ознак порівнюється з шаблоном, збереженим у базі даних. Якщо ступінь подібності перевищує заданий поріг, система підтверджує автентичність користувача.

6 етап – Прийняття рішень.

На кожному етапі застосовуються відповідні алгоритмічні методи, що визначають точність та швидкодію системи (таблиця 1.5).

Таблиця 1.5 – Основні методи розпізнавання облич

Метод	Принцип роботи	Переваги	Недоліки
Eigenfaces (PCA)	Аналіз головних компонент зображення	Простота реалізації	Чутливість до освітлення
Fisherfaces (LDA)	Лінійний дискримінантний аналіз	Краща стійкість до варіацій	Обмежена масштабованість
LBPH	Локальні бінарні шаблони	Стійкість до змін освітлення	Менша точність порівняно з CNN
CNN (Deep Learning)	Згорткові нейронні мережі	Висока точність, автоматичне виділення ознак	Потреба у значних обчислювальних ресурсах

Існують різні підходи до побудови систем розпізнавання, які можна класифікувати за типом алгоритмів. У сучасних електронних платіжних системах найчастіше застосовуються методи на основі глибокого навчання, що забезпечують високий рівень точності навіть у складних умовах.

Проаналізуємо архітектуру комп’ютерно-інтегрованої системи. У межах КІС технічного зору модуль розпізнавання облич функціонує як складова загальної системи автентифікації електронної платіжної платформи. Типова структура включає модуль захоплення зображення; модуль оброблення та

аналізу зображень; базу біометричних шаблонів; модуль прийняття рішення; інтерфейс інтеграції з платіжною системою.

Біометричний модуль є складовою загальної платіжної інфраструктури та взаємодіє з сервером автентифікації і базою даних. Інтеграція здійснюється через API або сервіс-орієнтовану архітектуру (SOA), що дозволяє використовувати біометричний модуль як окремий сервіс у загальній інформаційній системі банку або фінансової установи.

Біометрична система автентифікації на основі технічного зору поєднує методи цифрової обробки сигналів, комп'ютерного зору, алгоритмічного моделювання та інтеграції програмно-апаратних засобів.

У таблиці 1.6 розмішено переваги та недоліки біометричних систем автентифікації. Перевагами таких систем є безконтактність, висока швидкодія, зручність для користувача, складність підробки. Біометрична система автентифікації на основі технічного зору не потребує фізичного дотику до пристрою, що особливо важливо для банкоматів та публічних терміналів. Процес ідентифікації займає частки секунди. Відсутня необхідність запам'ятовувати складні паролі. Сучасні алгоритми із перевіркою «живості» (liveness detection) значно ускладнюють використання фотографій або відео для обходу системи. Попри значні переваги, біометричні системи має певні обмеження, а саме залежність від умов освітлення та якості камери; можливі похибки через зміну зовнішності (окуляри, борода, макіяж); потреба у захисті біометричних шаблонів, оскільки біометричні дані є незмінними; етичні та правові аспекти зберігання персональних даних.

Таблиця 1.6 – Переваги та недоліки розпізнавання облич

Переваги	Недоліки
Безконтактність	Залежність від освітлення
Висока швидкодія	Потреба в обчислювальних ресурсах
Зручність для користувача	Ризик атак типу spoofing
Неможливість «забути» біометрію	Складність захисту персональних даних

Оцінювання якості роботи біометричної системи розпізнавання облич здійснюється за такими статистичними показниками, як FAR (ймовірність помилкового допуску сторонньої особи), FRR (ймовірність помилкової відмови законному користувачу), EER (точка рівності FAR та FRR, що характеризує точність системи), швидкодія алгоритму та обчислювальна складність (таблиця 1.7).

Для електронних платіжних систем критично важливим є мінімізація показника FAR, оскільки навіть поодинокий випадок несанкціонованого доступу може призвести до фінансових втрат.

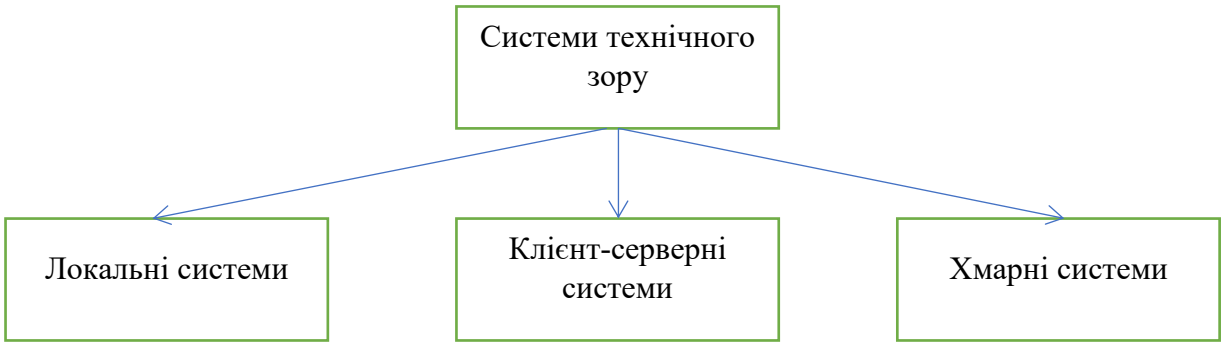
Таблиця 1.7 – Основні показники ефективності

Показник	Позначення	Характеристика
False Acceptance Rate	FAR	Ймовірність помилкового допуску сторонньої особи
False Rejection Rate	FRR	Ймовірність відмови законному користувачу
Equal Error Rate	EER	Точка рівності FAR та FRR
Accuracy	ACC	Загальна точність класифікації
Response Time	T	Час прийняття рішення

Біометрична автентифікація на основі розпізнавання облич є ефективним інструментом підвищення рівня безпеки електронних платіжних систем. Такий підхід забезпечує створення інтелектуальних систем керування доступом, які можуть бути інтегровані у фінансові, промислові та сервісні інфраструктури.

1.4 Аналіз існуючих систем технічного зору

Системи технічного зору є складовими комп'ютерно-інтегрованих технологій та призначені для автоматизованого отримання, оброблення й аналізу візуальної інформації з метою прийняття рішень без безпосереднього втручання людини. У контексті задач автентифікації в електронних платіжних системах СТЗ використовуються для ідентифікації особи за біометричними ознаками; перевірки «живості»; контролю доступу до банківських сервісів; моніторингу безпеки фінансових операцій. Сучасні системи технічного зору базуються на алгоритмах машинного навчання, глибоких нейронних мережах та високопродуктивних обчислювальних платформах. Аналіз існуючих СТЗ доцільно виконати за кількома ознаками: архітектура, сфера застосування, рівень інтелектуалізації та спосіб обробки даних. На рисунку 1.3 надано класифікацію систем технічного зору за архітектурою.



Рисунку 1.3 – Класифікація систем технічного зору за архітектурою

У таблиці 1.8 надано порівняння архітектур систем технічного зору.

Таблиця 1.8 – Порівняння архітектур СТЗ

Критерій	Локальна	Клієнт-серверна	Хмарна
Швидкодія	Висока	Середня	Залежить від мережі

Критерій	Локальна	Клієнт-серверна	Хмарна
Безпека даних	Висока	Середня	Залежить від провайдера
Масштабованість	Обмежена	Середня	Висока
Вартість впровадження	Низька	Середня	Змінна

У локальних системах обробка виконується безпосередньо на пристрої (смартфон, банкомат). Перевагами систем є швидкість, автономність, захист даних. До недоліків можна віднести обмежені обчислювальні ресурси.

У клієнт-серверних системах первинна обробка здійснюється на клієнті, розпізнавання – на сервері. Перевагами систем є баланс продуктивності та безпеки, недоліками – залежність від каналу зв’язку. У хмарних системах уся обробка відбувається в хмарній інфраструктурі. Перевагами таких систем є масштабованість, висока точність, недоліками – ризики витоку даних, затримки.

Технологічні рішення поділяються на традиційні алгоритмічні системи та системи на основі глибокого навчання. Ранні СТЗ базувалися на класичних алгоритмах Haar Cascade; HOG + SVM; PCA (Eigenfaces); LDA (Fisherfaces). Їх перевагами є простота реалізації, невисокі вимоги до ресурсів, недоліками – низька стійкість до змін освітлення, ракурсу, виразу обличчя.

Системи на основі глибокого навчання використовують згорткові нейронні мережі (CNN), що автоматично виділяють інформативні ознаки.

На рисунку 1.4 зображено узагальнену структуру нейромережевої системи розпізнавання.

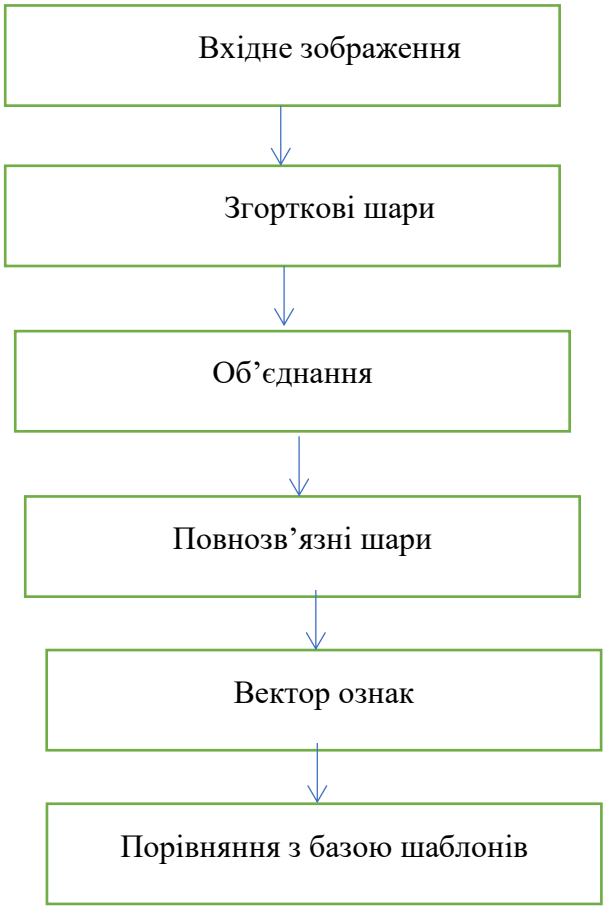


Рисунок 1.4 – Узагальнена структура нейромережевої системи розпізнавання

Такі системи демонструють точність понад 97–99 % за умов правильної навчальної вибірки.

У таблиці 1.9 порівнюються класичні та нейромережеві системи. У фінансових застосуваннях СТЗ повинні відповідати підвищеним вимогам безпеки, а саме, мінімальний FAR; перевірка «живості»; захист шаблонів; відповідність стандартам кібербезпеки.

Таблиця 1.9 – Порівняння класичних та нейромережевих систем

Критерій	Класичні методи	Нейромережеві методи
Точність	80–90 %	97–99 %
Стійкість до освітлення	Низька	Висока

Критерій	Класичні методи	Нейромережеві методи
Потреба у навчанні	Мінімальна	Значна
Обчислювальні ресурси	Низькі	Високі
Масштабованість	Обмежена	Висока

У таблиці 1.10 показані основні вимоги до СТЗ у фінансових системах. На рисунку 1.5 демонструється типова структура біометричної системи в банківському секторі.

На рисунку 1.5 – Типова структура біометричної системи в банківському секторі

Таблиця 1.10 – Основні вимоги до СТЗ у фінансових системах

Показник	Значення
FAR	≤ 0,1 %

Показник	Значення
FRR	≤ 1–3 %
Час відповіді	≤ 2 с
Доступність	≥ 99 %
Захист даних	Шифрування + TLS

Аналіз показує, що для задач автентифікації в електронних платіжних системах найбільш доцільним є використання нейромережевих систем технічного зору з клієнт-серверною або гібридною архітектурою. Це обумовлено високою точністю розпізнавання, можливістю реалізації перевірки «живості», гнучкістю інтеграції через API, масштабованістю при зростанні кількості користувачів, відповідністю сучасним стандартам безпеки.

У результаті аналізу існуючих систем технічного зору встановлено, що класичні алгоритмічні методи є недостатньо ефективними для фінансових систем; нейромережеві СТЗ забезпечують найвищу точність та адаптивність; оптимальною для електронних платіжних систем є клієнт-серверна або гібридна архітектура; критичними параметрами є мінімізація FAR та забезпечення кіберзахисту біометричних шаблонів. Отримані результати аналізу є підґрунтям для розробки власної комп’ютерно-інтегрованої системи технічного зору для задач автентифікації в електронних платіжних системах.

1.5 Формування вимог до комп’ютерно-інтегрованої системи автентифікації

Формування вимог до КІС автентифікації (див. рис. 1.6) є ключовим етапом проєктування, оскільки саме на цьому етапі визначаються функціональні можливості, технічні характеристики, показники надійності та безпеки майбутньої системи. У межах бакалаврської роботи розглядається система технічного зору, інтегрована з електронною платіжною системою,

призначена для біометричної автентифікації користувачів за обличчям. Тому вимоги формуються з урахуванням специфіки електронних платіжних систем; особливостей біометричної ідентифікації; принципів побудови комп'ютерно-інтегрованих систем; вимог інформаційної безпеки та захисту персональних даних.

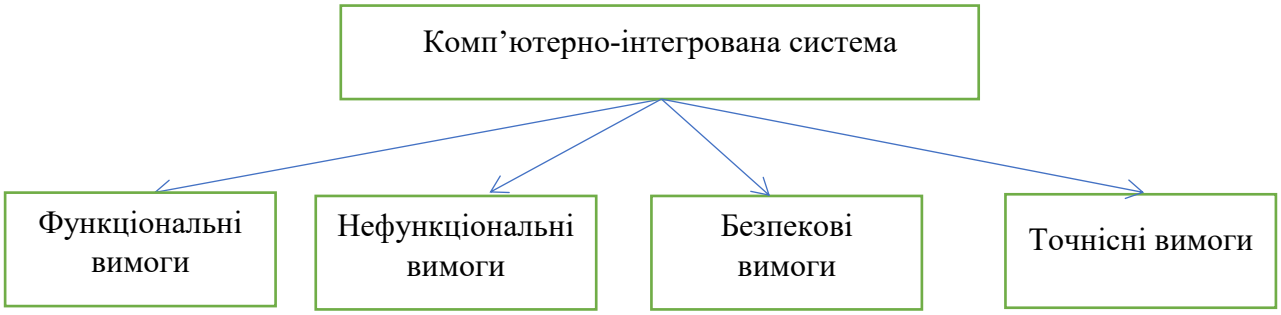


Рисунок 1.6 – Узагальнена структура вимог до системи

Функціональні вимоги (таблиця 1.11) визначають перелік задач, які повинна виконувати система, виходячи з її функцій. Основними функціями системи є захоплення зображення обличчя користувача з камери; попередня обробка зображення; детекція обличчя на зображенні; виділення ознак (формування біометричного шаблону); порівняння збереженого та поточного шаблонів; прийняття рішення про автентифікацію; передача результату до електронної платіжної системи; ведення журналу подій.

Таблиця 1.11 – Функціональні вимоги до системи

№	Функція	Опис	Результат виконання
1	Захоплення зображення	Отримання відеопотоку з камери	Кадр з обличчям
2	Детекція обличчя	Виявлення області обличчя	Координати ROI
3	Оброблення зображення	Нормалізація, масштабування	Підготовлене зображення
4	Розпізнавання	Порівняння з базою шаблонів	Коефіцієнт схожості

№	Функція	Опис	Результат виконання
5	Прийняття рішення	Порівняння з порогом	Доступ / Відмова
6	Інтеграція з ЕПС	Передача статусу автентифікації	Авторизація транзакції

Нефункціональні вимоги (таблиця 1.12) визначають якісні характеристики системи і складаються з вимог до безпеки, продуктивності, надійності. Вимоги до безпеки пов’язані із захистом біометричних шаблонів (шифрування); неможливістю відновлення зображення з шаблону; захистом каналу передачі даних (TLS/SSL); захистом від атак повторного відтворення та від підміни зображення. Вимоги до продуктивності стосуються часу автентифікації (не більше 1 –2 сек.), підтримки одночасної обробки декількох запитів; масштабованості при зростанні кількості користувачів. Вимоги до надійності чіпають безперервність роботи 24/7; відмовостійкість; збереження цілісності бази даних.

Таблиця 1.12 – Нефункціональні вимоги

Категорія	Вимога	Обґрунтування
Безпека	Шифрування шаблонів	Захист персональних даних
Продуктивність	Час відповіді ≤ 2 с	Комфорт користувача
Надійність	99 % доступності	Критичність платіжних операцій
Масштабованість	Підтимка >10000 користувачів	Можливість розширення системи

Оскільки система використовується в електронних платіжних системах, помилки автентифікації можуть призвести до фінансових втрат. У таблиці 1.13 надано значення цільових показників якості.

Таблиця 1.13 – Цільові показники якості

Показник	Рекомендоване значення
FAR	≤ 0,1 %
FRR	≤ 1–3 %
EER	≤ 1 %
Точність	≥ 97–99 %

З таблиці 1.13 можна зробити висновок, що для фінансових операцій критично важливо мінімізувати FAR, навіть якщо це призводить до незначного зростання FRR.

Розглянемо вимоги до апаратного забезпечення. Система повинна включати: веб-камеру або камеру мобільного пристрою; сервер або хмарну інфраструктуру для обробки; базу даних біометричних шаблонів; канал захищеного зв'язку. На рисунку 1.7 зображено схему інтеграції система автентифікації з електронною платіжною системою.

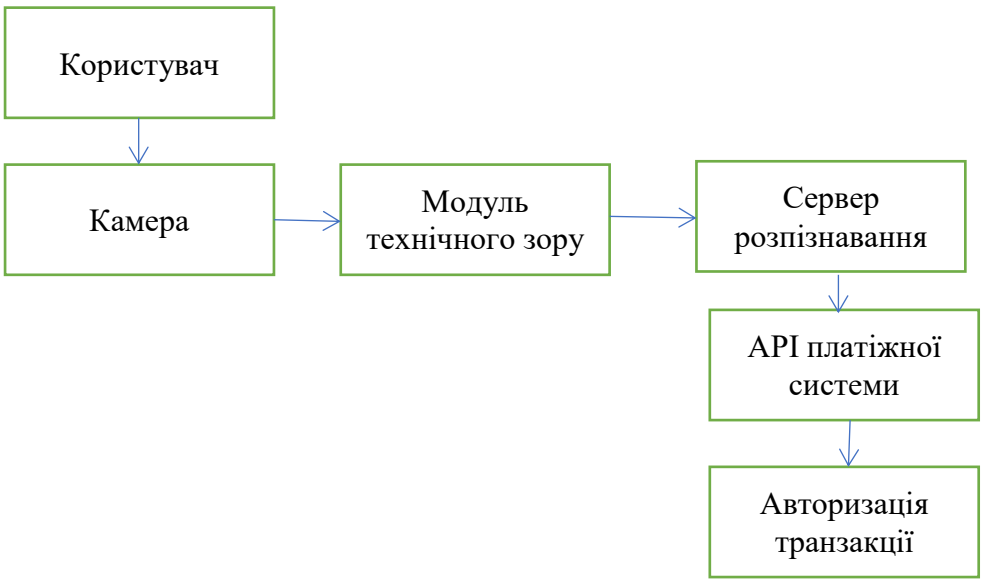


Рисунок 1.7 – Схема інтеграції системи автентифікації з електронною платіжною системою

Для інтеграції з електронною платіжною системою система автентифікації повинна працювати через API; підтримувати REST або SOAP-протоколи; забезпечувати журналювання операцій; підтримувати

двосторонній обмін даними. Інтеграція повинна бути незалежною від конкретної платіжної платформи та реалізована у вигляді окремого програмного модуля.

Ми сформували комплекс функціональних і нефункціональних вимог до комп'ютерно-інтегрованої системи автентифікації на основі технічного зору. Визначено показники точності, вимоги до безпеки, продуктивності та інтеграції з електронною платіжною системою. Запропоновані вимоги забезпечують високий рівень інформаційної безпеки; мінімізацію фінансових ризиків; швидкість і зручність користування; можливість масштабування системи. Сформований набір вимог є основою для подальшої розробки структурної та функціональної схеми комп'ютерно-інтегрованої системи технічного зору для задач автентифікації в електронних платіжних системах.

Висновок до розділу 1.

У розділі 1 проведено комплексний аналіз сучасних методів автентифікації та технологій технічного зору, що використовуються в електронних платіжних системах.

Розглянуто особливості функціонування електронних платіжних систем, їхню архітектуру, принципи взаємодії між клієнтською та серверною частинами, а також ключові вимоги до безпеки, надійності та швидкодії. Встановлено, що автентифікація користувача є критичним етапом процесу проведення фінансових операцій, оскільки саме на цьому рівні забезпечується запобігання несанкціонованому доступу та фінансовим втратам.

Проаналізовано сучасні методи автентифікації користувачів, зокрема парольні, багатофакторні та біометричні. Показано, що традиційні парольні механізми не забезпечують достатнього рівня захисту в умовах зростання кіберзагроз. Багатофакторна автентифікація підвищує рівень безпеки, проте ускладнює взаємодію з користувачем. Найбільш перспективним напрямом визначено біометричні методи, які базуються на унікальних фізіологічних

характеристиках людини. Детально розглянуто біометричну автентифікацію на основі розпізнавання облич.

Проаналізовано принцип роботи системи, етапи обробки зображення, показники точності (FAR, FRR, EER), а також переваги та обмеження даного підходу. Встановлено, що використання методів комп’ютерного зору та глибокого навчання дозволяє забезпечити високий рівень точності та швидкодії, що є критично важливим для фінансових застосувань.

Виконано аналіз існуючих систем технічного зору. Порівняно класичні алгоритмічні методи та сучасні нейромережеві підходи, а також розглянуто різні архітектури побудови систем (локальні, клієнт-серверні, хмарні). Обґрунтовано доцільність використання нейромережевих систем із клієнт-серверною або гібридною архітектурою для задач автентифікації в електронних платіжних системах.

Сформовано функціональні та нефункціональні вимоги до комп’ютерно-інтегрованої системи автентифікації. Визначено вимоги до точності, продуктивності, безпеки, масштабованості та інтеграції з електронною платіжною платформою. Особливу увагу приділено мінімізації показника помилкового допуску (FAR) та забезпеченню захисту біометричних даних.

У результаті виконаного аналізу обґрунтовано доцільність розробки комп’ютерно-інтегрованої системи технічного зору для біометричної автентифікації користувачів в електронних платіжних системах. Отримані результати створюють теоретичну та методологічну основу для подальшого проєктування структури, алгоритмічного забезпечення та програмної реалізації системи, що розглядається у наступних розділах роботи.

РОЗДІЛ 2. ПРОЄКТУВАННЯ КОМП'ЮТЕРНО-ІНТЕГРОВАНОЇ СИСТЕМИ ТЕХНІЧНОГО ЗОРУ

2.1 Загальна архітектура комп'ютерно-інтегрованої системи

Загальна архітектура КІС технічного зору визначає структуру взаємодії програмних і апаратних компонентів, принципи обробки даних та механізми інтеграції з електронною платіжною системою.

Метою проєктування архітектури є забезпечення високої точності біометричної автентифікації; мінімального часу прийняття рішення; захисту персональних даних; масштабованості та відмовостійкості; можливості інтеграції з існуючою ІТ-інфраструктурою. З урахуванням вимог, сформованих у попередньому розділі, доцільною є клієнт-серверна (гібридна) архітектура з елементами обробки на стороні клієнта та центральною серверною обробкою.

Архітектура КІС технічного зору складається з функціонально завершених модулів, кожен з яких виконує окрему задачу в загальному процесі автентифікації (див. табл 2.1).

Таблиця 2.1 – Основні компоненти системи

№	Компонент	Призначення	Особливості реалізації
1	Камера	Захоплення зображення	HD/Full HD, автофокус
2	Edge-модуль	Попередня обробка, детекція обличчя	Нормалізація, масштабування
3	Сервер розпізнавання	Виділення ознак, класифікація	CNN-модель
4	База шаблонів	Зберігання біометричних даних	Шифрування, хешування
5	API інтеграції	Обмін даними з ЕПС	REST, JSON
6	Модуль журналювання	Фіксація подій	Логи транзакцій

Попередня обробка виконується на клієнтському пристрої, що дозволяє зменшити обсяг переданих даних; підвищити швидкість реакції; зменшити навантаження на сервер. Основна частина розпізнавання реалізується на сервері, де доступні більші обчислювальні ресурси (GPU). На рисунку 2.1 зображено логічну схему функціонування.

Рисунок 2.1 – Логічна модель взаємодії модулів

Передача даних здійснюється через захищений канал (TLS). Біометричні шаблони зберігаються у вигляді векторів ознак, що унеможливлює

відновлення початкового зображення. Серверна частина може бути реалізована у вигляді окремого фізичного сервера; віртуалізованого середовища; контейнеризованої мікросервісної архітектури, що дозволяє горизонтально масштабувати систему при збільшенні кількості користувачів.

Кожен етап є окремим функціональним блоком, що дозволяє модернізувати систему без повної перебудови архітектури. Основні потоки даних систематизовано у таблицю 2.2.

Таблиця 2.2 – Основні потоки даних

Потік	Джерело	Призначення	Тип даних
Відеопотік	Камера	Edge-модуль	Зображення
Біометричний вектор	Сервер	База шаблонів	Числовий масив
Запит автентифікації	Клієнт	Сервер	JSON
Результат перевірки	Сервер	Платіжна система	Статус доступу

Архітектура реалізована мовою Python і включає:

- Клієнт (Edge) – захоплення зображення та попередня обробка
- Сервер (FastAPI) – виділення ознак, порівняння з шаблонами
- Базу шаблонів.

Серверна частина (FastAPI + Face Recognition) представлена Файлом server.py:

```
import uvicorn
import numpy as np
import face_recognition
import pickle
from fastapi import FastAPI, File, UploadFile
from fastapi.responses import JSONResponse

app = FastAPI()
```

```
DATABASE_FILE = "biometric_db.pkl"

# Завантаження бази шаблонів
try:
    with open(DATABASE_FILE, "rb") as f:
        biometric_db = pickle.load(f)
except:
    biometric_db = {}

# Збереження бази
def save_database():
    with open(DATABASE_FILE, "wb") as f:
        pickle.dump(biometric_db, f)

# Реєстрація користувача
@app.post("/register/{user_id}")
async def register(user_id: str, file: UploadFile = File(...)):
    image = face_recognition.load_image_file(file.file)
    encodings = face_recognition.face_encodings(image)

    if len(encodings) == 0:
        return JSONResponse({"status": "no face detected"}, status_code=400)

    biometric_db[user_id] = encodings[0]
    save_database()

    return {"status": "registered"}

# Автентифікація
```

```
@app.post("/authenticate")
async def authenticate(file: UploadFile = File(...)):
    image = face_recognition.load_image_file(file.file)
    encodings = face_recognition.face_encodings(image)

    if len(encodings) == 0:
        return JSONResponse({"status": "no face detected"}, status_code=400)

    unknown_encoding = encodings[0]

    for user_id, stored_encoding in biometric_db.items():
        matches = face_recognition.compare_faces(
            [stored_encoding], unknown_encoding, tolerance=0.5
        )

        if matches[0]:
            return {"status": "access granted", "user": user_id}

    return {"status": "access denied"}



if __name__ == "__main__":
    uvicorn.run("server:app", host="0.0.0.0", port=8000, reload=True)
```

Клієнтська частина (Edge-модуль) представлена Файлом: client.py

```
import cv2
import requests

SERVER_URL = "http://127.0.0.1:8000"
```

```
def capture_image():
    cap = cv2.VideoCapture(0)
    ret, frame = cap.read()
    cap.release()

    if not ret:
        raise Exception("Camera error")

    filename = "capture.jpg"
    cv2.imwrite(filename, frame)
    return filename


def register_user(user_id):
    image_path = capture_image()

    with open(image_path, "rb") as f:
        response = requests.post(
            f"{SERVER_URL}/register/{user_id}",
            files={"file": f}
        )

    print(response.json())


def authenticate():
    image_path = capture_image()

    with open(image_path, "rb") as f:
```

```
        response = requests.post(
            f"{SERVER_URL}/authenticate",
            files={"file": f}
        )

    print(response.json())


if __name__ == "__main__":
    print("1 - Register")
    print("2 - Authenticate")
    choice = input("Select option: ")

    if choice == "1":
        user_id = input("Enter user ID: ")
        register_user(user_id)
    elif choice == "2":
        authenticate()
```

Встановлення залежностей

pip install fastapi uvicorn face-recognition opencv-python requests numpy

Таблиця 2.3 – Логіка відповідності архітектурі

Архітектурний компонент	Реалізація у коді
Камера (Edge)	OpenCV (client.py)
Попередня обробка	Face detection всередині face_recognition
Сервер розпізнавання	FastAPI + face_recognition
База шаблонів	pickle (biometric_db.pkl)
API інтеграції	REST endpoints (/register, /authenticate)

Користувач проходить реєстрацію (створюється embedding). Під час автентифікації клієнт захоплює зображення, надсилає його на сервер, сервер генерує вектор ознак, виконується порівняння з базою, повертається статус доступу.

Перевагами запропонованої архітектури є висока точність завдяки використанню нейромережевих моделей; швидкодія за рахунок попередньої обробки на клієнті; захист персональних даних через шифрування та ізоляцію серверної частини; гнучкість масштабування; можливість інтеграції з різними електронними платіжними платформами.

Розроблена загальна архітектура КІС технічного зору для задач біометричної автентифікації в електронних платіжних системах дозволяє ефективно інтегрувати модуль технічного зору з платіжною інфраструктурою та створює основу для подальшого проєктування алгоритмічного і програмного забезпечення системи.

2.2 Структурна схема системи та опис її модулів

Структурна схема КІС технічного зору відображає взаємозв’язки між основними функціональними модулями та послідовність обробки даних у процесі біометричної автентифікації користувача. Система реалізує поетапну обробку вхідної візуальної інформації з подальшим прийняттям рішення щодо надання доступу до електронної платіжної системи (див. рис. 2.2).

Кожен модуль виконує окрему функціонально завершену задачу, що дозволяє забезпечити модульність, масштабованість і можливість модернізації системи.

Модуль захоплення зображення забезпечує отримання цифрового зображення або відеопотоку обличчя користувача з апаратного пристрою (веб-камера, камера смартфона, камера банкомата). Основними функціями модулю

захоплення зображення є ініціалізація камери; налаштування параметрів зйомки (роздільна здатність, фокус, експозиція); формування кадру для подальшої обробки; передача зображення до наступного модуля. У таблиці 2.4 розміщено вхідні та вихідні дані модулю захоплення зображення.

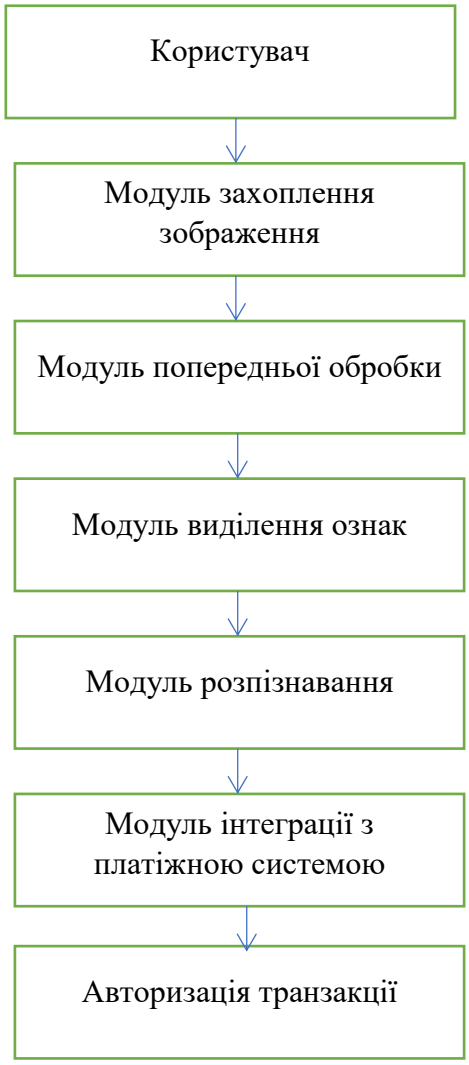


Рисунок 2.2 – Структурна схема КІС автентифікації

Таблиця 2.4 – Вхідні та вихідні дані модулю захоплення зображення

Параметр	Опис
Вхід	Сигнал з камери
Вихід	Цифрове зображення (RGB-матриця)

Модуль захоплення зображення повинен забезпечувати достатню якість зображення для коректної роботи алгоритмів розпізнавання. Бажана роздільна здатність – не менше 640×480 пікселів, доцільно реалізувати автоматичну перевірку наявності обличчя в кадрі.

Модуль попередньої обробки виконує підготовку зображення до виділення ознак, що дозволяє підвищити точність розпізнавання та зменшити вплив зовнішніх факторів. Провідними функціями модулю є детекція обличчя; виділення області інтересу (ROI); нормалізація освітлення; масштабування; вирівнювання обличчя відносно очей; зменшення шумів. У таблиці 2.5 розміщено вхідні та вихідні дані модулю попередньої обробки.

Таблиця 2.5 – Вхідні та вихідні дані модулю попередньої обробки.

Параметр	Опис
Вхід	Цифрове зображення
Вихід	Нормалізоване зображення обличчя

Попередня обробка мінімізує вплив різної інтенсивності освітлення; нахилу голови; масштабних відмінностей; цифрового шуму, що дозволяє забезпечити стабільність роботи системи у реальних умовах експлуатації.

Модуль виділення ознак формує компактне числове представлення обличчя (вектор ознак або embedding), що використовується для подальшого порівняння. Основними функціями модулю виділення ознак є обробка зображення згортковою нейронною мережею; формування вектора ознак фіксованої розмірності; передача вектора до модуля розпізнавання. У таблиці 2.6 розміщено вхідні та вихідні дані модулю виділення ознак.

Таблиця 2.6 – Вхідні та вихідні дані модулю виділення ознак

Параметр	Опис
Вхід	Нормалізоване зображення
Вихід	Вектор ознак (наприклад, 128 або 512 значень)

Нейронна мережа автоматично визначає такі інформативні характеристики обличчя, як геометрія; відстані між ключовими точками; текстурні особливості. Вектор ознак не містить безпосереднього зображення, що підвищує рівень захисту персональних даних.

Модуль розпізнавання здійснює порівняння отриманого вектора ознак із шаблонами, збереженими в базі даних, та приймає рішення про автентифікацію. Головними функціями модулю розпізнавання є завантаження еталонних шаблонів; обчислення метрики відстані (Euclidean, Cosine); порівняння з пороговим значенням; формування рішення (доступ/відмова). У таблиці 2.7 розміщено вхідні та вихідні дані модулю розпізнавання.

Таблиця 2.7 – Вхідні та вихідні дані модулю розпізнавання.

Параметр	Опис
Вхід	Поточний вектор ознак
Вихід	Рішення про автентифікацію

Відповідно до алгоритму роботи обчислюється відстань між векторами. Якщо відстань < встановленого порогу – доступ надається. Якщо відстань ≥ порогу – доступ забороняється. Коректний вибір порогового значення дозволяє мінімізувати показник FAR при збереженні прийнятного FRR.

Модуль інтеграції забезпечує обмін даними між системою технічного зору та електронною платіжною системою. Центральними функціями модулю інтеграції є формування запиту автентифікації; передача результату через API; журналювання операцій; обробка відповіді платіжної системи.

У таблиці 2.8 розміщено вхідні та вихідні дані модулю інтеграції. Особливостями реалізації модулю інтеграції є використання REST API; передача даних у форматі JSON; застосування захищеного протоколу HTTPS; підтримка механізмів журналювання та аудиту.

Таблиця 2.8 – Вхідні та вихідні дані модулю інтеграції

Параметр	Опис
Вхід	Результат розпізнавання
Вихід	Статус авторизації транзакції

Запропонована модульна структура забезпечує послідовність та логічність обробки даних; можливість модернізації окремих компонентів; високий рівень безпеки; інтеграцію з електронною платіжною системою. У таблиці 2.9 узагальнили інформацію щодо модулів.

Таблиця 2.9 – Функціональна характеристика модулів системи

Модуль	Основна задача	Тип обробки	Рівень відповідальності
Захоплення зображення	Отримання кадру	Апаратна	Якість даних
Попередня обробка	Підготовка зображення	Алгоритмічна	Стабільність
Виділення ознак	Формування embedding	Нейромережева	Унікальність
Розпізнавання	Порівняння шаблонів	Математична	Безпека
Інтеграція	Передача результату	Програмна	Узгодженість систем

Структурна організація системи відповідає вимогам до сучасних комп’ютерно-інтегрованих технологій та створює основу для подальшої алгоритмічної та програмної реалізації.

2.3 Інформаційні потоки та інтеграційні зв’язки

Інформаційні потоки КІС технічного зору визначають порядок передачі, обробки та зберігання даних між її функціональними модулями, а також взаємодію із зовнішніми інформаційними системами, зокрема електронною платіжною платформою. Раціональна організація інформаційних потоків забезпечує мінімізацію затримок при автентифікації; захист персональних даних; узгодженість роботи модулів; відмовостійкість та масштабованість системи. У межах розробленої архітектури реалізується багаторівнева схема передачі даних: від клієнтського пристрою до серверної частини та далі до платіжної системи. У системі можна виділити такі п’ять ключових інформаційних потоків, як потік візуальних даних, потік біометричних ознак, потік запитів автентифікації, потік результатів перевірки, потік службових та журналюючих даних (див. таблиця 2.10).

Таблиця 2.10 – Основні інформаційні потоки системи

№	Назва потоку	Джерело	Приймач	Тип даних	Рівень захисту
1	Візуальний потік	Камера	Модуль попередньої обробки	Зображення (RGB)	Локальний
2	Потік ознак	Модуль виділення ознак	Модуль розпізнавання	Вектор (embedding)	Внутрішній
3	Запит автентифікації	Клієнт	Сервер	JSON-запит	TLS
4	Результат перевірки	Сервер	Платіжна система	Статус (Access/Denied)	TLS
5	Лог-потік	Усі модулі	Система журналювання	Текстові записи	Обмежений доступ

Схема інформаційних потоків (див. рис. 2.3) відображає логічну послідовність передавання та обробки інформації в комп’ютерно-інтегрованій системі біометричної автентифікації. Схема демонструє, як візуальні дані трансформуються у рішення про авторизацію та передаються до платіжної інфраструктури. Розглянемо детально кожний етап.

1 етап Користувач → Модуль захоплення зображення.

Процес починається з ініціювання операції користувачем (наприклад, підтвердження платежу). Камера або інший сенсор формує первинний візуальний потік у вигляді цифрового зображення. На цьому етапі формується матриця пікселів RGB; можливе стиснення зображення; дані передаються у внутрішній буфер системи. Цей потік є найбільш об’ємним за розміром серед усіх інформаційних потоків.

2 етап Модуль захоплення → Модуль попередньої обробки.

Зображення передається до модуля попередньої обробки, де виконуються нормалізація освітлення; масштабування; вирівнювання обличчя; фільтрація шумів. Метою цього етапу є підготовка зображення до стабільного та точного виділення біометричних ознак. Тут зменшується вплив зовнішніх факторів (освітлення, ракурс, шум).

3 етап Модуль попередньої обробки → Модуль виділення ознак.

Після нормалізації система переходить до перетворення зображення у вектор ознак (embedding). На цьому етапі зображення подається на вхід нейронної мережі; формується числовий вектор фіксованої розмірності; вектор є компактним математичним представленням біометрії користувача. Цей потік значно менший за обсягом, ніж вихідне зображення, що оптимізує передачу та зберігання.

4 етап Модуль виділення ознак → Модуль розпізнавання.

Вектор ознак передається до модуля розпізнавання, де виконується порівняння з еталонними шаблонами; обчислення метрики схожості (косинусна відстань або евклідова відстань); прийняття рішення про

відповідність. Результатом є логічний статус успішна автентифікація; відмова в доступі.

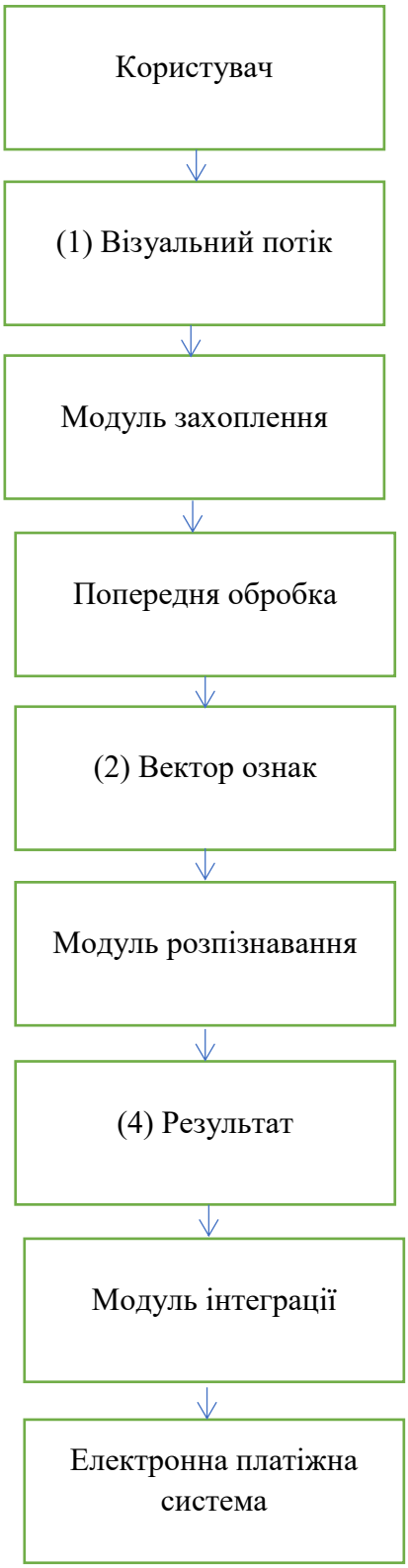


Рисунок 2.3 – Схема інформаційних потоків системи

5 етап Модуль розпізнавання → Модуль інтеграції.

Сформоване рішення передається до модуля інтеграції з платіжною системою. На цьому етапі формується структурований запит (наприклад, JSON); додається ідентифікатор транзакції; забезпечується шифрування каналу передачі (TLS).

6 етап Модуль інтеграції → Платіжна система.

Останній інформаційний потік спрямований до зовнішньої електронної платіжної інфраструктури. Передається статус авторизації; службова інформація транзакції; часові мітки. Платіжна система на основі отриманого статусупідтверджує транзакцію або відхиляє її.

Рисунок 2.4 демонструє структуровану модель руху даних у системі, де кожний інформаційний потік має чітко визначене джерело та приймач; змінює форму представлення даних; зменшує обсяг інформації; підвищує рівень абстракції.

Схема має логічні особливості, пов’язані із послідовністю обробки, зменшенням об’єму даних, розподілом функцій, ізоляцією зовнішньої інтеграції, захистом конфіденційності. Послідовність обробки передбачає, що дані проходять через систему поетапно без повернення до попередніх блоків. Зменшення об’єму даних відбувається від зображення до компактного вектора ознак. Кожний модуль виконує чітко визначене завдання.

Внутрішні зв’язки реалізуються між модулями системи технічного зору. Вони можуть бути локальними (у межах одного процесу); міжпроцесними; мережевими (у клієнт-серверній архітектурі). Система має певні особливості внутрішніх потоків, а саме, передача зображень відбувається у форматі матриць пікселів; передача векторів ознак здійснюється у вигляді числових масивів; рішення про автентифікацію формується як логічне значення або статус-код. З метою оптимізації швидкодії зображення можуть стискатися перед передачею на сервер, а обчислення векторів ознак частково виконуватись на клієнті (Edge-обробка).

Модуль інтеграції забезпечує взаємодію з електронною платіжною системою через програмний інтерфейс (API). Основними інтеграційними

механізмами (див. табл. 2.11) є REST API; HTTPS-протокол; JSON-формат повідомлень; токен-автентифікація (JWT); журналювання транзакцій.

Таблиця 2.11 – Інтеграційні параметри взаємодії

Параметр	**Значення**
Протокол	HTTPS
Формат даних	JSON
Метод передачі	POST/GET
Тип відповіді	Статус авторизації
Безпека	TLS + токен доступу

Послідовність передачі даних при транзакції наступна:

1. Користувач ініціює операцію
2. Камера захоплює зображення
3. Попередня обробка
4. Формування вектора ознак
5. Передача на сервер (TLS)
6. Порівняння з базою шаблонів
7. Формування рішення
8. Передача статусу до платіжної системи
9. Авторизація або відмова

Такий механізм забезпечує мінімальну затримку та високий рівень безпеки.

Платіжна система взаємодіє лише з модулем інтеграції, що підвищує безпеку. «Сирі» зображення не передаються до платіжної системи.

З огляду на використання біометричних даних, особлива увага приділяється захисту інформаційних потоків. Основними заходами захисту є шифрування каналів передачі (TLS 1.2+); зберігання не зображень, а лише векторів ознак; хешування і шифрування бази шаблонів; обмеження кількості спроб автентифікації; журналювання подій. Захист реалізується як на

мережевому рівні, так і на рівні прикладного програмного забезпечення. Організація інформаційних потоків у системі забезпечує: чітку послідовність обробки даних; розподіл функціонального навантаження між модулями; безпечну передачу конфіденційної інформації; інтеграцію з електронною платіжною інфраструктурою. Схема відображає повний цикл від біометричного захоплення → до фінансової авторизації, забезпечуючи одночасно ефективність, масштабованість та інформаційну безпеку системи.

2.4 Моделювання процесу автентифікації

Моделювання процесу автентифікації виконується з метою формалізації алгоритму роботи системи, аналізу її поведінки в різних умовах та оцінювання ефективності прийняття рішень. Формальна модель дозволяє описати послідовність операцій; визначити часові параметри процесу; оцінити ймовірність помилок; дослідити вплив порогових значень на точність розпізнавання; оптимізувати взаємодію з платіжною інфраструктурою.

Процес автентифікації розглядається як сукупність взаємопов'язаних етапів перетворення даних від моменту ініціювання транзакції до формування рішення про доступ.

Нехай I – вхідне зображення користувача; P(I) – результат попередньої обробки; F(P(I))) – функція виділення ознак; v – вектор біометричних ознак; v_i – еталонний вектор з бази даних; d(v,v_i) – метрика відстані; T – порогове значення прийняття рішення. Тоді рішення автентифікації визначається як:

$$Auth = \begin{cases} 1, & \text{якщо } d(\mathbf{v}, \mathbf{v_i}) \leq T \\ 0, & \text{якщо } d(\mathbf{v}, \mathbf{v_i}) > T \end{cases} \quad (2.1)$$

де 1 – успішна автентифікація; 0 – відмова в доступі.

Процес автентифікації зводиться до задачі порівняння векторів ознак у багатовимірному просторі. Функціональна модель процесу автентифікації зображена на рисунку 2.5

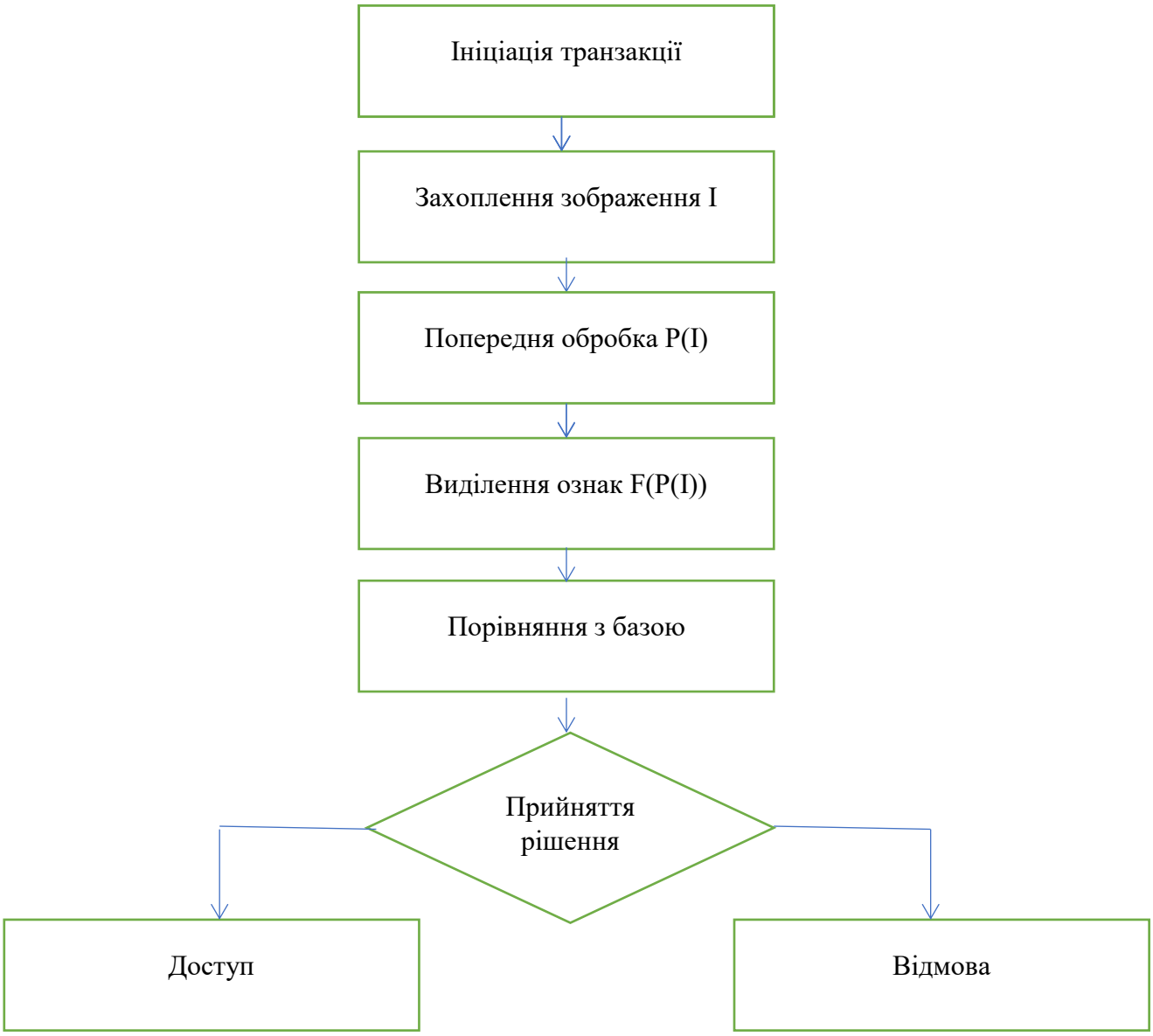


Рисунок 2.4 – Функціональна модель процесу автентифікації

Рисунок 2.4 демонструє повний функціональний цикл автентифікації: ініціація → отримання біометричних даних → математичне представлення → порівняння → логічне рішення → результат.

Модель відображає логічну послідовність перетворення вхідних даних у фінальне рішення про надання або відмову в доступі. Модель демонструє функціональну структуру процесу автентифікації без деталізації внутрішніх

алгоритмів, зосереджуючись на потоках обробки інформації. Розглянемо кожний етап детально.

1етап Ініціація транзакції.

Процес починається з дії користувача – наприклад, підтвердження платежу або запиту доступу до системи. На цьому етапі формується запит на проведення автентифікації. Система переходить із режиму очікування до активного режиму обробки.

2 етап Захоплення зображення III

Камера або інший сенсор формує цифрове зображення обличчя користувача. Це первинні «сирі» дані, які ще не придатні для безпосереднього порівняння. Формується матриця пікселів; можливе автоматичне визначення обличчя; забезпечується контроль якості зображення.

3 етап Попередня обробка P(I)

На цьому етапі виконується підготовка зображення до аналізу з метою мінімізувати вплив зовнішніх факторів та привести зображення до стандартизованого вигляду, а саме, нормалізація освітлення; масштабування; вирівнювання відносно осі; зменшення шумів.

4 етап Виділення ознак F(P(I))

Оброблене зображення подається на вхід алгоритму (зазвичай нейронної мережі), який формує вектор ознак – компактне числове представлення біометричних характеристик. Результатом є вектор фіксованої розмірності; зменшення обсягу даних; перехід від графічного до математичного представлення.

5 етап Порівняння з базою

Отриманий вектор порівнюється з еталонними шаблонами, що зберігаються в базі даних. Виконується обчислення метрики відстані; оцінка ступеня схожості; перевірка відповідності пороговому значенню. Цей етап є критичною точкою прийняття рішення.

6 етап Прийняття рішення

На основі результатів порівняння система формує один із двох варіантів Доступ – якщо рівень схожості перевищує встановлений поріг; Відмова – якщо умова не виконується. Цей блок логічно поділяє модель на дві гілки, що відображено на схемі. У разі позитивного результату система передає сигнал на виконання транзакції (наприклад, оплату). У разі відмови – інформує користувача та може запропонувати повторну спробу.

Функціональна модель має такі характеристики, як послідовність (етапи виконуються один за одним); детермінованість структури (чітко визначений порядок блоків); наявність точки розгалуження (після прийняття рішення); відсутність зайвих зворотних зв’язків, що спрощує реалізацію.

Модель дозволяє формалізувати структуру алгоритму; визначити ключові етапи оптимізації; оцінити вплив кожного блоку на загальну продуктивність системи. Функціональна модель є базою для програмної реалізації та подальшого математичного аналізу процесу біометричної автентифікації.

Процес автентифікації є стохастичним, оскільки можливі помилки двох типів:

False Acceptance Rate (FAR) – ймовірність помилкового прийняття;

False Rejection Rate (FRR) – ймовірність помилкової відмови.

Ймовірність правильного рішення розраховується за формулою:

$P_{correct}=1-(FAR+FRR)$	(2.2)

Оптимальне значення порогу T визначається в точці рівності:

$FAR=FRR$	(2.3)

що відповідає показнику EER (Equal Error Rate).

Загальний час автентифікації визначається як:

$t_{total}=t_{capture}+t_{preprocess}+t_{feature}+t_{match}+t_{integration}$	(2.4)

де $t_{capture}$ – час захоплення зображення;

$t_{preprocess}$ – час попередньої обробки;

$t_{feature}$ – час формування вектора ознак;

t_{match} – час порівняння;

$t_{integration}$ – час передачі результату до платіжної системи.

Для забезпечення зручності користування виконується умова:

$t_{total} \leq 2$ с	(2.5)

що відповідає вимогам до сучасних платіжних систем.

Процес автентифікації можна представити у вигляді скінченного автомата станів.

S0 – Очікування

S1 – Захоплення

S2 – Обробка

S3 – Порівняння

S4 – Рішення

S5 – Передача результату

S6 – Завершення

Перехід між станами відбувається послідовно. У випадку помилки можливе повернення до стану S1.

Взаємодія з платіжною системою моделюється як клієнт-серверний процес: Система формує запит автентифікації. Запит передається через захищений канал. Платіжна система отримує статус. Виконується фінансова операція. Інтеграційна модель передбачає асинхронну передачу повідомлень із підтвердженням доставки.

Моделювання показує, що процес автентифікації є послідовним; багаторівневим; стохастичним; часово обмеженим; інтегрованим із зовнішніми системами. Формалізація дозволяє визначити критичні точки затримки; оптимізувати порогові параметри; підвищити точність розпізнавання; забезпечити надійну інтеграцію з платіжною інфраструктурою.

Математична та функціональна моделі процесу автентифікації створюють основу для подальшої оптимізації та практичної реалізації комп’ютерно-інтегрованої системи біометричної ідентифікації.

Висновок до розділу 2.

У розділі 2 було здійснено комплексне проєктування комп’ютерно-інтегрованої системи технічного зору з урахуванням сучасних вимог до продуктивності, надійності, масштабованості та безпеки.

Визначено загальну архітектуру системи, що базується на модульному принципі побудови та передбачає чітке розмежування функціональних рівнів: збору даних, обробки зображень, прийняття рішень і взаємодії з користувачем. Такий підхід забезпечує гнучкість конфігурації та можливість подальшої модернізації системи.

Розроблено структурну схему системи та детально описано її основні модулі, зокрема модуль захоплення зображення, модуль попередньої обробки, модуль аналізу та розпізнавання, базу даних і інтерфейс взаємодії. Визначено їх функціональне призначення та взаємозв’язки, що дозволило сформувати цілісну логічну модель роботи системи.

Досліджено інформаційні потоки та інтеграційні зв’язки між компонентами системи. Описано механізми передавання, обробки та збереження даних, що забезпечують узгоджену та безперебійну роботу всіх підсистем. Особливу увагу приділено синхронізації процесів і забезпеченню цілісності даних.

Виконано моделювання процесу автентифікації як ключового функціонального сценарію системи. Побудована модель дозволила формалізувати алгоритм роботи системи під час ідентифікації користувача, визначити можливі стани, переходи та умови прийняття рішень, що підвищує ефективність та надійність реалізації.

РОЗДІЛ 3. ПРОГРАМНА РЕАЛІЗАЦІЯ КОМП'ЮТЕРНО-ІНТЕГРОВАНОЇ СИСТЕМИ ТЕХНІЧНОГО ЗОРУ

3.1 Опис програмної реалізації системи технічного зору

Програмна реалізація комп'ютерно-інтегрованої системи технічного зору для задач автентифікації в електронних платіжних системах спрямована на забезпечення швидкої, точної та безпечної ідентифікації користувача за біометричними ознаками обличчя. Розробка виконана з урахуванням вимог до продуктивності, масштабованості, захищеності персональних даних та можливості інтеграції з електронними платіжними сервісами.

Для реалізації системи використано мову програмування Python завдяки її широким можливостям у сфері комп'ютерного зору та машинного навчання.

Обробка зображень та базові операції комп'ютерного зору реалізовані із застосуванням бібліотеки OpenCV, яка забезпечує ефективні алгоритми фільтрації, нормалізації, перетворення кольорових просторів і роботи з відеопотоком.

Для побудови моделі розпізнавання облич використано фреймворк глибинного навчання TensorFlow, що дозволяє створювати та оптимізувати нейронні мережі для задач класифікації та верифікації.

Для організації серверної частини та створення REST API застосовано вебфреймворк Flask, який забезпечує взаємодію між клієнтською частиною системи та платіжним сервісом.

Збереження даних користувачів та біометричних шаблонів реалізовано із використанням реляційної системи керування базами даних PostgreSQL.

Модуль захоплення зображення забезпечує отримання відеопотоку з камери пристрою користувача. Виконується контроль якості кадру (освітлення, чіткість, положення обличчя). У разі невідповідності параметрів система ініціює повторне захоплення зображення.

Модуль попередньої обробки здійснює перетворення зображення в необхідний формат; нормалізацію яскравості та контрастності; масштабування

до фіксованого розміру; виділення області обличчя. Попередня обробка підвищує точність подальшого розпізнавання.

У модулі детекції та розпізнавання детекція обличчя виконується за допомогою алгоритмів, що дозволяють визначити координати обличчя на зображенні. Після цього формується вектор ознак (embeddings), який порівнюється з еталонним шаблоном, збереженим у базі даних. Для підвищення надійності використовується механізм порогового значення схожості, що визначає допустимий рівень відхилення між векторами ознак.

Модуль автентифікації приймає рішення про підтвердження або відхилення особи на основі результатів порівняння. У разі успішної ідентифікації формується токен доступу для подальшого здійснення платіжної операції. У випадку невдалої спроби передбачено механізм обмеження кількості повторних запитів.

У модулі інтеграції з платіжною системою інтеграція реалізована через REST API, що забезпечує обмін зашифрованими даними між системою технічного зору та електронною платіжною платформою. Передача інформації здійснюється із застосуванням протоколу HTTPS, що гарантує захист персональних даних.

У системі реалізовано такі механізми безпеки, як зберігання не самих зображень, а математичних векторів ознак; хешування службових даних; шифрування каналів передачі інформації; журналювання подій автентифікації; обмеження кількості невдалих спроб входу, що дозволяє мінімізувати ризики несанкціонованого доступу та відповідати вимогам інформаційної безпеки в електронних платіжних системах.

Програмна реалізація КІС технічного зору побудована на сучасних інструментах комп’ютерного зору та машинного навчання і забезпечує ефективну біометричну автентифікацію користувачів в електронних платіжних системах. Модульна архітектура, використання нейронних мереж та захищених протоколів обміну даними створюють основу для надійної, масштабованої та безпечної експлуатації системи в реальних умовах.

3.2 Реалізація алгоритмів розпізнавання облич

Реалізація алгоритмів розпізнавання облич у межах комп'ютерно-інтегрованої системи технічного зору для задач автентифікації в електронних платіжних системах є ключовим етапом програмної реалізації, оскільки саме від точності та швидкодії цього модуля залежить надійність підтвердження особи користувача. У розробленій системі застосовано сучасні методи глибинного навчання, які забезпечують високу стійкість до змін освітлення, ракурсу, часткових перекриттів обличчя та вікових змін.

Розглянемо загальну структуру алгоритму розпізнавання. Процес розпізнавання облич складається з 6 послідовних етапів.

1 етап Детекція обличчя на зображенні.

Для локалізації обличчя на зображенні використано алгоритми бібліотеки OpenCV, які реалізують каскадні класифікатори та глибокі нейронні мережі для виявлення об'єктів. На цьому етапі визначаються координати області обличчя (bounding box). У випадку виявлення кількох облич система виконує перевірку на наявність лише одного користувача в кадрі, що є вимогою безпеки для електронних платіжних операцій.

2 етап Вирівнювання та нормалізація зображення.

Після детекції здійснюється нормалізація зображення, а саме, масштабування до фіксованого розміру; перетворення до необхідного кольорового простору; вирівнювання обличчя за ключовими точками (очі, ніс, рот). Вирівнювання дозволяє мінімізувати вплив нахилу голови та покращити якість формування ознак.

3 етап Виділення ознак (feature extraction) за допомогою нейронної мережі

Для формування унікального біометричного шаблону використано згорткову нейронну мережу, реалізовану на основі фреймворку TensorFlow.

4 етап Формування вектора ознак (embedding).

Мережа перетворює зображення обличчя у багатовимірний вектор ознак (embedding), що відображає індивідуальні характеристики користувача. Такий підхід забезпечує інваріантність до освітлення та часткових змін зовнішності; високу точність розпізнавання; компактність представлення даних (замість збереження зображення зберігається числовий вектор). Розмірність вектора ознак визначається архітектурою моделі та становить фіксовану кількість числових параметрів.

5 етап Порівняння з еталонним шаблоном у базі даних.

Порівняння отриманого вектора з еталонним шаблоном у базі даних здійснюється за допомогою метрики косинусної подібності або евклідової відстані. Обчислюється значення відстані між векторами. Якщо відстань менша за встановлений поріг – автентифікація вважається успішною; якщо перевищує порогове значення – доступ відхиляється.

6 етап Прийняття рішення щодо автентифікації.

Порогове значення визначено експериментально з урахуванням компромісу між показниками FAR (False Acceptance Rate) та FRR (False Rejection Rate), що є критично важливим для фінансових систем.

З метою забезпечення безпеки в алгоритм додатково інтегровано перевірку «живості» (liveness detection) для запобігання використанню фотографій або відеозаписів; обмеження кількості невдалих спроб; журналювання результатів автентифікації; контроль часу відповіді алгоритму. Така інтеграція дозволяє підвищити стійкість системи до шахрайських дій у середовищі електронних платіжних сервісів.

З метою забезпечення роботи в режимі реального часу реалізовано попередню оптимізацію нейронної моделі; використання апаратного прискорення (GPU за наявності); асинхронну обробку запитів на серверному рівні. Середній час обробки одного запиту автентифікації відповідає вимогам електронних платіжних систем та не створює затримок під час проведення транзакцій. Кожен з етапів реалізований окремою функціональною

підсистемою, що забезпечує модульність і масштабованість програмного рішення.

3.3 Програмна реалізація комп'ютерно-інтегрованої системи технічного зору для задач автентифікації

Програмна реалізація КІС технічного зору для задач автентифікації зроблена на Python з використанням бібліотек OpenCV, face_recognition, Flask і демонструє базову архітектуру системи з модулями, а саме, захоплення зображення; детекція та кодування облич; реєстрація користувача; автентифікація; збереження біометричних шаблонів у БД; серверний API.

Встановлення залежностей

```
pip install opencv-python face_recognition flask numpy sqlite3
```

Структура проєкту

```
vision_auth_system/
│
├── app.py
├── camera_module.py
├── face_module.py
├── database.py
└── requirements.txt
```

Модуль роботи з камерою (camera_module.py)

```
import cv2

def capture_image():
    cap = cv2.VideoCapture(0)

    if not cap.isOpened():
```

```
        raise Exception("Не вдалося відкрити камеру")

    ret, frame = cap.read()
    cap.release()

    if not ret:
        raise Exception("Не вдалося отримати кадр")

    return frame
```

Модуль розпізнавання облич (face_module.py)

```
import face_recognition
import numpy as np
import cv2

def encode_face(image):
    rgb_image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
    face_locations = face_recognition.face_locations(rgb_image)

    if len(face_locations) != 1:
        raise Exception("На зображенні має бути лише одне обличчя")

    encodings = face_recognition.face_encodings(rgb_image, face_locations)
    return encodings[0]

def compare_faces(known_encoding, unknown_encoding, threshold=0.5):
    distance = np.linalg.norm(known_encoding - unknown_encoding)
    return distance < threshold, distance
```

Модуль бази даних (database.py)

```
import sqlite3
import numpy as np
import pickle

DB_NAME = "users.db"

def init_db():
    conn = sqlite3.connect(DB_NAME)
    cursor = conn.cursor()
    cursor.execute("""
        CREATE TABLE IF NOT EXISTS users (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            username TEXT UNIQUE,
            encoding BLOB
        )
    """)
    conn.commit()
    conn.close()

def save_user(username, encoding):
    conn = sqlite3.connect(DB_NAME)
    cursor = conn.cursor()
    data = pickle.dumps(encoding)
    cursor.execute("INSERT INTO users (username, encoding) VALUES (?, ?)", (username, data))
    conn.commit()
    conn.close()

def get_user(username):
    conn = sqlite3.connect(DB_NAME)
```

```
    cursor = conn.cursor()
    cursor.execute("SELECT encoding FROM users WHERE username=?", (username,))
    row = cursor.fetchone()
    conn.close()

    if row:
        return pickle.loads(row[0])
    return None
```

Серверна частина (app.py)

```
from flask import Flask, request, jsonify
from camera_module import capture_image
from face_module import encode_face, compare_faces
from database import init_db, save_user, get_user

app = Flask(__name__)
init_db()

@app.route("/register", methods=["POST"])
def register():
    username = request.json.get("username")

    try:
        image = capture_image()
        encoding = encode_face(image)
        save_user(username, encoding)
        return jsonify({"status": "success", "message": "Користувач зареєстрований"})
    except Exception as e:
```

```
        return jsonify({"status": "error", "message": str(e)}), 400


@app.route("/authenticate", methods=["POST"])
def authenticate():
    username = request.json.get("username")

    try:
        stored_encoding = get_user(username)
        if stored_encoding is None:
            return jsonify({"status": "error", "message": "Користувача не знайдено"}), 404

        image = capture_image()
        new_encoding = encode_face(image)

        match, distance = compare_faces(stored_encoding, new_encoding)

        if match:
            return jsonify({
                "status": "success",
                "message": "Автентифікація успішна",
                "distance": float(distance)
            })
        else:
            return jsonify({
                "status": "denied",
                "message": "Автентифікація неуспішна",
                "distance": float(distance)
            })
```

```
    except Exception as e:
        return jsonify({"status": "error", "message": str(e)}), 400


if __name__ == "__main__":
    app.run(debug=True)
```

Система функціонує у таких двох основних режимах, як Реєстрація користувача і Автентифікація користувача.

Принцип роботи у режимі реєстрації можна описати алгоритмом (див. рис. 3.1)

Рисунок 3.1 – Алгоритм процесу реєстрації

Користувач надсилає POST-запит /register. Камера захоплює зображення. Відбувається детекція одного обличчя. Формується вектор ознак (embedding). Вектор зберігається у базі даних.

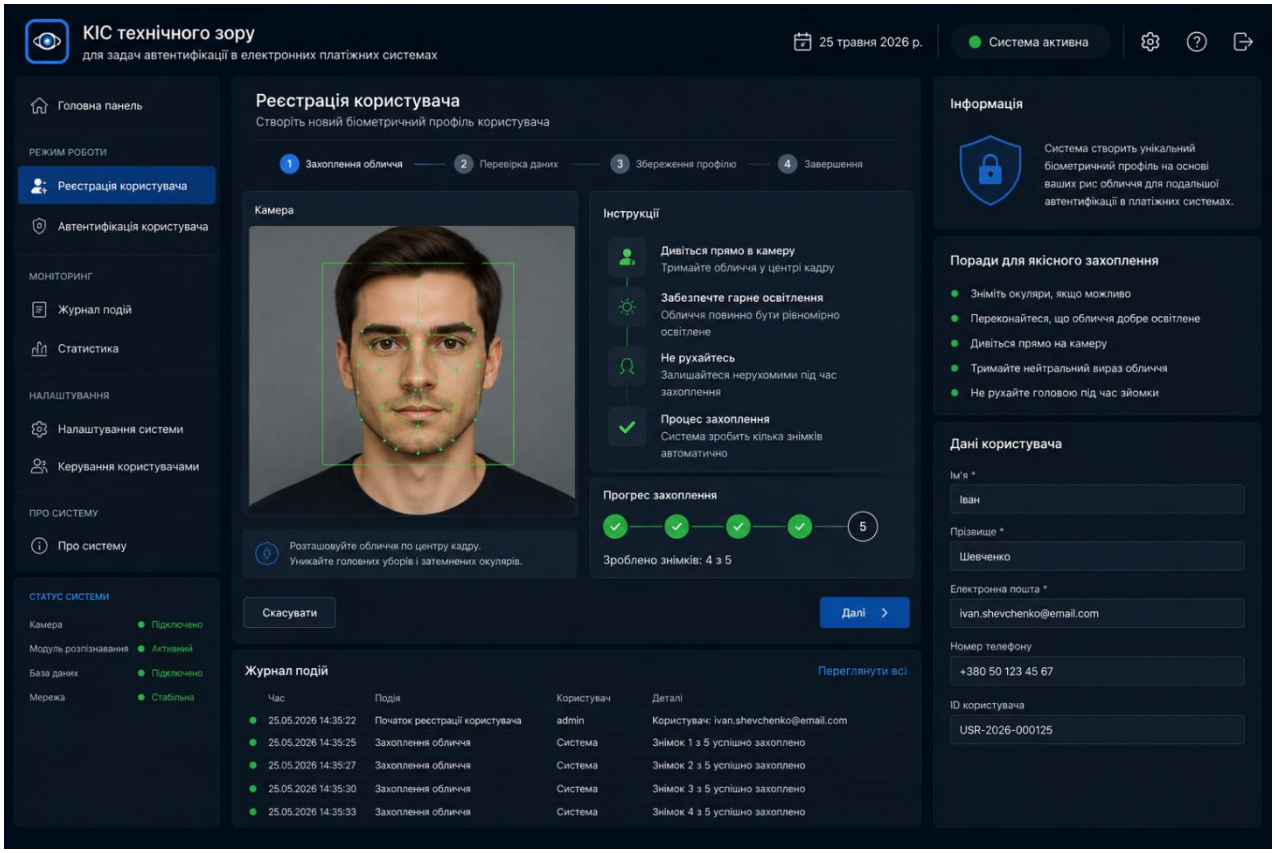


Рисунок 3.2 – Інтерфейс користувача КІС технічного зору для задач реєстрації

Логічна схема автентифікації зображена на рисунку 3.3

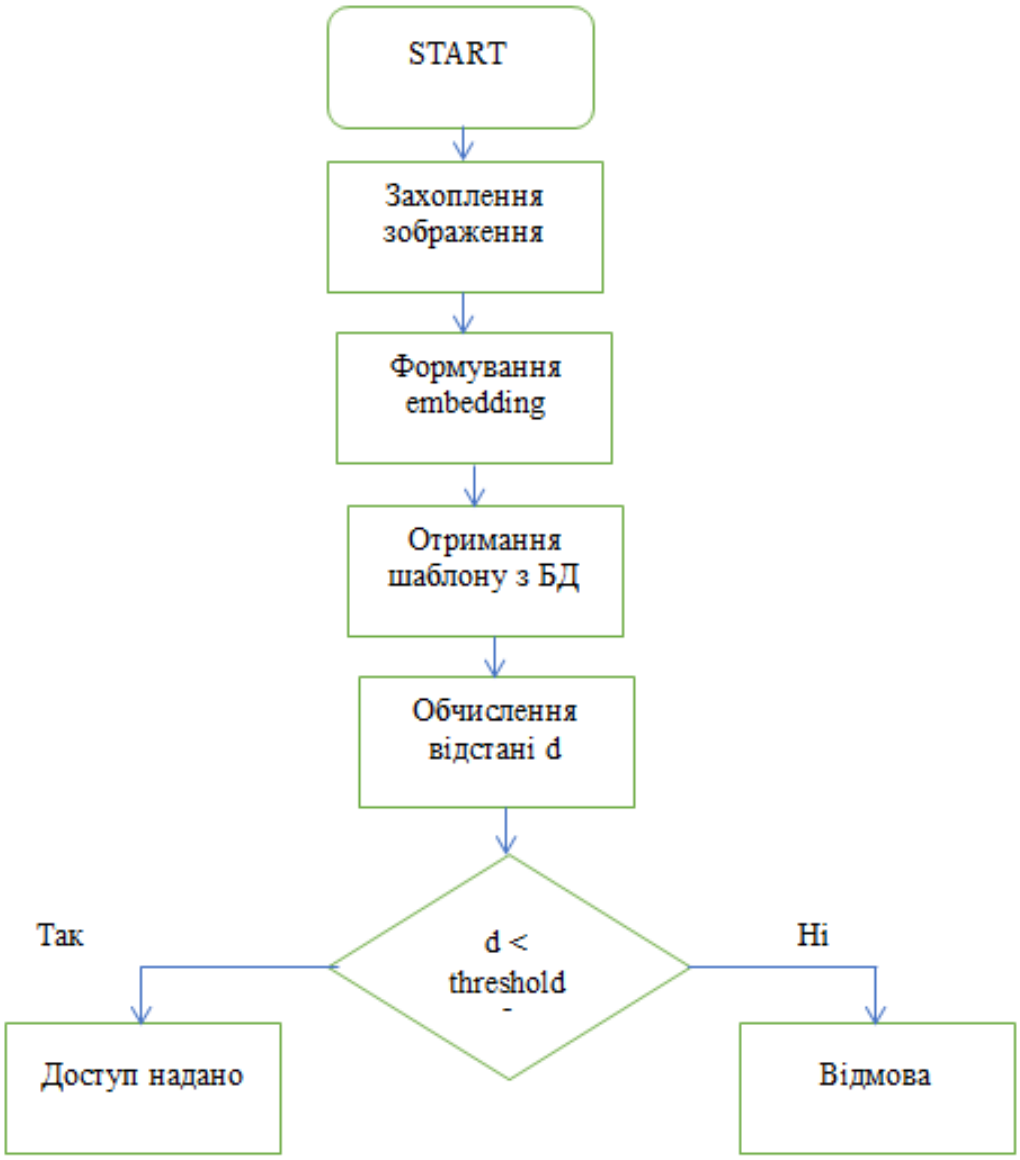


Рисунок 3.3 – Логічна схема автентифікації

Надсилається POST-запит /authenticate. Зчитується нове зображення. Отримання еталонного embedding з БД. Обчислюється відстань між векторами. Порівнюється з еталонним. Якщо distance < threshold → генерується токен. Якщо ні → збільшується лічильник спроб. Приймається рішення.

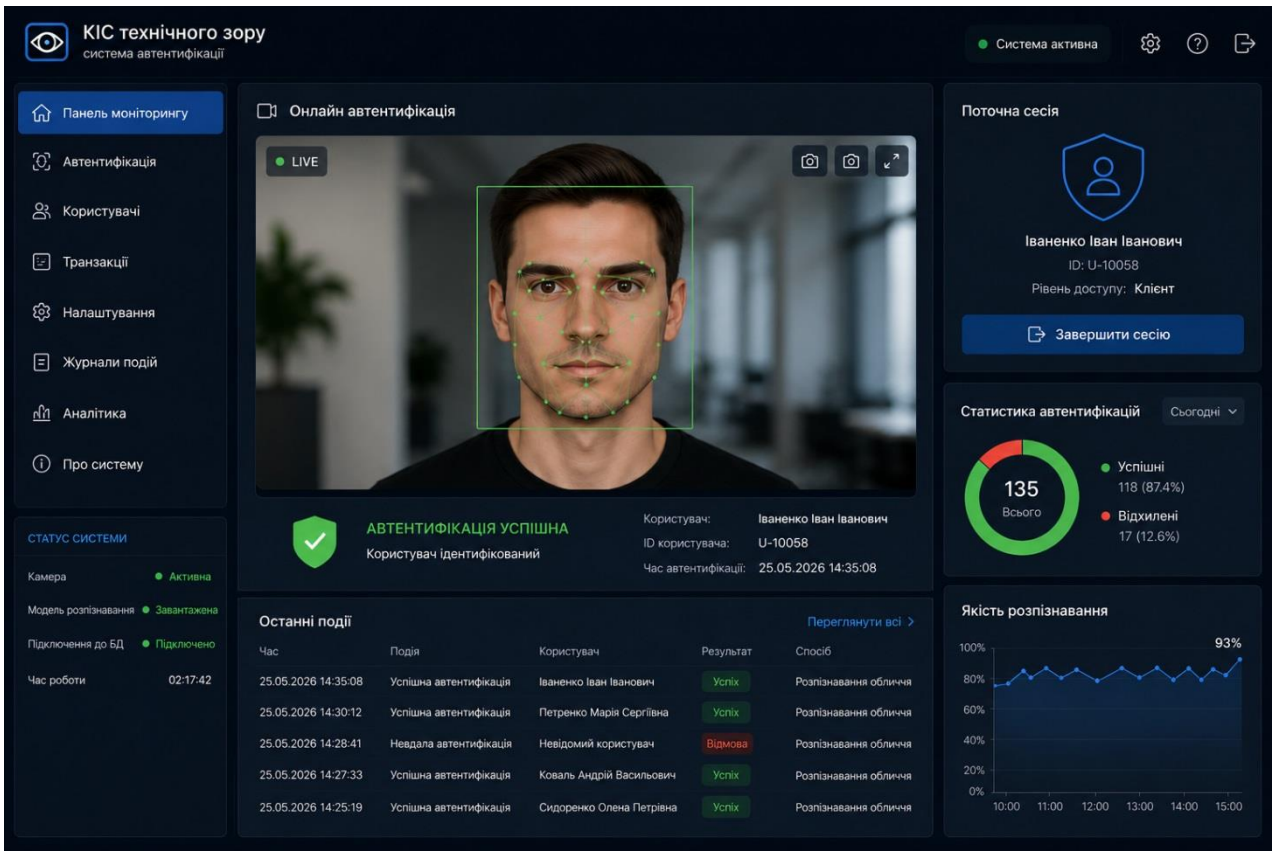


Рисунок 3.4 – Інтерфейс користувача КІС технічного зору для задач автентифікації

Для визначення схожості використовується евклідова відстань:

$$d = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (3.1)$$

де x_i – елементи нового embedding

y_i – елементи еталонного embedding

n – розмірність вектора.

Таблиця 3.1 – Характеристики системи

Параметр	Значення
Тип автентифікації	Біометрична

Параметр	Значення
Представлення даних	128-вимірний embedding
Метрика	Евклідова відстань
Захист	Liveness + ліміт спроб
Інтерфейс	REST API

Таблиця 3.2 – Ввідповідності етапів і модулів

№	Етап	Програмний модуль	Результат
1	Захоплення зображення	camera_module	Кадр з камери
2	Детекція обличчя	face_module	Координати обличчя
3	Формування embedding	face_module	Вектор ознак (128 значень)
4	Збереження	database.py	БД користувачів
5	Порівняння	face_module	Значення відстані
6	Прийняття рішення	app.py	Success / Denied

Таблиця 3.3 – Потоків даних

Джерело	Дані	Одержувач	Тип даних
Камера	Зображення	Модуль обробки	RGB-масив
Модуль обробки	Embedding	База даних	Вектор float
База даних	Еталонний embedding	Модуль порівняння	Вектор float
Модуль рішення	Статус	Платіжна система	JSON

Таблиця 3.4 – Приклад успішної автентифікації

Параметр	Значення
Обчислена відстань	0,38
Порогове значення	0,50
Результат	Доступ дозволено

Оскільки 0,38 < 0,50 — користувач автентифікований.

Таблиця 3.5 – Приклад відмови

Параметр	Значення
Обчислена відстань	0,72
Порогове значення	0,50
Результат	Відмова

Оскільки 0,72 > 0,50 — доступ заблоковано.

З метою інтеграції з платіжною системою після успішної автентифікації генерується токен доступу. Токен передається через REST API. Платіжна операція дозволяється.

Висновок до розділу 3.

У розділі 3 було розроблено та обґрунтовано програмну реалізацію комп’ютерно-інтегрованої системи технічного зору для задач автентифікації в електронних платіжних системах. Реалізація охоплює всі ключові функціональні компоненти, визначені на етапі проєктування, та підтверджує практичну придатність запропонованої архітектури.

Розроблено загальну структуру програмного забезпечення системи, визначено її модульну організацію та обґрунтовано вибір технологічного стеку. Система реалізована засобами мови програмування Python з використанням бібліотеки OpenCV для обробки зображень, фреймворку Flask для побудови серверного API та спеціалізованих інструментів розпізнавання облич. Модульна структура забезпечує гнучкість, масштабованість та можливість інтеграції із зовнішніми сервісами.

Реалізовано алгоритми розпізнавання облич на основі формування біометричного вектора ознак (embedding) та подальшого порівняння за допомогою метрики евклідової відстані. Запропонований підхід дозволяє зберігати не самі зображення, а їх математичне представлення, що підвищує рівень інформаційної безпеки. Реалізовано механізм порогового прийняття рішення, а також додаткові засоби підвищення надійності, зокрема перевірку «живості» та обмеження кількості спроб входу.

Представлено програмну реалізацію системи, яка об’єднує модулі захоплення зображення, обробки, розпізнавання, роботи з базою даних та серверної взаємодії. Реалізовано REST-інтерфейс для інтеграції з електронною платіжною системою, що дозволяє використовувати біометричну автентифікацію як частину фінансових транзакцій. Система формує токен доступу у разі успішної ідентифікації, що забезпечує можливість її практичного застосування у платіжних сервісах.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ

4.1. Організаційно-правові основи забезпечення безпеки праці

Стрімкий розвиток електронних платіжних систем та технологій комп'ютерного зору зумовлює необхідність створення надійних засобів автентифікації користувачів. Розробка комп'ютерно-інтегрованих систем технічного зору передбачає виконання робіт із програмування, навчання моделей машинного навчання, обробки цифрових зображень та адміністрування інформаційної інфраструктури. Виконання таких робіт потребує належної організації робочих місць та дотримання вимог охорони праці.

Безпека праці під час розробки програмно-технічних комплексів автентифікації є складовою загальної системи управління підприємством або організацією. Вона охоплює комплекс організаційних, правових, технічних і санітарно-гігієнічних заходів, спрямованих на збереження здоров'я працівників, підтримання їх працездатності та запобігання виникненню небезпечних ситуацій під час роботи з комп'ютерним і мережевим обладнанням.

Нормативно-правове регулювання охорони праці в Україні базується на положеннях Конституції України, Кодексу законів про працю України та Закону України «Про охорону праці». Крім того, діяльність, пов'язана з використанням біометричних даних користувачів, регламентується законодавством у сфері інформаційної безпеки та захисту персональних даних. Дотримання вимог зазначених нормативних документів є обов'язковою умовою під час створення та експлуатації інформаційних систем автентифікації.

Організація безпечних умов праці передбачає розподіл відповідальності між роботодавцем і працівниками. Роботодавець зобов'язаний забезпечити належний технічний стан обладнання, безпечне виробниче середовище та

проведення необхідних інструктажів, а працівники повинні дотримуватися встановлених правил безпеки, правильно використовувати технічні засоби та повідомляти про виявлені несправності або потенційно небезпечні ситуації.

4.2 Характеристика об’єкта та виявлення потенційних небезпек

Розробка комп’ютерно-інтегрованої системи технічного зору для автентифікації в електронних платіжних системах потребує уваги до безпеки праці та захисту обладнання. Основне завдання цього підрозділу полягає в оцінці можливих небезпек, які можуть виникати під час експлуатації системи, та у визначенні заходів їх запобігання. Це дозволяє забезпечити безпечні умови праці для операторів і стабільну роботу всіх компонентів системи.

Система технічного зору включає комп’ютерне обладнання, камери, освітлювальні прилади, сервери та програмне забезпечення. Усі ці елементи можуть створювати потенційні ризики для працівників і для обладнання. Наприклад, робота з електроприладами може спричинити електротравми або коротке замикання, якщо порушені правила експлуатації або використовуються пошкоджені кабелі. Камери та лампи освітлення при тривалому контакті можуть спричиняти опіки або механічні ушкодження. Також, оператори, які довго спостерігають за монітором, можуть відчувати напруження очей, спини та шиї.

Програмне забезпечення та сервери також можуть бути джерелом небезпеки. Несанкціонований доступ або помилки в програмі можуть призвести до втрати даних або до неправильної автентифікації користувачів. Мережна інфраструктура може зазнавати перебоїв електроживлення або DDoS-атак, що теж є потенційною небезпекою.

Надзвичайні ситуації, які можуть виникати, включають пожежі, аварійні відключення електроенергії, природні катастрофи або витоки газу чи води в

приміщенні. Всі ці випадки потребують наявності плану дій і заздалегідь розроблених інструкцій для персоналу.

Потенційні небезпеки представлено у таблиці 4.1.

Таблиця 4.1 – Потенційні небезпеки під час експлуатації КІС технічного зору для автентифікації в електронних платіжних системах

Компонент системи	Потенційна небезпека	Можливі наслідки
Комп'ютерне обладнання	Перегрів, коротке замикання	Пошкодження техніки, відключення системи
Камери та освітлення	Електротравми, опіки, механічні пошкодження	Травми персоналу, поломка обладнання
Сервери та програмне забезпечення	Втрата даних, помилки, несанкціонований доступ	Порушення автентифікації, втрати фінансових операцій
Робоче місце оператора	Тривале сидіння, напруження очей і спини	Погіршення здоров'я працівника
Мережа та комунікації	Перебої електроживлення, DDo S-атаки	Втрата доступу до системи, затримка операцій
Надзвичайні ситуації	Пожежа, повінь, землетрус, аварійні витоки	Пошкодження обладнання, ризик для життя персоналу

Робоче місце оператора комп'ютерно-інтегрованої системи технічного зору є одним із ключових елементів безпечної експлуатації системи. Від правильного облаштування та організації місця залежить ефективність роботи персоналу та збереження його здоров'я.

На робочому місці оператор взаємодіє з монітором, комп'ютером, клавіатурою, мишею та периферійними пристроями. Він спостерігає за

відеопотоком камер, перевіряє результати автентифікації користувачів і контролює роботу програмного забезпечення. Тривала робота в статичній позі може викликати втому очей, болі в спині та шиї, а також знижувати концентрацію уваги.

Однією з основних небезпек на робочому місці є фізичне навантаження. Оператор може довго перебувати в сидячому положенні перед монітором, що призводить до м’язового напруження. Недостатньо зручне крісло, невідповідна висота столу або розташування монітора можуть посилювати негативний ефект.

Ще однією потенційною небезпекою є перенапруження зору. Погане освітлення, бліки на екрані або довге спостереження за камерою можуть викликати втому очей, головний біль та зниження гостроти зору. Для зменшення цих ризиків рекомендується використовувати ергономічне освітлення, регульовані монітори та перерви під час роботи.

Психоемоційне навантаження є важливим фактором безпеки. Оператори можуть відчувати стрес під час пікових періодів роботи системи або при великій кількості запитів на автентифікацію. Це може призводити до помилок та зниження ефективності контролю.

Також на робочому місці необхідно враховувати загальні правила безпеки при роботі з електрообладнанням. Кабелі та розетки повинні бути справними та правильно заземленими. Периферійні пристрої мають бути надійно закріплені, щоб уникнути механічних травм.

Для поліпшення безпеки та комфорту робоче місце оператора має відповідати наступним вимогам: регульоване крісло, правильна висота столу, монітор на рівні очей, достатнє освітлення та відсутність бликів на екрані. Важливо також передбачати перерви кожні 45–60 хвилин для відпочинку очей і розминки м’язів.

Нижче наведена таблиця потенційних ризиків на робочому місці оператора та рекомендовані заходи їх усунення.

Таблиця 4.2 – Потенційні ризики та заходи безпеки на робочому місці оператора

Потенційний ризик	Можливі наслідки	Заходи безпеки та рекомендації
Тривале сидіння	Болі в спині, шиї, втома	Ергономічне крісло, регульована висота столу, перерви кожні 45–60 хв
Перенапруження очей	Втома очей, головний біль	Регульоване освітлення, монітор на рівні очей, антиблікове покриття
Психоемоційне навантаження	Стрес, помилки	Чіткі інструкції, розподіл навантаження, психологічні перерви
Механічні травми	Пошкодження рук або ніг	Справні кріплення обладнання, безпечне розташування кабелів
Електротравми	Ураження струмом	Перевірка кабелів, правильне заземлення, інструктаж персоналу
Неправильне освітлення	Втома зору, зниження концентрації	Використання регульованого освітлення та ламп без бликів

Правильна організація робочого місця оператора забезпечує комфорт, зменшує ризик травм та дозволяє підвищити ефективність роботи системи технічного зору. Важливо регулярно проводити інструктаж персоналу, перевірку обладнання та моніторинг умов праці.

4.3 Дослідження ризику реалізації потенційних небезпек на об’єкті проєктування та розробка заходів щодо їх попередження

Аналіз та оцінка ризиків є невід’ємною частиною розробки та експлуатації комп’ютерно-інтегрованої системи технічного зору. Головною метою цього підрозділу є визначення потенційних небезпек і оцінка їх впливу на працівників та обладнання. Комплексний підхід дозволяє передбачити ситуації, що можуть призвести до травм, пошкодження техніки або втрати даних. Першим кроком є ідентифікація всіх компонентів системи, які

взаємодіють між собою. До таких компонентів належать комп'ютери, сервери, камери, мережеве обладнання та робочі місця операторів. Важливо також враховувати програмне забезпечення та його інтеграцію з платіжною системою. Наступним кроком є визначення можливих джерел небезпеки для кожного компоненту. Наприклад, комп'ютерна техніка може перегріватися або виходити з ладу через коротке замикання.

Камери та освітлювальні прилади можуть створювати ризик електротравм або опіків. Сервери та програмне забезпечення піддаються ризику втрати даних та кібератак. Робоче місце оператора може стати джерелом фізичної втоми та психоемоційного перевантаження. Мережна інфраструктура піддається ризику перебоїв живлення та атак сторонніх користувачів. Надзвичайні ситуації, такі як пожежі, повені чи землетруси, можуть пошкодити обладнання та створити небезпеку для персоналу.

Після визначення джерел небезпеки необхідно оцінити ймовірність їх виникнення. Ймовірність може бути високою, середньою або низькою залежно від типу компонента та умов експлуатації. Для прикладу, коротке замикання в старих електропроводках має середню ймовірність. Перегрів серверного обладнання під час пікових навантажень має високу ймовірність. Кібератаки мають низьку ймовірність у разі використання сучасних систем захисту.

Наступним кроком є визначення тяжкості наслідків для кожного ризику. Тяжкість може варіювати від незначного пошкодження до серйозної травми або втрати даних. Наприклад, травма руки оператора через обрив кабелю може мати середню тяжкість.

Пожежа в серверній кімнаті може призвести до серйозних фінансових збитків та травм. Втрата даних автентифікації користувачів може спричинити порушення роботи платіжної системи.

Для оцінки ризику використовують таблицю "ймовірність × тяжкість". У цій таблиці кожен ризик отримує бали за ймовірність і за тяжкість наслідків.

Потім ці бали множаться або сумуються для отримання загального рівня ризику.

Рівень ризику дозволяє визначити пріоритети для впровадження заходів безпеки. Високі ризики потребують термінових заходів, середні – планових, а низькі – моніторингу. Важливо також враховувати сумарний ефект одночасного виникнення декількох ризиків.

Таблиця 4.3 – Приклад оцінки ризику

Компонент системи	Потенційний ризик	Ймовірність	Тяжкість	Рівень ризику
Комп’ютерне обладнання	Перегрів	Середня	Середня	Середній
Камери та освітлення	Електротравми	Низька	Середня	Низький
Сервери та ПО	Втрата даних	Низька	Висока	Середній
Робоче місце оператора	Втома очей і спини	Висока	Низька	Середній
Мережа та комунікації	Перебої електроживлення	Середня	Середня	Середній
Надзвичайні ситуації	Пожежа, повінь, землетрус	Низька	Висока	Високий

Аналіз та оцінка ризику дозволяють систематизувати інформацію про небезпеки, визначити пріоритети та розробити ефективні заходи для забезпечення безпеки персоналу та обладнання.

Комп’ютерно-інтегрована система технічного зору для задач автентифікації в електронних платіжних системах потребує дотримання правил безпеки у разі виникнення надзвичайних ситуацій (НЗС). Надзвичайні ситуації можуть бути технічного, природного чи соціального характеру.

Основними потенційними загрозами є пожежа, перебої електропостачання, аварійні витоки газу чи води, а також стихійні лиха.

Для забезпечення безпеки персоналу та збереження обладнання необхідно дотримуватися нормативних документів, зокрема:

ДБН В.2.5-56:2014 «Планування і забудова територій. Організація систем протипожежного захисту»;

НПАОП 0.00-1.41-04 «Пожежна безпека об’єктів»;

Закон України “Про охорону праці”;

ДСТУ ISO 31000:2019 «Управління ризиком. Принципи та керівництво»;

ДСТУ IEC 60950-1 щодо безпеки інформаційної техніки.

Основним завданням є розробка заходів для попередження НЗС та алгоритмів дій персоналу у випадку їх виникнення. Для цього важливо ідентифікувати джерела небезпеки та оцінити ймовірність і тяжкість наслідків.

Нижче наведено таблицю основних надзвичайних ситуацій, що можуть виникати на робочому місці оператора системи, та заходи безпеки, які зменшують їхній вплив.

Таблиця 4.4 – Потенційні надзвичайні ситуації та заходи безпеки

Надзвичайна ситуація	Потенційні наслідки	Заходи безпеки та рекомендації
Пожежа	Пошкодження обладнання, травми персоналу	Встановлення пожежної сигналізації, вогнегасників, евакуаційних виходів, проведення навчання персоналу
Витік газу	Загроза здоров’ю, вибух	Контроль герметичності систем, сигналізація витоку газу, наявність інструкцій для евакуації
Витік води / затоплення	Пошкодження обладнання, коротке замикання	Захист обладнання від вологи, регулярний огляд трубопроводів, план евакуації
Перебої електропостачання	Втрата даних, відключення системи	Використання безперебійного живлення (UPS), генераторів резервного живлення

Надзвичайна ситуація	Потенційні наслідки	Заходи безпеки та рекомендації
Землетрус / повінь	Пошкодження приміщень та обладнання	Міцне кріплення обладнання, евакуаційні маршрути, план дій для персоналу
Кібератаки / DDoS	Втрата доступу до системи, блокування транзакцій	Встановлення систем захисту, резервне копіювання даних, обмеження доступу

Для більш наочного відображення можна використовувати схему алгоритму дій персоналу у випадку надзвичайної ситуації, зображену на рисунку 4.1

Рисунок 4.1 – Алгоритм дій у надзвичайних ситуаціях

Важливо забезпечити регулярне навчання персоналу щодо дій у разі НЗС, включно з відпрацюванням евакуаційних маршрутів та користуванням первинними засобами пожежогасіння. Обладнання повинно бути розташоване так, щоб мінімізувати ризики у разі НЗС.

З метою ефективного управління ризиками рекомендовано вести реєстр надзвичайних ситуацій та ризиків, де фіксуються випадки НЗС, оцінка їхніх наслідків та застосовані заходи.

Таблиця 4.5 – Реєстр надзвичайних ситуацій

Дата	Тип НЗС	Об’єкт	Наслідки	Заходи усунення	Відповідальний
10.01.2026	Перебої електроен.	Серверна	Втрата даних	UPS, відновлення бекапу	Інженер мережі
15.02.2026	Пожежа	Робоче місце оператора	Легка паніка, без травм	Вогнегасники, евакуація	Керівник відділу
22.03.2026	Витік води	Серверна	Коротке замикання	Відключення електрики, висушування	Технік сервера

Дотримання зазначених норм і процедур забезпечує мінімізацію ризиків для персоналу та обладнання, а також гарантує безперебійну роботу системи технічного зору під час надзвичайних ситуацій. Система повинна функціонувати у відповідності до нормативних документів, що регламентують безпеку праці та протипожежний захист.

Висновок до розділу 4.

У розділі 4 було проведено комплексний аналіз охорони праці та безпеки у надзвичайних ситуаціях для експлуатації комп’ютерно-інтегрованої системи технічного зору. Було визначено основні потенційні небезпеки, які можуть виникати під час роботи з обладнанням та програмним забезпеченням,

зокрема електротравми, механічні ушкодження, перевантаження органів зору, психоемоційний стрес операторів та ризики для мережевої інфраструктури.

Особливу увагу приділено організації робочого місця оператора, яке повинно відповідати принципам ергономіки та вимогам безпеки праці. Було надано рекомендації щодо регульованих крісел, висоти столу, положення монітора та освітлення, що дозволяє зменшити фізичне та психоемоційне навантаження на персонал.

Крім того, проведено аналіз надзвичайних ситуацій та ризиків, які можуть виникати на об’єкті. Для кожного типу НЗС було визначено ймовірність виникнення, тяжкість наслідків та розроблено відповідні заходи безпеки. Зокрема, розроблено алгоритми дій персоналу у випадку пожежі, витоку газу чи води, перебоїв електропостачання та стихійних лих, а також рекомендовано систематичне навчання персоналу та ведення реєстру НЗС.

Виконані оцінка ризиків та розробка заходів безпеки забезпечують мінімізацію загроз для життя та здоров’я операторів, збереження обладнання та безперебійну роботу системи. Дотримання нормативних документів, таких як ДБН В.2.5-56:2014, НПАОП 0.00-1.41-04, Закон України “Про охорону праці” та ДСТУ ISO 31000:2019, гарантує відповідність системи вимогам безпеки та дозволяє впроваджувати її у реальних електронних платіжних системах.

Розділ 4 підтвердив необхідність системного підходу до безпеки та охорони праці при розробці та експлуатації комп’ютерно-інтегрованої системи технічного зору, а також показав практичну придатність розроблених рекомендацій для забезпечення надійної та безпечної роботи персоналу та обладнання.

ЗАГАЛЬНІ ВИСНОВКИ

У бакалаврській роботі проведено комплексне дослідження сучасних методів автентифікації та технологій технічного зору, що дозволило виявити основні тенденції розвитку електронних платіжних систем та систем біометричного розпізнавання, зокрема розпізнавання обличь. Було проаналізовано існуючі системи технічного зору, визначено їхні переваги та обмеження, а також сформульовано вимоги до комп’ютерно-інтегрованої системи автентифікації.

Основною метою було визначення ефективних підходів до автентифікації на базі біометричних технологій та розробка практичного рішення, що поєднує алгоритми розпізнавання облич з інтеграцією в інформаційні системи. Робота включає як теоретичний аналіз, так і практичну реалізацію системи, що дозволяє оцінити доцільність та ефективність обраних рішень.

У першому розділі проведено детальний аналіз сучасних методів автентифікації та технологій технічного зору. Розглянуто особливості функціонування електронних платіжних систем, що дає розуміння контексту використання автентифікаційних рішень у фінансових процесах. Досліджено сучасні методи автентифікації користувачів, включаючи паролі, токени та двофакторну автентифікацію, а також розглянуто біометричну автентифікацію на основі розпізнавання облич, що дозволяє підвищити точність та безпеку ідентифікації. Проведено аналіз існуючих систем технічного зору та визначено їхні переваги і недоліки, що дозволило сформувати чіткі вимоги до комп’ютерно-інтегрованої системи автентифікації. Цей розділ заклав фундамент для подальшого проектування системи, визначивши ключові функціональні та технічні критерії.

Другий розділ присвячений проектуванню комп’ютерно-інтегрованої системи технічного зору. Було розроблено загальну архітектуру системи, яка забезпечує злагоджену роботу всіх модулів та обмін інформацією між ними.

Описано структурну схему системи, виділено основні модулі та їхні функції, визначено інформаційні потоки та інтеграційні зв’язки між компонентами. Цей розділ показав, як теоретичні вимоги можна реалізувати у практичній схемі, забезпечуючи надійність та масштабованість системи.

Третій розділ охоплює програмну реалізацію системи технічного зору. Було створено алгоритми розпізнавання облич, розроблено програмні модулі для інтеграції всіх компонентів системи та забезпечено їхню взаємодію для виконання процесів автентифікації. Програмна реалізація підтверджує доцільність обраних алгоритмів та демонструє можливість використання системи в різних сферах, зокрема у фінансових сервісах, контролі доступу та безпеці інформаційних систем.

Четвертий розділ присвячено питанням охорони праці та безпеки в надзвичайних ситуаціях. Було проведено постановку завдання та ідентифікацію потенційних небезпек під час експлуатації системи, оцінено ризики та запропоновано заходи щодо їх мінімізації. Особлива увага приділяється безпеці користувачів та операторів, а також сценаріям реагування на надзвичайні ситуації, що забезпечує комплексний підхід до безпечної експлуатації системи в різних умовах.

Виконана робота демонструє ефективність застосування комп’ютерно-інтегрованих систем технічного зору для підвищення безпеки та надійності процесів автентифікації. Дослідження показало, що інтеграція сучасних методів біометричної ідентифікації, грамотне проектування архітектури та програмна реалізація дозволяють створити надійну та масштабовану систему. Робота поєднує теоретичні та практичні аспекти, враховує безпеку та охорону праці, що робить її цілісним дослідженням у сфері сучасних технологій автентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України Про охорону праці (Відомості Верховної Ради України (ВВР), 1992, № 49, ст.668). https://zakon.rada.gov.ua
2. Методичні вказівки до виконання розділу «Охорона праці та безпека в надзвичайних ситуаціях». Харків : ХНУМГ ім. О. М. Бекетова, 2021.
3. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень.
4. ДБН В.2.5-28:2018 Природне і штучне освітлення
5. ДСТУ 4297:2004 Пожежна техніка. Технічне обслуговування вогнегасників. Загальні технічні вимоги
6. ДСТУ EN 54-1:2022 Системи виявлення пожежі та пожежної сигналізації - Частина 1: Вступ (EN 54–1:2021, IDT)
7. Біометрична автентифікація: сучасні методи та технології / за ред. В.І. Коваленка. – К., 2020. – 256 с.
8. Комп'ютерний зір та його застосування у безпеці / І.І. Сидоренко. – Харків: ХНУРЕ, 2021. – 198 с.
9. Технології інтегрованих систем у сучасних інформаційних мережах / А.В. Бондаренко. – К., 2021. – 240 с.
10. EL Fadel N. Facial Recognition Algorithms: A Systematic Literature Review // *J. Imaging*. – 2025. – Vol. 11, No. 2:58. – 2025. DOI:10.3390/jimaging11020058.
11. Журавель Ю. І., Лісовський Б. В. Аналіз моделей та алгоритмів автентифікації на основі біометричних даних // *Сучасний захист інформації*. – 2025. – № 2(62). – С.51 -58. DOI: 10.31673/2409-7292.2025.022701.
12. Ghedia, N., Vithalani, C., Kothari, A. M., Thanki, R. M., "Moving Objects Detection Using Machine Learning" Springer International Publishing, Switzerland, 2022, pp. 65-68.
13. Булботка Н., Польшакова О. Застосування комп'ютерного зору для автоматизованої системи відстеження об'єктів // *Адаптивні системи*

автоматичного управління. – 2025. – С.22-34. DOI:10.20535/1560-8956.46.2025.323655.

14. Олексів Н. Т. Ідентифікація користувачів за райдужною оболонкою ока в автоматизованій системі управління // *Scientific Bulletin of UNFU*. – 2024. – С. 146-151. DOI: https://doi.org/10.36930/40350217

15. Сторчак К. П., Ткаленко О. М., Полоневич О. В., Тушич А. М., Усик М. Л. Застосування технології розпізнавання облич для запобігання інсайдерським атакам // *Зв'язок*. – 2022. – С.32-39. DOI:10.31673/2412-9070.2022.023239.

16. Корченко О., Терейковський О. Метод біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужної оболонки ока із застосуванням нейромережевих засобів // *Безпека інформації*. – 2025. – Т.1 – № 29 – С. 92-106. DOI: https://doi.org/10.28925/2663-4023.2025.29.866

ДОДАТОК А

Програмна реалізація комп’ютерно-інтегрованої системи технічного зору для задач автентифікації в електронних платіжних системах на Python.

1. Структура проєкту

vision_system/

│

├── app.py

├── vision/

│ ├── camera.py

│ ├── recognition.py

│ ├── liveness.py

│

├── database.py

├── security.py

└── config.py

2. config.py

```
THRESHOLD = 0.5
MAX_ATTEMPTS = 3
DATABASE_NAME = "users.db"
```

3. Модуль камери (vision/camera.py)

```
import cv2


def capture_frame():
    cap = cv2.VideoCapture(0)
    if not cap.isOpened():
        raise Exception("Камеру не знайдено")

    ret, frame = cap.read()
    cap.release()

    if not ret:
        raise Exception("Помилка захоплення кадру")

    return frame
```

4. Модуль розпізнавання (vision/recognition.py)

```
import face_recognition
import numpy as np
import cv2
```

```
def get_face_encoding(frame):
    rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
    locations = face_recognition.face_locations(rgb)

    if len(locations) != 1:
        raise Exception("Має бути одне обличчя")

    encodings = face_recognition.face_encodings(rgb, locations)
    return encodings[0]

def compare_embeddings(known, unknown):
    distance = np.linalg.norm(known - unknown)
    return distance
```

5. Перевірка "живості" (vision/liveness.py)

```
import cv2

def check_liveness(frame):
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    variance = cv2.Laplacian(gray, cv2.CV_64F).var()
```

```
    # Якщо різкість занадто низька — можливо фото
    if variance < 50:
        return False
    return True
```

6. Робота з базою даних (database.py)

```
import sqlite3
import pickle
from config import DATABASE_NAME


def init_db():
    conn = sqlite3.connect(DATABASE_NAME)
    cursor = conn.cursor()
    cursor.execute("""
        CREATE TABLE IF NOT EXISTS users (
            username TEXT PRIMARY KEY,
            encoding BLOB,
            attempts INTEGER DEFAULT 0
        )
```

```
    """)
    conn.commit()
    conn.close()


def save_user(username, encoding):
    conn = sqlite3.connect(DATABASE_NAME)
    cursor = conn.cursor()
    data = pickle.dumps(encoding)
    cursor.execute("INSERT INTO users (username, encoding) VALUES (?, ?)",
                   (username, data))
    conn.commit()
    conn.close()


def get_user(username):
    conn = sqlite3.connect(DATABASE_NAME)
    cursor = conn.cursor()
    cursor.execute("SELECT encoding, attempts FROM users WHERE username=?",
                   (username,))
```

```
    row = cursor.fetchone()
    conn.close()

    if row:
        return pickle.loads(row[0]), row[1]
    return None, None


def update_attempts(username, attempts):
    conn = sqlite3.connect(DATABASE_NAME)
    cursor = conn.cursor()
    cursor.execute("UPDATE users SET attempts=? WHERE username=?",
                   (attempts, username))
    conn.commit()
    conn.close()
```

7. Модуль безпеки (security.py)

```
import hashlib
import time


def generate_token(username):
```

```
    raw = f"{username}{time.time()}"
    return hashlib.sha256(raw.encode()).hexdigest()
```

8. Основний сервер (app.py)

```
from flask import Flask, request, jsonify
from vision.camera import capture_frame
from vision.recognition import get_face_encoding, compare_embeddings
from vision.liveness import check_liveness
from database import init_db, save_user, get_user, update_attempts
from security import generate_token
from config import THRESHOLD, MAX_ATTEMPTS

app = Flask(__name__)
init_db()

@app.route("/register", methods=["POST"])
def register():
    username = request.json.get("username")
```

```
    try:
        frame = capture_frame()
        encoding = get_face_encoding(frame)
        save_user(username, encoding)
        return jsonify({"status": "registered"})
    except Exception as e:
        return jsonify({"error": str(e)}), 400


@app.route("/authenticate", methods=["POST"])
def authenticate():
    username = request.json.get("username")

    encoding_db, attempts = get_user(username)

    if encoding_db is None:
        return jsonify({"error": "Користувач не знайдений"}), 404

    if attempts >= MAX_ATTEMPTS:
```

```
    return jsonify({"error": "Акаунт заблоковано"}), 403


try:
    frame = capture_frame()

    if not check_liveness(frame):
        return jsonify({"error": "Не пройдено перевірку живості"}), 400

    encoding_new = get_face_encoding(frame)
    distance = compare_embeddings(encoding_db, encoding_new)

    if distance < THRESHOLD:
        token = generate_token(username)
        update_attempts(username, 0)
        return jsonify({
            "status": "success",
            "token": token,
            "distance": float(distance)
        })
```

```
        else:
            update_attempts(username, attempts + 1)
            return jsonify({
                "status": "denied",
                "distance": float(distance)
            })

    except Exception as e:
        return jsonify({"error": str(e)}), 400


if __name__ == "__main__":
    app.run(debug=True)
```

ДОДАТОК В

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА імені О.М. БЕКЕТОВА
Навчально-науковий інститут енергетичної, інформаційної та транспортної інфраструктури
Кафедра автоматизації та комп'ютерно-інтегрованих технологій

Комп'ютерно-інтегрована система технічного зору для задач автентифікації в електронних платіжних системах

здобувача вищої освіти групи СІНЖ 2022-1
Спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології»
Борзенка Кирила Сергійовича
Керівник Білецький Ігор Васильович, д.е.н., проф., проф. кафедри АКІТ

МЕТА

Метою бакалаврської роботи є розробка та дослідження комп'ютерно-інтегрованої системи технічного зору для автоматизованої автентифікації користувачів в електронних платіжних системах з метою підвищення рівня безпеки та надійності платіжних операцій.

Для досягнення поставленої мети в роботі необхідно розв'язати такі задачі:

- Проаналізувати сучасні методи та засоби автентифікації користувачів в електронних платіжних системах.
- Дослідити принципи побудови комп'ютерно-інтегрованих систем технічного зору та можливості їх застосування для задач автентифікації.
- Розробити структурну та функціональну схеми комп'ютерно-інтегрованої системи технічного зору.
- Обгрунтувати вибір алгоритмів оброблення зображень і розпізнавання обличь для автентифікації користувачів.

2

АКТУАЛЬНІСТЬ

Актуальність теми бакалаврської роботи обумовлена інтенсивним розвитком електронних платіжних систем і зростанням кількості дистанційних фінансових операцій, що супроводжується підвищенням ризиків несанкціонованого доступу та шахрайства. Традиційні методи автентифікації, такі як паролі або PIN-коди, дедалі частіше виявляються недостатньо надійними та зручними для користувачів. У цьому контексті впровадження комп'ютерно-інтегрованих систем технічного зору, здатних автоматично ідентифікувати користувачів за біометричними ознаками, є перспективним напрямом підвищення рівня безпеки платіжних операцій. Застосування таких систем забезпечує ефективну інтеграцію процесів автентифікації з існуючими інформаційними та керуючими підсистемами, що відповідає сучасним вимогам автоматизації та цифровізації.

3

Об'єкт і предмет дослідження

Об'єктом дослідження є процеси автоматизованої автентифікації користувачів у електронних платіжних системах.

Предметом дослідження є методи, алгоритми та програмно-апаратні засоби технічного зору, що використовуються у складі комп'ютерно-інтегрованої системи для автентифікації користувачів електронних платіжних систем.

4

Методи дослідження

У процесі виконання бакалаврської кваліфікаційної роботи застосовано комплекс взаємопов'язаних методів дослідження, вибір яких зумовлений специфікою теми та вимогами до побудови комп'ютерно-інтегрованих систем.

Метод аналізу й узагальнення науково-технічної літератури та нормативних джерел у галузі електронних платіжних систем і біометричної автентифікації застосовано з метою визначення сучасного стану проблеми, виявлення переваг і недоліків існуючих підходів, а також формування обґрунтованих вимог до розроблюваної системи, що дозволило спиратися на актуальні технологічні рішення та стандарти інформаційної безпеки.

Системний аналіз використано для дослідження структури комп'ютерно-інтегрованої системи технічного зору, визначення її функціональних модулів, інформаційних потоків і взаємозв'язків із платіжною інфраструктурою. Застосування цього методу забезпечило цілісне бачення об'єкта дослідження як складної багаторівневої системи та дало змогу обґрунтувати її архітектуру відповідно до принципів інтеграції та автоматизації.

Методи математичного та алгоритмічного моделювання застосовано для розробки й формалізації алгоритмів оброблення зображень і розпізнавання обличчя, що дозволило описати процеси виділення ознак, порівняння біометричних параметрів та прийняття рішення про автентифікацію у формалізованому вигляді, забезпечуючи можливість подальшої оптимізації та оцінювання точності роботи системи.

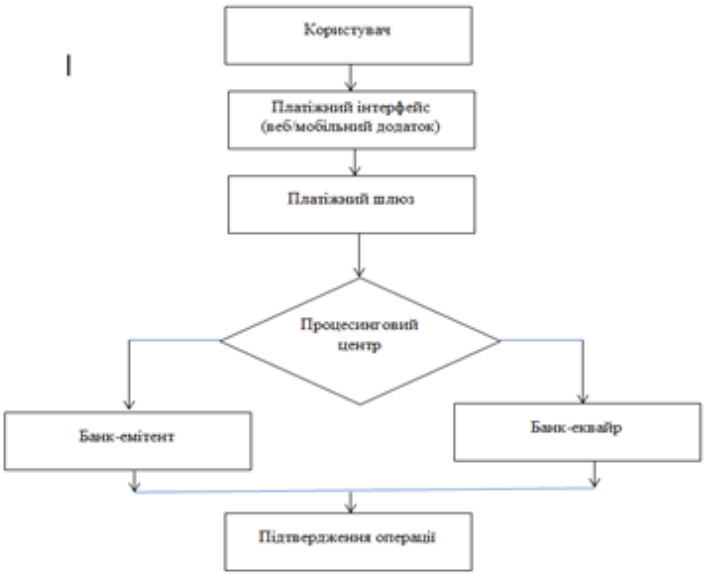
5

Основні компоненти електронної платіжної системи

№	Компонент	Функціональне призначення
1	Користувач (платник)	Ініціює платіжну операцію
2	Отримувач коштів	Приймає оплату
3	Платіжний шлюз	Забезпечує передачу даних транзакції
4	Процесинговий центр	Обробляє запит, виконує перевірку та маршрутизацію
5	Банк-емітент	Перевіряє рахунок платника та авторизує операцію
6	Банк-еквайр	Забезпечує зарахування коштів отримувачу

6

Схема проходження платіжної транзакції



7

Ключові вимоги до електронних платіжних систем

Характеристика	Опис
Швидкодія	Обробка транзакцій у режимі реального часу
Надійність	Безперервність роботи та відмовостійкість
Масштабованість	Можливість обробки великої кількості операцій
Захищеність	Криптографічний захист даних і контроль доступу
Інтегрованість	Взаємодія з банківськими та зовнішніми сервісами

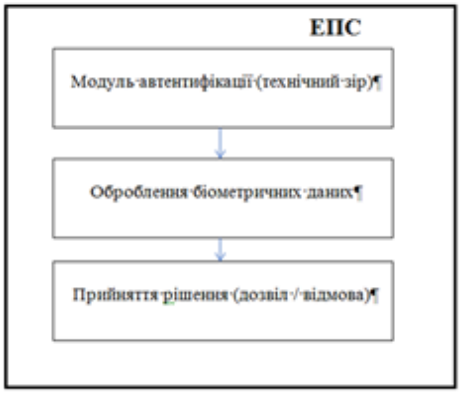
8

Порівняння методів автентифікації

Метод	Переваги	Недоліки
Пароль	Простота реалізації	Низька стійкість до атак
SMS-код	Додатковий рівень захисту	Можливість перехоплення
Токен	Висока безпека	Потребує додаткового пристрою
Біометрія (обличчя)	Висока зручність і надійність	Потребує технічного забезпечення

9

Інтеграція системи автентифікації в ЕПС



У сучасних умовах модуль автентифікації інтегрується у загальну архітектуру платіжної системи.

10

Порівняння методів автентифікації користувачів

Критерій порівняння	Парольна автентифікація	Багатофакторна автентифікація (MFA)	Біометрична автентифікація
Принцип роботи	Перевірка знання користувачем секретного пароля або PIN-коду	Комбінація двох або більше факторів: знання (пароль), володіння (токен, телефон), властивість (біометрія)	Перевірка унікальних фізіологічних або поведінкових характеристик (обличчя, відбиток пальця, райдужка ока)
Рівень безпеки	Низький або середній	Високий	Високий
Стійкість до атак	Вразлива до фішингу, brute-force, перехоплення	Значно підвищена за рахунок декількох факторів	Висока, але можлива підробка (spoofing) без додаткового захисту
Зручність використання	Висока, проста реалізація	Середня (потребує додаткових дій користувача)	Висока (швидке розпізнавання без запам'ятовування паролів)
Необхідність додаткового обладнання	Ні	Можливе (смартфон, токен, смарт-карта)	Так (камера, сканер відбитків, сенсори)

11

Порівняння методів автентифікації користувачів

Критерій порівняння	Парольна автентифікація	Багатофакторна автентифікація (MFA)	Біометрична автентифікація
Вартість впровадження	Низька	Середня	Вища (потрібне спеціалізоване обладнання та ПЗ)
Масштабованість	Висока	Висока	Середня (залежить від обчислювальних ресурсів)
Ризик компрометації	Високий (може бути викрадений або переданий)	Низький	Низький (біометричні дані складно передати третім особам)
Можливість відновлення доступу	Легке відновлення через зміну пароля	Можливе через резервні механізми	Ускладнене (біометричні дані незмінні)
Доцільність застосування в платіжних системах	Для базового рівня доступу	Для фінансових операцій середнього та високого ризику	Для швидкої та безпечної автентифікації в мобільному банкінгу та терміналах

12

Загальна структура процесу розпізнавання обличь

1 етап – Захоплення зображення здійснюється за допомогою камери, вбудованої у смартфон, банкомат або термінал самообслуговування, з якої отримується цифрове зображення або відеопотік обличчя користувача.

На 2 етапі – Виявлення обличчя: алгоритм визначає на зображенні область, що містить обличчя. Застосовуються класичні методи (Haar-каскади, HOG) або сучасні глибокі нейронні мережі.

3 етап – Попередня обробка зображення передбачає нормалізацію яскравості, масштабування, вирівнювання обличчя відносно очей, усунення шумів, що підвищує точність подальшого розпізнавання.

На 4 етапі – Виділення ознак: формується вектор ознак, який відтворює компактне числове представлення унікальних характеристик обличчя. У сучасних системах використовуються згорткові нейронні мережі (CNN), які автоматично виділяють інформативні ознаки.

На 5 етапі – Порівняння з еталоном: Отриманий вектор ознак порівнюється з шаблоном, збереженим у базі даних. Якщо ступінь подібності перевищує заданий поріг, система підтверджує автентичність користувача.

6 етап – Прийняття рішень.

13

Основні методи розпізнавання обличь

Метод	Принцип роботи	Переваги	Недоліки
Eigenfaces (PCA)	Аналіз головних компонент зображення	Простота реалізації	Чутливість до освітлення
Fisherfaces (LDA)	Лінійний дискримінантний аналіз	Краща стійкість до варіацій	Обмежена масштабованість
LBPH	Локальні бінарні шаблони	Стійкість до змін освітлення	Менша точність порівняно з CNN
CNN (Deep Learning)	Згорткові нейронні мережі	Висока точність, автоматичне виділення ознак	Потреба у значних обчислювальних ресурсах

14

Переваги та недоліки системи розпізнавання обличь

Переваги	Недоліки
Безконтактність	Залежність від освітлення
Висока швидкодія	Потреба в обчислювальних ресурсах
Зручність для користувача	Ризик атак типу spoofing
Неможливість «забути» біометрію	Складність захисту персональних даних

15

Основні показники ефективності

Показник	Позначення	Характеристика
False Acceptance Rate	FAR	Ймовірність помилкового допуску сторонньої особи
False Rejection Rate	FRR	Ймовірність відмови законному користувачу
Equal Error Rate	EER	Точка рівності FAR та FRR
Accuracy	ACC	Загальна точність класифікації
Response Time	T	Час прийняття рішення

16

Класифікація систем технічного зору за архітектурою

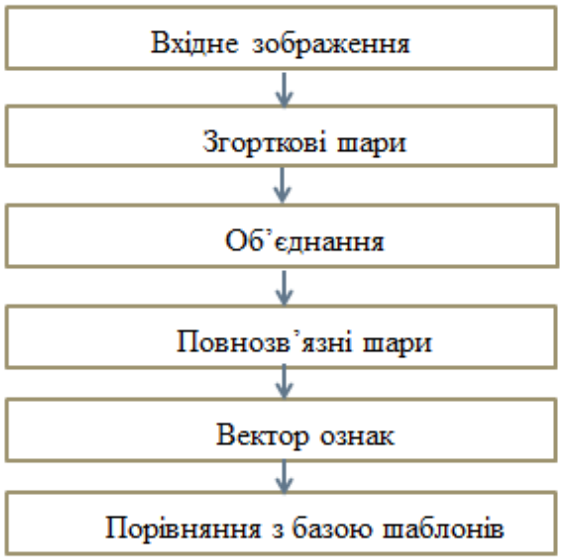
17

Порівняння архітектури систем технічного зору

Критерій	Локальна	Клієнт-серверна	Хмарна
Швидкодія	Висока	Середня	Залежить від мережі
Безпека даних	Висока	Середня	Залежить від провайдера
Масштабованість	Обмежена	Середня	Висока
Вартість впровадження	Низька	Середня	Змінна

18

Узагальнена структура нейромережевої системи розпізнавання



19

Узагальнена структура вимог до системи

20

Функціональні вимоги до системи

№	Функція	Опис	Результат виконання
1	Захоплення зображення	Отримання відеопотоку з камери	Кадр з обличчям
2	Детекція обличчя	Виявлення області обличчя	Координати ROI
3	Оброблення зображення	Нормалізація, масштабування	Підготовлене зображення
4	Розпізнавання	Порівняння з базою шаблонів	Коефіцієнт схожості
5	Прийняття рішення	Порівняння з порогом	Доступ / Відмова
6	Інтеграція з ЕПС	Передача статусу автентифікації	Авторизація транзакції

21

Нефункціональні вимоги до системи

Категорія	Вимога	Обґрунтування
Безпека	Шифрування шаблонів	Захист персональних даних
Продуктивність	Час відповіді ≤ 2 с	Комфорт користувача
Надійність	99 % доступності	Критичність платіжних операцій
Масштабованість	Підтимка >10000 користувачів	Можливість розширення системи

22

Цільові показники якості

Показник	Рекомендоване значення
FAR, ймовірність помилкового допуску сторонньої особи	≤ 0,1 %
FRR, ймовірність помилкової відмови законному користувачу	≤ 1–3 %
EER, точка рівності FAR та FRR, що характеризує точність системи	≤ 1 %
Точність	≥ 97–99 %

23

Основні компоненти системи технічного зору

№	Компонент	Призначення	Особливості реалізації
1	Камера	Захоплення зображення	HD/Full HD, автофокус
2	Edge-модуль	Попередня обробка, детекція обличчя	Нормалізація, масштабування
3	Сервер розпізнавання	Виділення ознак, класифікація	CNN-модель
4	База шаблонів	Зберігання біометричних даних	Шифрування, хешування
5	API інтеграції	Обмін даними з ЕПС	REST, JSON
6	Модуль журналювання	Фіксація подій	Логи транзакцій

24

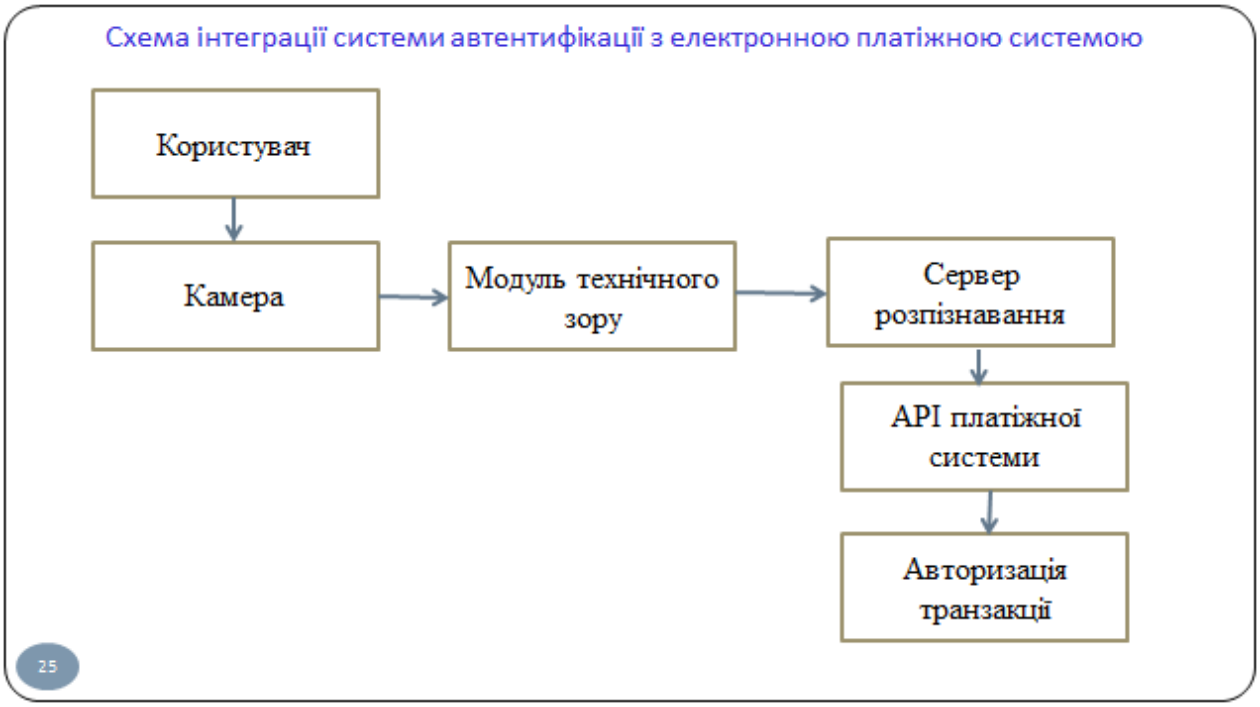


Схема інтеграції системи автентифікації з електронною платіжною системою
Користувач
Камера
Модуль технічного зору
Сервер розпізнавання
API платіжної системи
Авторизація транзакції
25

Алгоритм процесу реєстрації

26

Інтерфейс користувача КІС технічного зору для задач реєстрації

27

Алгоритм процесу автентифікації

28

Інтерфейс користувача КІС технічного зору для задач автентифікації

29

Загальні висновки

У бакалаврській роботі проведено комплексне дослідження сучасних методів автентифікації та технологій технічного зору, що дозволило виявити основні тенденції розвитку електронних платіжних систем та систем біометричного розпізнавання, зокрема розпізнавання обличь. Було проаналізовано існуючі системи технічного зору, визначено їхні переваги та обмеження, а також сформульовано вимоги до комп'ютерно-інтегрованої системи автентифікації.

У першому розділі проведено детальний аналіз сучасних методів автентифікації та технологій технічного зору. Розглянуто особливості функціонування електронних платіжних систем, що дає розуміння контексту використання автентифікаційних рішень у фінансових процесах. Досліджено сучасні методи автентифікації користувачів, включаючи паролі, токени та двофакторну автентифікацію, а також розглянуто біометричну автентифікацію на основі розпізнавання облич, що дозволяє підвищити точність та безпеку ідентифікації. Проведено аналіз існуючих систем технічного зору та визначено їхні переваги і недоліки, що дозволило сформувати чіткі вимоги до комп'ютерно-інтегрованої системи автентифікації.

Другий розділ присвячений проектуванню комп'ютерно-інтегрованої системи технічного зору. Було розроблено загальну архітектуру системи, яка забезпечує злагоджену роботу всіх модулів та обмін інформацією між ними. Описано структурну схему системи, виділено основні модулі та їхні функції, визначено інформаційні потоки та інтеграційні зв'язки між компонентами.

Третій розділ охоплює програмну реалізацію системи технічного зору. Було створено алгоритми розпізнавання облич, розроблено програмні модулі для інтеграції всіх компонентів системи та забезпечено їхню взаємодію для виконання процесів автентифікації.

Четвертий розділ присвячено питанням охорони праці та безпеки в надзвичайних ситуаціях.

30

Дякую за увагу!

31