

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Інформаційних управляючих систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Розробка ІТ-сервісу «Онлайн ідентифікація особистості»
інформаційної системи банку

(тема)

Виконав:

здобувач 4 року навчання,

групи ІТУ-21-2

Олексій ЛІБІН

(власне ім'я, прізвище)

Спеціальність 122 Комп'ютерні науки

(код і повна назва спеціальності)

Тип програми освітньо-професійна

(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні технології
управління

(повна назва освітньої програми)

Керівник: ст.викл. Анжеліка КАЛЬНИЦЬКА

(посада, власне ім'я, прізвище)

Допускається до захисту

Зав. кафедри ІУС



(підпис)

Костянтин ПЕТРОВ

(власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук


Кафедра Інформаційних управляючих систем

Рівень вищої освіти перший (бакалаврський)

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

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні технології управління
(повна назва)

ЗАТВЕРДЖУЮ: 
Зав. кафедри _____
(підпис)
“ 19 ” травня 2025 р.

ЗАВДАННЯ**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

здобувачеві Лібіну Олексію Євгеновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка IT-сервісу «Онлайн ідентифікація особистості»
інформаційної системи банку

затверджена наказом по університету від “ 19 ” травня 2025 р. № 370Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії “ 16 ” червня 2025 р.

3. Вихідні дані до роботи опис банку як об'єкта автоматизації,
технічне завдання на розробку IT-сервісу для онлайн ідентифікації особистості.


4. Перелік питань, що потрібно опрацювати у роботі Огляд і аналіз сучасного стану
задачі. Опис структурних і функціональних особливостей задачі та основних видів її
забезпечення. Постановка задачі. Розробка інформаційного забезпечення задачі.


Обґрунтування вибору математичного забезпечення задачі. Розробка елементів
програмного забезпечення задачі. Вибір та обґрунтування технічного забезпечення задачі.
Методичні рекомендації щодо використання задачі.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Аналіз діяльності об'єкту автоматизації	19.05.25 – 22.05.25	Виконано
2	Огляд і аналіз типових рішень зі створення ІТ-сервісу	23.05.25 – 25.05.25	Виконано
3	Опис постановки задачі аналізу даних	26.05.25 – 28.05.25	Виконано
4	Розробка інформаційного забезпечення ІТ-сервісу онлайн ідентифікації особистості	29.05.25 – 31.05.25	Виконано
5	Розробка математичного забезпечення ІТ-сервісу онлайн ідентифікації особистості	01.06.25 – 03.06.25	Виконано
6	Розробка елементів програмного забезпечення ІТ-сервісу онлайн ідентифікації особистості	04.06.25 – 06.06.25	Виконано
7	Обґрунтування вибору комплексу технічних засобів	07.06.25 – 08.06.25	Виконано
8	Оформлення пояснювальної записки та графічного матеріалу	09.06.25 – 10.06.25	Виконано
9	Перевірка на плагіат	10.06.25	Виконано
10	Попередній захист кваліфікаційної роботи	15.06.25	Виконано
11	Захист кваліфікаційної роботи в екзаменаційній комісії	16.06.25	Виконано

Дата видачі завдання 19.05.2025 р.

Студент 
(підпис)

Керівник роботи 
(підпис) ст. викл. Анжелыка КАЛЬНИЦЬКА
(посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 70 сторінку, 15 таблиць, 40 рисунків, 9 джерел, 2 додатки.

БАНК, ІДЕНТИФІКАЦІЯ ОСОБИСТОСТІ, БАЗА ДАНИХ, ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ, НАУКОВО-ДОПОМІЖНІ ФОНДИ, ОСНОВНІ ФОНДИ, ХУДОЖНІЙ МУЗЕЙ, API, IT-SERVIS, DFD.

Об'єктом дослідження кваліфікаційної роботи є установа банку.

Метою кваліфікаційної роботи є розробка IT-сервісу онлайн ідентифікації особистості.

Методом дослідження є системний аналіз з використанням об'єктно-орієнтованого підходу.

У роботі проведено аналіз предметної області, функціональних особливостей банку, аналіз організаційної структури, розроблено діаграми Use Case та Activity, наведено опис вимог і виконана постановка задачі, розроблено елементи інформаційного, математичного та програмного забезпечень IT-сервісу, обґрунтовано вибір технічного забезпечення сервісу.

Галузь застосування – банківська справа.

Кваліфікаційну роботу було виконано за методичними вказівками до організації виконання та захисту кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти спеціальності 122 Комп'ютерні науки за освітньою програмою «Комп'ютерні науки» для студентів усіх форм навчання [1]. Також робота була оформлена за стандартами ДСТУ 3008:2015 [2].

ABSTRACT

The explanatory note to the qualification work contains: 70 pages, 15 tables, 40 figures, 9 sources, 2 appendices.

BANK, IDENTITY IDENTIFICATION, DATABASE, INFORMATION SUPPORT, SCIENTIFIC AND AUXILIARY FUNDS, FIXED FUNDS, ART MUSEUM, API, IT SERVICE, DFD.

The object of the qualification work is a bank institution.

The purpose of the qualification work is to develop an IT service for online identity identification.

The research method is a system analysis using an object-oriented approach.

The work includes an analysis of the subject area, functional features of the bank, analysis of the organizational structure, development of Use Case and Activity diagrams, description of requirements and formulation of the task, development of elements of information, mathematical and software support of the IT service, justification of the choice of technical support of the service.

Application area – banking.

The qualification work was carried out according to the methodological instructions for the organization of the performance and defense of the qualification work for the first (bachelor) level of higher education in the specialty 122 Computer Science under the educational program «Computer Science» for students of all forms of education [1]. Also, the work was designed according to the standards of DSTU 3008:2015 [2].

ЗМІСТ

	С.
Скорочення та умовні позначки.....	7
Вступ.....	8
1 Огляд і аналіз сучасного стану задачі.....	9
1.1 Цифрова ідентичність.....	9
1.2 Електронна ідентифікація.....	10
1.3 Мобільні NFC технології для електронної ідентифікації особистості.....	12
2 Опис структурних і функціональних особливостей задачі.....	13
2.1 Аналіз та опис об'єкта автоматизації.....	13
2.2 Обґрунтування мети вирішення задачі.....	15
2.3 Функціональна структура ІТ-сервісу	16
2.4 Вимоги до ІТ-сервісу	20
3 Постановка задачі.....	22
3.1 Характеристика поставленої задачі.....	22
3.2 Вихідна інформація задач.....	23
3.3 Вхідна інформація.....	25
4 Розробка та обґрунтування інформаційного забезпечення ІТ-сервісу.....	30
5 Математичне забезпечення ІТ-сервісу.....	35
6 Розробка елементів програмного забезпечення ІТ-сервісу.....	37
7 Вибір та обґрунтування комплексу технічного забезпечення.....	40
8 Методичні рекомендації щодо використання сервісу.....	42
Висновки.....	49
Перелік джерел посилання.....	50
Додаток А Альбом документів.....	52
Додаток Б Графічний матеріал кваліфікаційної роботи.....	55

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БД – база даних

ІС – інформаційна система

ПК – персональний комп'ютер

СУБД – система управління базами даних

API – Application Programming Interface

eIC – Electronic Identification Card

eID – Electronic Identity Document

ICAO – International Civil Aviation Organization

ISO-1443 – стандарт, що описує частотний діапазон, метод модуляції та протокол обміну безконтактних пасивних карт (RFID) ближнього радіусу дії (до 10 см) на магнітозв'язаних індуктивностях

NFC – Near Field Communication

OTP – One-Time Password

RFID – Radio Frequency Identification

SDK – Software Development Kit

UI – User Interface

ВСТУП

Персональна ідентифікаційна інформація означає інформацію, яка ідентифікує людину, включаючи її фотографію, номер соціального страхування, номер водійського посвідчення, ім'я, адресу електронної пошти, адресу проживання або номер телефону [3].

Кожен тип електронної ідентифікації особистості полегшує життя людей. Завдяки раніше впровадженим службам стало можливо швидко подати заявку на допомогу дитини, подавати документи на субсидію, зареєструвати свою підприємницьку діяльність, зареєструватися до лікаря та багато іншого [3].

Таким чином, електронну ідентифікацію особистості незабаром можна буде використовувати як універсальний ключ до входу до електронних порталів замість логіна та пароля [3].

Особливі переваги електронна ідентифікація особистості надає у бізнесі, оскільки дозволяє підписувати документи в електронній формі через систему та отримувати дані та документи з однієї бази даних. Підприємці зможуть відкрити, внести зміни та закрити свій бізнес за допомогою iPad. Для них та для інших сегментів населення це хороша можливість уникати черг, бюрократії та черг у офісах, щоб отримати необхідні документи. [3].

З огляду на сучасні напрямки розвитку у сфері використання мобільних пристроїв і мобільних технологій, розробка ІТ-сервісу для цифрової ідентифікації особистості може суттєво спростити різні напрямки життєдіяльності людини.

1 ОГЛЯД І АНАЛІЗ СУЧАСНОГО СТАНУ ЗАДАЧІ

1.1 Цифрова ідентичність

Інтернет назавжди змінив концепцію ідентичності. В офлайн-світі ми могли б визначити це як відповідь на те, ким ми є насправді. В Інтернеті ідентичність – це будь-яке обличчя, яке людина може показати у цифровому всесвіті. Це, у поєднанні зі зростанням кількості ботів і генеративного штучного інтелекту, створює значний ризик для конфіденційності та безпеки кожного в Інтернеті [4].

Розуміння цифрової ідентифікації.

В онлайн-еру ідентифікація виходить далеко за межі імені чи фотографії. Зараз можна визначити цифрову ідентичність як набір інформації, дій і взаємодій, які людина залишає під час кожного кроку в Інтернеті, що дозволяє ідентифікувати особу. Мова йде про такі дані, як особиста інформація (ім'я, прізвище, вік, місцезнаходження, тощо), активність у соціальних мережах (коментарі, дописи, реакції та ін.), онлайн-взаємодія (покупки, пошук, підписки, тощо) та інші [4].

Подібно до ідентичності в реальному та фізичному світі, цифрова ідентичність також має кілька унікальних особливостей, які відрізняють її від інших концепцій [4].

Цифрову ідентичність можна розуміти наступним чином: вона є особистою і не підлягає передачі, належить унікальній особі; є безпечною, тому ніхто, крім власника цієї ідентичності, не зможе отримати до неї доступ; її можна багаторазово використовувати, що дозволяє людям автентифікуватися та підтверджувати себе в будь-якій службі, фізичній чи цифровій; вона децентралізована, що дозволяє людям контролювати свою інформацію, не залежачи від централізованих служб; вона є повною, що дозволяє людям мати повну унікальну особистість і доступ до глобальної економіки в єдиному середовищі [4].

1.2 Електронна ідентифікація

У епоху цифрових технологій підтвердження особи людини стало найважливішим, особливо коли мова йде про електронні транзакції. Електронна ідентифікація (Electronic Identity Document, eID) – це важлива концепція, яка стосується використання цифрових рішень для перевірки особистості особи чи організації в Інтернеті [5].

Електронна ідентифікація (eID) – це система, яка дозволяє окремим особам і організаціям підтверджувати свою особу в електронному вигляді. Цей процес передбачає використання цифрових облікових даних, таких як електронні підписи або цифрові сертифікати, для безпечної автентифікації користувача. Основна мета eID – переконатися, що особа, яка бере участь у онлайн-транзакції, є тим, за кого себе видає [5].

Приклади електронної ідентифікації (eID).

1. Цифрові посвідчення особи, що видаються державою. Такі країни, як Естонія, використовують цифрові посвідчення особи, які видаються державою. Вони дозволяють громадянам безпечно отримувати доступ до різних електронних послуг, включаючи голосування та цифрове підписання документів [5].

2. Банківські ідентифікатори. Фінансові установи часто випускають системи цифрової ідентифікації, що дозволяють клієнтам входити до системи онлайн-банкінгу та авторизувати транзакції.

3. Рішення для мобільної ідентифікації. Додатки, які генерують одноразові паролі (One-Time Password, OTP) або використовують біометричну автентифікацію (наприклад, розпізнавання відбитків пальців чи осіб) для підтвердження особи користувача [5].

4. Перевірка в соціальних мережах. Такі платформи, як LinkedIn або Facebook, які використовують перевірку електронною поштою або мобільним телефоном для підтвердження профілів користувачів [5].

Однією з форм eID є електронна ідентифікаційна карта (Electronic Identification Card, eIC), яка є фізичною ідентифікаційною картою. Її можна використовувати для онлайн-і офлайн-особистої ідентифікації або автентифікації.

eIC є смарт-карткою у форматі ID-1 звичайної банківської картки з ідентифікаційною інформацією, вбудованою у мікročіпі Radio Frequency Identification (RFID), подібні до тих, що є в біометричних паспортах. Чіп зберігає інформацію, надруковану на карті (наприклад, ім'я власника та дату народження), а також фотографію(і) власника [5].

Карта також може зберігати відбитки пальців власника та використовуватися для онлайн-автентифікації, наприклад, для перевірки віку або додатків електронного уряду. Електронний підпис, який надається приватною компанією, також може зберігатися на чіпі [5].

1.3 Мобільні NFC технології для електронної ідентифікації особистості

За допомогою сучасних пристроїв мобільного зв'язку можна спростити різні мобільні послуги, наприклад, отримати доступ до електронної ідентифікаційної інформації людини з метою перетворення її на мобільний формат даних з електронного паспорта, посвідчення особи, електронного посвідчення водія, будь-якого іншого сертифікату особистості, за умови, що пристрої сумісні з технологіями NFC та International Civil Aviation Organization (ICAO) [6].

Компанія ЧАО "ВТІ" розробила мобільний додаток eCredential, який дозволяє використовувати смартфон з підтримкою Near Field Communication (NFC) у якості портативного пристрою для аутентифікації електронного ідентифікаційного документа, читання даних з чіпа

ідентифікаційного документа та дисплея, а також ідентифікувати людину людиною.

Додаток поєднує в собі дві речі: сумісний з NFC пристрій та документ ідентифікації, і у такий спосіб дозволяє створити мобільну версію особистості. Тепер, щоб отримати доступ до свого ідентифікаційного документа, потрібно лише встановити Ecderential на пристрій з підтримкою технології NFC [8].

Електронний паспорт та електронне посвідчення особи, що відповідають стандартам ICAO, містять безконтактний чіп ISO-1443 і повністю сумісні з технологією NFC. Мобільний пристрій з підтримкою NFC може показувати наступні дані документа: біографічні дані, фотографію, підпис власника документа, тощо. Фото може бути масштабоване для перегляду у повно екранному режимі.

Переваги використання подібного програмного забезпечення – це спрощення процесів самостійного обслуговування в галузі електронної комерції та електронного уряду; перевірка особистості та віддалений збір даних в електронних онлайн-системах; портативні станції перевірки в галузі прикордонного контролю та діяльності правоохоронних органів; перевірка документів та фізичних осіб на поїздах та круїзних лайнерах [8].

Також до складу розробки входить програмний компонент для системних інтеграторів, тобто додаток надає технологію Application Programming Interface (API) для інтеграції.

Це не єдиний мобільний додаток, який дозволяє здійснювати електронну ідентифікацію особистості. Проте, типові рішення не завжди підходять для окремих предметних галузей.

Таким чином, для відкриття рахунку у банку за допомогою мобільного додатку потрібно розробити програмне забезпечення, яке буде відповідати всім вимогам банку.

2 ОПИС СТРУКТУРНИХ І ФУНКЦІОНАЛЬНИХ ОСОБЛИВОСТЕЙ ЗАДАЧІ

2.1 Аналіз та опис об'єкта автоматизації

Об'єктом автоматизації є операційний і клієнтський відділи комерційного банку.

Організаційний устрій комерційних банків відповідає загальноприйнятій схемі управління акціонерним товариством..

Поточне керівництво діяльністю комерційного банку здійснюється її одноосібним виконавчим органом, тобто колегіальним виконавчим органом – правлінням банку, яке:

- визначає та затверджує структуру банку;
- здійснює добір кадрів, встановлює чисельність персоналу та розмір оплати праці;
- контролює виконання працівниками вимог законодавства;
- розглядає та затверджує звіти підрозділів банку;
- визначає принципи відсоткової політики та ін.

Правління несе відповідальність перед загальними зборами акціонерів та радою директорів банку. Правління складається з голови правління, його заступників та інших членів.

Голова правління (президент) банку:

- організує виконання рішень загальних зборів та ради директорів банку;
- керує роботою правління банку та ін.

Засідання правління банку проводяться регулярно. Рішення ухвалюються більшістю голосів. За рівності голосів голос голови є вирішальним. Рішення правління оформлюються у формі наказу голови правління банку.

За правління банку створюється кредитний комітет. До функцій

кредитного комітету входять:

- розробка кредитної політики банку, структури коштів, що залучаються, та їх розміщення;
- підготовка висновків щодо надання позичок;
- розгляд питань, пов'язаних з інвестуванням та веденням трастових операцій.

На рисунку 2.1. наведено схему організаційної структури банку

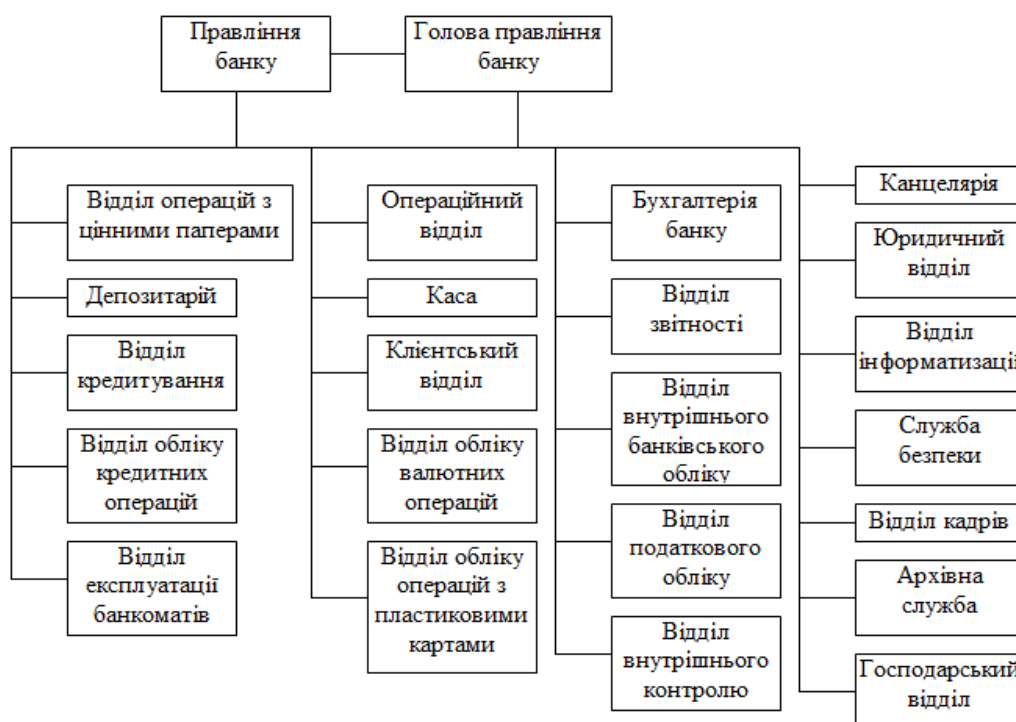


Рисунок 2.1 – Схема організаційної структури комерційного банку

До банківських операцій належать:

- залучення коштів фізичних та юридичних осіб у вклади (до запитання та на визначений строк);
- розміщення залучених коштів від свого імені та за свій рахунок;
- відкриття та ведення банківських рахунків фізичних та юридичних осіб;
- здійснення розрахунків за дорученням фізичних та юридичних

осіб, у тому числі банків-кореспондентів, за їх банківськими рахунками;

– інкасація грошових коштів, векселів, платіжних та розрахункових документів та касове обслуговування фізичних та юридичних осіб;

– купівля-продаж іноземної валюти у готівковій та безготівковій формах;

– залучення у вклади та розміщення дорогоцінних металів;

– видача банківських гарантій.

2.2 Обґрунтування мети вирішення задачі

Стандартна процедура відкриття рахунків передбачає особисту присутність людини, яка збирається відкрити рахунок у відділенні банку. Також необхідна наявність документів для підтвердження особистості та пакет документів, визначених чинним законодавством.

Людина, яка відкриває рахунок, має заповнити відповідну заяву та укласти угоду з банком у письмовій формі.

Працівник банку (співробітник операційного відділу) перевіряє документи, які підтверджують особистість того, хто відкриває рахунок, фактично вручну (або з використанням електронної системи).

Якщо запроваджувати відкриття рахунку дистанційно, за допомогою мобільного додатку, то верифікація особистості є ключовим питанням, оскільки заповнення заяви та угоди і завантаження копій документів для сучасних мобільних пристроїв не є проблемою.

Цифрове рішення для підтвердження особистості громадянина допоможе вирішити цю проблему. Крім онлайн-аутентифікації та входу в систему є інші можливості використання онлайн перевірки особистості, оскільки багато різних служб, як державних, так і комерційних, у такий спосіб можуть надавати різні послуги.

2.3 Функціональна структура IT-сервісу

Функціональна структура IT-сервісу онлайн ідентифікації особистості подана у вигляді UML-діаграм типу Use Case та Activity.

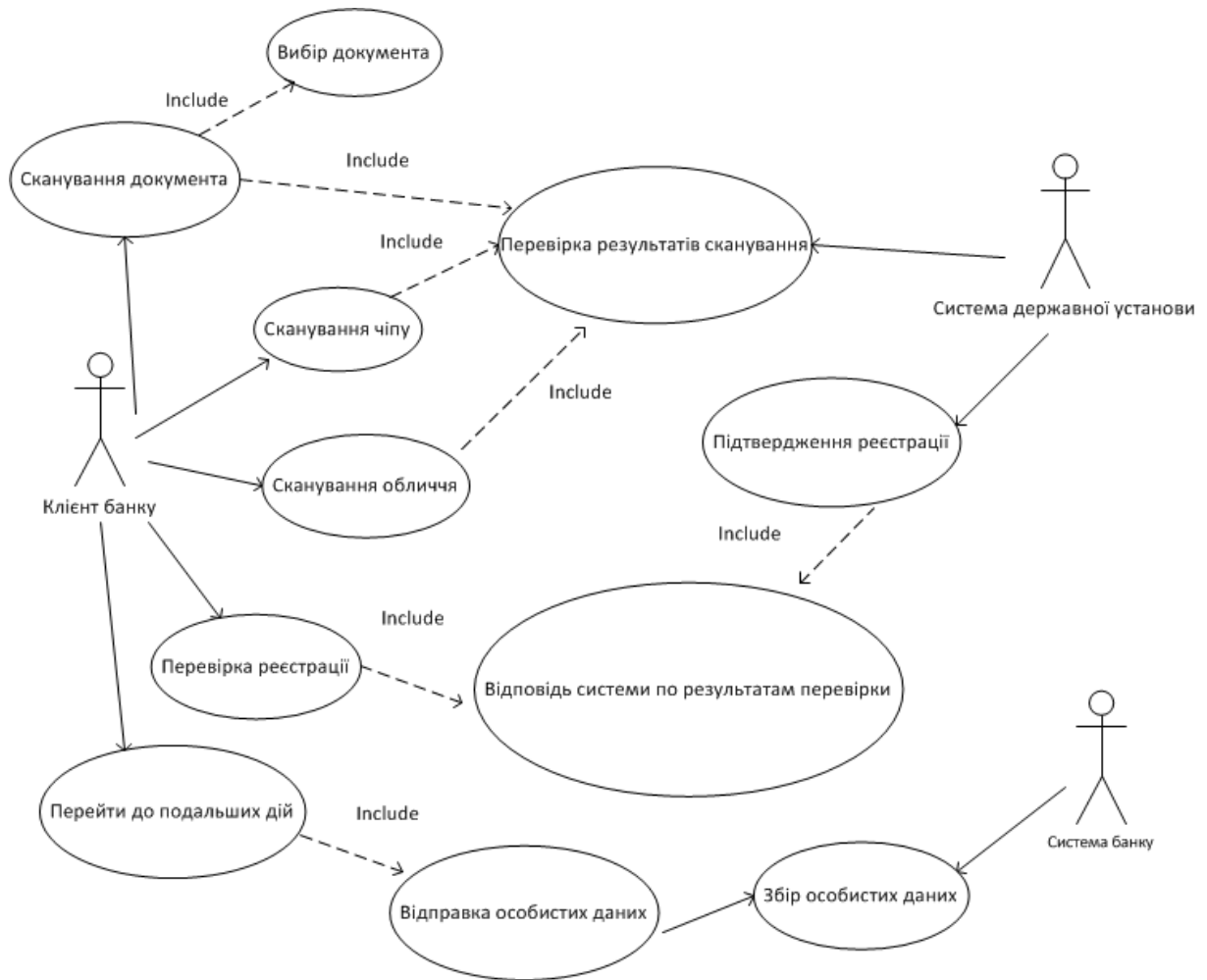


Рисунок 2.2 – Діаграма Use Case

Діаграма налічує дев'ять варіантів використання та три включення (include), які означають, що базова послідовність дій не може бути виконана без них.

Актори діаграми:

- клієнт банку – користувач IT-сервісу онлайн ідентифікації

особистості;

– система державної установи – це система, яка зберігає та перевіряє особисті дані особи;

– система банку отримує від мобільного додатку особисті дані потенційного клієнта.

У таблиці 2.1 наведений опис варіантів використання.

Таблиця 2.1 – Опис варіантів використання

Назва	Опис
1	2
Сканування документу	Сканування документу з лицьового та зворотного боку (за умови, що документ обраний). Відправка даних до державної системи.
Сканування чіпу	Сканування електронного чіпу на документі. Відправка даних до державної системи.
Сканування обличчя	Сканування обличчя (selfie). Відправка даних до державної системи.
Перевірка реєстрації	Заповнення адреси проживання (прописка/реєстрація). Відправка даних до державної системи.
Перевірка результатів сканування	Система державної установи здійснює перевірку всіх відправлених даних.

Кінець таблиці 2.1

1	2
Підтвердження реєстрації	Прописка/реєстрація перевіряється в останню чергу. Після цього система надає відповідь стосовно результатів перевірки.
Перейти до подальших дій	Клієнт переходить до подальших дій після успішної перевірки особистості.
Збір особистих даних	Система банку зберігає особисті дані потенційного клієнта у своїй базі даних.

Для варіанту використання "Перевірка реєстрації" створена діаграма діяльності наведена на рисунку 2.3.

Цей пункт виконання програми передбачає, що потрібно ввести дані місця проживання (адресу, місто, країну, тощо), відправити їх до системи. У випадку підтвердження реєстрації процедуру ідентифікації особистості буде завершено. Якщо під час введення даних були зроблені помилки, то система поверне форму для вводу даних з повідомленням про помилку.

Після виправлення помилок форму потрібно відправити повторно. Якщо реєстрація підтверджена, то процедуру онлайн ідентифікації особистості завершено успішно. В іншому випадку буде отримано повідомлення, що ідентифікація не відбулася.

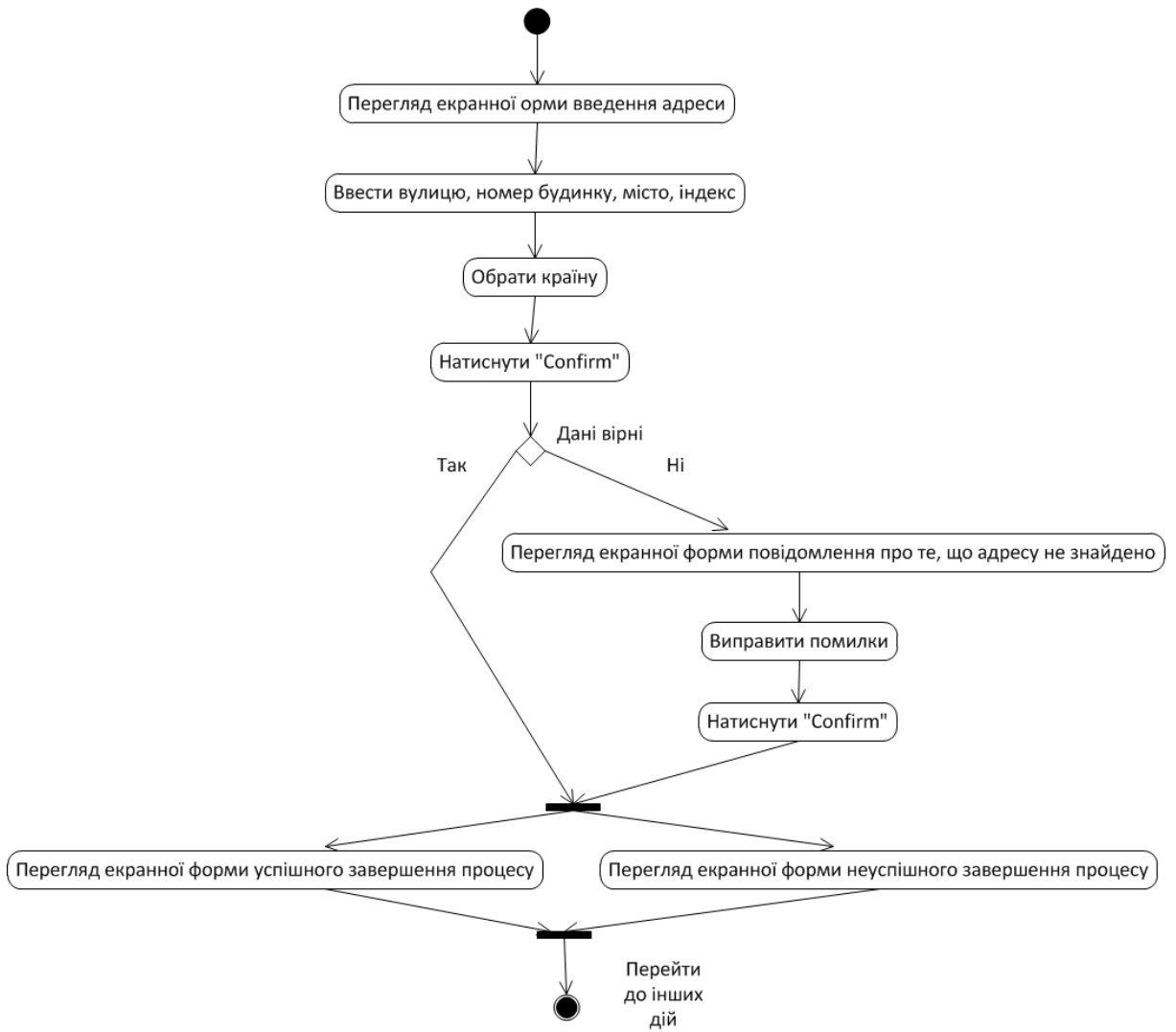


Рисунок 2.3 – Діаграма Activity для варіанту використання "Перевірка реєстрації"

2.4 Вимоги до IT-сервісу

IT-сервіс для онлайн ідентифікації особистості має інтуїтивно зрозумілий інтерфейс, тому не потребує додаткового навчання користувачів. Також, майже кожна дія сервісу супроводжується детальними інструкціями.

Вимоги до технічного забезпечення.

У якості технічного забезпечення виступають дівайси як з боку установи банку, так і з боку користувача (людини, яка відкриває рахунок).

З боку установи банку – це сервери та службові дівайси працівників операційного відділу. З боку користувача має бути мобільний пристрій, який підтримує технології NFC та ICAO, а також дозволяє сканувати RFID-чіпи.

Також пристрій користувача повинен бути здатний сканувати фото високої роздільної здатності. Тобто онлайн-перевірка має на увазі, що смартфон користувача є зчитувачем ідентифікаторів, де проводяться всі перевірки. Як сторонній елемент ланцюжка він може бути зброєю для шахраїв, які можуть використовувати ін'єкційні атаки, повертаючи змінені результати перевірки у систему. У нульовій довірі до мобільної перевірки сервер компанії бере активну участь у процесі як периметр довіри, де виконується фактичний сеанс перевірки або де результати перевірки, згенеровані на пристрої користувача, повторно перевіряються. Це дозволяє запобігти шахрайському вторгненню в процес перевірки за допомогою таких змін, як зміна результату перевірки електронного посвідчення особи з «не пройдено» на «пройдено».

Вимоги до програмного забезпечення.

Програмне забезпечення для перевірки особистості може також забезпечити автоматизацію введення даних, позбавляючи користувачів необхідності заповнювати заяви та реєстраційні форми. В результаті

отримуємо безпечний потік без друкарських помилок і незадоволених клієнтів.

Проте, комерційні компанії не можуть повною мірою використовувати весь потенціал електронних посвідчень особи в онлайн-сценарії, оскільки вони не можуть отримати доступ до всіх даних, що зберігаються на RFID-чипі. Конфіденційні дані, такі як відбитки пальців, можуть бути зчитані та перевірені лише органами влади. Це означає, що для підприємств перевірка NFC зводиться до перевірки наявності та цілісності RFID-чипа у поданому посвідченні особи.

У IT-сервісі ідентифікація та біометрична перевірка об'єднані через запит селфі користувача для визначення його життєздатності та спробу зіставити його з усіма портретами власника у посвідченні особи, щоб переконатися, що документ належить користувачеві.

Вимоги до інформаційного забезпечення.

Після запиту на відкриття рахунку з боку комерційного банку буде створено обліковий запис клієнта. Дані, які формують обліковий запис, будуть збережені з боку комерційної структури. Частково вони будуть розташовані у базі даних, а частково зберігатимуться у файлах різного формату. Наприклад, ПІБ, адреса, серія та номер паспорта клієнта будуть зберігатися у базі даних (БД), а заявка на відкриття рахунку та угода, будуть збережені у вигляді текстових документів.

3 ПОСТАНОВКА ЗАДАЧІ

3.1 Характеристика поставленої задачі

Метою розробки IT-сервісу онлайн ідентифікації особистості є створення цифрового рішення для підтвердження особистості громадянина під час використання послуг, які надаються банком.

Користувачами IT-сервісу фактично будуть усі поточні та потенційні клієнти банку.

Завдання не може бути виконано, якщо:

- відсутнє з'єднання з мережею Інтернет;
- особливості тарифу користувача (обмежена кількість Гб) не дозволяють виконати дії з ідентифікації;
- відсутнє з'єднання з серверами банку або державної установи, до якої відправляється запит на перевірку.

Електронна ідентифікація гарантує справжність документа і те, що людина, яка її проходить, є тим, за кого себе видає. Конфіденційні документи захищені від несанкціонованого доступу, у такий спосіб забезпечується конфіденційність.

Також електронна ідентифікація пришвидшує процес підписання, роблячи його зручнішим порівняно з традиційними методами.

Електронна ідентифікація підвищує надійність та цілісність електронних транзакцій завдяки правилам та стандартам перевірки електронних підписів.

Ідентифікація особистості пов'язана з задачами операційного відділу, такими як облік відкритих і закритих рахунків приватних та юридичних осіб, залучення грошових коштів на депозити, розташування залучених засобів, валютно-обмінні операції та ін.

3.2 Вихідна інформація задачі

Таблиця 3.1 – Перелік вихідних повідомлень IT-сервісу онлайн ідентифікації особистості

Повне найменування	Ідентифікатор	Форма подання	Періодичність і термін видачі	Допустимий час затримки
Повідомлення про завершення процесу	completion	Відеограма	За вимогою	5 секунд
Повідомлення про незнайдену адресу	address	Відеограма	За вимогою	5 секунд
Інструкції сканування	instruction	Відеограма	За вимогою	5 секунд

Таблиця 3.2 – Опис структурних одиниць вихідного повідомлення "Повідомлення про завершення процесу" (completion)

Повне найменування	Ідентифікатор	Тип інформації	Загальна кількість символів	Форма подання
Текст повідомлення	text	Символьний	256	Текст

Таблиця 3.3 – Опис структурних одиниць вихідного повідомлення "Повідомлення про незнайдену адресу" (address)

Повне найменування	Ідентифікатор	Тип інформації	Загальна кількість символів	Форма подання
Текст повідомлення	text	Символьний	256	Текст
Вулиця	street	Символьний	50	Текст
Будинок	number	Символьний	10	xxx
Місто	city	Символьний	50	Назва
Країна	country	Символьний	50	Назва
Поштовий індекс	code	Цифровий	7	XXXXXX

Таблиця 3.4 – Опис структурних одиниць вихідного повідомлення "Інструкції сканування" (instruction)

Повне найменування	Ідентифікатор	Тип інформації	Загальна кількість символів	Форма подання
Текст інструкції	text	Символьний	256	Текст

3.3 Вхідна інформація задачі

Таблиця 3.5 – Перелік вхідних повідомлень IT-сервісу онлайн ідентифікації особистості

Повне найменування	Ідентифікатор	Формат подання	Періодичність отримання	Джерело
Відсканований документ	document	Відеограма	За вимогою	Клієнт банку
Відсканований біометричний чіп	chip		За вимогою	Клієнт банку
Відскановане обличчя	face		За вимогою	Клієнт банку
Адреса прописки/реєстрації	address		За вимогою	Клієнт банку

Таблиця 3.6 – Опис структурних одиниць вхідного повідомлення "Відсканований документ" (document)

Повне найменування	Ідентифікатор	Тип інформації	Тимчасові інтервали і частота одержання	Спосіб введення
1	2	3	4	5
Унікальний ID сканування	Number mf	Символьний	За вимогою	Сканування

Кінець таблиці 3.7

1	2	3	4	5
Номер документа	number_doc	Символьний	За вимогою	Сканування
Тип документа	type_doc	Символьний	За вимогою	Сканування
Країна	country	Символьний	За вимогою	Сканування
Прізвище	surname	Символьний	За вимогою	Сканування
Ім'я	name	Символьний	За вимогою	Сканування
По батькові	patronymic	Символьний	За вимогою	Сканування
Дата народження	date_b	Символьний	За вимогою	Сканування
Стать	gender	Символьний	За вимогою	Сканування
Громадянство	nation	Символьний	За вимогою	Сканування
Дата видачі	date_is	Символьний	За вимогою	Сканування
Термін дії	validity	Символьний	За вимогою	Сканування

Таблиця 3.7 – Опис структурних одиниць вхідного повідомлення
"Відсканований біометричний чіп" (chip)

Повне найменування	Ідентифікатор	Тип інформації	Тимчасові інтервали і частота одержання	Спосіб введення
1	2	3	4	5
Номер документа	number_doc	Символьний	За вимогою	Сканування
Тип документа	type_doc	Символьний	За вимогою	Сканування
Країна	country	Символьний	За вимогою	Сканування
Прізвище	surname	Символьний	За вимогою	Сканування
Ім'я	name	Символьний	За вимогою	Сканування
По батькові	patronymic	Символьний	За вимогою	Сканування
Дата народження	date_b	Символьний		
Стать	gender	Символьний		
Громадянство	nation	Символьний		
Дата видачі	date_is	Символьний		
Термін дії	validity	Символьний		
Фото обличчя	photo	Зображення		
Формат зображення	format_im	Зображення		
Ширина зображення	width	Числовий		

Кінець таблиці 3.7

1	2	3	4	5
Висота зображення	height	Числовий	За вимогою	Сканування
Номер пальця	finger	Числовий		
Біометричне зображення	image	Зображення		
Формат	format	Символьний		

Таблиця 3.8 – Опис структурних одиниць вхідного повідомлення "Відскановане обличчя" (face)

Повне найменування	Ідентифікатор	Тип інформації	Тимчасові інтервали і частота одержання	Спосіб введення
Відскановане обличчя	face	Зображення	За вимогою	Сканування

Таблиця 3.9 – Опис структурних одиниць вхідного повідомлення "Адреса прописки/реєстрації" (address)

Повне найменування	Ідентифікатор	Тип інформації	Тимчасові інтервали і частота одержання	Спосіб введення
1	2	3	4	5
Вулиця	street	Символьний	За вимогою	З клавіатури
Будинок	number	Символьний	За вимогою	З клавіатури
Місто	city	Символьний	За вимогою	З клавіатури

Кінець таблиці 3.9

1	2	3	4	5
Країна	country	Символьний	За вимогою	3 клавіатури
Поштовий індекс	code	Цифровий	За вимогою	3 клавіатури

4 РОЗРОБКА ТА ОБҐРУНТУВАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ІТ-СЕРВІСУ

До складу ІТ-сервісу онлайн ідентифікації особистості входить база даних, яка зберігає паспортні дані людини, що збирається віддалено відкривати рахунок у банку. Оскільки сервіс є проміжною ланкою під час процедури відкриття рахунку, то база даних сервісу містить тільки дані, які підтверджують особистість, і статус підтвердження (у випадку, якщо підтвердження відбулося).

ІТ-сервіс онлайн ідентифікації особистості налічує 5 сутностей. Сутності Document, Person і Doctype зв'язані між собою за принципом "один-до-багатьох". Сутності Document, Chip і Address зв'язані між собою за принципом "один-до одного". Таким чином document_id у таблицях Chip та Address є полем підстановки, яке шукає значення індекса документу у таблиці Document, тобто виключає можливість додавання коду документа, якого не існує.

Сутності, типи зв'язків та атрибути наведено у таблицях 4.1, 4.2 та 4.3 відповідно.

Таблиця 4.1 – Відомості про сутності

Ім'я сутності	Визначення
1	2
Person	Інформація про персону
Document	Інформація про документ
Doctype	Інформація про тип документу
Chip	Інформація про чіп з документу
Address	Інформація про адресу з документу

Таблиця 4.2 – Відомості про типи зв'язків

Ім'я сутності	Тип зв'язку	Тип сутності	Кардинальність
Document	містить	Doctype	М : 1
Chip	містить	Document	1 : 1
Address	містить	Document	1 : 1
Document	містить	Person	М : 1

Таблиця 4.3 – Відомості про атрибути

Ім'я сутності	Атрибут	Опис	Тип даних, довжина	Обмеження	Допустимість Null
1	2	3	4	5	6
Person	person_id	Унікальний ідентифікатор сутності	INTEGER	PK	Ні
	name	Ім'я	VARCHAR(15)		Ні
	surname	Прізвище	VARCHAR(15)		Ні
	patronymic	По батькові	VARCHAR(15)		
	status	Статус підтвердження	VARCHAR(20)		Ні
Document	document_id	Унікальний ідентифікатор сутності	INTEGER	PK	Ні
	doctype_id	Ідентифікатор типу документу	INTEGER	FK	Ні

Продовження таблиці 4.3

1	2	3	4	5	6
	person_id	Ідентифікатор персони	INTEGER	FK	Hi
	number	Номер/серія документу	VARCHAR(20)		Hi
	datebirth	Дата народження	DATETIME		Hi
	date	Дата видачі	DATETIME		Hi
	gender	Стать	VARCHAR(1)		Hi
	country	Опис	VARCHAR(10)		Hi
	expiry	Термін дії	DATETIME		Hi
	photo	Фото	BLOB		Hi
Doctype	doctype_id	Унікальний ідентифікатор сутності	INTEGER	PK	Hi
	name	Назва типу документу	VARCHAR(20)		Hi
Chip	chip_id	Унікальний ідентифікатор сутності	INTEGER	PK	Hi
	document_id	Ідентифікатор документа	INTEGER	PK	Hi
	f_index	Номер пальця	INTEGER		Hi
	image	Зображення	BLOB		Hi
Address	address_id	Унікальний ідентифікатор сутності	INTEGER	PK	Hi

Кінець таблиці 4.3

1	2	3	4	5	6
	document_id	Ідентифікатор документа	INTEGER	PK	Hi
	street	Номер акту	VARCHAR(20)		Hi
	number	Номер будинку	INTEGER		Hi
	city	Місто	VARCHAR(20)		Hi
	country	Країна	VARCHAR(20)		Hi
	postcode	Індекс	INTEGER		Hi

Схеми логічної та фізичної моделі даних наведені на рис. 4.1 та 4.2.

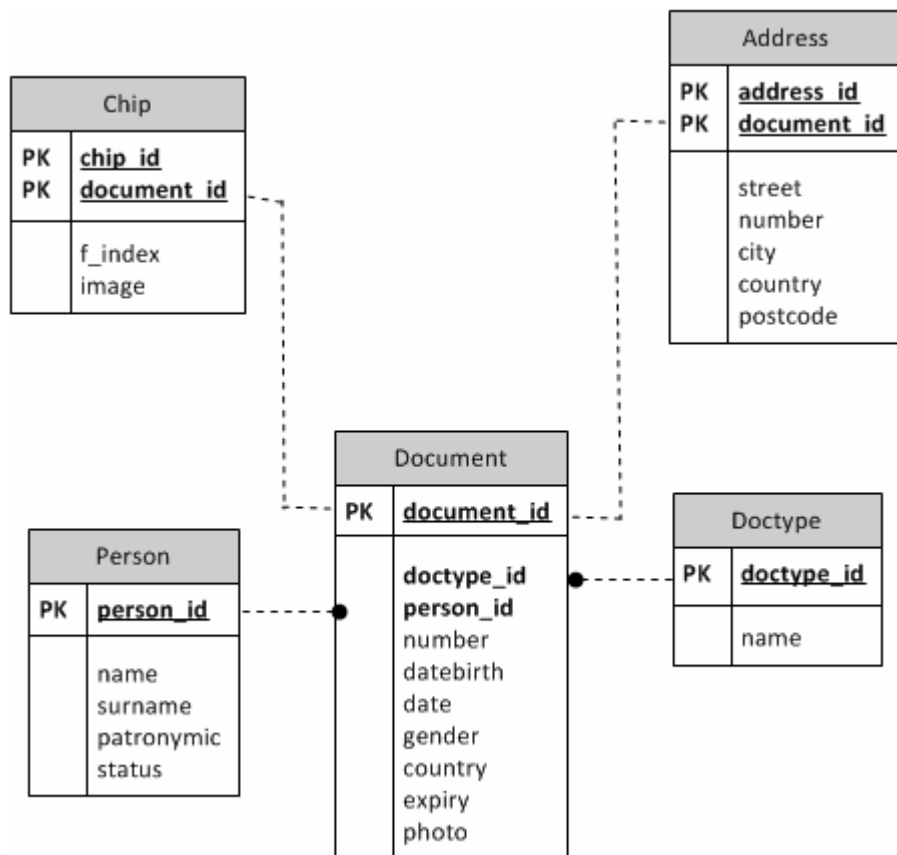


Рисунок 4.1 – Схема логічної моделі даних

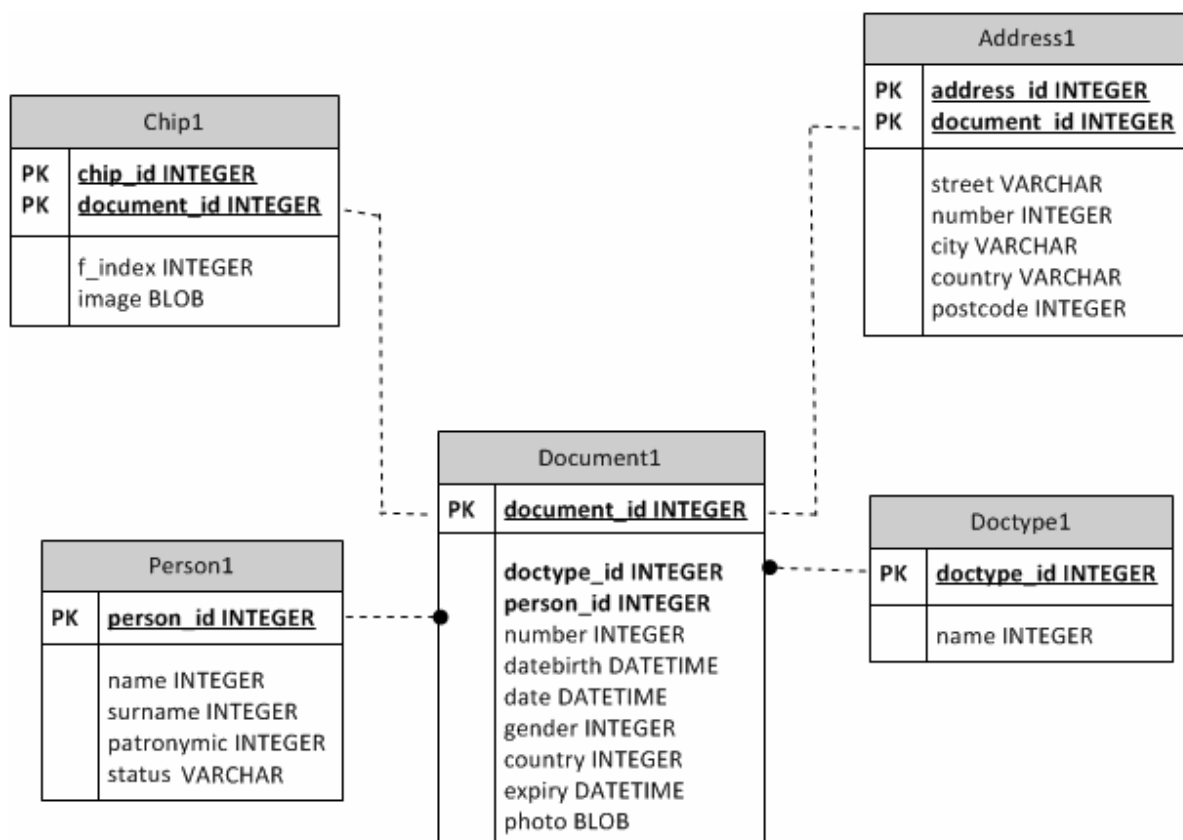


Рисунок 4.2 – Схема фізичної моделі даних

5 МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ ІТ-СЕРВІСУ

Математичне забезпечення ІТ-сервіс для онлайн ідентифікації особистості наведено у вигляді схеми роботи сервісу.

Під час поточної роботи ІТ-сервісу генеруються наступні вихідні документи:

1. Повідомлення про завершення процесу (текст повідомлення залежить від успішного або неуспішного завершення ідентифікації).
2. Повідомлення про незнайдену адресу (буде отримано у випадку помилок у адресі) містить поля для повторного введення адреси.
3. Інструкції сканування (текст, який описує порядок сканування документів).

Схема роботи ІТ-сервісу наведена на рисунку 5.1, аркуш 1.

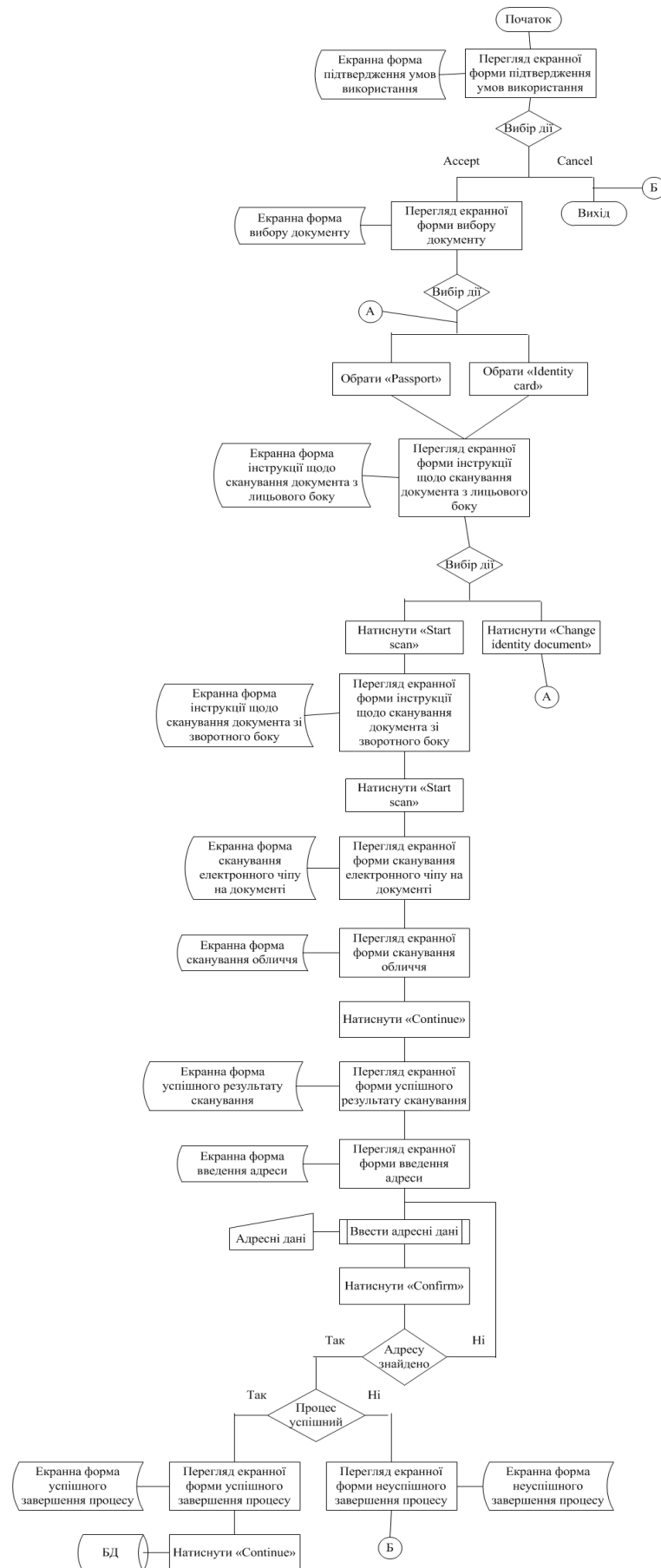


Рисунок 5.1 – Схема роботи ІТ-сервіс для онлайн ідентифікації особистості

6 РОЗРОБКА ЕЛЕМЕНТІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ IT-SERVІСУ

Розроблений програмний продукт є фреймворком Software Development Kit (SDK), який інтегрується в проект замовника як зовнішня залежність.

SDK – комплект засобів розробки, який дозволяє фахівцям з програмного забезпечення створювати програми для певного пакета програм, програмного забезпечення базових засобів розробки, апаратної платформи, комп'ютерної системи, ігрових консолей, операційних систем та інших платформ.

У розробці запропоновано рішення для Frontend (Web + мобільні додатки iOS та Android) та Backend. Після інтеграції замовник отримує працюючий процес (Flow) для ідентифікації особи користувача з підсумковим результатом – чи то успіх (Success), помилка (Failed), скасування процесу користувачем (User cancelled process) або технічною помилкою (User encountered a technical error).

Backend-частина розробки надає інструкції про подальші кроки для успішної ідентифікації, а Frontend-частина на основі цих інструкцій візуалізує відповідний інтерфейс користувача (User Interface, UI).

Процес ідентифікації може містити кілька етапів, таких як сканування документа з обох боків, сканування голограми та чіпа (якщо він присутній), а також сканування особи користувача для порівняння з фотографію на документі.

У деяких випадках можлива додаткова верифікація, наприклад, підтвердження адреси або відеодзвінок з оператором для перевірки даних вручну. Після завершення процесу інтегратор отримує фінальний результат про те, чи були всі дії завершені успішно, чи ні.

Для початку процесу інтегратор надсилає запит на сервер розробленого додатку для відкриття сесії, у відповіді на які повертається унікальний ідентифікатор сесії. Цей ідентифікатор необхідний для роботи продукту і дозволяє відстежувати активність замовника, встановлювати ліміти на використання продукту та виставляти рахунки виходячи з кількості створених сесій, оскільки всі дані обробляються на боці розробленого додатку.

Для інтеграції розробленого програмного продукту Backend програмного забезпечення замовника має підключити його як зовнішню залежність. При отриманні запиту на ідентифікацію користувача Backend замовника звертається до розробленого ПЗ Backend для створення нової сесії.

Сервер розробленого ПЗ автоматично відкриває сесію та повертає унікальний ідентифікатор, який передається на Frontend замовника. Frontend замовника також має інтегрувати розроблений SDK як зовнішню залежність та налаштувати необхідні параметри конфігурації.

Після налаштування та отримання ідентифікатора сесії, переданого з Backend, процес може бути запущений. Усі подальші дії, що стосуються користувацького інтерфейсу та логіки процесу ідентифікації виконує розроблений програмний продукт.

Розроблений додаток надає екрани для всіх етапів процесу, включаючи сканування документів та особи. Інтерфейс побудований за принципом "white-labeled app", що дозволяє замовнику адаптувати зовнішній вигляд екранів під свої потреби – змінювати кольори, локалізацію, зображення, анімації і навіть замінити деякі екрани своїми. Це забезпечує гнучкість у налаштуванні продукту під конкретний дизайн інтегратора.

Підтримка для інтегратора. Інтегратори завжди можуть зв'язатися з менеджерами компанії-розробника ПЗ для вирішення виникаючих питань чи проблем. Інтеграторам також надається доступ до спеціальної дошки у

Jira, де вони можуть створювати баг-репорти, описуючи знайдені помилки, щоб розробники могли оперативно виправити їх у наступних релізах.

У окремих випадках менеджери можуть налагодити прямий контакт з розробниками для глибших технічних питань.

Інтегратор має обмежений доступом до даних. Під час процесу ідентифікації будуть передані логи, що дозволяють програмістам з боку інтегратора відстежувати, що відбувається, без розкриття особистої інформації користувача, що важливо для дотримання конфіденційності.

У логах фіксується активність дії користувача у процесі ідентифікації, а також поточний стан системи (у тому числі регулярні повідомлення від сервера розробленого ПЗ про перебіг процесу)

Інтегратори повинні коректно опрацьовувати всі кінцеві точки розробленого SDK. Процес може завершитися з різними результатами (Success, Failure, Error, тощо), та кожен з цих випадків має бути оброблений з боку замовника.

У випадку необхідності замовник може надати власну кастомізацію, а також вказати контактну інформацію служби підтримки, яка буде доступна користувачам у випадку виникнення питань чи проблем під час процесу.

7 ВИБІР ТА ОБҐРУНТУВАННЯ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ

IT-сервіс для онлайн ідентифікації особистості – це мобільний додаток, який є частиною загальної інформаційної системи банку. Дані, які будуть отримані та сформовані в результаті ідентифікації особистості для відкриття рахунку, будуть збережені на серверах банку. Вони потраплять туди через мережу Інтернет після сканування за допомогою пристрою користувача та розробленого мобільного додатку.

У таблиці 7.1 наведено типові характеристики окремих пристроїв, які можуть бути задіяні у комплексі технічних засобів.

Таблиця 7.1 – Специфікація типового обладнання

Іменування	Характеристика
1	2
Смарфон	NFC; Android 10.0; GSM, 3G, 4G; GPRS, EDGE, UMTS, HSPA+, LTE; 2 SIM; Nano-SIM + Nano-SIM + microSD; Qualcomm Snapdragon 450, 1.8 ГГц, 8 ядер; 8x1.8 ГГц Cortex-A53; Adreno 506; 2 Гб; 32 Гб (eMMC 5.1); microSD до 512 Гб; 6.4", 1560x720 (19.5:9), 268 ppi; 13 Мп, f/1.8, 27 мм; 5 Мп, f/2.2, 115°; 2 Мп, f/2.4; 1080p (30 к/с); 8 Мп, f/2.0; 1080p (30 к/с); Wi-Fi 4 (802.11n); Bluetooth 4.2; USB Type-C, mini-Jack 3.5 mm; GPS (A-GPS), Galileo, BeiDou; сканер обличчя; сканер відбитка пальця.

На рисунку 7.1 зображено схему підключення технічних засобів

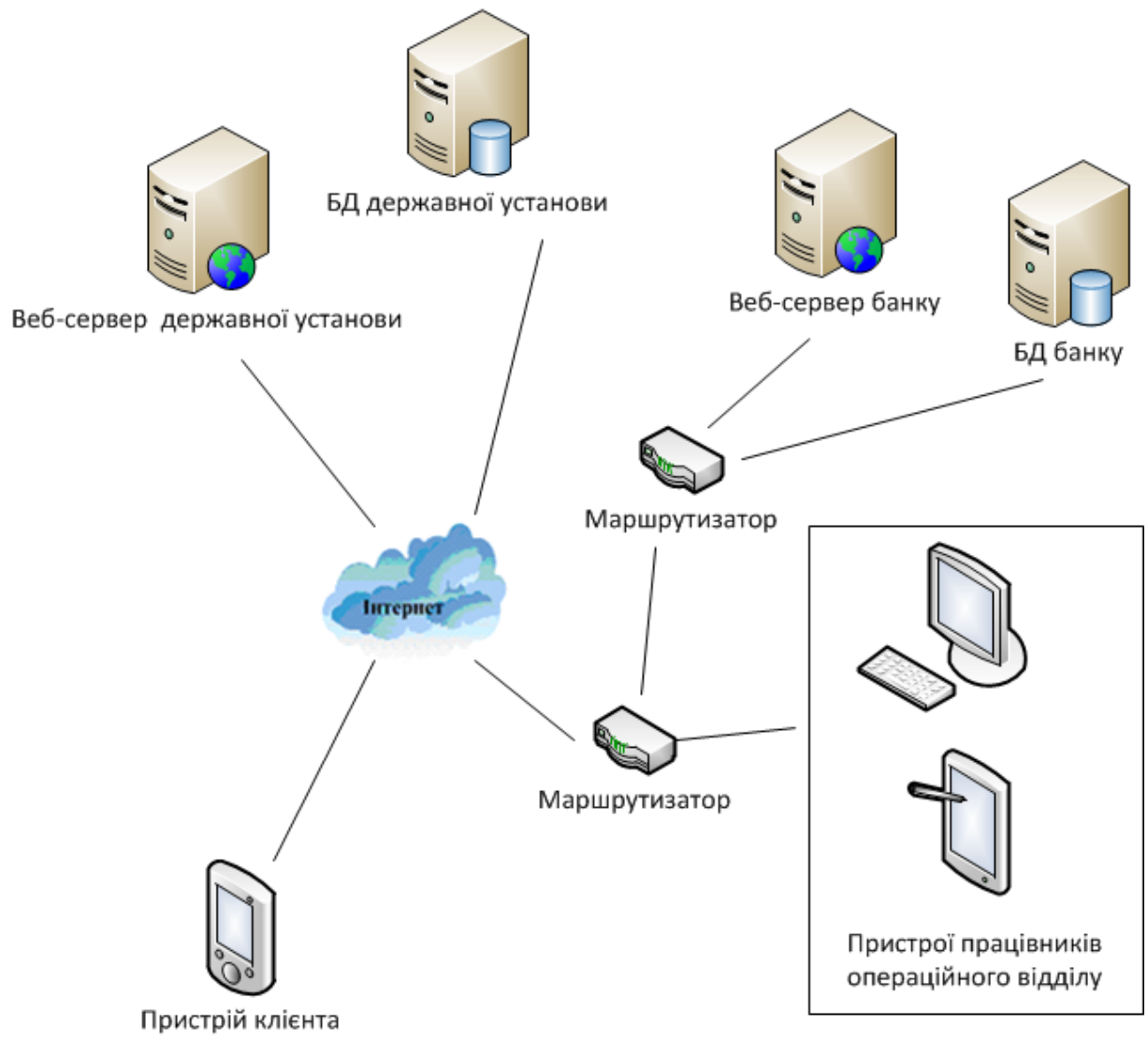


Рисунок 7.1 – Схема підключення технічних засобів

8 МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ СЕРВІСУ

Для онлайн ідентифікації особистості було створено ІТ-сервіс у вигляді мобільного додатка. Після запуску додатка буде відкрита стартова екранна форма (рисунок 8.1) з переліком інструкцій та умов використання. Для того, щоб почати процедуру ідентифікації, потрібно ознайомитись з умовами використання та натиснути "Асепт".

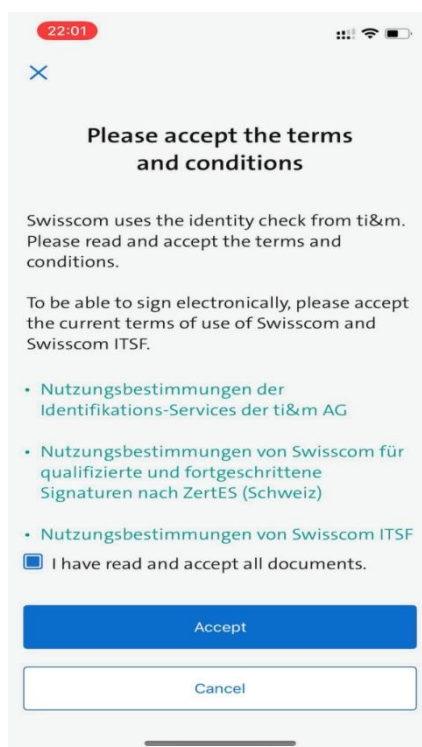


Рисунок 8.1 – Екранна форма підтвердження умов використання

Наступний крок – це вибір документа для підтвердження особистості (рисунок 8.2). Можна обирати один з двох варіантів: паспорт або ідентифікаційна карта. Після вибору документа потрібно натиснути на одну з двох позначок. Після цього буде відкрита екранна форма з інструкціями сканування документа з лицьового боку (рисунок 8.3).

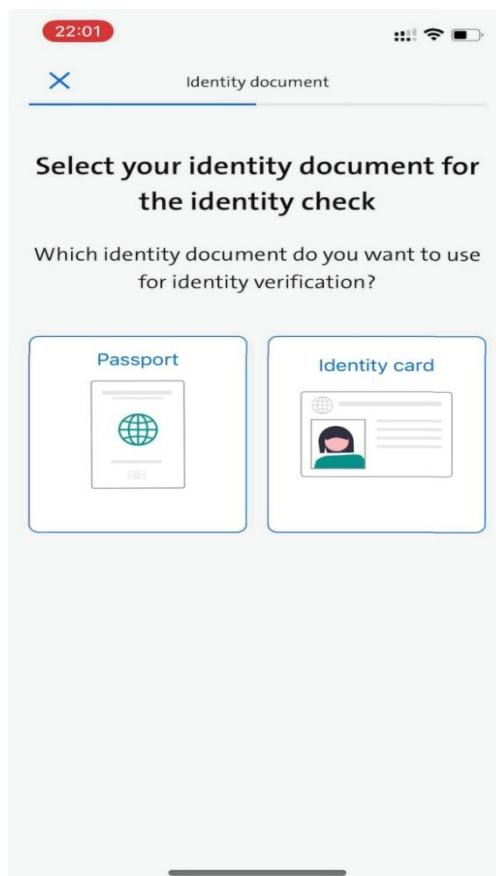


Рисунок 8.2 – Екранна форма вибору документу для підтвердження особистості

Після ознайомлення з інструкцією потрібно натиснути "Start scan" або обрати інший документ для сканування. Наступна екранна форма (рисунок 8.4) містить інструкції для сканування зворотного боку документа. Після ознайомлення, також потрібно натиснути "Start scan".

Оскільки на документі може бути електронний чіп, його також потрібно сканувати. Екранна форма на рисунку 8.5 описує сканування чіпа.

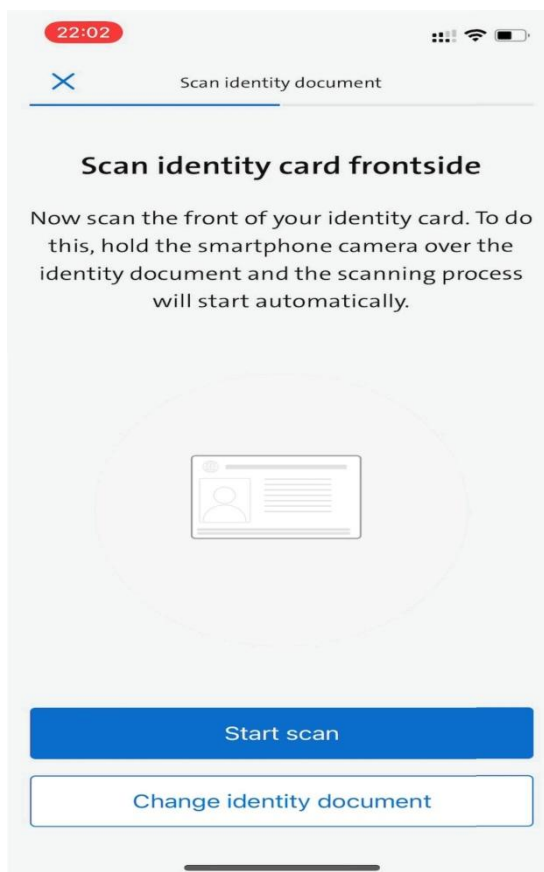


Рисунок 8.3 – Екранна форма інструкції щодо сканування документа з лицьового боку

Після сканування документа потрібно відсканувати обличчя для підтвердження особистості (рисунок 8.6). Якщо сканування відбулося успішно, то буде відкрита екранна форма з повідомленням "Success" (рисунок 8.7).

Останній етап підтвердження особистості – перевірка адреси. Потрібно ввести адресу прописки/реєстрації (екранна форма на рисунку 8.8). Якщо була помилка під час введення адреси, то буде відкрита екранна форма з повідомленням про помилку (рисунок 8.9). Потрібно виправити помилку та повторно відправити дані. В результаті обробки даних буде прислано повідомлення про успішне (рисунок 8.11) або неуспішне (рисунок 8.10) завершення процесу ідентифікації особистості.

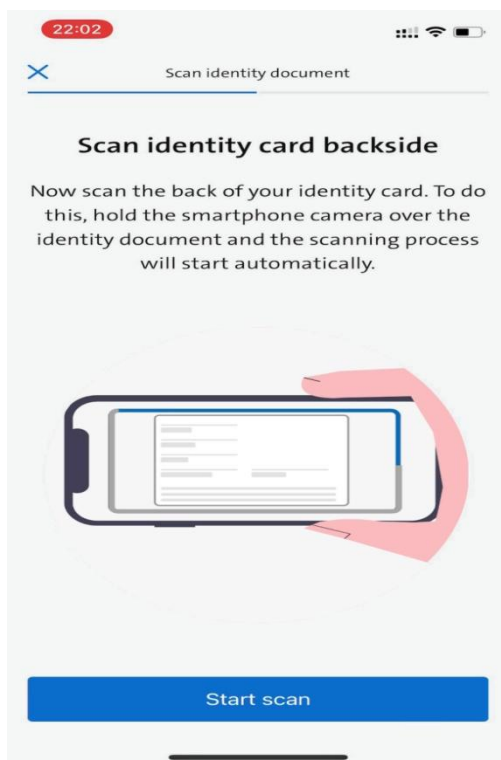


Рисунок 8.4 – Екранна форма інструкції щодо сканування документа зі зворотного боку

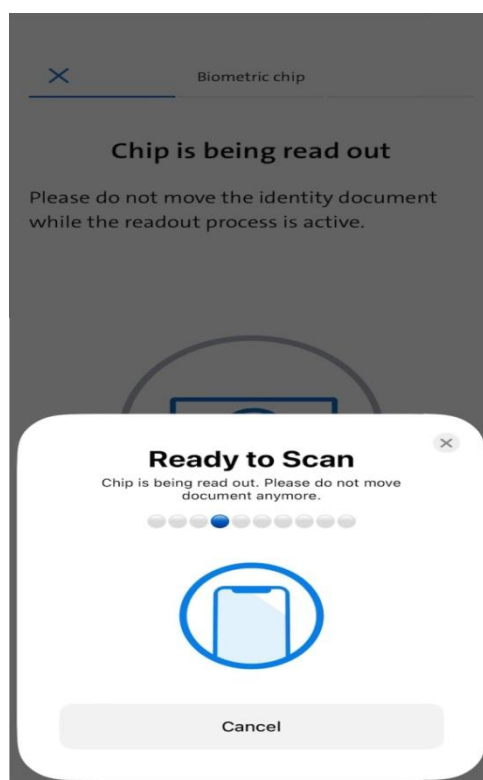


Рисунок 8.5 – Екранна форма сканування електронного чіпу на документі

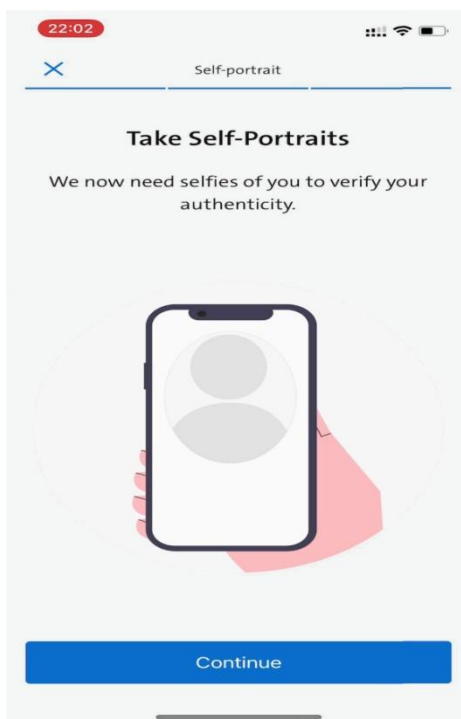
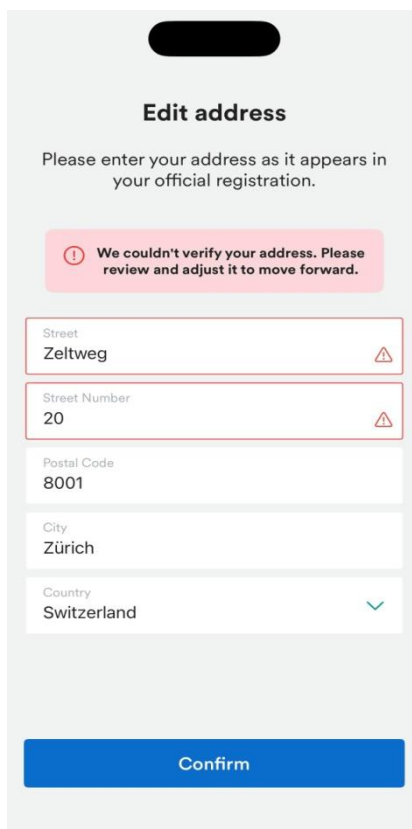


Рисунок 8.6 – Екранна форма сканування обличчя для підтвердження особистості

A screenshot of a mobile application interface for editing an address. The title 'Edit address' is centered at the top in bold black text. Below the title is the instruction 'Please enter your address as it appears in your official registration.' in a smaller black font. The form consists of five stacked input fields, each with a light gray border and a white background. The first field is labeled 'Street' and contains the text 'Zeltweg'. The second field is labeled 'Street Number' and contains '20'. The third field is labeled 'Postal Code' and contains '8001'. The fourth field is labeled 'City' and contains 'Zürich'. The fifth field is labeled 'Country' and contains 'Switzerland', with a small green checkmark icon to its right. At the bottom of the screen, there is a prominent blue button with the white text 'Confirm'.

Рисунок 8.7 – Екранна форма введення адреси



Edit address

Please enter your address as it appears in your official registration.

We couldn't verify your address. Please review and adjust it to move forward.

Street
Zeltweg

Street Number
20

Postal Code
8001

City
Zürich

Country
Switzerland

Confirm

Рисунок 8.8 – Екранна форма повідомлення про те, що адресу не знайдено

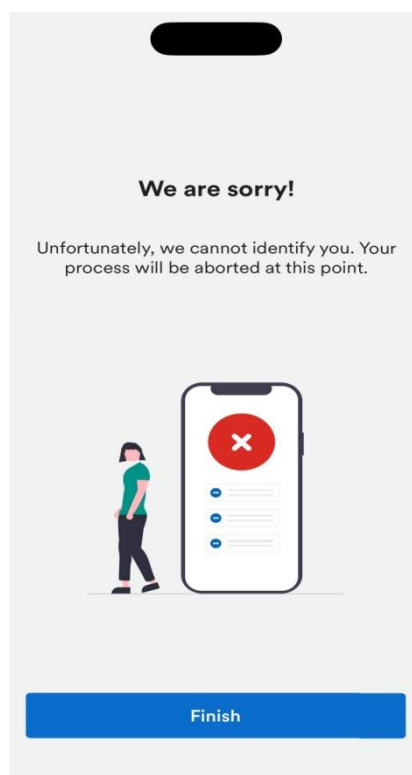


Рисунок 8.9 – Екранна форма неуспішного завершення процесу

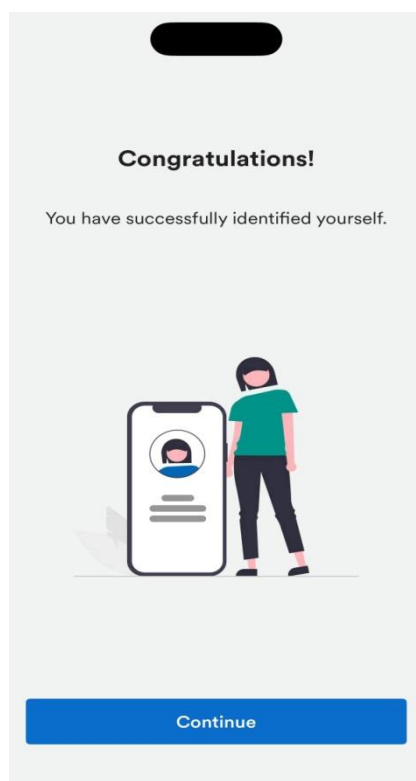


Рисунок 8.10 – Екранна форма успішного завершення процесу

ВИСНОВКИ

Кваліфікаційна робота на тему Розробка IT-сервісу «Онлайн ідентифікація особистості» інформаційної системи банку була виконана з метою реалізації можливості електронної ідентифікації особистості. Оскільки підтвердження особи людини є важливим завданням в умовах використання електронних транзакцій, тема роботи досить актуальна.

У роботі були розглянуті основні технології, пов'язані з цифровою ідентифікацією особистості, надані загальні визначення та наведені приклади сфери застосування.

IT-сервіс був розроблений як мобільний Web-додаток для iOS і Android, який легко може бути інтегрований у Web-додаток установи банку.

Подібний IT-сервіс може бути використаний для онлайн ідентифікації особистості під час отримання послуг, які надають відповідні державні установи, установи банків, різні комерційні підприємства, тощо. Результати онлайн ідентифікації особистості також можуть бути використані для здійснення мобільних платежів, підписання електронних документів за допомогою цифрового підпису, перевірки віку та з іншою метою.

Завдяки IT-сервісу онлайн ідентифікації особистості клієнти банку – приватні особи можуть безпечним способом здійснювати транзакції в Інтернеті з впевненістю та легкістю.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методичні вказівки до організації виконання та захисту кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти спеціальності 122 Комп'ютерні науки за освітньою програмою «Інформаційні технології управління» для студентів усіх форм навчання / Упоряд.: К.Е. Петров, А.В. Міхнова, М.С. Кудрявцева, М.В. Євланов, Т.І. Борисенко. Електронне видання. Харків: ХНУРЕ, 2024. 68 с. pdf

2. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура і правила оформлювання. Чинний від 22.06.2015. Київ: ДП «УкрНДНЦ», 2016. 31 с.

3. В Україні запрацювала електронна ідентифікація особистості URL:

https://ti.ua/news/v_ukraini_zapratsovala_elektronna_identifikatsiya_osobistosti/?srsltid=AfmBOopPIylsHE2lrc7HHZ0qQb2SpvgnEtDKHtp4Jcu06hJA5nflftd4/ (дата звернення: 18.04.2025).

4. Electronic-Identification-eID? URL: https://goodsign.io.translate.goog/glossary/Electronic-Identification-eID?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=rq/ (дата звернення: 18.04.2025).

5. Electronic-Identification-eID URL: <https://goodsign.io/glossary/Electronic-Identification-eID/> (дата звернення: 18.04.2025).

6. Electronic_identification? URL: https://en-m-wikipedia-org.translate.goog/wiki/Electronic_identification?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=rq/ (дата звернення: 18.04.2025).

7. What-is-digital-identity URL: <https://didit.me/ru/blog/what-is-digital-identity/> (дата звернення: 18.04.2025).

8. Про затвердження Інструкції про порядок відкриття та закриття

рахунків користувачам надавачами платіжних послуг з обслуговування рахунків: Постанова від 29.07.2022 № 162 // База даних «Законодавство України». /ВР України. URL: <https://zakon.rada.gov.ua/laws/show/v0162500-22#Text> (дата звернення: 18.04.2025).

9. ДСТУ 8302:2015. Інформація та документація. Бібліографічні посилання. Загальні положення та правила складання. Чинний від 04.03.2016. Київ: ДП «УкрНДНЦ», 2016. 20 с.