Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Штучного інтелекту
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти другий (магістерський)
(рівень вищої освіти)

«Дослідження інтелектуальних методів ідентифікації в системах безконтактних платежів»

(тема)

Виконав: студент 2 курсу, групи СШІм-18-1
Єремєєв Є.Ю.
(прізвище, ініціали)

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

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

Освітня програма Системи штучного інтелекту (СШІ)
(повна назва освітньої програми)

Керівник доцент кафедри ШІ Золотухін О.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Філатов В.О.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Штучного інтелекту
(повна назва)

Рівень вищої освіти другий (магістерський)

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

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

Освітня програма Системи штучного інтелекту
(повна назва освітньої програми)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

« » _____ 2019 р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ АТЕСТАЦІЙНУ РОБОТУ

студентові Єрємєєву Євгену Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження інтелектуальних методів ідентифікації в системах безконтактних платежів

затверджена наказом по університету від " 04 " листопада 2019р. № 1623 Ст

2. Термін здачі студентом закінченої роботи 13 грудня 2019 р.

3. Вихідні дані до роботи документація Master Card

4. Перелік питань, що потрібно опрацювати в роботі

огляд і аналіз методів, моделей і систем електронних платежів

дослідження методів і моделей систем безконтактних електронних платежів

дослідження отриманих наукових результатів

практичне використання результатів досліджень

5. Перелік графічного матеріалу із зазначенням обов'язкових рисунків

Схема сервісів безконтактних платежів MasterCard; схема структури бази даних системи; діаграми класів серверної частини; діаграми послідовності дій процесу ідентифікації, діаграма діятельності метода ідентифікації, екранні форми.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім’я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
	доц. Золотухін О.В.		

КАЛЕНДАРНИЙ ПЛАН

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд і аналіз методів, моделей і систем електронних платежів	04.11.2019	
2	Формування вимог до системи безконтактних електронних платежів	07.11.2019 – 10.11.2019	
3	Дослідження існуючих методів, моделей і механізмів систем платежів	11.11.2019 – 15.11.2019	
4	Дослідження сучасних технологій ідентифікації, методів ідентифікації систем, технологій	16.11.2019 – 20.11.2019	
5	Дослідження переваг і недоліків існуючих систем безконтактних електронних платежів	21.11.2019 – 25.11.2019	
6	Особливості застосування безконтактної ідентифікації в системах платежів	26.11.2019 – 27.11.2019	
7	Особливості застосування вдосконаленого методу ідентифікації	28.11.2019 – 30.11.2019	
8	Реалізація методу ідентифікації безконтактних платежів	01.12.2019- 02.12.2019	
9	Розробка моделей ідентифікації безконтактних платежів	03.12.2019- 04.12.2019	
10	Практична реалізація системи	05.12.2019- 06.12.2019	
11	Оформлення пояснювальної записки та графічного матеріалу	07.12.2019- 10.12.2019	
12	Захист атестаційної роботи	18.12.2019	

Дата видачі завдання 04 листопада 2019 року

Студент _____
(підпис)

Керівник роботи _____ доц. Золотухін О.В.
(підпис) (посада, прізвище, ім'я, по батькові)

РЕФЕРАТ

Пояснювальна записка до атестаційної роботи містить: 78 стор., 14 рис., 4 табл., 26 джерел.

СИСТЕМА БЕЗКОНТАКТНИХ ПЛАТЕЖІВ, ГЕОЛОКАЦІЇ, БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ, МЕТОД ІДЕНТИФІКАЦІЇ БЕЗКОНТАКТНИХ ПЛАТЕЖІВ, MASTERCARD.

Атестаційна робота присвячена дослідженню та аналізу процесу ідентифікації клієнтів в безконтактних платіжних системах, дослідження існуючих методів, моделей, стандартів, технологій ідентифікації.

Об'єктом дослідження в рамках атестаційної роботи є процес ідентифікації клієнтів в безконтактних платіжних системах.

Предметом дослідження є методи ідентифікації безконтактних платежів.

Метою роботи є підвищення ефективності ідентифікації та безпеки платежів в системах безконтактних платежів за рахунок удосконалення методу ідентифікації клієнтів в частині біометричної ідентифікації і геолокації користувача.

В рамках наукових результатів, в роботі удосконалено метод ідентифікації на підставі моделей стандартної ідентифікації, геолокації і біометричних даних користувача.

В рамках практичних результатів використання методу і моделей ідентифікації клієнтів в рамках системи безконтактних платежів дозволяє розширити використання нової технології безконтактних платежів за рахунок спрощення способу ідентифікації для кінцевого користувача, збільшення швидкості і зручності здійснення платежів і підвищення їх безпеки.

ABSTRACT

Explanatory note to attestation work contains: 78 p., 14 fig., 4 tab., 26 src.

CONTACTLESS PAYMENTS SYSTEM, GEOLOCATION, BIOMETRICS IDENTIFICATION, CONTACTLESS PAYMENTS METHODS IDENTIFICATION, MASTERCARD.

Attestation work is devoted to the researches and analysis of the customer identification process in contactless payment systems, the research of existing methods, models, standards, identification technologies.

The object of research in the framework of the certification work is the process of identifying clients in contactless payment systems.

The subject of research are methods for the identification of contactless payments.

The aim is to improve the efficiency of identification and payment security in contactless payment systems by improving the method of identification of customers in terms of biometric user identification and geolocation.

As part of the research results, the improved method of identification based on a standard model identification, geolocation and biometric user data.

In terms of the practical results, using of methods and models to identify customers as part of a contactless payment system allows you to expand the use of new contactless payment technology by simplifying the identification method for the end user, increasing the speed and convenience of making payments and improve their security.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 7

ВСТУП……..... 8

1 ОГЛЯД І АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ, МОДЕЛЕЙ І СИСТЕМ ЕЛЕКТРОННИХ ПЛАТЕЖІВ.... 10

1.1 Огляд і аналіз організації контактної і безконтактної систем електронних платежів..... ... ...……. 10

1.2 Аналіз існуючих систем електронних платежів 14

1.3 Огляд і аналіз проблем систем електронних платежів .....…….. 16

1.4 Формування вимог до платіжних систем ..... …… 18

1.5 Постановка задачі 23

2 ДОСЛІДЖЕННЯ МЕТОДІВ ІМОДЕЛЕЙ СИСТЕМ БЕЗКОНТАКТНИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ..... 25

2.1 Дослідження існуючих методів, моделей і механізмів систем електронних платежів .. 25

2.2 Дослідження сучасних технологій ідентифікації 28

2.3 Дослідження методів ідентифікації систем безконтактних електронних платежів 30

3 ДОСЛІДЖЕННЯ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ ……..... 33

3.1 Особливості вибору і застосування систем безконтактних електронних платежів …... 33

3.2 Особливості застосування вдосконаленого методу ідентифікації ……..... 37

3.3 Реалізація методу ідентифікації безконтактних платежів 47

3.4 Опис і застосування методу ідентифікації безконтактних платежів 52

4 ПРАКТИЧНЕ ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ 54

4.1 Проектування інформаційної системи безконтактних електронних платежів з використанням UML-діаграм ..... ……..…… 54

4.2 Реалізація програмного забезпечення системи безконтактних електронних платежів . 69

ВИСНОВКИ 75

ПЕРЕЛІК ПОСИЛАНЬ..... 76

Додаток А…….. 78

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

API - Application Programming Interface, інтерфейс програмування додатків;

ARQC - Authorization Request Cryptogram, криптограма запиту авторизації;

ATC - Application Transaction Counter, лічильник фінансових транзакцій;

CAM - Card Authentication Method, метод аутентифікації карти;

CSR - Customer Service Representative, клієнтське уявлення сервісу;

CVC - Card Verification Code, код верифікації карти;

CVM - Cardholder Verification Method, метод верифікації власника карти;

DSRP - Digital Secure Remote Payment, захищений віддалений цифровий платіж;

EMV - Europay, MasterCard and Visa;

ID & V - Identification and Verification, ідентифікація і верифікація;

MD - Mobile Device Authentication, аутентифікація мобільного пристрою;

NFC - Near Field Communication, комунікація ближнього радіусу дії;

PAN - Primary Account Number, первинний номер карти;

PTC - PIN Try Counter, лічильник введення пароля;

RNS - Remote Notification Service, віддалений сервіс повідомлень;

UMD - User and Mobile Device Authentication, аутентифікація користувача і мобільного пристрою;

CASE - computer-aided software engineering, автоматизована розробка програм;

UML - unified modeling language, уніфікована мова моделювання.

ВСТУП

Стрімкий розвиток комп'ютерної техніки і її можливостей, розширення використання засобів інформаційних технологій сприяє впровадженню нових технологій в сфері електронних платежів.

Безконтактні технології платежів активно впроваджуються в різноманітні мобільні пристрої - смартфони, планшети, ноутбуки. Це дозволяє споживачам здійснювати покупки швидше і з великою зручністю як в онлайн, так і в офлайн режимах.

Актуальність завдання обумовлена гнучкістю використання технології безконтактних платежів, сумісністю з різними пристроями, спрощення процесів оплати, що сприяють підвищенню привабливості впровадження даної технології банками.

Об'єктом дослідження в рамках атестаційної роботи є процес ідентифікації клієнтів в безконтактних платіжних системах.

Предметом дослідження є методи ідентифікації безконтактних платежів.

Метою роботи є підвищення ефективності ідентифікації та безпеки платежів в системах безконтактних платежів за рахунок удосконалення методу ідентифікації клієнтів в частині біометричної ідентифікації і геолокації користувача.

Дана робота присвячена аналізу і дослідженню наступних питань:

- аналіз організації контактної і безконтактної систем електронних платежів;
- аналіз існуючих систем електронних платежів;
- аналіз проблем систем електронних платежів;
- формування вимог до розроблюваної системі безконтактних електронних платежів;
- дослідженняіснуючих методів, моделей і механізмів систем електронних платежів;

- дослідження сучасних технологій ідентифікації;
- дослідження методів ідентифікації систем безконтактних електронних платежів;
- дослідження переваг і недоліків існуючих систем безконтактних електронних платежів: Android Pay, Apple Pay, Samsung Pay, MasterCard Pay Pass;
- дослідження існуючих стандартів ідентифікації систем електронних платежів, методів ідентифікації систем безконтактних електронних платежів;
- особливості застосування безконтактної ідентифікації в системах безконтактних платежів;
- особливості застосування вдосконаленого методу ідентифікації;
- реалізація методу ідентифікації безконтактних платежів;
- моделювання та підтримка всіх фаз процесу розробки системи безконтактних електронних платежів за допомогою UML-діаграм;
- практична реалізація системи - розробка рішення у вигляді серверної частини, яке буде продаватися банкам, які надають своїм клієнтам можливість безконтактної оплати.

Результати атестаційної роботі оформлені у вигляді пояснювальної записки, перший розділ якої присвячений огляду та аналізу існуючих методів, моделей і систем електронних платежів. У другому розділі представлені результати досліджень методів і моделей систем безконтактних електронних платежів. Третій розділ містить дослідження отриманих наукових результатів і реалізацію методу ідентифікації безконтактних платежів. Четвертий розділ присвячений практичним використанням результатів дослідження в рамках розробки проектних рішень.

Атестаційна робота виконана і оформлена згідно з методичними вказівками [1].

1 ОГЛЯД І АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ, МОДЕЛЕЙ І СИСТЕМ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

1.1 Огляд і аналіз організації контактної і безконтактної систем електронних платежів

В даний час Інтернет-комерція стала невід'ємною частиною бізнесу в сфері інформаційних технологій. При цьому важливу роль в системах Інтернет-комерції грають системи електронних платежів.

Система електронних платежів - це спеціалізована інформаційна система безготівкових розрахунків, укладання контрактів і переказу грошей між продавцями і покупцями, банками і їх клієнтами за допомогою засобів електронної комунікації для здійснення взаєморозрахунків у мережі Інтернет із застосуванням засобів кодуванні інформації та її автоматичної обробки [2].

Масове поширення в світі банківських карт в розрахунках, платежах, кредитних відносинах доводить, що використання цього банківського інструменту істотно спрощує взаємини продавців і покупців товарів, робіт, послуг, зняття з рахунків фізичних осіб готівкових коштів.

Для населення більшості країн це основний спосіб зберігання і захисту заощаджень. Компанії дозволяє її власнику оперативно і практично в більшості країн світу здійснювати покупки або отримувати готівку в будь-який час доби, контролюючи стан банківського рахунку в режимі реального часу. Банківські пластикові картки є потужним інструментом споживчого кредиту, опосередуя стратегію продавців товарів і послуг щодо знижок і програм лояльності покупців. Дана система платежів дозволяє населенню контролювати розмір і структуру своїх витрат у часі.

Підвищення ефективності економіки багато в чому залежить від організації платіжних систем, їх надійності та зручності для всіх учасників

ринку. Країни, зацікавлені в прозорості фінансових потоків (зокрема, роздрібної торгівлі, громадського харчування, транспорту), зниженні витрат платіжної системи, зростанні споживчого кредиту та розвитку роздрібної банківської мережі, зазвичай прагнуть розвинути систему розрахунків банківськими картами, включаючи спеціальні заходи для скорочення сфери готівкових розрахунків [3].

Розвиток безготівкових платіжних систем супроводжувалося державним стимулюванням і конкуренцією між основними міжнародними картковими системами в США і Європі. Після об'єднання Master Card з Europay склалася глобальна система, представлена конкуруючими American Express, Diners Club, Master Card і Visa і різними локальними або навіть національними системами, які доповнюють міжнародні мережі. Конкуренція між цими мережами і меншими компаніями, а також можливості науково-технічного прогресу призвели до значного технологічного картковому прориву, включаючи зниження витрат обігу, підвищення швидкості, надійності проведення платежів, оперативності всіх розрахунків, посилення захисту від шахрайства, розширення функціональності карт [3].

Роздрібні електронні платежі за допомогою банківських карт є кращим засобом платежу, що дозволяє значно скоротити труднощі обміну паперових грошей, платіжних документів і доступу до товарів і послуг. Розвиток багатьох галузей глобальної економіки, особливо подорожей, відпочинку та розваг стимулює попит на електронні гроші.

На сьогоднішній день розширилися можливості виконання електронних платежів. Депозит можна поповнити як через контактний, так і безконтактний інтерфейс, а також використовуючи Інтернет. Хоча цифрова карта фактично містить два електронних гаманця - для безконтактних (наприклад, для оплати проїзду) і контактних платежів (наприклад, для виконання дебетової і кредитової функцій), обидва вони прозорі для користувача, оскільки сучасна система обслуговування карт

забезпечує надійну синхронізацію депозитів в обох гаманцях . Гнучкість в користуванні і сумісність з різного роду супутніми пристроями сприяють підвищенню привабливості використання карт [4].

Компанії пластикова карта, прив'язана до одного або кількох розрахунковим рахункам в банку. Всередині пластикової карти знаходиться мікропроцесор і антена. На процесорі встановлена операційна система з платіжним додатком і даними конкретного клієнта (персоналізаційного даними). При випуску карти банк передає персоналізаційного дані в організацію з виготовлення карт, яка здійснює підготовку і запис даних на мікропроцесор в пластиковій оболонці, карту клієнт отримує у відділенні банку.

При використанні чиповой карти в банківському терміналі на касі або піднесенні до терміналу безконтактної карти мікропроцесор всередині пластика отримує достатню для роботи харчування і запускає встановлений на ньому платіжний додаток. На основі закладених правил і ключів воно генерує одноразові платіжні дані, які передаються на банківський термінал в торговій точці, а потім в банк.

Безконтактні картки, які використовуються для оплати проїзду в метро і наземному транспорті, працюють за схожим принципом. При цьому, у транспортних карт є своя особливість - на них зберігається ще й інформація про залишок грошей або поїздок на рахунку. Це дозволяє економити час на взаємодію терміналу і банку і, як наслідок, швидше пропускати пасажирів [5].

При випуску «хмарної» платіжної картки банк передає персоналізаційного дані клієнта в компанію, що забезпечує випуск карти і її роботу на протязі всього терміну дії. За даний процес відповідає платформа Cloud-Based Payments Platform (CBPP). У телефон передаються тільки одноразові платіжні дані в зашифрованому вигляді. Платіжні дані шифруються за допомогою додаткового пароля (Mobile PIN), відомого тільки користувачеві і ніколи не зберігається в телефоні.

При тому, що піднесло телефону до банківського терміналу, NFC-антена (Near Field Communication) телефону потрапляє в його поле дії. Завдяки технології HCE (Host Card Emulation), яка дозволяє запускати карткові додатки безпосередньо в операційній системі і передавати результат їх роботи назад в телефон для проведення оплати, одноразові платіжні дані, завантажені з хмарної платформи, передаються на термінал, який, в свою чергу, за стандартною схемою передає їх в банк для проведення транзакції [6].

В даний час актуальним способом здійснення різного виду платежів є застосування безконтактних технологій, потенціал яких полягає в тому, щовони в рівній мірі приносять вигоду всім задіяним в транзакції сторонам: споживачам, фінансовим і торговельним підприємствам.

Мобільні пристрої в майбутньому повинні стати головним інструментом для здійснення платежів, але банківські карти ще довго збережуть свою актуальність через різні темпів впровадження нових технологій в різних регіонах.

Як технології для безконтактних платежів розглядається технологія NFC (Near Field Communication), яка реалізується у вигляді чіпа (адаптера), вбудованого в мобільний телефон.

Безконтактні технології платежів, засновані на стандарті радіозв'язку ближнього радіусу дії NFC, активно впроваджуються зараз в різноманітні мобільні пристрої - смартфони, планшети, ноутбуки.

Технології безконтактних платежів дозволяють проходження операцій на малі суми тільки прикладанням карти до магнітного зчитувача – без введення ПІН-коду. При цьому карта не передається в руки касирові. Крім того передбачена можливість «вбудовування» пристроїв (чіпів) в будь-які форми (мобільний телефон, годинник, брелоки), можливість суміщення безконтактної карти з іншими пристроями (пропуски, проїзні, студентські квитки і т.д.).

Безконтактні платіжні технології мають безліч переваг, серед яких інноваційність, оперативність, простота, швидкість проведення операцій, значна економія часу, зниження черг і, найголовніше, більш високий рівень безпеки проведення операцій і зниження злочинності.

Цільовий сегмент, в якому безконтактні платежі найбільш затребувані: торговельні підприємства з великим людино-потоком і малою сумою середнього чека, як правило, це мережі швидкого харчування, магазини косметики та побутової хімії, продуктові супермаркети; великі музичні фестивалі.

1.2 Аналізіснуючих систем електронних платежів

Проведемо аналіз існуючих платіжних систем електронних платежів.

Системи контактних електронних платежів представлені платформами Visa International та MasterCard.

Visa International - це електронна платіжна система, яка об'єднує більше 21 000 банків-членів по всьому світу. Visa виконує посередницьку роль між банками, займається організацією розрахунків і забезпечує технічну взаємодію між учасниками системи. Емісією і організацією прийому карт займаються самі банки. Для платіжної системи Visa основною валютою є американський долар. Це означає, що операції, пов'язані з конверсією валют, будуть проходити через долар.

Поширення і прийом карток Visa з магнітною смугою по всьому світу стали можливим завдякивпровадження та дотримання платіжної індустрією єдиного глобального стандарту. Visa, об'єднавши зусилля з Europay і MasterCard, розробила індустріальний стандарт EMV (Europay, MasterCard, Visa) для платіжних чіпових карт з кредитно-дебетовими додатками. Використання стандарту EMV означає, що чіпові карти приймаються в торгово-сервісній мережі та банкоматах у всьому світі і в подальшому отримають таке ж широке поширення, як і карти з магнітною

смугою. Мікропроцесорна технологія дозволяє забезпечити надійний механізм оплати товарів і послуг через різні інформаційні канали зв'язку у віртуальному середовищі [7].

Одним з найбільш значних досягнень платіжної системи є карта з вбудованим мікропроцесором. Картка з мікропроцесором є пластиковою карткою з імплантованою інтегральною схемою. На відміну від стандартної карти з магнітною смугою, смарт-карта або інтелектуальна карта може застосовуватися не тільки для оплати товарів і послуг і зняття готівки в банкоматах, а й використовуватися для реалізації додаткових неплатіжних схем по цій карті, наприклад, системи знижок або преміальних балів, різних ідентифікаційних додатків, індивідуальних корпоративних програм. На сьогоднішній день Visa є найбільшої платіжною системою в Україні.

MasterCard Worldwide або MasterCard Incorporated - міжнароднаплатіжна система,транснаціональна фінансовакорпорація, яка об'єднує 22 тисячі фінансових установ в 210 країнах світу. Кріммагнітних і чіпових технологій, мобільні програми розширені безконтактними платежами. Для платіжної системи MasterCard основною валютою може бути як американський долар, так і євро[8].

В роботі проаналізовано існуючі систем безконтактних електронних платежів: Android Pay, Apple Pay, Samsung Pay, MasterCard Pay Pass.

Безконтактна технологія дозволяє здійснювати покупки в один дотик. Досить піднести картку, мобільний телефон або інший пристрій до зчитувального пристрою на касі і покупка буде оплачена.

Apple Pay - платіжна платформа, система проведення безконтактних платежів для користувачів iPhone.

Samsung Pay - платіжна платформа для Android-смартфонів, що дозволяє на відміну від Apple Pay, розплачуватися смартфоном в тих терміналах, які підтримують і технологію NFC, і технологію MST

(Magnetic Secure Transmission), що дає користувачеві можливість платити в будь-яких терміналах, які працюють з магнітною смугою карти.

Android Pay - це інтерфейс програмування додатків, платформа для Android-смартфонів, яка дозволяє розробникам додати нові можливості захищених платежів в інтернет-магазинах і в роздрібних торгових точках.

MasterCard PayPass - цебезконтактна технологія проведення платежу, Що надає власникам картокMasterCard PayPass і Maestro PayPass спосіб здійснення оплати шляхом близького піднесення або дотику платіжною карткою або іншим платіжним інструментом, таким як телефон або брелок для ключів, до зчитувального платіжному терміналу замість проведення нею для зчитування або вставки її в термінал.

1.3 Огляд і аналіз проблем систем електронних платежів

Відповідно до стандарту EMV, типовий цикл проведення EMV-транзакції складається з 12 етапів[9]:

- вибір додатки;
- ініціалізація обробки додатка;
- читання даних програми;
- аутентифікація емітента в режимі офлайн;
- обробка обмежень;
- аутентифікація власника картки;
- перевірка параметрів управління ризиками на стороні терміналу;
- аналіз дій терміналу;
- перевірка параметрів управління ризиками на стороні карти;
- аналіз дій карти;
- якщо потрібно, то авторизація транзакції в режимі онлайн;
- завершення транзакції.

Ці операції вимагають інтенсивного обміну і обчислень як на стороні карти, так і на стороні терміналу і займають по мірках онлайн-систем багато часу. При цьому карта постійно знаходиться в зчитувачі терміналу, а клієнт чекає відповідь системи.

Для великих торгових мереж дорога кожна секунда, а сучасні клієнти хочуть оперативно, без затримок отримати свій товар. Платіжна система Visa запропонувала для магазинів і покупців технологію безконтактного обслуговування карт. Крім швидкості оплати, клієнти отримали ще одну перевагу - тепер стандартна пластикова карта може стати зайвою, дані для оплати записуються в телефон з NFC.

Разом з платіжними системами розвиваються і технології забезпечення їх безпеки. Оскільки на сьогоднішній день жодна електронна платіжна система не може існувати без хороших технологій і систем безпеки, які в свою чергу забезпечують безпечну транзакцію грошових операцій, проблема безпеки і підвищення рівня вимог з безпеки є актуальними. Так як інтернет одночасно є і надзвичайно ефективним комунікативним засобом і середовищем, що викликає досить велика недовіра у користувачів, безпеку електронних платежів є досить серйозним критерієм успіху конкретної системи і використовує її електронного бізнесу. Важливо, щоб при будь-якої реалізації в системі не залишалося погано захищених ділянок, здатних привести до великомасштабного шахрайства.

Недоліками безконтактних платежів є невелика кількість торгових точок, які готові працювати з такими системами. І другий недолік - досить дороге обладнання для проведення безконтактних платежів, багато банків не вважають за доцільне вкладати в нього гроші.

Однак, найбільші банки України вже впроваджують дану технологію, а це значить, що незабаром значна кількість торгових підприємств зможе обслужити власників безконтактних карт. Допомогти власникам оцінити переваги даної технології допоможе випуск

комбінованих карт - держатель завжди зможе скористатися такою картою як за безконтактною технологією, так і традиційним, контактним способом.

1.4 Формування вимог до платіжних систем

Визначимо вимоги до розробки системи безконтактних електронних платежів. Вимоги до розроблюваної системі безконтактних електронних платежів: багатомовність (наявність покриття у всіх країнах світу): мультиплатформеність (IOS і Android) і охоплення максимального набору пристроїв;безпеку;простота використання (робота без карти);адаптованість до динамічних змін. Вимоги до вирішення:

- швидка розробка;
- можливість динамічних змін;
- дешевизна підтримки;
- використання сучасних технологій;
- повне охоплення тестування.

Розглянемо вимоги більш детально.

Вимоги безпеки:

- виключення можливості списання коштів з аккаунта платника третіми особами;
- забезпечення можливості легітимного підтвердження платником перед третіми особами (наприклад, судом) факту здійснення платежу, його отримання отримувачем і призначення даного платежу (наприклад, отримання товару належної якості);
- забезпечення можливості легітимного підтвердження одержувачем перед третіми особами факту отримання платежу і його призначення;

- забезпечення можливості легітимного підтвердження емітентом факту проведення всіх авторизованих транзакцій з даного аккаунту дійсним власником даного облікового запису;
- забезпечення гарантій, що переміщується з аккаунта сума не буде вкрадена в момент передачі і потрапить точно і виключно за призначенням;
- виключення можливостей підробки квитанцій емітента користувачам;
- забезпечення вирішення всіх спірних питань між емітентом і користувачами виключно електронним чином за допомогою повідомлень з цифровим підписом;
- забезпечення можливості вирішення спірних питань між користувачами без участі емітента; система в цілому повинна бути стійка до шахрайських дій, в тому числі в разі форс-мажорних обставин.

Вимоги по конфіденційності.

І інтернет в цілому, і будь-які платежі завжди тісно пов'язані з поняттям конфіденційності. Тому необхідно, щоб платіжна система сама по собі не нав'язувала користувачам ніяких порушень конфіденційності, а надання розширеної і додаткової інформації завжди залишалося на розсуд користувача. Таким чином, вимоги щодо конфіденційності включають в себе:

- виключення можливості отримання інформації про дії користувачів сторонніми спостерігачами;
- забезпечення необхідного ступеня анонімності платника для одержувача платежу;
- виключення можливості отримання емітентом інформації про призначення платежу;
- виключення можливості отримання емітентом інформації про те, з ким із надходжень на аккаунт одержувача пов'язано кожне з списань з аккаунта платника.

Вимоги щодо реалізації.

− вимоги до реалізації зазвичай спрямовані на простоту і надійність роботи системи, оскільки відмови в таких рішеннях можуть привести до великих фінансових втрат сторін. Вимоги щодо реалізації зазвичай полягають в наступному:

− система повинна бути простою як з точки зору користувачів, так і для розробників. Простота системи здешевлює і прискорює її реалізацію і технічну підтримку, сприяє розширенню спільноти застосовують її організацій і приваблює споживачів;

− система повинна базуватися на добре перевіреної і надійної технології, що також буде запорукою простоти її реалізації та впевненості в достатньому рівні безпеки;

− система повинна мати можливість працювати з користувачами ззовні організації, що використовує дану платіжну систему, так як безліч потенційних користувачів не є співробітниками цієї організації.

Інші вимоги.

До будь-якої платіжної системи застосовні традиційні для будь-якої онлайнової системи вимоги по гнучкості, масштабованості і ефективності.

При створенні платіжних систем необхідно приділити якомога більше уваги захисту та забезпечення їх безпеки. Зазвичай різниться внутрішня і зовнішня безпека. Внутрішня безпека повинна забезпечувати цілісність програм і даних, забезпечення нормальної роботи всієї системи. Зовнішня - повинна захищати від будь-яких загрозливих збоєм в системі проникнень. В даний час існує два підходи до побудови захисту платіжних систем:

− комплексний підхід - об'єднує різноманітні методи протидії загрозам;

− фрагментарний підхід - протидія певним загрозам (антивірусні засоби і т. п.).

Комплексний підхід застосовується для захисту великих систем (наприклад, міжнародні міжбанківські мережі). Політика безпеки, т. Е. Сукупність норм, правил і методик, на основі яких в подальшому будується діяльність інформаційної системи в галузі поводження, зберігання, розподілу критичної інформації. Політика безпеки визначає:

- мети, завдання, пріоритети системи безпеки;
- гарантований мінімальний рівень захисту;
- обов'язки персоналу щодо забезпечення захисту;
- санкції за порушення захисту;
- області дії окремих підсистем.

Аналіз ризику, який складається з декількох етапів:

- опис складу системи (тобто документація, апаратні засоби, дані, персонал і т. д.);
- визначення по кожному елементу системи вразливих місць;
- оцінка ймовірності реалізації загроз;
- оцінка очікуваних розмірів втрат;
- аналіз методів і засобів захисту;
- оцінка оптимальності пропонованих заходів.

Остаточно аналіз ризику виливається в стратегічний план забезпечення безпеки, важливим при цьому є розбивка інформації на категорії. Найбільш простий метод такого розмежування інформації наступний:

- конфіденційна інформація - доступ до якої строго обмежений;
- відкрита інформація - доступ до якої сторонніх не пов'язаний з матеріальними та іншими втратами.

Для комерційної діяльності такої градації цілком достаточно.Наіболее поширеними загрозами безпеці являются[10]:

- несанкціонований доступ, т. е. отримання користувачем доступу до об'єкта без відповідного дозволу;

− «Злом системи», т. Е. Умисне проникнення (основне навантаження захисту в цих випадках несе програма входу);

− «Маскарад», т. Е. Виконання будь-яких дій одним користувачем банківської системи від імені іншого;

− вірусні програми, т. е. вплив на систему спеціально створеними програмами, які збивають процес обробки інформації, і т. д.

Проблема забезпечення своєї інформаційної безпеки виходить за рамки однієї країни. Жоден з користувачів мережі не захищений на всі 100%.Залежно від існуючих загроз, розрізняють наступні напрямкизахисту електронних систем [11]:

1) захист апаратури і носіїв інформації від пошкодження, викрадення, знищення;

2) захист інформаційних ресурсів від несанкціонованого використання.

3) захист інформаційних ресурсів від несанкціонованого доступу.

4) захист інформації в каналах зв'язку і вузлах комутації (блокує загрозу «підслуховування»),

5) захист юридичної значимості електронних документів.

6) захист систем від вірусів.

Існують різні програмно-технічні засоби захисту.

До класу технічних засобів відносяться: засоби фізичного захисту територій, мережі електроживлення, апаратні та апаратно програмні засоби управління доступом до персональних комп'ютерів, комбіновані пристрої і системи.

До класу програмних засобів захисту відносяться: перевірка паролів, програми шифрування (криптографічного перетворення), програми цифрового підпису, засоби антивірусного захисту програми відновлення і резервного зберігання інформації. Наприклад, розробники платіжної системи Webmoney Transfer зробили підвищені заходи безпеки для всіх повідомлень в системі за допомогою їх кодування. Використання

спеціального алгоритму захисту інформації (схожого на алгоритм RSA, де довжина ключа більше 1024 біт) і використання спеціальних ключів при кожному сеансі передачі інформації дозволяє захистити інформацію про призначення і суму платежу від чужого цікавості[12].

Технологій захисту даних багато, проте постійно з'являються нові. Тому удосконалення методу ідентифікації платежів, запропоноване в даній роботі, є актуальним засобом підвищення безпеки здійснення платежів.

1.5 Постановка задачі

Об'єктом дослідження в рамках атестаційної роботи є процес ідентифікації клієнтів в безконтактних платіжних системах.

Предметом дослідження є методи ідентифікації безконтактних платежів.

Метою роботи є підвищення ефективності ідентифікації та безпеки платежів в системах безконтактних платежів за рахунок удосконалення методу ідентифікації клієнтів в частині біометричної ідентифікації і геолокації користувача.

Дана робота присвячена дослідженню наступних питань:

- формування вимоги до розроблюваної системі безконтактних електронних платежів;
- дослідженняіснуючих методів, моделей і механізмів систем електронних платежів;
- дослідження сучасних технологій ідентифікації;
- дослідження методів ідентифікації систем безконтактних електронних платежів;
- дослідження переваг і недоліків існуючих систем безконтактних електронних платежів: Android Pay, Apple Pay, Samsung Pay, MasterCard Pay Pass;
- дослідження існуючих стандартів ідентифікації систем

електронних платежів, методів ідентифікації систем безконтактних електронних платежів;

- особливості застосування безконтактної ідентифікації в системах безконтактних платежів;
- особливості застосування вдосконаленого методу ідентифікації;
- реалізація методу ідентифікації безконтактних платежів;
- опис і застосування методу ідентифікації безконтактних платежів;
- моделювання та підтримка всіх фаз процесу розробки системи безконтактних електронних платежів за допомогою UML-діаграм;
- практична реалізація системи - розробка рішення у вигляді серверної частини, яке буде продаватися банкам, які надають своїм клієнтам можливість безконтактної оплати.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ІМОДЕЛЕЙ СИСТЕМ БЕЗКОНТАКТНИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

2.1 Дослідженняіснуючих методів, моделей і механізмів систем електронних платежів

Розглянемо класифікацію моделей електронних платежів.

Електронні платежі[12]:

- прямі / непрямі системи електронних платежів. Різняться в залежності від наявності / відсутності прямого зв'язку між платником і одержувачем. У непрямий системі платіжна операція відбувається її ініціатором і її учасниками є ініціатор і банк. Прикладом прямого платежу є платіж готівкою або чеком. Прикладом непрямого - постійний наряд-замовлення. Більшість сучасних систем пропонує прямий спосіб платежу;
- системи заздалегідь оплачених / поточних / відкладених платежів. Різняться в залежності від того, в який момент часу ініціатор платежу вважає платіж завершеним і в який момент часу кошти дійсно вилучаються у платника. Заздалегідь сплачені платежі аналогічні платежах готівкою, а поточні та відстрочені платежі схожі: в обох випадках користувачеві необхідно мати рахунок в банку, і платіж завжди відбувається шляхом пересилки деякої форми від платника одержувачу (чека, сліпа кредитної картки, ін.). Їх навіть можна об'єднати в єдину систему платежів, аналогічних чеками;
- модель систем збережених сум (аналог електронних монет, кредитних карт і готівки): системи збережених сум дозволяють користувачам завантажувати кошти з їх банківських рахунків на належать користувачам інструменти - смарт-карти (пристрої, в яких електронним чином на вбудованому чіпі закодована збережена сума) або PC-файли. При здійсненні покупки за допомогою таких інструментів спочатку відбувається перевірка наявності на них необхідної суми, потім ця сума

віднімається від поточного залишку покупця і додається до інформації, що зберігається сумі постачальника. Смарт-карти мають додаткові переваги: портативність, можливість здійснювати покупки і поповнювати рахунок як по мережі, так і в офлайні, аутентифікація за допомогою генерується при кожному використанні унікальної цифрового підпису та ін. Прикладами є: Common Electronic Purse Specification (CEPS), European Electronic Purse (EEP), Mondex, Proton, Visa Cash, WorldPay. PC-файли зберігають грошові суми безпосередньо на персональному комп'ютерному пристрої (комп'ютері, телевізійної приставки, PDA) в зашифрованому файлі, захищеному відомим користувачеві паролем і не вимагають спеціального апаратного забезпечення. Прикладами є: Globe ID Payment System, Millicent, NetBill;

− модель систем електронних чеків: тоді як реальні чеки дещо втратили свої позиції за останні роки, електронні чеки все ще мають досить широке поширення, оскільки є практично повними аналогами реальних чеків, зберігаючи всі їх переваги (наприклад, вимагають обмеженої інформації про одержувача), але при цьому можуть застосовуватися для електронних платежів в області B2B і також не мають потреби в обов'язковому онлайновому режимі платника в момент покупки. Прикладами є: Mandate II, eCheck.

− модель систем електронних грошових транзакцій. Ця модель може бути розбита на кілька груп: за змістом транзакцій (кредитові, дебетові, просто записи), сфері дії (наприклад, бізнес-транзакції), видам спонсорів (банки, провайдери) і в залежності від того, чи використовується в процесі транзакції якийсь посередник - банк, інший фінансовий інститут або віртуальна організація електронної комерції. На відміну від попередніх двох категорій, кожна з цих систем реалізує певний сценарій транзакцій, що включає обробку замовлень, платежів, інструкції, процедури і протоколи для переказу коштів між рахунками. Крім того, незважаючи на те, що дана система вимагає онлайнового режиму від платника, одержувач

платежу може перебувати в онлайні (що виключно вигідно з точки зору витрат). У цю групу відносяться різні платіжні середовища,

Розглянемо основні механізми підтримки проведення електронних платежів[12]:

− дистанційне керування фінансами (home banking)включає в себе: завантаження списку банківських рахунків, завантаження списку кредитних карт, перекази грошових коштів, клієнтські платежі, бізнес-платежі. На базі цього механізму працюють багато систем електронного банкінгу та онлайнові біржі. Приклади стандартів: Bank Internet Payment System (BIPS), Homebanking Computer Interface (HBCI), Open Financial Exchange (OFX);

− угоди про способи оплати -угоди між платником і одержувачем про те, який інструмент вони збираються використовувати для проведення платіжних транзакцій. До їх числа відносяться протокол SET, що дозволяє проводити платіжні транзакції в зашифрованому вигляді цифрових підписів. Крім того, для більш дрібних сум використовується загальна розмітка для мікроплатежів Common Markup for Micropayment Per-Fee, що дозволяє проводити оплату, вибираючи певну посилання, що містить таку нормативну, організаційну та фінансову інформацію, необхідну для платежу;

− системи електронних грошових переказів -даний механізм являє собою обмін даними між двома комп'ютеризованими системами, обробними фінансові транзакції і інформацію про них. Аналогом цих систем в реальному світі можуть служити системи для міжбанківських розрахунків, наприклад, система SWIFT. В електронному середовищі такі системи використовуються і для інших платежів, наприклад, для роботи біржових трейдерів і для home banking. Так як більшість таких систем використовує EDI, прикладами стандартів в даному випадку можуть служити UN / EDIFACT EDI Payment messages і SWIFT EDI Bank-to-Bank messages;

− електронний гаманецьявляє собою додаток чи службу, що допомагає покупцям проводити онлайнові транзакції, зберігаючи інформацію про виставлені рахунки, доставці, платежах і використовуючи цю інформацію для заповнення контрольних сторінок продавця. Електронні гаманці реалізуються різними способами: як вбудовані компоненти або допоміжні програми для браузерів, як окремі клієнтські програми або в якості серверних додатків. Їх можна розділити на дві групи - клієнтські і серверні. Існують додатки, незалежні від продавця, і додатки, що працюють тільки з конкретним продавцем. Зазвичай пропоновані електронні гаманці пов'язані з торговим порталом. Як приклад стандартів в цій галузі можна назвати ECML (European Centre for Modern Languages) - мова розмітки для електронної комерції.

2.2 Дослідження сучасних технологій ідентифікації

На сьогоднішній день існують кілька стандартів обміну інформацією, які відповідають вимогам віддаленого взаємодії з клієнтом і при цьому використовують сучасні технології. Ці стандарти включають в себе опис та вимоги до способів ідентифікації при здійсненні передачі даних між користувачем і системою. Деякі з них описують передачу даних для контактних і безконтактних карт, деякі описують передачу даних між величезним рядом пристроїв для різних потреб, але при цьому можуть бути використані для передачі платіжної інформації. Існують такі нормативні документи для контактних і безконтактних платежів[13]:

- RFID-стандарт ISO / IEC 14443 призначений для безконтактних карт, описує передачу даних для безконтактних карт, що виконують обмін інформацією на невеликих відстанях, але відносно великими швидкостями обміну даними. Стандарт був розроблений спільними зусиллями деяких компаній, що надають послуги платіжних систем, і в наслідку на підставі цього стандарту стали працювати багато рішень на ринку платіжних

засобів, такі як:системи безконтактної оплати payWave, PayPass, ExpressPay та ідентифікації особистості, електронні паспортиі візи. Надалі на базі цього стандарту була створена, протестована і застосована в сучасних рішеннях технологіяNFC для двостороннього обміну повідомленнями та даними між різними пристроями для широкого спектра задач.

Технологія NFC є логічним продовженням і розширенням стандарту ISO 14443, Яке об'єднуєінтерфейс смарт-картиі зчитувача в єдиний пристрій. Це дозволяє охопити в стандарті більш широкий спектр завдань і стандартизувати набагато більший набір пристроїв. На даний момент NFC активно використовується перш за все у величезній кількостіцифрових мобільних пристроях, Таких як мобільні телефони, в які NFC чіпи вбудовуються за замовчуванням, а також використовується вгромадському транспорті і платіжних системах;

- ISO / IEC 7816 - цей стандарт був розроблений для опису взаємодій з контактнимисмарт-карткамиі. У ньому описується величезний набір параметрів смарт карт, такі як: форма карти, форма контактів, їх розташування і призначення, параметри; опис протоколу обміну і деякі аспекти по роботі з даними і передачі інформації. Цей стандарт є базовим для всіхсмарт-карт [14];

- EMV - міжнародний стандарт для операцій побанківськими картками з чіпом, спільно розроблений компаніями світових платіжних систем, такими як Europay, MasterCard і Visa, щоб підвищити рівень безпеки фінансових операцій, включити набір додаткових функцій, а також доопрацювати механізм безконтактної передачі даних на коротких дистанціях для відповідності сучасним реаліям. Основна відмінність для користувача карти стандарту EMV - переважне вимога введенняПІН-кодупри проведенні будь-якого платежу через термінал (наприклад, в магазинах, ресторанах). Підвищений рівень безпеки забезпечується за рахунок відходу від візуального контролю (перевірка продавцем

голограми, підписи, звірка імені з посвідченням особи) до використання ПІН-коду і криптографічних алгоритмів для аутентифікації карти [15];

- ISO / IEC 15693 описує частотний діапазон, метод модуляції і протокол обміну безконтактних пасивних карт дальнього радіусу дії (більше 10 см). Стандарт призначений для карт з великою дальністю читання (десятки см) і малими швидкостями обміну даними. В основному це ринок промислової, транспортної і торгової логістики [15].

2.3 Дослідження методів ідентифікації систем безконтактних електронних платежів

Виявлення та протидія шахрайським операціям - одна з ключових завдань всіх міжнародних платіжних систем. Безпека онлайн-платіжних транзакцій відстежується безліччю систем на різних рівнях і етапах проходження платежу. При проведенні операцій з грошовими коштами або іншим майном банк зобов'язаний провести ідентифікацію клієнта.

Ідентифікація - це сукупність заходів щодо встановлення визначених законодавством відомостей про клієнтів і їх представників, з підтвердженням достовірності цих відомостей, використовуючи оригінали документів, належним чином завірені копії [16].

Методи ідентифікації - пропоновані в різних платіжних системах інформаційні засоби по ідентифікації користувача для здійснення ним різних операцій.

Проаналізуємо існуючі методи ідентифікації:

Методи ідентифікації, вбудовані в платформу MasterCard PayPass:

− ідентифікація по PIN паролю - перевірка справжності користувача шляхом порівняння введеного їм особистого ідентифікаційного номера з паролем, збереженим вбазі даних користувачів;

- ідентифікація клієнта довіреною особою з перевіркою документів клієнта - процедура реєстрації включає в себе процес ідентифікації клієнта і укладення договору на надання послуг. Для проходження процедури ідентифікації клієнт повинен надати співробітникам банку певний комплект документів. При проведенні певних операцій з грошовими коштами або при виникненні підозр у легальності проведення операцій співробітник банку може зажадати додатково пред'явити документи;
- набір AES (Advanced Encryption Standard) і DES (Data Encryption Standard) Ключів всередині призначеного для користувача пристрої. До цих ключам відносяться ключ пристрою (з його допомогою відбувається підтвердження транзакції призначеним для користувача пристроєм тоді, коли у мобільного пристрою є зв'язок з сервісами MasterCard PayPass, а також для отримання одноразових ключів), транспортні ключі (використовуються для передачі інформації між мобільним пристроєм і веб-сервісами банку-клієнта системи MasterCard PayPass, а також передачі інформаціїміж мобільним пристроєм і самою системою MasterCard PayPass), ключі до зашифрованих даних (карткова інформація) на пристрої. Всі вони зберігаються тільки в мобільному пристрої, регулярно оновлюються і зашифровані PIN паролем.
- одноразові ключі-паролі. Дійсні тільки для одного сеансу аутентифікації, Тобто для проведення одного невеликого платежу. Дія одноразового пароля також може бути обмежене певним проміжком часу;
- Fraud контроль - дозволяє вирішити задачу встановлення несанкціонованого доступу, контролю якості та встановлення шахрайства (fraude detection). Антіфрод-системи різних банків завдяки комплексному контролю та обміну даними з іншими банками, викривають сотні злочинних, шахрайських угруповань, які працюють в різних країнах світу і здійснюють злочини з використанням платіжних карт. Комплекс сервісів,

що працюють з використанням технологій machine learning. Моніторинг і антіфрод-контроль виробляються в автоматичному і ручному режимах.

Проаналізуємо додаткові заходи захисту, що застосовуються різними платіжними системами:

− перевірка відбитка пальця під час виконання платежу - прив'язавши свій відбиток пальця до платіжної системи, авторизувавшись по відбитку пальця (замість введення імені користувача і пароля), можна використовувати його для входу в систему оплати в будь-якому додатку;

− використання фізичного ключа-флешки - це електронний ключ для доступу, фізичного пристрою, що використовується для спрощенняаутентифікації, використовується дляідентифікації його власника, безпечного віддаленого доступу до інформаційних ресурсів Токени призначені для електронного посвідчення особи (наприклад, клієнта, який отримує доступ до банківського рахунку), при цьому вони можуть використовуватися як замість пароля, так і разом з ним.

3 ДОСЛІДЖЕННЯ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

3.1 Особливості вибору і застосування систем безконтактних електронних платежів

На основі дослідження існуючих систем безконтактних електронних платежів: Android Pay, Apple Pay, Samsung Pay, MasterCard Pay Pass визначені характеристики, переваги та критичні недоліки систем у вигляді рекомендацій вибору конкретного рішення, результати яких наведені таблиці 3.1.

Таблиця 3.1 - Характеристики, переваги і критичні недоліки систем безконтактних електронних платежів

Системи безконтактних платежів	Характеристика	Переваги	Недоліки
Apple Pay	Система мобільних платежів від корпорації Apple. за технологією NFC	набір сервісів для зручного і гнучкого виконанняплатежів в магазинах і інтернеті, безпеку	Пристрої - тільки iOS, складність підключення - необхідна картка, з комісією за кожну покупку за допомогою сервісу Apple
Android Pay	Система платежів компанії Google, що дозволяє здійснювати покупки на платформі Android з використанням програми та технології NFC.	Використання сканера відбитку пальців для ідентифікації оплати, надійні механізми безпеки	Пристрої - с ОС Android, складність підключення - необхідна картка

Продовження таблиці 3.1

Samsung Pay	Зручний і безпечний мобільний платіжний сервіс для смартфонів фірми Samsung. Приймається до оплати скрізь, де можна здійснити покупку за звичайною банківською картою з безконтактної технології або магнітній смузі.	Працює не тільки з терміналами, що підтримують безконтактну оплату за технологією NFC, і власну технологію- MST (Magnetic Secure Transmission - магнітна безпечна передача), що дає можливість оплачувати покупки за допомогою смартфона на практично будь-якому терміналі, що приймає банківські карти.	Покриття - Корея, Китай, пристрої - Samsung, складність підключення - необхідна картка
MasterCard Pay Pass	Безконтактна Технологія Проведення Платежу з використанням технології NFC для всіх типів пристроїв	Покриття - весь світ, підтримує всі пристрої і ОС	Складність підключення - необхідна картка, банк, в якому користувач зареєстрував картку, повинен мати сервер і мобільний додаток для роботи з сервісами MasterCard - потрібні ресурси і кваліфіковані програмісти

У таблиці 3.2 представлені критичні недоліки платіжних систем.

Таблиця 3.2 - Критичні недоліки систем безконтактних електронних платежів

Платіжна система	покриття	Тип пристрою і ОС	простота підключення
Apple Pay	Увесь світ	тільки IOS	необхідна картка
Android Pay	Увесь світ	тільки Android	необхідна картка
Samsung Pay	Корея, Китай	тільки Samsung	необхідна картка
Master Card	Увесь світ	всі	необхідна картка

На підставі виділених критеріїв недоліків:покриття, тип пристрою і операційної системи, складність підключення - представлені рекомендацій для розробки нового рішення для безконтактної оплати, обрана платіжна система MasterCard Pay Pass.

Схема сервісів безконтактних платежів MasterCard представлена на рис.3.1

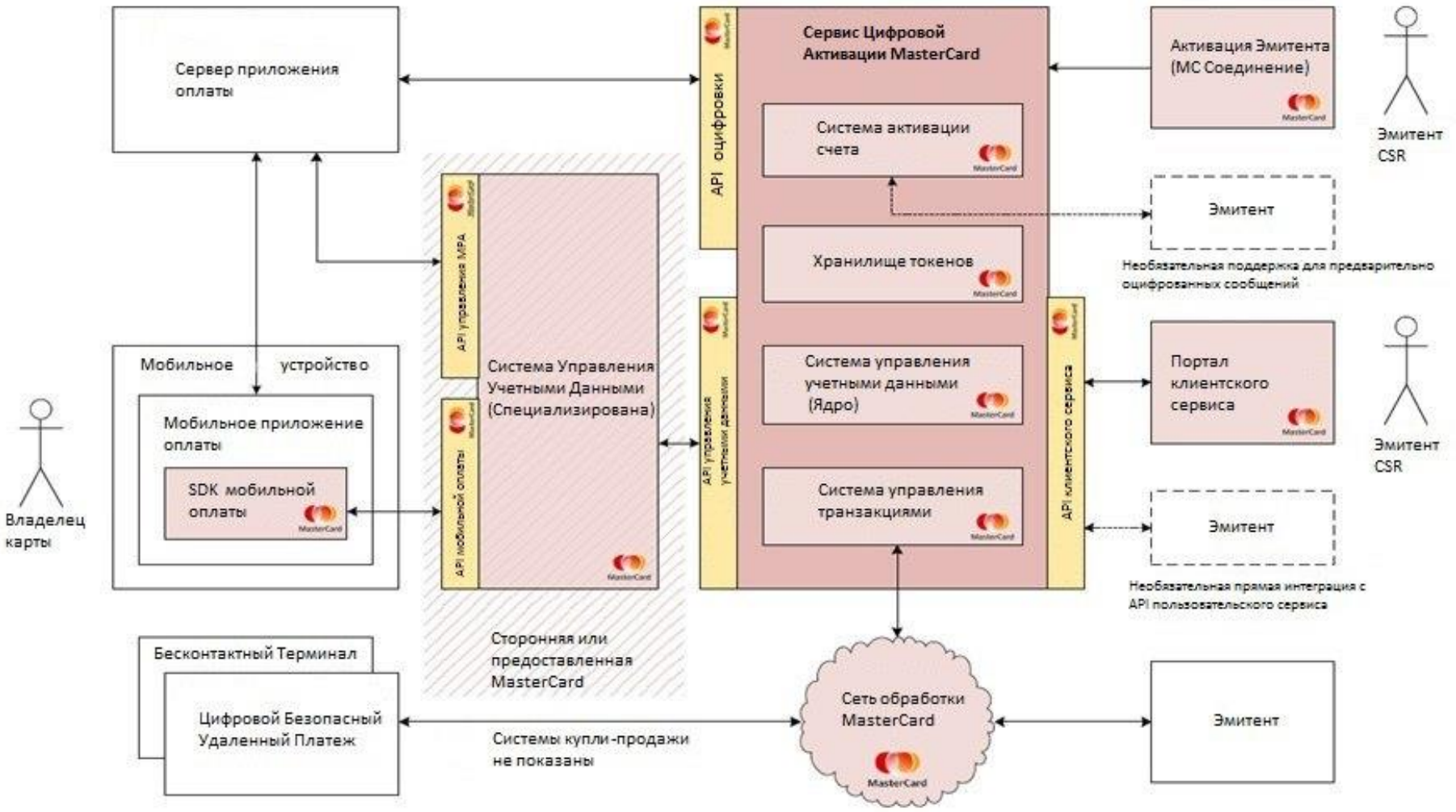

Рис. 3.1 - Схема сервісів безконтактних платежів MasterCard

3.2 Особливості застосування методів ідентифікації безконтактних електронних платежів

Вибір методу ідентифікації безконтактних електронних платежів здійснюєтьсяна підставі існуючих основних і додаткових методів ідентифікації, їх характеристик, переваг і недоліків, наведених у таблиці 3.3.

В якості основних методів ідентифікації, застосовуваних різними платіжними системами, розглянуті:

- ідентифікація по PIN паролю;
- ідентифікація клієнта довіреною особою з перевіркою документів клієнта;
- використання набору AES і DES ключів всередині призначеного для користувача пристрої;
- використання одноразових ключів;
- Fraud контроль.

В якості додаткових методів ідентифікації розглянуті:

- перевірка відбитка пальця під час виконання платежу;
- використання фізичного ключа-флешки.

Таблиця 3.3 Методи ідентифікації, застосовувані різними платіжними системами

Метод	Характеристика	Переваги	Недоліки
Основні методи ідентифікації, застосовувані різними платіжними системами			
Ідентифікація по PIN паролю	Правильний введення пароля мається на увазі системою як майже стовідсотковий ознака того, що платіж здійснюється власником карти. Пароль користувача ніде не зберігається і використовується лише в момент підтвердження платежу, після чого відразу ж видаляється з пам'яті пристроїв. Пароль можна ввести неправильно обмежене число раз, після чого буде потрібна додаткова ідентифікація для користування пристроєм. Це зроблено для запобігання перебору пароля. Як правило з використанням PIN пароля шифрується набір призначених для користувача паролів всередині мобільного пристрою.	Давно випробуваний і повсюдно впроваджений метод, не вимагає від пристрою користувача зв'язку з системою, з включеною перевіркою пароля зламати платіжне пристрій практично неможливо	Введення пароля видно всім, термінал оплати вимагає зв'язку з системою

Продовження таблиці 3.3

Ідентифікація клієнта довіреною особою з перевіркою документів клієнта	Використовується зазвичай для реєстрації в банку-клієнта системи MasterCard PayPass, а також для відновлення контролю над рахунком після крадіжки / втрати пароля	Майже 100% гарантія, практично неможливо підробити	вкрай незручно
Використання набору AES і DES ключів всередині призначеного для користувача пристрої	До цих ключам відносяться ключ пристрою (з його допомогою відбувається підтвердження транзакції призначеним для користувача пристроєм тоді, коли у мобільного пристрою є зв'язок з сервісами MasterCard PayPass, а також для отримання одноразових ключів), транспортні ключі (використовуються для передачі інформації між мобільним пристроєм і веб-сервісами банку-клієнта системи MasterCard PayPass, а також передачі інформації між мобільним пристроєм і самою системою MasterCard PayPass), ключі до зашифрованих даних (карткова інформація) на пристрої.	Забезпечують додатковий надійний шар криптографії для зберігання і передачі даних.	При поточному рівні розвитку обчислювальної потужності - немає.

Продовження таблиці 3.3

Використання одноразових ключів	Використовуються для підпису платежів мобільним пристроєм тоді, коли у нього немає зв'язку з платіжною системою (але у терміналу є). Мають термін придатності, кожен ключ підписує лише один платіж, як правило це платіж не великого розміру.	Дозволяють здійснювати платежі без постійного контакту мобільного пристрою з серверами MasterCard PayPass.	Раз в певний проміжок часу їх необхідно оновлювати, для цього потрібна зв'язок з MasterCard PayPass.
Fraud контроль	Комплекс сервісів, що працюють з використанням технологій machine learning. Визначає не типову або підозрілу активність на карті.	Значно скорочує витрату ресурсів на аналіз платежів.	Все одно вимагає контролю людини
Додаткові методи ідентифікації, застосовувані різними платіжними системами			
Перевірка відбитка пальця під час виконання платежу	Використовується такими системами, як Apple Pay і Samsung Pay, замість PIN	Простіше і швидше введення пароля, оточуючі не можуть підглянути відбиток	Не всі пристрої мають сенсор відбитка пальця, сучасні сенсори зламуються за допомогою скотча, камери і принтера якщо є доступ до речей клієнта роздруковується і прикладається до сенсора)
Використання фізичного ключа-флешки	Містить в собі набір криптографічних асиметричних ключів, однозначно ідентифікують пристрій.	Захист корпоративного рівня	Дорого, потрібно модернізації всіх наявних терміналів

На підставі наведених рекомендацій можна зробити висновок, що методи стандартної ідентифікації мають багато недоліків, основним є безпека, що є критичним, тому що може призводити до втрати фінансових коштів банками і клієнтами, до штрафів банків компаніями платіжних систем.

Пропонується використання біометричної ідентифікації - процес докази і перевірки автентичності через пред'явлення користувачем свого біометричного способу і шляхом перетворення цього образу відповідно до заздалегідь визначених протоколом аутентифікації. Біометричні системи аутентифікації - системи аутентифікації, що використовують для посвідчення особи людей їх біометричні дані.

Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення. Апаратні засоби включають в себе біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, малюнок вен на долоні або пальці) і перетворять отриману інформацію в цифрову модель, доступну комп'ютера. А програмні засоби ці дані обробляють, співвідносять з базою даних і визначають, авторизований клієнт знаходиться перед сканером [17].

В якості методів, пропонованих в якості удосконалення процедури ідентифікації, пропонується, крім основних і додаткових методів, використовувати методиідентифікації за матеріальним становищем і методи біометричної ідентифікації, представлені в таблиці 3.4.

Пропонується використовувати наступні методи:

– ідентифікація по фотографії - метод біометричної ідентифікації. Під час здійснення платежу з додатком необхідно надати фотокартку особи користувача. Цю фотографію аналізують нейронні мережі та набір алгоритмів для визначення параметрів особи. В результаті оцінки виходить ймовірність того, що людина, яка робить платіж, є власником карти. Для цього попередньо потрібно зробити кілька знімків особи власника картки під час реєстрації в платіжній системі;

– ідентифікація по ході - метод біометричної ідентифікації. У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані з датчиків прискорення (акселерометрів). Ці дані зберігаються в одному великому масиві. Після з цього масиву за допомогою статистичних методів рядів Фур'є відбувається виділення патернів ходи власника карти. У момент скоєння фінансової транзакції мобільний пристрій бере дані з акселерометрів за останні дві хвилини і звіряє їх з існуючими довіреними паттернами. На підставі цього виходить імовірнісна оцінка того, що останні дві хвилини телефон був у руках у свого власника, відповідно саме він і робить платіж;

– ідентифікація за даними про пересування -методідентифікації за матеріальним становищем (геолокаційні). У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані про переміщення власника пристрою за допомогою отримання даних з датчиків GPS, а також отримання ідентифікаторів всіх найближчих WI-FI точок. Ці дані зберігаються в одному великому масиві. Після цього за допомогою різних методів, наприклад, методів машинного навчання або простого статистичного аналізу, визначаються патерни переміщення людини в залежності від часу доби і дня тижня. На підставі цих даних можна визначити ймовірність того, що власник карти буде здійснювати фінансову транзакцію в даному місці, в даний час доби, на дану суму. На підставі цього можна оцінити в момент скоєння користувачем фінансової

транзакції, ймовірність того, що людина, що здійснює платіж є власником мобільного пристрою;

− ідентифікація за датою і місцем скоєних покупок - методідентифікації за матеріальним становищем. Після нетривалого користування платіжною системою в базі даних зберігаються дані про всі покупки користувача платіжної системи. На підставі цих даних можна порахувати, де і в який час користувач найчастіше робить покупки. Маючи ці дані можна дуже достовірно оцінити, зробив би власник мобільного пристрою платіж в даній час в даному місці. Наприклад, якщо платіж відбувається в іншій країні, то це швидше за все не власник карти. Для цього проводиться аналіз існуючих фінансових транзакцій користувача, і, коли користувач робить платіж, система звіряє дату і місце розташування платежу, намагаючись оцінити, наскільки здійснюються купівля статистично схожа на попередні покупки користувача. На підставі цього виходить імовірнісна оцінка того, що людина, що здійснює платіж, є власником карти.

Таблиця 3.4 Методи ідентифікації за матеріальним становищем і методи біометричної ідентифікації

Метод	Характеристика	Переваги	Недоліки
Ідентифікація по фотографії	Під час здійснення платежу з додатком необхідно надати фотокартку особи користувача, яка аналізується і оцінюється.	У цьому методі не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки. Наприклад, PIN код може бути подсмотрен.	1) Недосконалість алгоритмів обробки і аналізу особи по фотографії. 2) особу просто підробити. Зловмисник може поставити фотографію власника карти перед камерою мобільного пристрою в момент скоєння фінансової транзакції

Продовження таблиці 3.4

Ідентифікація по ході	У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані з датчиків прискорення (акселерометрів). Ці дані зберігаються, здійснюється відбувається виділення патернів ходи власника карти. Дані з акселерометрів в момент фінансової операції звіряються їх з існуючими довіреними паттернами.	Не потребує ніяких дій від користувача. Для оплати необхідно лише піднести телефон до терміналу. У цьому методі не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки. Наприклад, PIN код може бути подсмотрен. Дані акселерометрів дуже складно підробити через відмінності в анатомії двох будь-яких людей. І навіть якщо вдасться підібрати потрібні параметри, то це буде дуже складно для крадіжки одного телефону, і майже неможливо для систематичних крадіжок. Не дає хибно позитивних результатів.	Через постійне відстежування даних акселерометра відбувається постійний розряд батареї пристрою, що негативно позначається на тривалість періоду, після і стан батареї. Незважаючи на те, що метод не дає помилково позитивних результатів, метод дуже часто дає помилково негативні результати, через що його дуже складно застосовувати як основний метод ідентифікації. Як правило, його застосовують в зв'язці з іншими методами. Наприклад з перевіркою PIN коду тоді, коли оцінка ходи вказує, що платіж виконує не власник карти.

Продовження таблиці 3.4

Ідентифікація за даними про пересування	У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані про переміщення власника пристрою за допомогою отримання даних з датчиків GPS, а також отримання ідентифікаторів всіх найближчих WI-FI точок. Ці дані зберігаються, визначаються патерни переміщення людини. На підставі цього можна оцінити в момент скоєння користувачем фінансової транзакції, ймовірність того, що людина, є власником мобільного пристрою.	Не вимагає абсолютно ніяких дій від користувача. Для оплати необхідно лише піднести телефон до терміналу. У цьому методі не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки. Дані GPS складно підробити, і ще складніше і затратним підробляти їх для здійснення систематичних розкрадань коштів. Помилково позитивні результати вкрай рідкісні.	Через постійне відстежування даних про переміщення відбувається постійний розряд батареї пристрою, що негативно позначається на тривалість періоду, після і стан батареї. Незважаючи на те, що метод не дає помилково позитивних результатів, метод дуже часто дає помилково негативні результати, через що його дуже складно застосовувати як основний метод ідентифікації. Як правило його застосовують в зв'язці з іншими методами. Наприклад, з перевіркою PIN коду тоді, коли оцінка пересування вказує, що перед нами не власник карти.

Продовження таблиці 3.4

Ідентифікація за датою і місцем скоєних покупок	На підставі даних, що зберігаються про всі покупки користувача можна враховувати, де і в який час користувач найчастіше робить покупки. Проводиться аналіз існуючих фінансових транзакцій користувача, і система звіряє дату і місце розташування платежу, оцінюючи, наскільки здійснюються купівля статистично схожа на попередні покупки користувача. На підставі цього виходить імовірнісна оцінка того, що людина, що здійснює платіж, є власником карти.	Не вимагає абсолютно ніяких дій від користувача. Для оплати необхідно лише піднести телефон до терміналу. У цьому методі не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки. Дату і місце здійснення платежу важко підробити. 1) для цього доведеться протягом деякого часу спостерігати за жертвою, перш, ніж вкрасти телефон, і зробити платіж там і під час, де його б зробив власник телефону; 2) у багатьох місцях, де використовується безконтактні платежі, встановлені відеокамери, через що робити платіж там, де власник карти, для зловмисника	Відсутні для користувача платіжної системи. Практично відсутні для банку-клієнта платіжної системи. Єдині недоліки - необхідність використання спеціально розробленого ПО разом з навченими операторами, перевіряючими підозрілі транзакції.

Продовження таблиці 3.4

		небезпечно; 3) в якості нагороди зловмисник може отримати товар з магазинів, в яких здійснював покупки власник карти.	

3.3 Особливості застосування вдосконаленого методу ідентифікації

Процес ідентифікації складається з наступних етапів:

− реєстрація користувача в відділенні банку-клієнта системи MasterCard PayPass;

− установка платіжного додатка користувачем на свій мобільний пристрій;

− спостереження за користувачем платіжної системи і збір масиву ідентифікуючої інформації;

− обчислення ймовірнісної оцінки ідентифікації користувача в момент вчинення ним платежу за допомогою безконтактної системи;

− якщо ймовірна оцінка вище довірчого значення - здійснюємо платіж, інакше виконується:

− ідентифікація по PIN коду;

− здійснення платежу.

Розглянемо ці етапи більш детально:

1) реєстрація користувача в відділенні банку-клієнта системи MasterCard PayPass.

Користувач проходить реєстрацію у відділенні банку-клієнта системи MasterCard PayPass. Користувач надає паспорт, ідентифікаційний код, номер телефону, в обмін отримує дані своїх платіжних карт і PIN код;

2) установка платіжного додатка користувачем на свій мобільний пристрій.

Користувач вводить свої дані в мобільний додаток банку-клієнта системи MasterCard PayPass і засвідчує свою особистість шляхом використання перевірочного коду, отриманого в повідомленні SMS на номер мобільного телефону, зазначеного при реєстрації, і ввівши пароль, виданий йому при реєстрації в банку.

Користувачеві приходить набір криптографічних ключів для шифрування інформації, переданої між мобільним додатком, сервісами банку-клієнта і сервісами MasterCard PayPass. Також генеруються ключі для підпису фінансових транзакцій та інших дій користувача на подобі редагування карткових даних;

3) спостереження за користувачем платіжної системи і збір масиву ідентифікуючої інформації.

Протягом деякого часу користувач здійснює платежі, вводячи PIN код при оплаті (або прикладаючи палець до пристрою, що зчитує відбиток пальця, якщо такий пристрій передбачено).

З початку реєстрації користувача в банку мобільний додаток відстежує переміщення користувача за допомогою GPS, збору адрес доступних точок WI-FI, відстеження сигналів з веж стільникового зв'язку. Цей набір даних є кортеж виду:

{Date: "21.05.12 12:12:12",

GPS: "N 41 ° 47 '23' ' W 87 ° 35 '59' ' ",

SSID: ["adfas", "asfdsad", "asdfa"],

terminalID: "th656h45g34",

money: "37,24",

paymentData: [owner: "Ayvasovscki II",

LicenseID: "65456584658",

Kassir: "Vladislavna TT"

Check: [{name: "Mylo", price: "13.12"},

{Name: "Shampun", price: "11.00"},

{Name: "Gel", price: "13.12"}]}

де *date* -дата і час здійснення платежу в форматі "dd.mm.yy 00:00:00",

GPS -координати місця розташування в форматі "N 0 ° 0 '0' ' *W 0 ° 0 '0' ' ",*

SSID- wifi ідентифікатори в форматі ["xxxxx", "xxxxx", "xxxxx"],

terminalID -ідентифікатор терміналу, в якому здійснений платіж, в форматі: "xx000x00x00",

money -сума грошей, витрачена за покупку в форматі "00 000,00",

paymentData- інша доступна інформація про покупку в форматі: ["власник терміналу, ліцензія, касир, список покупок, ціна і т.д."]

Переміщення користувача до коректного введення PIN коду при покупці вважається достовірним, переміщення після здійснення покупки вважається недостовірною, і стає достовірним тільки після коректного введення PIN коду.

Дана інформація зберігається і на телефоні користувача, і на серверах банку-клієнта.

Також збирається інформація з акселерометрів пристрою про координати місця розташування в форматі {x: "-0.0015456", y: "0.9554654", z: "0.456546546"}.

З цих даних вибираються повторювані ділянки (ходьба, стояння в черзі), за допомогою перетворення рядів Фур'є.

Дані ділянки перетворюються і зберігаються в такому вигляді в пам'яті мобільного пристрою і на серверах компанії.

Достовірність даних та ж, що і для переміщення;

4) обчислення ймовірнісної оцінки ідентифікації користувача в момент вчинення ним платежу за допомогою безконтактної системи

На підставі цих даних формується таблиця статистичної ймовірності здійснення платежу користувачем в даний час доби в даний день тижня в даному магазині на дану суму.

Кластерізіруем набір даних про переміщення клієнта і здійснення ним покупок. У момент здійснення платежу вираховуємо відстані від точки <Xp, Yp, Tp>, що характеризує координати положення здійснення платежу і час, до кордонів наявних кластерів, отримуємо мінімальну відстань S min.

Якщо Smin <K (K - довірена відстань) то користувач ідентифікований;

5) ідентифікація по PIN коду.

Ідентифікація по PIN коду відбувається тільки, якщо етапи 3 і 4 не ідентифікована користувача по ході і переміщенню.

На підставі PIN коду додаток розшифровує призначені для користувача криптографічні ключі та підписує транзакцію;

6) здійснення платежу.

Стандартний алгоритм MasterCard PayPass вимагає введення пароля. Банк-клієнт має право скасувати введення пароля або зберігати його в призначеному для користувача пристрої.

Перед тим як вимагати пароль від клієнта, перевіряється ряд параметром платежу, і, якщо вони задовільні, то додаток користувача не питає пароль. Повторна перевірка відбувається на серверах банку, який визначає чи потрібно підтвердження PIN коду перед вчиненням платежу.

Аналогічна перевірка відбувається на серверах MasterCard PayPass (fraud контроль), але там вони мають інформацію лише про платежі, а не про переміщеннях.

Якщо користувач ідентифікований, то здійснюється платіж, інакше виконується перехід до п. 5.

Таким чином, перевагами і вдосконаленнями запропонованого методу ідентифікації є такі.

Отримуємо від терміналу тип платежу (чи потрібно його підтверджувати паролем чи ні, цю інформацію надає банк клієнт, на підставі зібраної раніше інформації про попередні транзакції і переміщеннях користувача), тобто виконується перевірка на серверній стороні.

Якщо сервер на підставі зібраної інформації вимагає пароль, - однозначно запитується пароль у користувача.

Якщо сервер не вимагає пароля, додаток вирішує, чи потрібно питати у користувача пароль на підставі вже своїх даних.

Якщо додаток вирішує, що користувач коректний, тоді програма не запитує пароль і просто робить платіж, інакше - вимагає пароль.

Рішення здійснюється наступним чином:

1) звіряються дані про дату, суму, місці поточного платежу, перелік оточуючих wifi точок з даними, накопиченими в пункті 3 Підготовчий етап (збір даних для ідентифікації);

Виходить ймовірність того, що користувач авторизований. Інакше запитується пароль.

2) якщо користувач пройшов перевірку пункту 1, перевіряються дані за останні 2 хвилини з його акселерометрів;

Звіряються з даними з пункту 3 «Спостереження за користувачем платіжної системи і збір масиву ідентифікуючої інформації»;

3) якщо п.1 та п.2 пройдені з імовірністю більше 95%, то здійснюється платіж без пароля.

В основі методу ідентифікації лежать наступні припущення.

Вартість втрат від шахрайства включає суму вкрадених грошей Mst і штрафи від компанії MasterCard PayPass банкам Mp.

Для підвищення безпеки банки повинні впроваджувати рішення з вартістю, Mimpl

Вартість ресурсів, що витрачаються шахраєм на крадіжку грошей з банківського рахунку, Ms Кількість грошей, які шахрай здатний безпечно перевести в готівку, Mg.

Відповідно дві нерівності повинні виконуватися:

$$M_g - M_s \to 0,.$$
$$M_{impl} < M_p \quad (3.1)$$

при тому, що платіж повинен бути простіше готівкового розрахунку.

3.4 Опис і застосування методу ідентифікації безконтактних платежів

Стандартна ідентифікація безконтактних платежів має вигляд

$$M_{is} =< P_{pin}, K_{mob}, K_{sin} > , \quad (3.2)$$

де - PIN пароль,P_{pin}

K_{mob} - підпис мобільного пристрою,

K_{sin} - підпис одноразовим ключем.

Опис методу ідентифікації з переміщення (геолокація)

Для ідентифікації необхідно зібрати масив даних про переміщення користувача.

Елемент масиву має вигляд: $P_i =< X_i, Y_i, T_i >$ де Xi - широта, Yi - довгота, Ti - дата і час.

Елементи масиву розміщуємо в тривимірному просторі.

Кластерізіруем дані за допомогою методу K-means.

У момент здійснення платежу за допомогою алгоритму Anomaly detection перевіряємо наскільки розташування користувача в момент покупки відрізняється від його звичайних пересувань і отримуємо оцінку відмінностіS_{min}

якщо $S_{min} < K$, Де K - довірена відміну) то користувач ідентифікований.

Опис біометричного методу ідентифікації

Набір даних з датчиків прискорення пристрою користувача може бути представлений у вигляді

$$D = < T_i, X_i, Y_i, Z_i >, \quad (3.3)$$

де Ti - час зняття виміру

Xi - дані першого акселерометра в момент часу Ti

Yi - дані другого акселерометра в момент часу Ti

Zi - дані третього акселерометра в момент часу Ti

Нехай A - набір даних за певний проміжок часу Ti- Ti + 1

Проводимо перетворення методом рядів Фур'є за формулою:

$$f(x) = \sum_{k=-\infty}^{+\infty} \hat{f}_k e^{i2\pi \frac{k}{\tau} x},$$

Отримуємо Z - чисельне представлення хвиль (патерн руху користувача)

У момент платежу порівнюємо накопичені за час дані з даними за останні дві хвилини за допомогою методів квадратів. Отримуємо різницю між паттернами.

Розраховуємо процентну різницю $G = dZ/Z \times 100\%$, Отримуємо оцінку схожості патернів руху. Якщо G> 95%, то користувач ідентифікований.

4 ПРАКТИЧНЕ ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ

4.1 Проектування інформаційної системибезконтактних електронних платежів з використанням UML-діаграм

В процесі розробки фізичної моделі даних виділені інформаційні об'єкти (сутності), які відповідають вимогам нормалізації даних і визначені зв'язки між ними. Отримана модель відображає реальну структуру БД.

Схема фізичної моделі даних системи безконтактних платежів представлена на рис. 4.1.

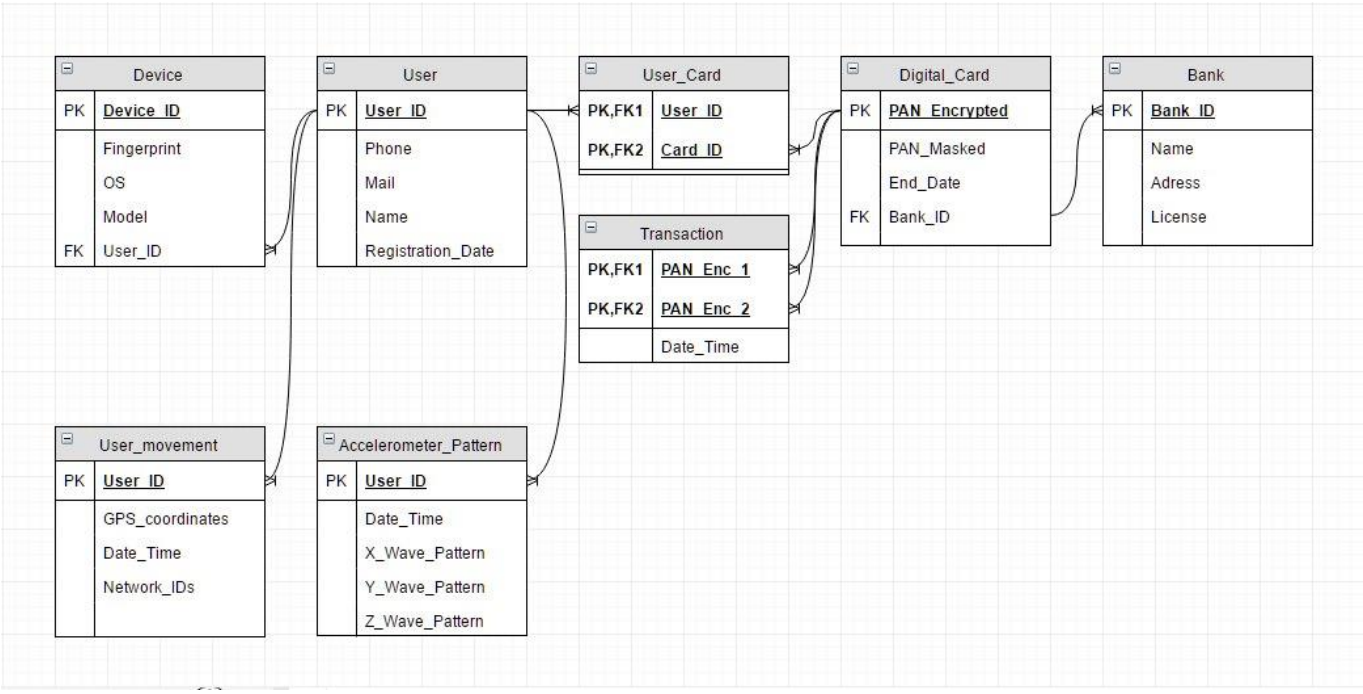

Рис.4.1 Схема структури БД системи

Опис моделі логічної структури представлено у вигляді діаграм класів (class diagram) серверного додатка, наведених на рис. 4.2-4.5.

Діаграма класів використовуються при моделюванні систем. Вони є однією з форм статичного опису системи з точки зору її проектування, показуючи її структуру. На діаграмах класів показуються класи, інтерфейси і відносини між ними [17-19]. На рисунках 4.2-4.5 наведені різні уявлення діаграм класів.

На рис. 4.2 приведена загальна діаграма серверної частини, яка містить класи без полів і функцій.

На рис 4.3 представлена діаграма класів сутностей, що представляють об'єкти, що зберігають в полях інформацію і не мають функцій.

На рис. 4.4 представлена схема шару DAO (Data Access Object) серверної частини, що описує допоміжні класи для збереження сутностей в БД.

На рис. 4.5 представлена схема сервісного шару, що описує розташування сервісів серверного додатка.

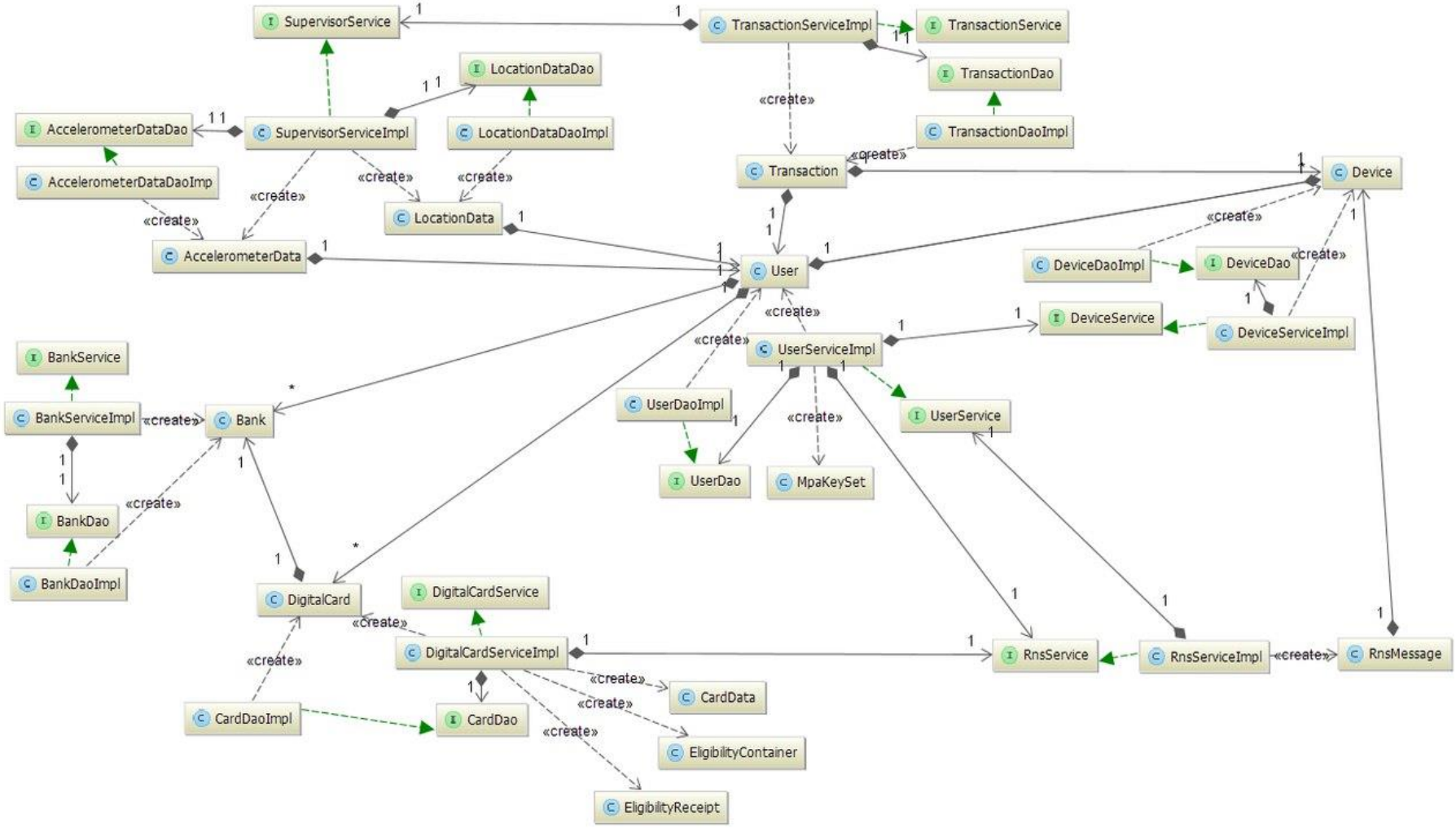

Рис. 4.2 Загальна діаграма класів серверної частини

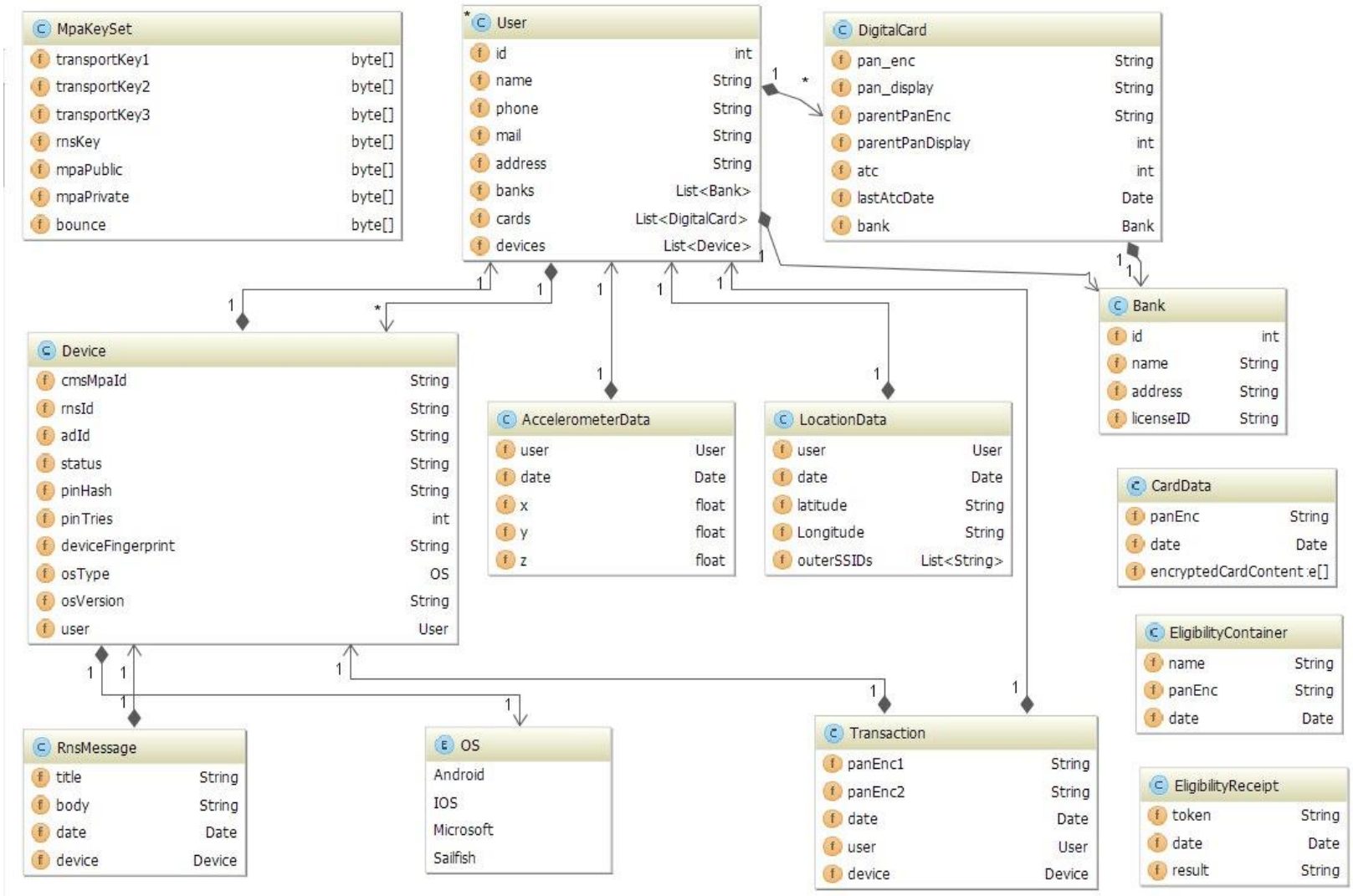

Рис. 4.3 Діаграма класів сутностей

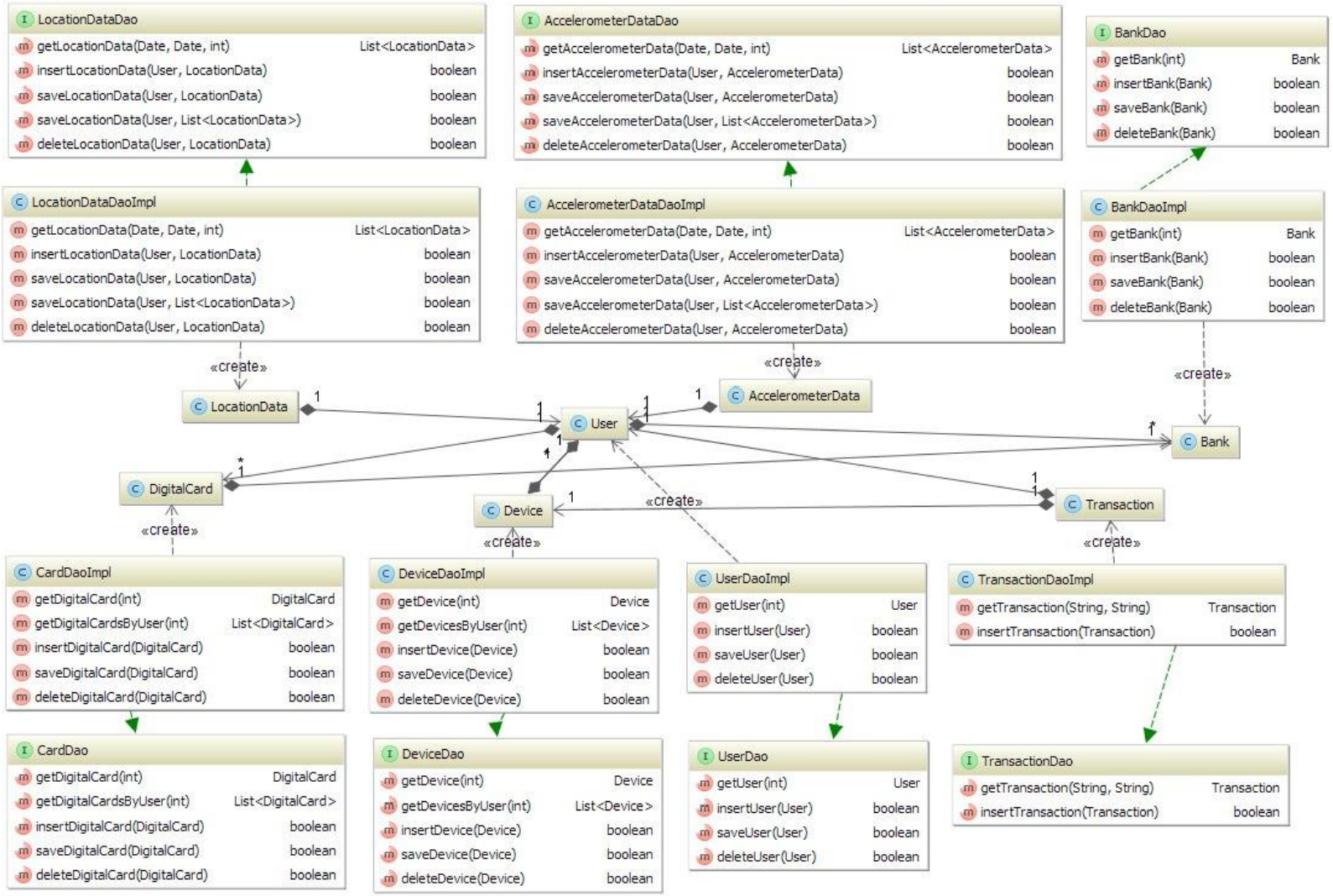

Рис. 4.4 Схема класів шару DAO серверної частини

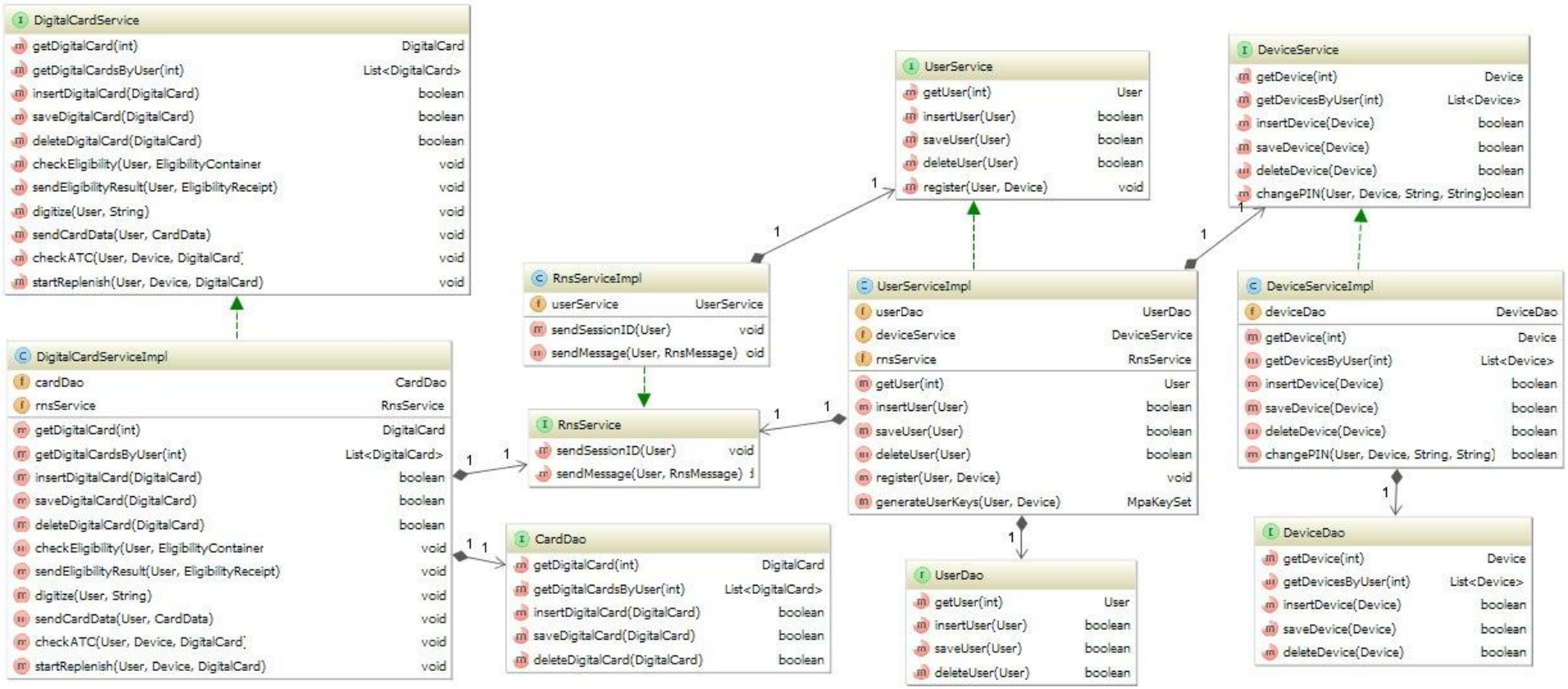

Рис. 4.5 Схема класів сервісного шару

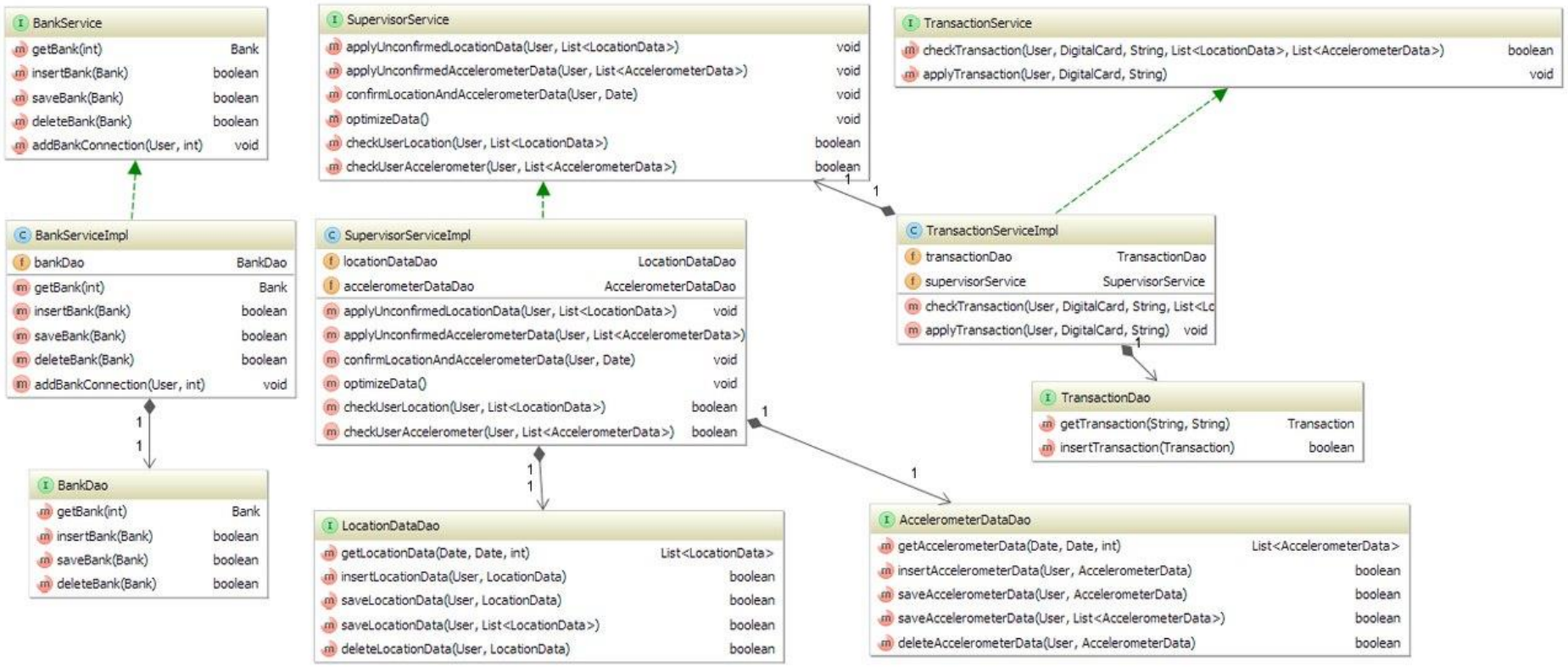

Рис. 4.5 (продовження) Схема класів сервісного шару

Опис моделі взаємодії об'єктів системи представлено у вигляді діаграм послідовності, які представлені на малюнках 4.6-4.8.

На рис. 4.6 представлена діаграма послідовності дій «Реєстрація даних клієнта в банку».

На рис. 4.7 представлена діаграма послідовності дій «Реєстрація даних клієнта в безконтактної системі».

На рис. 4.8 представлена діаграма послідовності дій «Оцифровка карти».

На рис. 4.9 Діаграма послідовності дій скоєння безконтактного платежу.

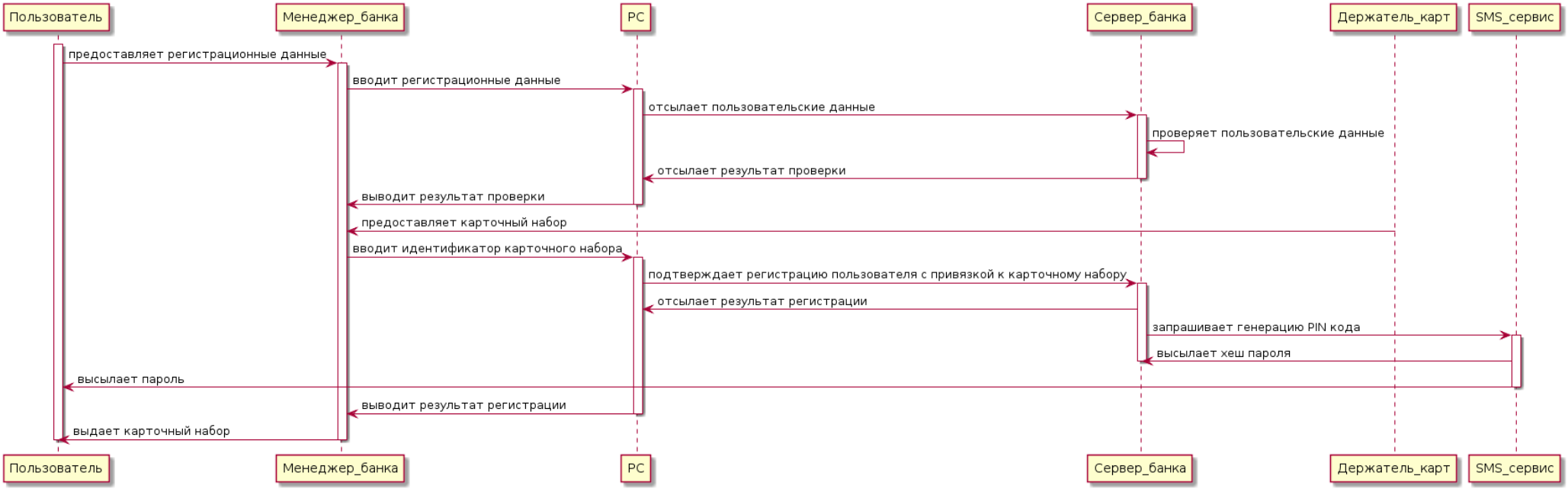

Рис. 4.6 Діаграма послідовності дій «Реєстрація даних клієнта в банку»

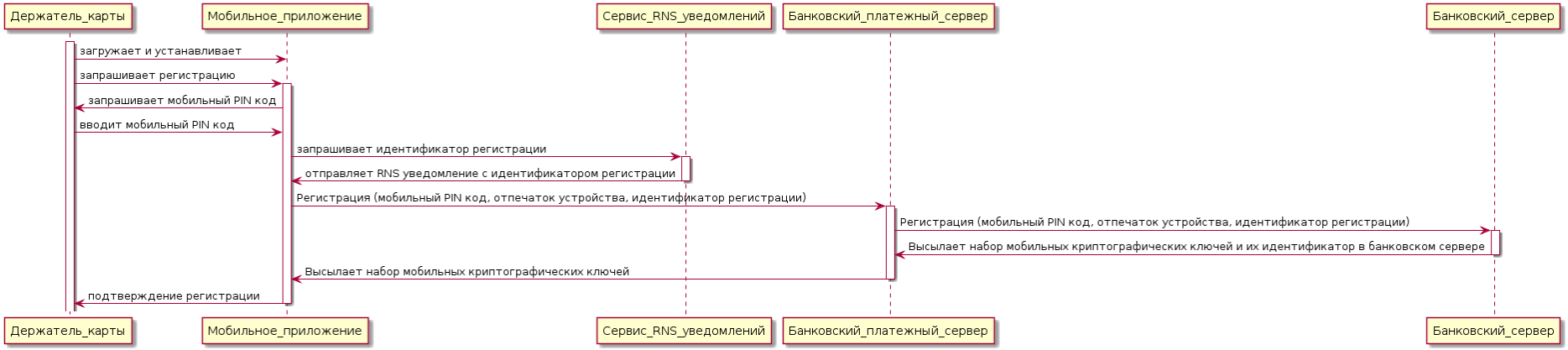

Рис. 4.7 Діаграма послідовності дій «Реєстрація даних клієнта в безконтактної системі »

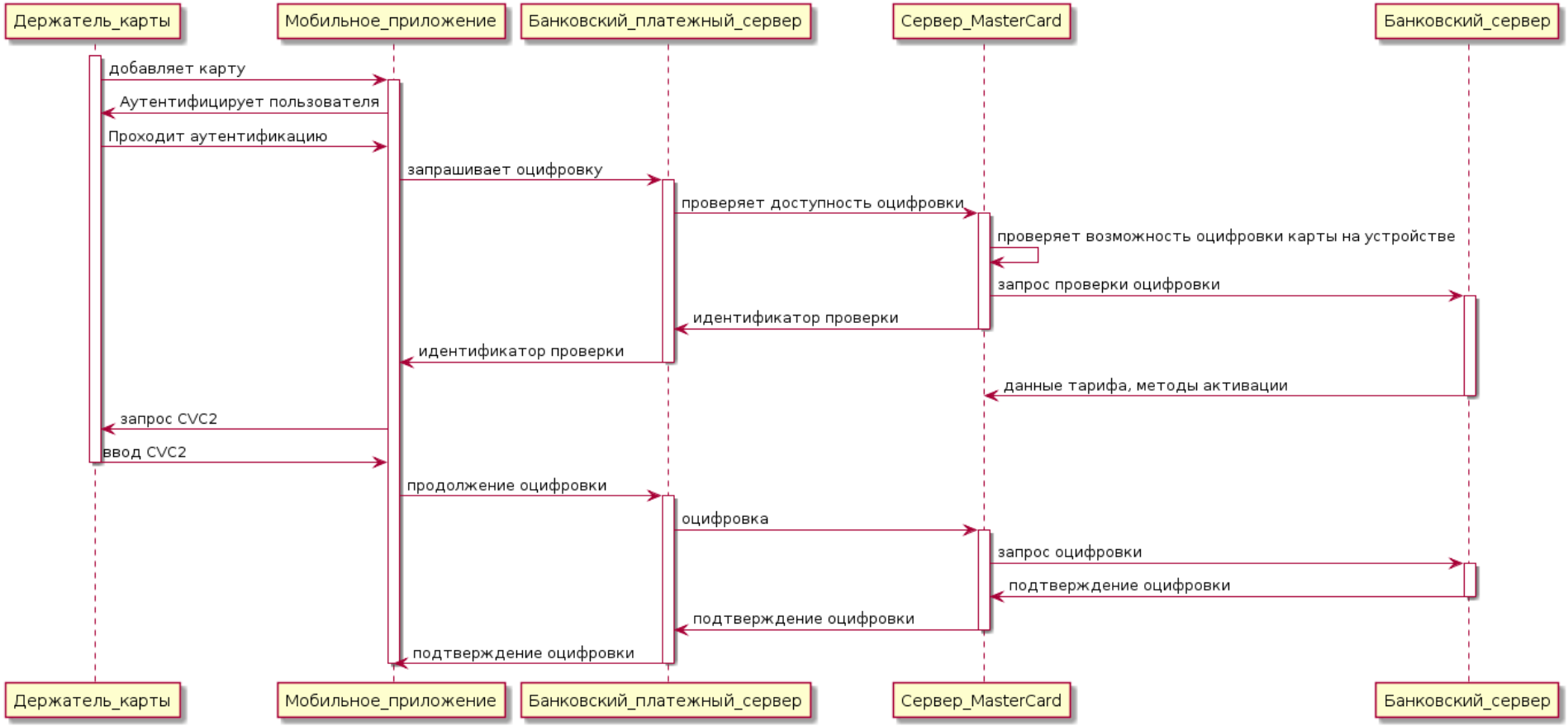

Рис. 4.8 Діаграма послідовності дій «Оцифровка карти»

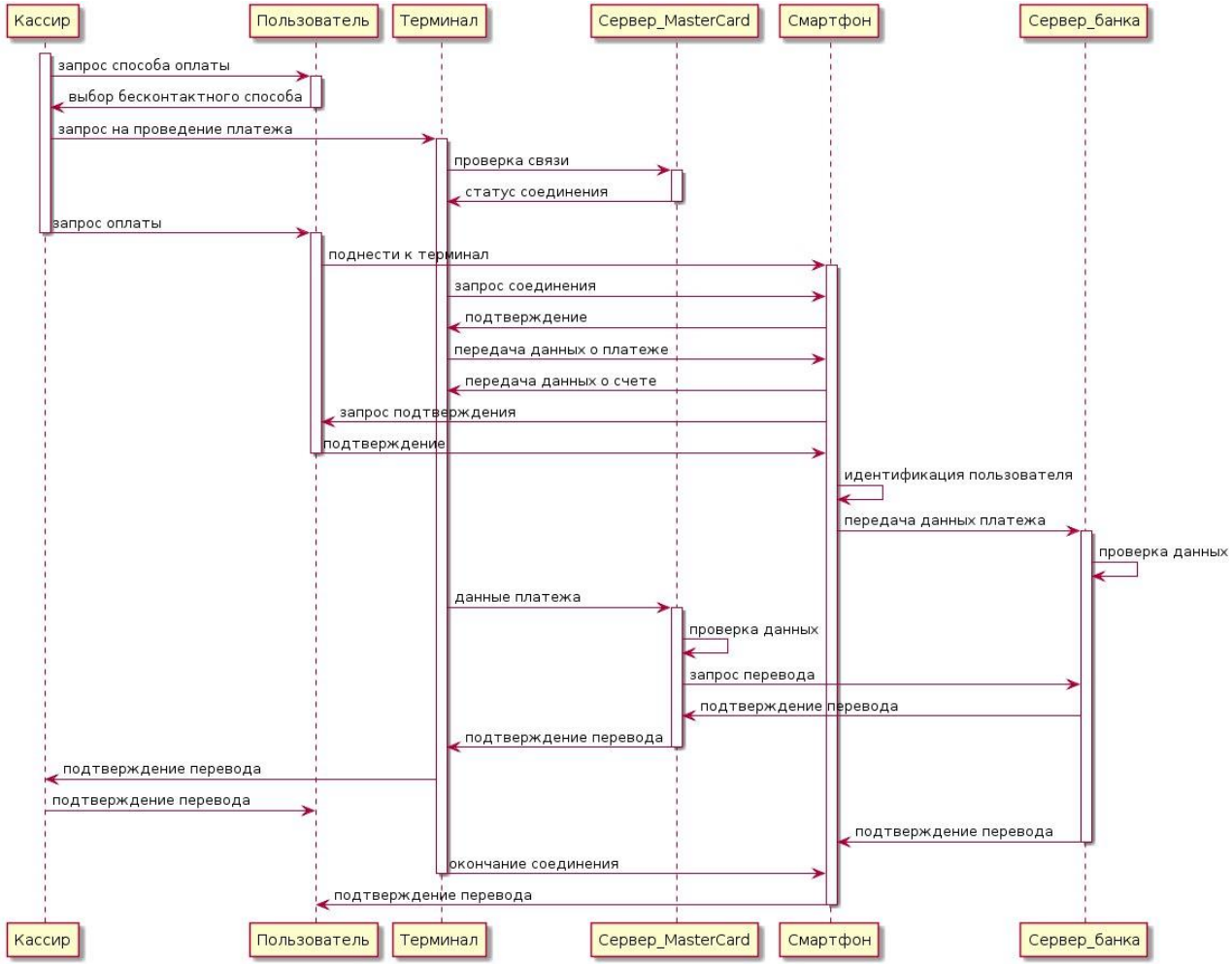

Рис. 4.9 Діаграма послідовності дій скоєння безконтактного платежу

Опис моделі поведінки системи представлено у вигляді діаграми діяльності (activity).

Опис методу ідентифікації можна представити у вигляді діаграми діяльності, представленої на рис. 4.9.

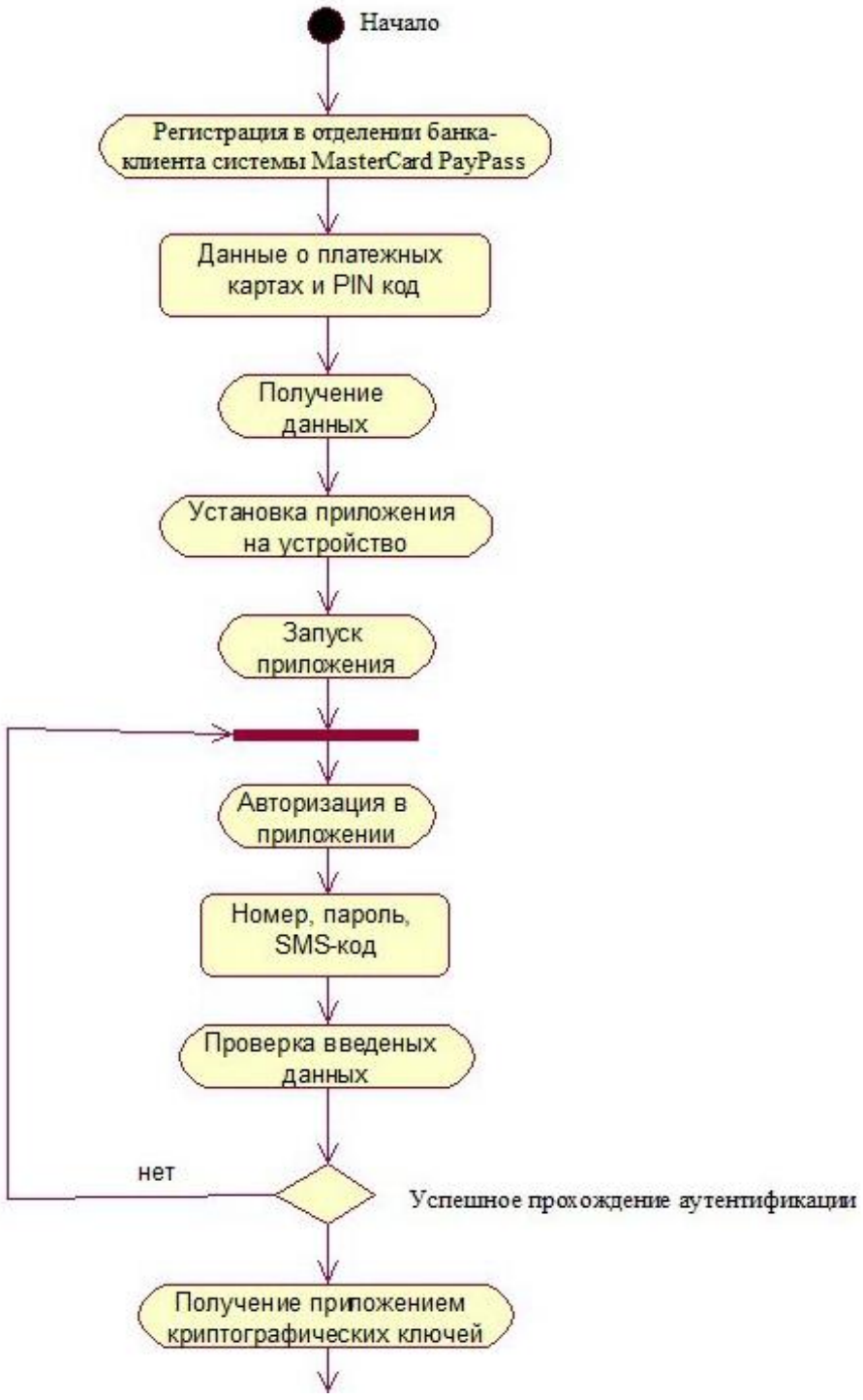

Рис. 4.9 (лист 1) Діаграма діяльності методу ідентифікації


Генерация приложением ключей для подписи транзакций
Отслеживание и сбор данных приложением
GPS координаты пользователя, адреса доступных точек Wi-Fi и точек вышек сотовой связи, информация с акселерометра устройства
Определение приложением повторяющихся участков на основе данных о перемещении, с помощью преобразования рядов Фурье
Сохраниение данных на устройство
Отправка данных на сервер
Формирование приложенем таблицы статистических вероятностей совершения платежа
Кластеризация приложением набора данных о перемещении и совершении покупок
Совершение попытки платежа через терминал
Данные о плтаеже
Отправка данных на сервер

Рис. 4.9 (лист 2)

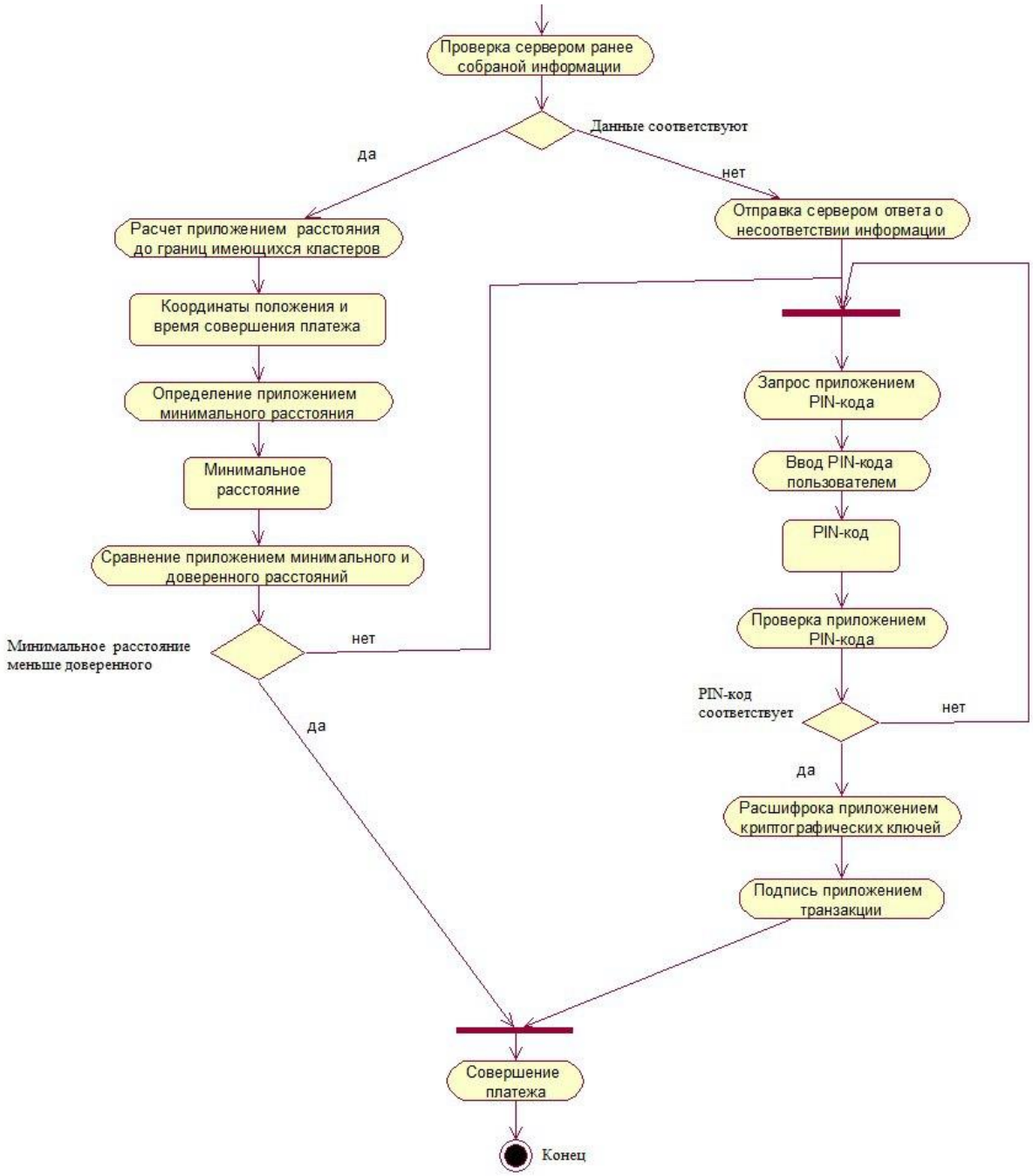
Проверка сервером ранее собраной информации
Данные соответствуют
да
нет
Расчет приложением расстояния до границ имеющихся кластеров
Отправка сервером ответа о несоответствии информации
Координаты положения и время совершения платежа
Определение приложением минимального расстояния
Минимальное расстояние
Сравнение приложением минимального и доверенного расстояний
Минимальное расстояние меньше доверенного
нет
да
Запрос приложением PIN-кода
Ввод PIN-кода пользователем
PIN-код
Проверка приложением PIN-кода
PIN-код соответствует
нет
да
Расшифрока приложением криптографических ключей
Подпись приложением транзакции
Совершение платежа
Конец

Рис. 4.9 (лист 3)

4.2 Реалізація програмного забезпечення системи безконтактних електронних платежів

Програмне забезпечення, що розробляється складається з трьох елементів [21-25]:

- системне програмне забезпечення;
- інструментальне програмне забезпечення;
- функціональне програмне забезпечення.

До складу системного та інструментального програмного забезпечення входять: операційна система (ОС), система управління базами даних (СКБД), стек н (абор технологій, бібліотек, фреймворків) середовище розробки.

Для сервера необхідно наступне ПО:

- ОС - Ubuntu Server (Linux);
- СУБД - Oracle, Cassandra, Tarantool;
- стек - Spring, Hibernate, JAX-RS 3.0 + Apache CXF. Netty. AngularJS. JBoss Fuse. Mobocards Cryptography. Nginx, OpenSSL;
- середовище розробки Intellij Idea /
- Для мобільного телефону під ОС Android:
- ОС - Android 4.4.0 і вище;
- стек Android SDK, Mobocards Cryptography (mobile). OpenSSL, Android Compatibility Package, Spring Android.

Для мобільного телефону під ОС IOS:

- ОС - IOS 10+;
- стек iOS SDK, Mobocards Cryptography (mobile). OpenSSL. objc.io, Device Frameworks.

Розроблене функціональне ПО являє собою платіжну систему у вигляді серверного додатка для банків, як прошарок між сервісами банку і сервісами платіжної системи, що надає своїм користувачам можливість здійснювати безконтактні платежі в мережі Master Card.

Екранна форма «Список підозрілих транзакцій проведення платежів по терміналах», представлена на рис. 4.6, дозволяє оператору переглянути підозрілі транзакції на підставі відсотка їх схожості з попередніми транзакціями користувача, які його ідентифікують (хода, місце розташування, дата, покупка) і прийняти рішення, шахрайська транзакція проведена або авторизована транзакція (надає інформацію, на підставі якої оператор може зателефонувати, наприклад, власнику карти і уточнити легальність проведення операції).

На рис. 4.7 представлений інтерфейси транзакції одного користувача. на рис. 4.8 представлена форма модального вікна анулювання підозрілої транзакції.

Date	Location	Terminal Owner	Money	Pan Encrypted	User ID	Location Confidence	Position Confidence
June 6th 2016, 4:16:30	N 1° 56' 8" W 10° 53' 13"	Store ID:98465496, Lafanov A.D.	$140.97	C72EF48D215E4276	8763601484447	0.80%	0.74%
July 5th 2016, 4:16:30	N 73° 47' 0" W 57° 40' 56"	Store ID: 9865466, Kotskii L.P.	$197.21	0BC9E75B05F58462	9871586287824	0.81%	0.76%
November 12th 2016, 4:16:30	N 49° 59' 6" W 29° 44' 55"	Class Moll	$90.11	CF8FA5BD6B053B66	1527707557839	0.97%	0.84%
June 4th 2016, 4:16:30	N 10° 47' 46" W 46° 15' 40"	Store ID:98465496, Lafanov A.D.	$17.61	F7BACFBD2C29AB2C	1326983184578	0.93%	0.79%
September 20th 2016, 4:16:30	N 1° 10' 45" W 80° 46' 5"	Pharmacy Pills	$73.66	229D7101C4EFADC3	3018414905890	0.99%	0.80%
December 15th 2016, 4:16:30	N 39° 39' 26" W 80° 18' 10"	Rost Moll	$234.35	F8DDF5D315933AE3	1284973769071	0.99%	0.90%
June 16th 2016, 4:16:30	N 31° 35' 47" W 32° 17' 34"	Class Moll	$100.79	54945B6F1BC7BC4B	4070572656885	0.76%	0.78%
December 2nd 2016, 4:16:30	N 67° 24' 2" W 72° 30' 20"	undefined	$83.97	7672A34F84ED02A7	6956123599508	0.91%	0.82%
August 17th 2016, 4:16:30	N 40° 38' 6" W 11° 33' 5"	Metro Cash&Carry	$183.30	EEB5B6671BC1CFFD	8842467188230	0.95%	0.75%
August 12th 2016, 4:16:30	N 60° 3' 21" W 62° 44' 40"	Class Moll	$211.1	56178EC412CBBF00	5874174051949	0.76%	0.99%
March 26th 2016, 4:16:30	N 53° 59' 51" W 53° 25' 20"	Rost Moll	$180.7	7B1F6544F0CC9672	8120307756727	0.85%	0.85%
November 7th 2016, 4:16:30	N 61° 10' 39" W 8° 18' 32"	SCJP Privat Bank	$19.4	3AF25A8D501E2407	3803456772400	0.92%	0.80%
September 13th 2016, 4:16:30	N 20° 28' 12" W 46° 60' 25"	Store ID: 9865466, Kotskii L.P.	$57.0	547FAB465B11F6D2	7248194994315	0.78%	0.72%
July 16th 2016, 4:16:30	N 81° 22' 3" W 38° 0' 19"	SCJP Privat Bank	$74.71	B956F1E07F9E0B4D	2120955945164	0.98%	0.97%
September 25th 2016, 4:16:30	N 61° 9' 53" W 79° 44' 49"	Metro Cash&Carry	$89.13	874832DEBCF21611	6560153975433	0.82%	0.82%
September 10th 2016, 4:16:30	N 70° 9' 58" W 3° 46' 4"	Pharmacy Pills	$215.1	89BF81FEDB529AC6	7347243703977	0.88%	0.71%

Рис. 4.6 Список підозрілих транзакцій проведення платежів по терміналах

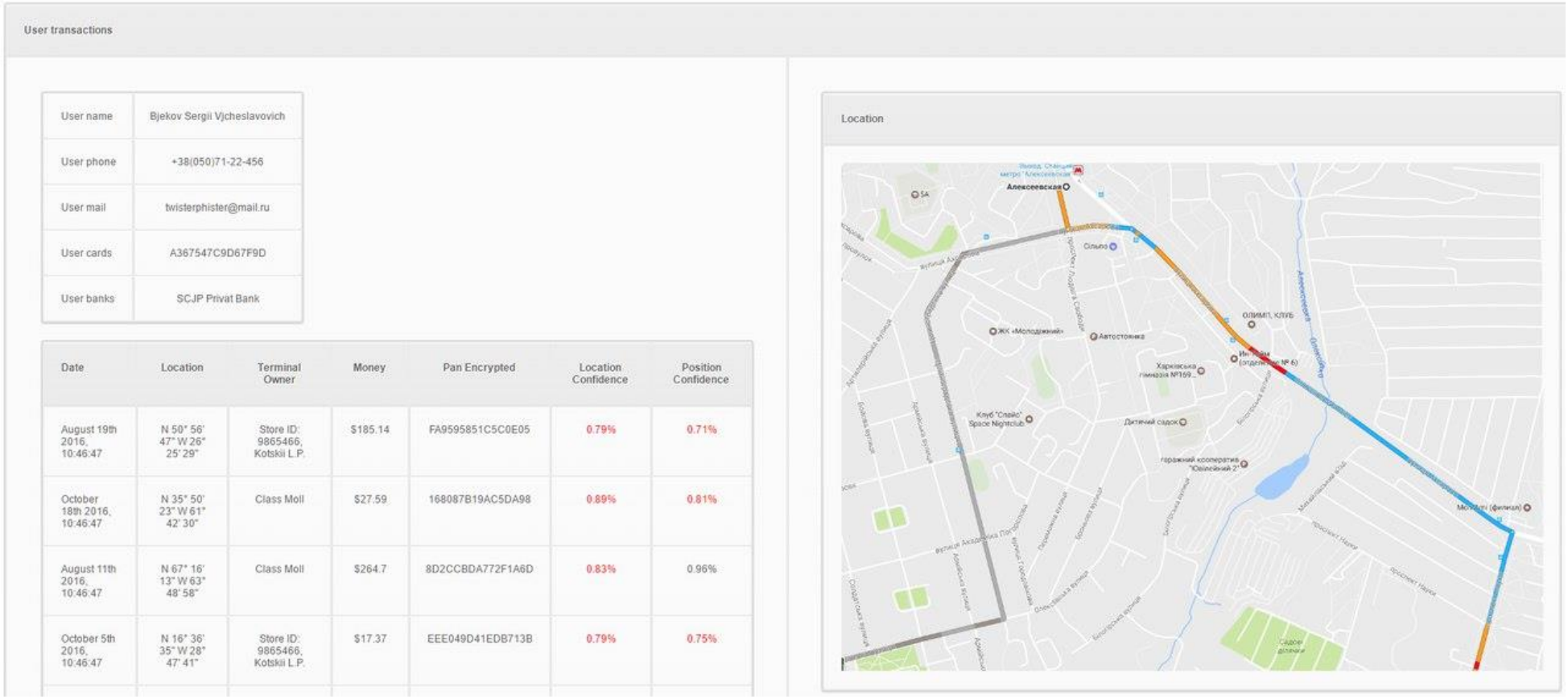

Рис. 4.7 Інтерфейс транзакції одного користувача

March 28th 2016, 10:46:47	N 45° 55' 0" W 27° 6' 39"	Store ID:65465418, Borisov A.G.	$241.62	F00DA91A62248C63	0.82%	0.74%
November 9th 2016, 10:46:47	N 35° 54' 32" W 54° 19' 51"	Class Moll	$22.85	DB1112E20E8AFE35	0.88%	0.89%
October 30th 2016, 10:46:47	N 89° 58' 57" W 44° 3' 15"	Store ID:65465418, Borisov A.G.	$216.7	77F7E9A2E87DB62D	0.74%	0.72%
October 11th 2016, 10:46:47	N 57° 58' 0" W 41° 19' 20"	SCJP Privat Bank	$248.46	0CA85F6072EBCEB2	0.82%	1.00%
May 14th 2016, 10:46:47	N 25° 28' 47" W 30° 56' 52"	Store ID: 9865466, Kotskii L.P.	$230.8	D35CF953AEB4834C	0.71%	0.82%
November 30th 2016, 10:46:47	N 55° 50' 20" W 67° 44' 44"	Rost Moll	$229.40	DBEEC6122D33022E	0.79%	1.00%
August 25th 2016, 10:46:47	N 5° 51' 56" W 31° 19' 11"	Store ID:98465496, Lafanov A.D.	$133.65	D470235BE6B076B7	0.80%	0.79%
September 7th 2016, 10:46:47	N 53° 42' 18" W 85° 50' 12"	Store ID:98465496, Lafanov A.D.	$135.38	76441BD202BFE11D	0.76%	0.78%
April 17th 2016, 10:46:47	N 65° 41' 30" W 33° 47' 24"	undefined	$246.63	1F45EA31FF905EA8	0.75%	0.91%
August 7th 2016, 10:46:47	N 56° 12' 35" W 58° 37' 34"	undefined	$8.9	712A146F44EC15DA	0.75%	0.92%
April 28th 2016, 10:46:47	N 63° 0' 50" W 52° 34' 4"	Class Moll	$13.33	A2643115FC3AD6B8	0.81%	0.90%

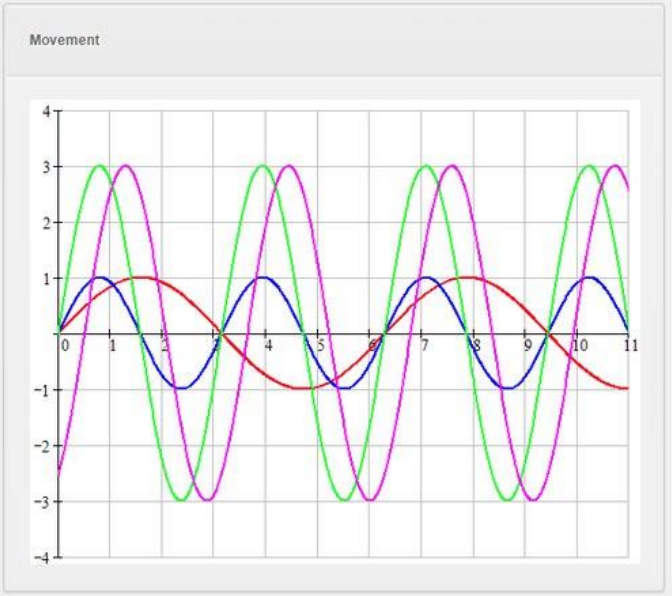

Рис. 4.7 (продовження) Інтерфейс транзакції одного користувача

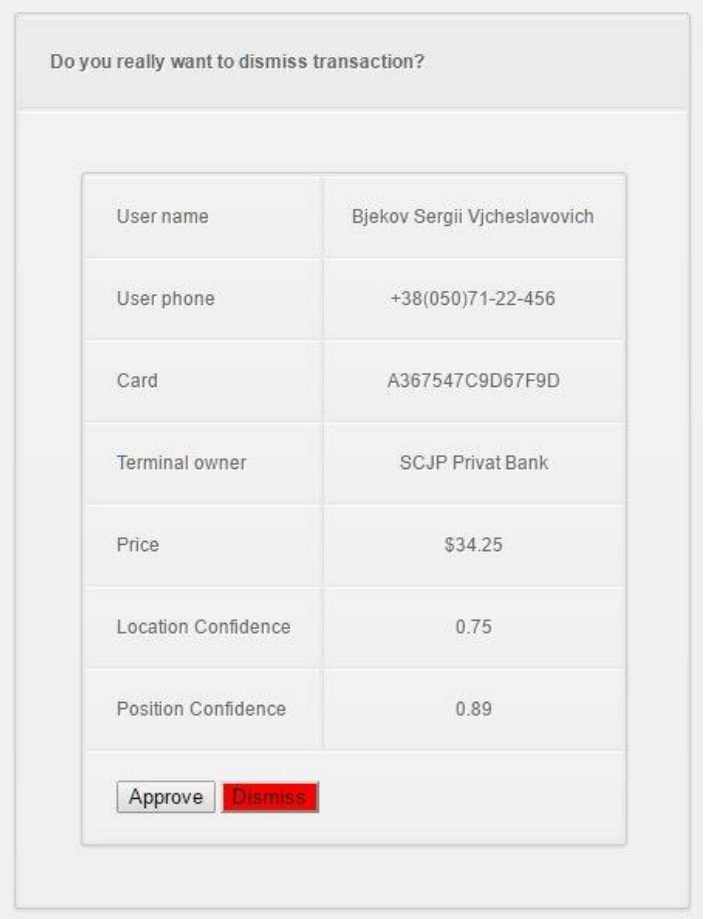

Рис. 4.8 Форма модального вікна анулювання підозрілої транзакції

Запропонована в роботі система безконтактних електронних платежів дозволяє підвищити ефективність роботи більшості сучасних Android телефонів і планшетів, оснащених NFC адаптерами, з можливістю швидкого обміну контентом і безконтактної оплати послуг.

ВИСНОВКИ

В результаті виконання атестаційної роботи досліджені критичні недоліки платіжних систем, обрана для реалізації система MasterCard Pay Pass; проаналізовані існуючі методи ідентифікації, на підставі яких виділені недоліки і поставлено завдання удосконалення методів ідентифікації безконтактних платежів. В роботі удосконалено метод ідентифікації на підставі стандартної ідентифікації, геолокації (переміщення власника пристрою за допомогою отримання даних з датчиків GPS) і біометричних даних користувача (відстеження даних з акселерометрів).

В рамках атестаційної роботи виконано аналіз організації контактної і безконтактної систем електронних платежів; аналізіснуючих систем електронних платежів;аналіз проблем систем електронних платежів; формування вимоги до розроблюваної системі безконтактних електронних платежів; дослідженняіснуючих методів, моделей і механізмів систем електронних платежів; дослідження сучасних технологій ідентифікації; дослідження методів ідентифікації систем безконтактних електронних платежів;дослідження переваг і недоліків існуючих систем безконтактних електронних платежів: Android Pay, Apple Pay, Samsung Pay, MasterCard Pay Pass; дослідження існуючих стандартів ідентифікації систем електронних платежів, методів ідентифікації систем безконтактних електронних платежів; особливості застосування безконтактної ідентифікації в системах безконтактних платежів; особливості застосування вдосконаленого методу ідентифікації; реалізація методу ідентифікації безконтактних платежів; опис і застосування методу ідентифікації безконтактних платежів;моделювання та підтримка всіх фаз процесу розробки системи безконтактних електронних платежів за допомогою UML-діаграм; практична реалізація системи - розробка рішення у вигляді серверної частини, яке буде продаватися банкам, які надають своїм клієнтам можливість безконтактної оплати.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні вказівки до організації виконання та захисту кваліфікаційної роботи ОКР «бакалавр» за напрямом 122 «Комп'ютерні науки» для студентів усіх форм навчання Упоряд.: М.В. Євланов, В.Г. Іванов, Л.М. Ребезюк, Н.В. Рябова. Харків: ХНУРЕ, 2016, 58 с.

2. Автоматизовані інформаційні технології в економіці. М.: ЮНИТИ, 2005.- 235 с.

3. Головеров Д.В., Кемрадж А.С. та ін. Правові аспекти використання Інтернет-технологій. М .: Книжковий світ, 2008.

4. Деднев М. А., Дильнов Д. В., Іванов М. А. Захист інформації в банківській справі та електронному бізнесі. - М .: ІД КУДИЦ-ОБРАЗ, 2004.- 512с.

5. http://www.e-commerce.ru/ - Інтернет-ресурси інформаційно-консалтингового центру з електронного бізнесу (дата звернення 15.11.2019).

6. http://www.e-management.ru/ - консультаційний центр розвитку електронного бізнесу (дата звернення 16.11.2019)..

7. MCBP Use Cases v1.0.2-2015. MasterCard Cloud-Based Payments Use Cases Description. MasterCard Digital Enablemet Service, 2015. - 50 с.

8. MCBP API Specification v1.0.4-2015. MasterCard Cloud-Based Payments API Specification. M .: MasterCard Digital Enablemet Service, 2015. - 642 с.

9. MasterCard Cloud-Based Payments - Credentials Management System Functional Description v1.0.0-2015. MasterCard Cloud-Based Payments Credential Managment System Functional Description. M .: MasterCard Digital Enablemet Service, 2015. - 503 с.

10. MasterCard Cloud-Based Payments - Product Description v1.0.0.-2015. MasterCard Cloud-Based Payments Product Description. M.: MasterCard Digital Enablemet Service, 2015. - 103 с.

11. Transaction Management System Functional Description v1.0.0.-2015. MasterCard Cloud-Based Payments Transaction Management System Specification. M .: MasterCard Digital Enablemet Service, 2015. - 486 с.

12. Issuer Cryptographic Algorithms v1.1.0-2015. MasterCard Cloud-Based Payments Issuer Cryptographic Algorithms Specification. M.: MasterCard Digital Enablemet Service, 2015. - 246 с.

13. ISO / IEC_14443-2011.Contactless integrated circuit cards. M.: ISO / IEC, 2011. - 60 с.

14. ISO / IEC_15693-2010. Vicinity cards: Physical characteristics. M.: ISO / IEC, 2010. - 137 с.

15. ISO / IEC_18000-2008. Radio frequency identification for item management. M .: ISO / IEC, 2008. - 312 с.

16. ISO / IEC_7816-2016. Cryptographic information application. ISO / IEC, 2016. - 312 с.

17. Граді Буч, Джеймс Рамбо, Івар Якобсон UML. Класика CS. Видання друге. - СПб .: Пітер, 2006. - 736 с.

18. Джеймс Рамбо, Айвар Якобсон, Греді Буч UML. Спеціальний довідник. - СПб .: Пітер, 2002. - 656 с.

19. Мартін Фаулер UML. Основи. Короткий посібник з стандартному мови об'єктного моделювання. - СПб .: Символ-Плюс, 2006. - 192 с.

20. Граді Буч, Джеймс Рамбо, Івар Якобсон Мова UML. Керівництво користувача. - М .: ДМК Пресс, 2007. - 496 с.

21. Крег Ларман Застосування UML 2.0 і шаблонів проектування. Введення в об'єктно-орієнтований аналіз, проектування і ітеративну розробку. - М .: Вільямс, 2012. - 736 с.

22. Джим Арло, Айла Нейштадт UML 2 і Уніфікований процес. Практичний об'єктно-орієнтований аналіз і проектування. - СПб .: Символ-Плюс, 2007. - 624 с.

23. Леоненков А.В. Об'єктно-орієнтований аналіз та проектування з використанням UML і IBM Rational Rose. - М .: Біном. Лабораторія знань, 2006. - 320 с.

24. Пол Кіммел UML. Основи візуального аналізу і проектування. М .: НТ Пресс, 2008. - 272 с.