Вінницький національний технічний університет
Факультет інтелектуальних інформаційних технологій та автоматизації
Кафедра комп'ютерних наук

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Інформаційна технологія автентифікації клієнтів в режимі реального часу»

Виконав: студент 2-го курсу, групи КН-21м
Спеціальності 122 – «Комп`ютерні науки»
Магльона В. В.
(прізвище та ініціали)

Керівник: професор кафедри комп'ютерних науки
Савчук Т. О. (прізвище та ініціали)
«15» 12 2022 р.

Опонент: к.т.н., професор. каф. АІІТ
Паламарчук Є. А.
(прізвище та ініціали)
«15» 12 2022 р.

Допущено до захисту
Завідувач кафедри КН
д.т.н., проф. Яровий А.А.
(прізвище та ініціали)
«16» 12 2022 р.

Вінниця ВНТУ - 2022 рік

Вінницький національний технічний університет
Факультет інтелектуальних інформаційних технологій та автоматизації
Кафедра комп'ютерних наук
Рівень вищої освіти II-й (магістерський)
Галузь знань – 12 "Інформаційні технології"
Спеціальність – 122 "Комп'ютерні науки"
Освітньо-професійна програма – "Системи штучного інтелекту"

ЗАТВЕРДЖУЮ
Завідувач кафедри КН
д.т.н., проф. Яровий А.А.
(підпис)
"14" 09 **2022 року**

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Магльоні Віталію Валентиновичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Інформаційна технологія автентифікації клієнтів в режимі реального часу
   керівник роботи професор кафедри комп'ютерних наук Савчук Т. О.
   затверджені наказом вищого навчального закладу від "14" 09 2022 року № 203
2. Строк подання студентом роботи 18 листопада 2022 року
3. Вихідні дані:
   мова клієнта – англійська / українська;
   кількість одночасних клієнтських дзвінків не менше 100;
   кількість голосових відбитків збережених в БД не менше 1000;
   процес від передачі вхідного голосу до збереження його голосового відбитку з базі даних не перевищує 1 хв;
   потужність бази знань не менше 10;
   мова програмування – об'єктно-орієнтована.
4. Зміст текстової частини: вступ, обгрунтування доцільності розробки інформаційної технології автентифікації клієнтів в режимі реального часу, розробка інформаційної технології автентифікації клієнтів в режимі реального часу, програмна реалізація інформаційної технології автентифікації клієнтів в режимі реального часу, економічна частина, висновки, перелік використаних джерел, додатки.
5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень).
   Аналіз сучасних інформаційних технологій автентифікації клієнта, основні етапи методу автентифікації клієнтів в режимі реального часу, структура інформаційної технології автентифікації клієнтів в режимі реального часу, схема алгоритму функціонування інформаційної технології автентифікації

забезпечення автентифікації клієнтів в режимі реального часу.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціалита посада консультанта	Підпис, дата	
		завдання видав	виконан прийня
1-3	Савчук Т. О., професор кафедри комп'ютерних наук	14.09.22	
4	[illegible]		
	[illegible]	14.09.22р	12.12.22р

7. Дата видачі завдання 14.09 2022 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи
1	Обгрунтування доцільності розробки інформаційної технології автентифікації клієнтів в режимі реального часу	01.09.2022 - 15.09.2022
2	Розробка інформаційної технології автентифікації клієнтів в режимі реального часу	16.09.2022 – 01.10.2022
3	Програмна реалізація інформаційної технології автентифікації клієнтів в режимі реального часу	01.10.2022 – 20.11.2022
4	Підготовка економічної частини	20.11.2022 - 29.11.2022
5	Апробація та/або впровадження результатів дослідження	29.11.2022 - 10.12.2022
6	Оформлення пояснювальної записки, графічного матеріалу та презентації	10.12.2022 - 16.12.2022

Студент (підпис) Магльона В. В.

Керівник роботи Савчук Т. О.

АНОТАЦІЯ

УДК 004.8

Магльона В. В. Інформаційна технологія автентифікації клієнтів в режимі реального часу. Магістерська кваліфікаційна робота зі спеціальності 122 – комп'ютерні науки, освітня програма - комп'ютерні науки. Вінниця: ВНТУ, 2022. 93 с. На укр. мові. Бібліогр.: 20 назв; рис.: 17; табл. 6

Дана магістерська кваліфікаційна робота присвячена розробці інформаційної технології автентифікації клієнтів в режимі реального часу.

Було проаналізовано сучасні підходи та інформаційні технології автентифікації клієнтів в режимі реального часу. Проаналізовані класифікатори для процесу автентифікації та обрано K - NN. Обгрунтовано вибір математичного методу MFCCs для автентифікації клієнта за голосом. Удосконалено математичну модель та метод процесу автентифікації клієнтів в режимі реального часу. Розроблено структуру інформаційної технології автентифікації клієнтів в режимі реального часу. Обгрунтовано вибір мови програмування C# та середовища Visual Studio. Розроблено алгоритм роботи та реалізовано програмне забезпечення автентифікації клієнтів в режимі реального часу. Проведено тестування та аналіз результатів роботи програмного забезпечення - швидкість процесу автентифікації збільшилась на 9%.

Результатом дослідження є розроблена інформаційна технологія автентифікації клієнтів в режимі реального часу за рахунок поєднання удосконаленої математичної моделі процесу автентифікації та введення коефіцієнта автентифікації R, який дозволяє визначити результат процесу автентифікації.

Графічна частина складається з 6 плакатів.

У економічному розділі розраховано суму витрат на розробку та виготовлення нового технічного рішення, яка складає 577025,65 гривень, спрогнозовано орієнтовану величину витрат по кожній з статей витрат, розраховано чистий прибуток, термін окупності витрат для виробника 1,29 роки та економічний ефект для споживача при використанні даної розробки.

Ключові слова: автентифікація, автентифікація в режимі реального часу, розпізнавання голосу, виявлення шахрая, буферизація звуку, порівняння голосу.

ABSTRACT

Mahlona V. V. Information technology of client authentication in real time. Master's qualification thesis on specialty 122 - computer science, educational program - computer science. Vinnytsia: VNTU, 2022. 93 p. In Ukrainian speech Bibliography: 20 titles; fig.: 17; table 6

This master's qualification thesis is devoted to the development of information technology for customer authentication in real time.

Modern approaches and information technologies of client authentication in real time were analyzed. Analyzed classifiers for the authentication process and selected K - NN. The choice of the MFCCs mathematical method for authenticating the client by voice is justified. The mathematical model and method of the client authentication process in real time have been improved. The structure of the information technology of authentication of customers in real time has been developed. The choice of the C# programming language and the Visual Studio environment is justified. The work algorithm was developed and real-time client authentication software was implemented. The software was tested and analyzed - the speed of the authentication process increased by 9%.

The result of the research is the developed information technology of client authentication in real time due to the combination of an improved mathematical model of the authentication process and the introduction of the authentication coefficient R, which allows you to determine the result of the authentication process.

The graphic part consists of 6 posters.

In the economic section, the amount of costs for the development and production of a new technical solution is calculated, which is 577,025.65 hryvnias, the estimated amount of costs for each of the cost items is predicted, the net profit is calculated, the payback period for the manufacturer is 1.29 years and the economic effect for the consumer at using this development.

Keywords: authentication, real-time authentication, voice recognition, impostor detection, audio buffering, voice comparison.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Протягом усього свого життя люди спілкувалися переважно за допомогою голосу, оскільки в ранні часи вони освоювали відповідні навички та продовжували покладатися на усне спілкування та розвивати його. Спілкування за допомогою усної мови набагато ефективніше, аніж за допомогою клавіатури та миші. Відповідно, процес автентифікації клієнта також буде ефективніший та безпечніший, якщо буде відбуватись розпізнавання голосу клієнта та порівняння його з існуючим, тобто голосовим відбитком, за яким відбувалась його реєстрація у відповідній системі.

Тема магістерської кваліфікаційної роботи є актуальною, оскільки існує потреба у процесі автентифікації клієнта державних та приватних установ, які мають велику кількість клієнтів та ймовірність атаки на їх дані збоку шахраїв з метою здійснити спробу представити себе як іншу особу для отримання доступу до конфіденційної інформації, а наявні програмні засоби є недостатньо ефективними для її розв’язування.

Зв'язок роботи з науковими програмами, планами, темами.

Магістерська робота виконана відповідно до напрямку наукових досліджень кафедри комп’ютерних наук Вінницького національного технічного університету 22 К1 «Моделі, методи, технології та пристрої інтелектуальних інформаційних систем управління, економіки, навчання та комунікацій» та плану наукової та навчально-методичної роботи кафедри.

Мета та завдання дослідження.

Метою дослідження магістерської кваліфікаційної роботи є підвищення швидкості процесу автентифікації клієнтів в режимі реального часу.

Для досягнення поставленої мети необхідно виконати такі завдання:

- провести аналіз сучасних підходів до автентифікації клієнтів в режимі реального часу;
- провести аналіз сучасних інформаційних технологій автентифікації клієнтів в режимі реального часу;
- провести аналіз класифікаторів для процесу автентифікації клієнтів в режимі реального часу;

- провести аналіз методів для автентифікації клієнтів за голосом;
- удосконалити математичну модель автентифікації клієнтів в режимі реального часу;
- удосконалити метод процесу автентифікації клієнтів в режимі реального часу згідно з метою дослідження;
- розробити структуру інформаційної технології автентифікації клієнтів в режимі реального часу;
- реалізувати інформаційну технологію автентифікації клієнтів в режимі реального часу;
- провести тестування інформаційної технології та виконати аналіз отриманих результатів.

Об'єкт дослідження – процес автентифікації клієнтів в режимі реального часу.

Предмет дослідження – програмні засоби автентифікації клієнтів в режимі реального часу.

Методи дослідження. У роботі використано такі методи наукових досліджень: метод системного аналізу для аналізу структури інформаційної технології; теорія математичних методів для реалізації інформаційної технології до автентифікації клієнтів в режимі реального часу; методи математичної статистики для розробки процесу кластеризації та обрахунків результатів експериментів над програмним засобом; методи об'єктно-орієнтованого програмування для автоматизації розрахунків.

Наукова новизна одержаних результатів полягає у такому:

- удосконалена математична модель процесу автентифікації клієнтів в режимі реального часу за рахунок введення коефіцієнта автентифікації R, який дозволяє автентифікувати клієнта з високою точністю;
- удосконалений метод процесу автентифікації клієнтів в режимі реального часу, який базується на поєднанні математичного методу MFCCs щодо голосових відбитків та класифікатора K-NN голосових відбитків, що дозволило підвищити швидкість автентифікації та не погіршити точність автентифікації клієнта.
- удосконалено інформаційну технологію автентифікації клієнтів в режимі реального часу, яка забезпечує аналіз голосових відбитків клієнта та

реалізує удосконалений метод автентифікації клієнтів в режимі реального часу, що дозволило підвищити швидкість процесу автентифікації.

Практичне значення одержаних результатів полягає у такому:

- розроблено алгоритм процесу автентифікації в режимі реального часу, що передбачає зчитування голосу даних, його конвертацію, обробку та отримання результату автентифікації;
- розроблено структуру інформаційної технології автентифікації в режимі реального часу, яка не є великою, що дозволяє швидко впроваджувати її та автентифікувати клієнтів.

Розроблені алгоритми можуть бути впроваджені в начальний процес як лекції на тему «Математичний метод MFCCs для автентифікації клієнтів в режимі реального часу» дисципліни «Нечіткі моделі і методи обчислювального інтелекту».

Достовірність теоретичних положень магістерської кваліфікаційної роботи підтверджується строгістю постановки задач, коректним застосуванням математичних методів під час доведення наукових положень, строгим виведенням аналітичних співвідношень, порівнянням результатів з відомими та збіжністю результатів математичного моделювання з результатами, що отримані під час впровадження розроблених програмних засобів.

Особистий внесок здобувача. Усі результати, наведені у магістерській кваліфікаційній роботі, отримані самостійно.

Апробація результатів роботи. Результати роботи були апробовані на міжнародних науково-практичних конференціях “LI Науково-технічна конференція факультету інтелектуальних інформаційних технологій та автоматизації (2022)”, “III Міжнародній науково-практична конференція. SCIENTIFIC PROGRESS: INNOVATIONS, ACHIEVEMENTS AND PROSPECTS, 4-6.12.2022 Мюнхен, Німеччина” [1-3].

Публікації. За результатами магістерської кваліфікаційної роботи опубліковано тези двох доповідей науково-технічної та науково-практичної конференцій [1,2], подано статтю до фахового видання [3] та отримано свідоцтво на реєстрацію авторського права на комп’ютерну програму [4].

1 ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ АВТЕНТИФІКАЦІЇ КЛІЄНТІВ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

1.1 Аналіз сучасних підходів до автентифікації клієнтів в режимі реального часу

Щороку нові сервіси зачіпають важливі функції, несанкціонований доступ до яких негативно впливає на їх безпеку. Тому завдання забезпечення безпеки цих сервісів є важливою при їх створенні. Для забезпечення безпеки інформаційних технологій використовуються різні прийоми. Часто при автентифікації клієнта використовується пара логін-пароль. Але коли потрібна підвищена безпека при вході в інформаційну технологію застосовують додаткові засоби. Одним з варіантів є розпізнавання особистості клієнта за його біометричним даним, зокрема голосу.

Завдання автентифікаці клієнта за голосом була поставлена більш ніж 40 років тому, але дослідження в цій області триває і в даний час. Останнім часом спостерігається значне підвищення якості автентифікації, проте основна проблема автоматичної автентифікації клієнта в будь-якій сфері ще далека від ідеалу. Тому актуальні як дослідження вже існуючих алгоритмів, так і пошук нових рішень в цій області.

При вході в будь-яку інформаційну технологію з розмежованими правами доступу клієнт проходить кілька етапів перевірки його спроб входу на безпеку і правомірність. Першим етапом є автентифікація – це процедура перевірки автентичності клієнта при спробі входу в інформаційну технологію. Далі починається ідентифікація – це процес призначення або пошуку відповідності індивідуального ідентифікатора (унікальної ознаки об'єкта) клієнту. У разі успішного проходження автентифікації клієнт проходить процедуру авторизації, тобто призначення клієнту прав на виконання певних дій в інформаційній технології, а також процес перевірки прав при спробі виконання цих дій.

В інформаційних технологіях використовуються такі методи автентифікації:

- однобічна автентифікація, коли клієнт інформаційної технології для доступу до інформації доводить свою автентичність;
- двобічна автентифікація, коли, крім клієнта, свою автентичність повинна підтверджувати і інформаційна технологія (наприклад, банк);
- трибічна автентифікація, коли використовується так звана нотаріальна

служба автентифікації для підтвердження достовірності кожного з партнерів в обміні інформацією.

Методи автентифікації також умовно можна поділити на однофакторні та двофакторні.

Однофакторні методи діляться на:

- логічні (паролі, ключові фрази, які вводяться з клавіатури комп'ютера чи клавіатури спеціалізованого пристрою);
- ідентифікаційні (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, тарт-карта, штрих-кодова карта тощо. Недоліками є те, що для зчитування інформації з фізичного об'єкта (носія) необхідний спеціальний рідер - носій можна загубити, випадково пошкодити, його можуть викрасти або зробити копію);
- біометричні (в їх основі – аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя. Недоліками є те, що біометричні методи дорогі і складні в обслуговуванні та чутливі до зміни параметрів носія інформації. Методт володіють низькою достовірністю та призначені тільки для автентифікації людей, а не програм або інших ресурсів).

Переваги засобів доступу за відбитком пальця - простота використання, зручність і надійність. Весь процес автентифікаці здійснюється досить швидко і не вимагає особливих зусиль від клієнтів. Вірогідність помилки при автентифікації клієнта набагато менша порівняно з іншими біометричними методами.

Метод використання геометрії руки застосовується в більш ніж 8000 організацій, включаючи Колумбійський законодавчий орган, Міжнародний Аеропорт Сан-Франциско, лікарні і імміграційні служби. Переваги автентифікаці за геометрією долоні в порівнянні з автентифікацією за відбитком пальця в надійності, хоча пристрій для прочитування відбитків долонь займає більше місця. Наприклад, пристрій Handkey сканує як внутрішню, так і бічну сторону руки.

Перевагою автентифікації за райдужною оболонкою ока є те, що зразок плям на оболонці знаходиться на поверхні ока і від клієнта не вимагається спеціальних зусиль. Відеозображення ока може бути відскановане на відстані метра, що робить можливим використання таких сканерів в банкоматах. Ідентифікуючі параметри

можуть сканuватися і кодуватися, зокрема, і у людей з ослабленим зором, але непошкодженою райдужною оболонкою.

Автентифікація за сітківкою ока відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Сканери для сітківки ока набули великого поширення в інформаційних технологіях контролю доступу, оскільки ці засоби автентифікації характеризуються низьким відсотком відмови в доступі зареєстрованим клієнтам.

Автентифікація за рисами особи (за геометрією особи) швидко розвивається в біометричній індустрії. Розвиток цього напряму пов’язаний з швидким зростанням мультимедійних відео-технологій.

Двофакторні методи автентифікації отримують в результаті комбінації двох різних однофакторних методів, частіше всього ідентифікаційного та логічного. Наприклад: «пароль + дискета», «магнітна карта + PIN».

Кожен клас методів має свої переваги і недоліки. Недоліком є незахищеність від компрометації автентифікатора.

Для забезпечення безпечної і надійної процедури входу застосовуються додаткові заходи захисту: введення багатофакторної автентифікації, застосування ідентифікаторів пов'язаних з реальним світом і за допомогою біометричних даних людини. Біометрія – це методи автоматичної автентифікації людини, на підставі її фізіологічних або поведінкових характеристик, які не схильні до змін залежних від клієнта і порівняно легко можуть бути отримані. Інші способи менш затребувані в якості факторів автентифікації, наприклад, голос, хода або почерк, але їх набагато складніше підробити потенційному зловмиснику, так як вони є процесом, а не статичним зображенням, що отже є безумовною перевагою над іншими методами.

Розвиток у людини такого складного голосового апарату призвело до придбання їм голосу – здатності людини видавати різні звуки за допомогою звукових зв'язок, які при проходженні через них повітря створюють звукові коливання. Унікальні характеристики голосу утворюються при проходженні звуку через природні резонатори: трахею, носову та ротову порожнину, гортань.

Завдяки голосу став можливим подальший розвиток мови, за допомогою якої людина отримала можливість будувати складну комунікацію з іншими людьми. Це відкрило нові можливості для передачі і зберігання інформації. Мова

використовується не тільки для обміну інформацією, але і для передачі емоційного стану, а також для визначення особистості диктору, що використовується людиною на інтуїтивному рівні і в поєднанні зі здатністю виділяти мову іншої людини серед сторонніх шумів для розпізнавання його мови дає результати, які наразі не досяжні для штучних інформаційних технологій. Але за останні 20 років в галузі розпізнавання мови людини спостерігається прогрес – спеціалізовані інформаційні технології навчилися не тільки розпізнавати хто говорить, але і що говорить. Якщо програмне забезпечення для розпізнавання мови перейшло в нішу електронних помічників і персональних секретарів, то інформаційні технології розпізнавання особи людини за голосом в сектор забезпечення безпеки доступу.

Автентифікація клієнта за голосом знаходить застосування в багатьох сферах: криміналістика і судова експертиза, антитерористичний моніторинг, безпека, застосування в системах розмежування доступу.

Розпізнавання особистості за голосом або розпізнавання диктора (англ. Speaker recognition) відрізняється від проблеми розпізнавання мови тим, що проводиться розпізнавання особистості диктора, а не його мови. Існує два підходи: текстозалежні і текстонезалежні (таб. 1.1) [5].

Таблиця 1.1 – Порівняльні характеристики підходів розпізнавання голосу (тексозалежні і текстонезалежне)

	Текстозалежне	Текстонезалежне
Особливості	Використовують фіксовані слова або речення, як на етапі верифікації, так і на етапі навчання.	Не прив'язані до визначених висловлювань і працюють з висловлюваннями будь-якої довжини.
Переваги	Інформаційні технології легше створювати, тимчасові осі ідентифікованого диктора і записаного шаблону вирівняні, а також точність такого методу вище.	Відсутність прив'язки до певних фраз-паролів.
Недоліки	Неможливість застосовувати висловлювання відрізняються від закладених в інформаційну технологію і чутливість до природних змін в мові людини, які виникають через зміни емоційного стану.	Підвищена складність розробки.

Отже, за результатами проведеного аналізу сучасних підходів до процесу автентифікації клієнтів в режимі реального часу, було обрано текстонезалежний підхід автентифікації по голосу, який буде використано в розробці інформаційної технології автентифікації клієнтів в режимі реального часу.

1.2 Аналіз сучасних інформаційних технологій автентифікації клієнта

Серед сучасних інформаційних технологій виділимо та проаналізуємо відомі.

Інформаційна технологія мультибіометричної автентифікаці AMIS (Automation Media Identification System). Застосовується в масштабних проектах державних і комерційних структур при обробці великих масивів даних про клієнтів фінансових,

транспортних, платіжних і т.д. сервісів, а також в державних системах паспортно-візових документів нового покоління. Підтримує автентифікацію за відбитками пальців, зображеннями осіб, відеоряду, голосу. Надає можливість швидкого підключення будь-яких інших біометричних автентифікаторів відповідно до вимог Міжнародної організації зі стандартизації (ISO) та Міжнародної організації цивільної авіації (ICAO).

Як масштабована інформаційна технологія мультибіометричної автентифікації BioLink AMIS реалізує наступні основні функції:

- реєстрація та обробка біометричних та інших персональних даних клієнтів;
- пошук відомостей про клієнтів за різними запитами, на основі одного або декількох біометричних ідентифікаторах та іншої інформації (ПІБ, паспортні дані, структурований словесний портрет і т. д.);
- моніторинг і аудит, управління обробкою запитів, захист інформації циркулюючої в інформаційній технології BioLink AMIS.

Модульна клієнт-серверна архітектура BioLink AMIS має високу гнучкість, що гарантує високу ефективність, продуктивність і масштабованість всієї інформаційної технології мультибіометричної автентифікації. Одночасно забезпечується можливість швидкого підключення додаткових модулів, їх інтеграція не позначається на функціонуванні інформаційної технології, не вимагає припинення її роботи або переконфігурації [6].

Основні компоненти BioLink AMIS:

- алгоритми біометричної автентифікації за відбитками пальців, обличчям, голосом, почерком, а також алгоритм комплексної мультибіометричної автентифікації , розроблений компанією BioLink;
- програмне забезпечення "проміжного" рівня (middleware) і сервіси біометричної автентифікації , що реалізують згадані алгоритми;
- сервери бізнес-логіки та програмне забезпечення клієнтських робочих місць;
- кластери серверів біометричної автентифікації та системи управління БД.

Математичний метод, який використовується в BioLink AMIS – MFCC, розпізнавання голосового відбитку відбувається за алгоритмом bushderby, його

точність близько 95 відсотків та час розпізнавання 5 секунд.

Переваги BioLink AMIS:

1. Використання методу MFCCs для процесу автентифікації клієнта за голосом (час розпізнавання голосового відбитку приблизно 5 секунд).
2. Розпізнавання голосового відбитку алгоритмом bushderby, який враховує дисперсію голосів та точніше автентифікує клієнта (точність 95 відсотків).

Недоліки BioLink AMIS:

1. Висока вартість;
2. В якості методу розпізнавання голосового відбитка використовуються нейронні мережі, що в свою чергу вимагає великих обчислювальних потужностей.

Технологія автентифікації за голосом Voice Key заснована на унікальності геометрії мовного тракту кожної людини. У Voice Key використовується спектрально-формантний метод, що базується на різних спектральних характеристиках мови різних людей. Спектрально-формантний метод заснований на аналізі поведінки трьох і більше формант, що відображають унікальність геометрії мовного тракту індивідиума.

Найбільш явно відмінність спектральних характеристик проявляється у вокалізованих відрізках мови.

Використовуваний в Voice Key спектрально-формантний метод заснований на виділенні і порівнянні положення і динаміки поведінки трьох і більше формант. Використовується кілька десятків параметрів, що характеризують формантну структуру мови [7].

Принцип роботи включає 4 основних етапи:

1. Створення шаблону – відомості про фізіологічну або поведінкову характеристику перетворюються в форму, доступну комп'ютерним технологіям, і зберігаються в пам'ять біометричної системи;
2. Виділення – з пред'явленого ідентифікатора виділяються унікальні ознаки, аналізовані інформаційною технологією;
3. Порівняння – зіставляються відомості про знову пред'явленому і раніше зареєстрованому ідентифікаторі;
4. Рішення – вноситься висновок про те, збігаються або не збігаються знову

пред'явлений і раніше зареєстрований ідентифікатор.

Технічна характеристика:

- мовно- та акценто-незалежна технологія автентифікації;
- динамічно мінлива парольна фраза;
- автентифікація за парольною фразою довжиною 3-5 секунд;
- адаптивна шумоочистка мовного сигналу;
- стійка робота в каналах зв'язку, що використовують стиснення мовного сигналу;
- (GSM, VoIP, ISDN);
- клієнт-серверна архітектура;
- механізми контролю якості та актуалізації еталонів;
- засоби адміністрування клієнтів і аудиту автентифікації;

Можливі варіанти застосування:

- автентифікація дикторів в каналах телефонного зв'язку;
- голосові паролі для доступу до інтернет-ресурсів;
- підтвердження персоналом своїх дій при проведенні важливих операцій (доступ до даних, проведення транзакцій);
- контроль фізичного доступу в приміщення;

Можливості:

- немає необхідності пам'ятати довгі секретні символьні комбінації;
- не потрібні дорогі зчитувачі біометричної інформації;
- автентифікація людини за індивідуальними біометричними ознаками, а не за виданим йому документом-картою, кодом, ключем, паролем і т. д. виключаються випадки несанкціонованих дій у разі втрати, крадіжки і передачі звичайного символьного пароля або електронного ключа;
- скорочуються витрати на обслуговування викликів і підвищення лояльності клієнтів;
- скорочення кількості «помилкових» з'єднань з оператором;
- можливість організації пріоритетних черг для VIP клієнтів;
- надання персоналізованої інформації в автоматичному режимі;
- природний і інтуїтивно зрозумілий для людини спосіб взаємодії з інформаційною технологією за допомогою голосу

Переваги Voice Key:

1. Використання методу PLP, який є найточнішим для процесу автентифікації клієнта за голосом (точність розпізнавання голосового відбитку приблизно 98 відсотків).

Недоліки Voice Key:

1. Велика вартість;
2. Використання алгоритму Витерби для розпізнавання голосу, який не враховує дисперсію голосів;
3. Володіє надлишком функцій, внаслідок чого має складне налаштування.

Інформаційна технологія VocalPassword призначена для перевірки пароля або PIN-коду і підтвердження особи абонента за голосом. Інформаційна технологія розпізнає голос, ідентифікує клієнта, отримує доступ до бази голосових відбитків і потім виявляє, чи відповідає інформація голосовому відбитку, що зберігається в базі. Цей продукт відноситься до класу інформаційних технологій автентифікації із залежністю від тексту. Фактично це двофакторна автентифікація за голосом і відомої клієнту інформації. Щоб при цьому уникнути використання записаного голосу, пароль просять ввести кілька разів, і результати не повинні повністю збігатися. У підсумку можна досягти досить високих показників за надійністю, проте клієнт повинен витратити на таку процедуру більше часу. А якщо він до того ж забув пароль або назвав його неправильно, то процедура може розтягнутися.

Переваги VocalPassword:

1. Поєднання методів MFCC та PLP, які дають гарні показники точності та швидкості (точність розпізнавання голосового відбитку приблизно 97 відсотків, час розпізнавання – 30 секунд).

Недоліки Voice Key:

1. Для проходження автентифікації клієнт має витратити 30 секунд, свого часу, що насправді є занадто довго;
2. Використання алгоритму Витерби для розпізнавання голосу, який не враховує дисперсію голосів;
3. Володіє надлишком функцій, внаслідок чого має складне налаштування.

Розглянемо більш детально характеристики, використані методи, переваги та недоліки наведених вище інформаційних технологій (таблиця 1.2) [8].

Таблиця 1.2 Порівняльна таблиця інформаційних технологій автентифікації клієнтів в режимі реального часу

Назва інф. технології	BioLink AMIS	Voice Key	VocalPassword
Витяг ознак	MFCC	PLP, voicedness	MFCC, PLP
Розпізнавання голосового відбитку	Алгоритм bushderby	Алгоритм Витерби	Алгоритм Витерби
Точність	95%	98%	97%
Час розпізнавання	5 сек	12 сек	30 сек
Переваги	Великий відсоток точності розпізнавання	Велика швидкість розпізнавання голосового відбитку	Надійна інф. технологія розпізнавання голосового відбитку
Недоліки	В якості розпізнавального алгоритму використовується нейронна мережа	Велика кількість функцій, тому важкий в налаштуванні	Мала швидкість розпізнавання голосового відбитку

Отже, за результатами проведеного аналізу сучасних інформаційних технології автентифікації клієнта можемо зазначити такий недолік як час розпізнавання голосового відбитку. Метою дослідження є збільшення швидкості процесу автентифікації, тобто час розпізнавання має бути менший за час розпізнавання існуючого аналогу – BioLink AMIS, а точність повинна залишитись як 98% (Voice Key).

1.3 Аналіз класифікаторів для процесу автентифікації клієнтів в режимі реального часу

Особливо важливу роль в процесу автентифікації клієнтів в режимі реального часу відіграють класифікатори голосового відбитку, а визначення найбільш точного

класифікатора серед існуючих - сприятиме підвищенню точності автентифікації клієнтів в режимі реального часу [9].

Серед сучасних класифікаторів слід відзначити такі:

- K-NN (K-Nearest neighbours classifier, тобто К-найближчих сусідів);
- MLP (Multilayer perceptron, тобто Багатошаровий перцептрон);
- SVM (Support vector machine, метод Опорних векторів);
- Decision tree classifier (класифікатор на основі Дерев ухвалення рішень);
- Random forest classifier (класифікатор на основі Випадкового лісу);
- AdaBoost classifier (класифікатор на основі бустінгу під назвою AdaBoost);
- Gaussian NB (Gaussian Naive Bayes classifier, тобто Наївний баєсів класифікатор)..

З метою визначення класифікатора, який доцільно використати при автентифікації клієнта, було проведено їх порівняння за точністю у 80 експериментах щодо голосового відбитку одного клієнта (зразку) для 40-ка різних клієнтів з використанням таких методів тестування [10]:

1. Парний t-критерій повторної вибірки, який передбачає врахування дисперсії голосових відбитків, так як голос клієнта частково може змінюватись в залежності від його стану здоров’я, захриплості чи дорослішання.
2. Перехресно перевірений парний t-тест, який також враховує дисперсію голосових відбитків, що й попередній, але замість того, щоб використовувати тестові голосові відбитки для кожного випробування, запускається перехресна перевірка. Це усуває проблему накладання наборів тестів, оскільки кожен зразок перевірятиметься на різних даних, що забезпечить випадки фальсифікації, коли голос клієнта може бути записаний. Даний тест був використаний декілька разів для кожного класифікатора, щоб уникнути хибних результатів класифікації голосових відбитків.
3. Перехресної перевірки 5x2, що покриває інший критерій класифікаторів – нульову гіпотезу для визначення коефіцієнту схожості матриць голосових відбитків [11].

В якості критеріїв точності для порівняння класифікаторів були взяті значення

Allow-True (кількість вірно розпізнаних голосових зразків клієнтів, тобто вірно визначених осіб) та Allow-False (кількість помилок першого роду при автентифікації, тобто невірно визначених осіб).

Результати порівняння точності класифікаторів при розпізнаванні голосових відбитків зображено на рис. 1.3.

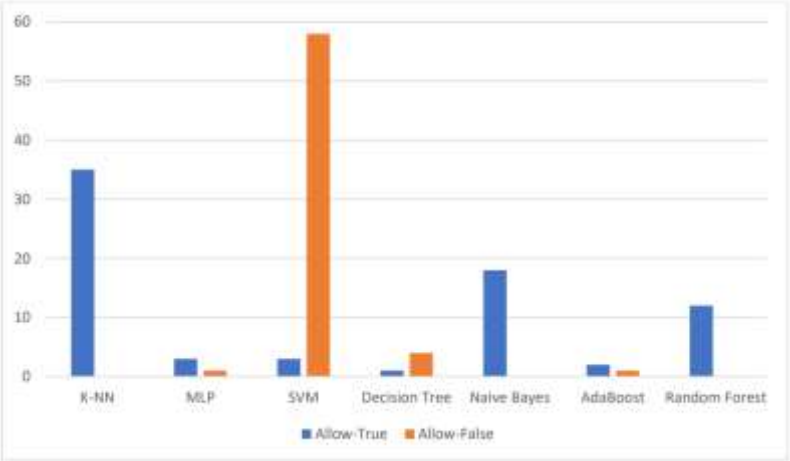


Рисунок 1.3 - Порівняння точності семи різних класифікаторів за критеріями

За результатами проведеного порівняльного аналізу найбільш точним класифікатором для процесу автентифікації клієнтів за голосом в режимі реального часу виявився K-NN (k-найближчих сусідів). За друге місце змагаються класифікатори Naive Bayes та Random Forest. Найменш точним в даному експерименті виявився класифікатор SVM (SupportVector Machine).

Отже, при автентифікації клієнта за голосовим відбитком в режимі реального часу доцільно використовувати класифікатор K-NN.

1.4 Аналіз методів для автентифікаці клієнта за голосом

Для процесу розпізнавання голосу існує два найвідомі математичні методи DTW та MFCCs. Проведемо їх аналіз та визначимо найбільш точний.

Розглянемо Dynamic Time Warping (DTW) – Динамічне викривлення часу – метод, який приймає рішення поділу звукових сигналів (тобто часових рядів) на рівні частини. Коли буде знайдено оптимальний шлях (найкоротший шлях) для кожної підпроблеми (частини голосового відбитку), буде утворено оптимальне рішення для основного процесу автентифікації [12].

DTW створює зсув у часі та відображає кожен елемент серії з найближчим

елементом іншої серії. DTW знаходить оптимальну відстань між елементами під час виконання цього відображення. Таким чином буде створено часовий зсув.

Результатом роботи методу DTW буде матриця однакової розмірності 8x8 для будь-якого записаного голосу.

Але саме через відсутність можливості конфігурувати розмірність матриці – важливої характеристики, яка використовується в алгоритмі процесу автентифікації клієнтів в режимі реального часу – погіршується точність для частини голосових відбитків. Так як нам потрібно гарантувати консистентність результатів автентифікації – цей метод не може бути частиною удосконаленого алгоритму процесу автентифікації.

Тепер розглянемо метод при отриманні голосового відбитку клієнта, який має високий рейтинг серед інформаційних технологій голосової біометрії, а саме MFCCs (Mel-Cepstral Coeficients), основні етапи якого представлено на рис. 1.4 [13].

Рисунок 1.4 – Основні етапи методу MFCCs для вилучення голосового відбитку клієнта

Відповідно до рисунку 2.2 першим етапом є неперервне мовлення клієнта, що передбачає його прийом, шляхом отримання звуку через мікрофон.

Другий етап – відцифровка, тобто трансформація безперервного сигналу на дискретний (розбиття сигналу на дискрети, простіше кажучи на «семпли») [14].

Під час третього етапу відбувається отримання цих блоків (семплів) та формування так названих “вікон” – поєднання отриманих даних та додаткової інформації – метаданих для автентифікаці вікон. У подальшому, після фінального етапу роботи алгоритму, будь-яке вікно матиме вектор мел-кепстральних коефіцієнтів.

Четвертим етапом є отримання спектру, шляхом відокремлювання будь-яких частот у діючому сигналі. Fast Fourier Transform (FFT) є основою у такому перетворенні.

П’ятий етап є найбільш важливий в методі MFCCs завдяки основній гіпотезі - мел-частотному перетворенню. Суть гіпотези полягає в тому, що частоти голосу клієнта, які отримані завдяки вищезазначеному перетворенню FFT, необхідно трансформувати у діапазон частот, що відповідає діапазону слуху людини. Іншими словами мел-діапазону, що має логарифмічне звукосприйняття людини. Вище було зазначено, що метод MFCCs необхідний для вилучення голосового відбитку клієнта під час його безперервного мовлення. У подальшому цей відбиток голосу буде представляти матрицю мел-кепстральних коефіцієнтів. Спочатку необхідно обрати якою буде кількість K коефіцієнтів, адже потрібно, щоб вона була однаковою для порівняння відбитків поточного відбитку голосу та збереженого, тобто обрати вимірність матриці, що не змінюватиметься в процесі автентифікації. Виходячи з цього, одна із характеристик методу MFCCs – кількість K мелкепстральних коефіцієнтів [15].

Шостий етап - відокремлення частот із сигналу (вилучення Кепстру), що можна подати у вигляді:

$$\mathrm{C}_n = \sum_{K=1}^{K} (\log S_K)[n(k - \frac{1}{2})\frac{\pi}{K}] \,, \qquad (1)$$

де Cn – кепстральний коефіцієнт n-го номера; Sk – k-та складова вектору голосового відбитку отриманого після мел-частотного перетворення; K – кількість мел-кепстральних коефіцієнтів (параметр MFCCs), $n \in [1, K]$ – поточна кількість мел-кепстральних коефіцієнтів [16].

На останньому етапі отримуємо відбиток голосу клієнта, що є матрицею дійсних чисел. Тобто, отримана матриця може слугувати як прототип для навчання для будь-якого класифікатора для процесу автентифікації клієнтів в режимі реального часу.

Таким чином доцільно використати саме метод MFCCs для автентифікації клієнта в режимі реального часу, який підвищить швидкість процесу автентифікації клієнтів в режимі реального часу, але також для збереження точності необхідно обрати класифікатор, який в поєднанні з методом MFCCs удосконалить процес автентифікації клієнтів в режимі реального часу.

1.5 Постановка задачі

Нехай задано вхідний вектор X(x1, x2, x3, x4), де

- x1 – мова клієнта, якою він спілкується під час розмови з агентом;
- x2 – записаний голосовий відбиток клієнта;
- x3 – список збережених голосів шахраїв в інформаційній технології;
- x4 – список існуючих голосів клієнтів в інформаційній технології;

Тоді, задачу автентифікації клієнтів в режимі реального часу можна подати у вигляді:

$$F(X) = Y,$$

де Y – вихідний вектор (результат автентифікації клієнта у вигляді “Клієнт автентифікований успішно”/”Автентифікації клієнта не виконана”).

1.6 Висновок

Отже, порівняльний аналіз існуючих методів, програмних засобів та сучасних інформаційних технологій автентифікації клієнтів дозволив виявити основні недоліки сучасних рішень, обгрунтувати вибір математичного методу для автентифікації голосу клієнта, а також сформувати задачу створення відповідної інформаційної технології.

2 РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ АВТЕНТИФІКАЦІЇ КЛІЄНТІВ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

2.1 Удосконалення математичної моделі автентифікації клієнтів в режимі реального часу

Для досягнення мети дослідження необхідно створити швидку інформаційну технологію автентифікації клієнтів в режимі реального часу. Тому доцільніше використати проаналізований та обраний метод MFCCs (Mel-Cepstral Coeficients) при отриманні голосового відбитку клієнта.

Основою методу MFCCs є мел-частотне перетворення або основна гіпотеза. Застосування методу MFCCs при автентифікації передбачає, що частоти голосу клієнта будуть трансформуватись у певний діапазон частот, що відповідає діапазону слуху людини. Метод MFCCs необхідний для вилучення голосового відбитку клієнта під час його безперервного мовлення та у подальшому цей відбиток голосу буде представлятись матрицею мел-кепстральних коефіцієнтів. Обирана кількість мелкепстральних коефіцієнтів *K*, як основна характеристика методу MFCCs, буде однаковою для коректного порівняння відбитків поточного відбитку голосу та збереженого, визначить вимірність матриці, що не змінюватиметься в процесі автентифікації. Тому, основна характеристика методу MFCCs це кількість *K* мелкепстральних коефіцієнтів.

Кожний кепстральний коефіцієнт буде визначатись формулою 1.

Як результат отримуємо відбиток голосу клієнта, що є матрицею дійсних чисел. Тому, отриманий набір може слугувати як прототип для навчання для будь-якого класифікатора.

Процес класифікації виконує функції ідентифікатора / автентифікатора та першого верифікатора.

В якості класифікатора був обраний K-NN (k – найближчих сусідів), який задовольняє поставлену мету роботи, а саме: збільшення швидкості процесу автентифікації клієнтів в режимі реального часу.

В процесі навчання алгоритм просто запам'ятовує всі вектори ознак і відповідні їм мітки класів, які виступають голосовими відбитками, сформованими математичним методом MFCCs. При роботі з голосовими відбитками обчислюється

різниця між значеннями векторів мел-кепстральних коефіцієнтів [17].

Саме використання методу MFCCs та класифікатора K-NN надає перевагу у швидкості.

Для визначення результату процесу автентифікації потрібно ввести такий термін як “коефіцієнт автентифікації” та його еталонне значення.

Коефіцієнт автентифікації буде визначатись як результат процесу автентифікації та мати значення від 0 до 1, тобто, тим це значення ближче до 1 – голосові відбитки більш схожі, та навпаки.

Еталонний коефіцієнт автентифікації – це значення з яким повинен порівнюватись отриманий коефіцієнт після процесу автентифікації та який буде визначати, що процес автентифікації пройшов успішно чи ні.

Також важливу частину в математичній моделі відіграє мова, якою спілкується клієнт, так як під кожну з них будується своя модель формування голосового відбитку. Її ідентифікатор представлений як x1 у формулі 2.

Крім порівняння створеного голосового відбитку з існуючими – проводиться порівняння зі списком голосових відбитків шахраїв, які представлені параметром x3 у формулі 2.

Сформуємо математичну модель, яка буде визначатись як сукупність результатів формування голосового відбитку методом MFCCs та коефіцієнту автентифікації клієнта класифікатором K-NN (формула 2).

$$R = \sum_{K=1}^{K} \left[\sum_{K=1}^{K} x2 * (\log S_K)[x3 * n(k - \tfrac{1}{2}) \tfrac{\pi}{K}] \right] * x1 * [N_k] * \log x4 \qquad (2)$$

де:

Sk – кепстральний коефіцієнт k-го номера (елемент вектору голосового відбитку);

Nk – коефіцієнт класифікації елементу вектора автентифікації, k ∈ [1, K];

R – коефіцієнт автентифікації клієнта в режимі реального часу, 0 < R < 1;

x1 – мова клієнта;

x2 – голосовий відбиток клієнта;

x3 – список збережених голосових відбитків шахраїв;

x4 – список голосових відбитків існуючих клієнтів.

Для визначення еталонного R_e з яким буде відбуватись порівняння коефіцієнта автернтифікації R необхідно провести тестування процесу автентифікації для різних

значень R_e. Для кожного обраного значення R_e було проведено близько 1000 різних тестових автентифікацій. Результати тестування подані в таблиці 2.2.

Таблиця 2.2 – Результати тестування значень константи А

R_e	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
Точність, %	25	40	53	69	77	82	93	99	93	82

Тому, якщо R > R_e є підстави стверджувати, що клієнт автентифікований успішно, в іншому випадку голосові відбитки дуже відрізняються та автентифікація не є успішною. Отже, за результатами проведених досліджень, найбільш точним виявились автентифікації з $R_e = 0{,}8$.

Таким чином, удосконалена математична модель процесу автентифікації клієнтів в режимі реального часу на основі математичного методу MFCCs за рахунок введення коефіцієнта автентифікації R дозволить швидко автентифікувати клієнтів, при цьому точність розпізнавання голосу не погіршиться за рахунок використання класифікатора KNN.

2.2 Удосконалений метод процесу автентифікації клієнтів в режимі реального часу

Завдяки використанню методу MFCCs та класифікатора K-NN швидкість процесу автентифікації буде збільшена, а точність порівняння голосових відбитків збережена. На рисунку 2.2 зображено схему удосконаленого методу процесу автентифікації клієнтів в режимі реального часу.

Метод процесу автентифікації клієнтів в режимі реального часу складається з таких етапів:

1. Отримання вхідних аналогових даних, тобто голосу клієнта.
2. Формування голосового відбитку з отриманих даних за допомогою математичного методу MFCCs.
3. Автентифікація клієнта за допомогою класифікатора K-NN зі збереженням точності автентифікації .
4. Виведення результату процесу автентифікації клієнта.

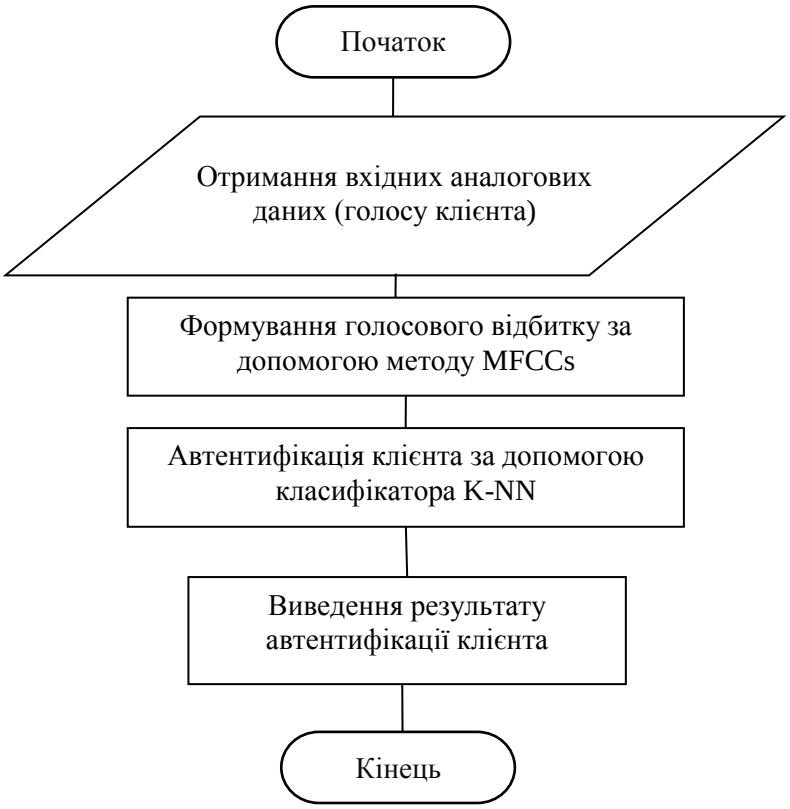


Рисунок 2.2 – Основні етапи процесу автентифікації клієнтів в режимі реального часу

Удосконалення методу автентифікації клієнтів в режимі реального часу досягається поєднанням математичного методу MFCCs щодо голосових відбитків та класифікатора K-NN голосових відбитків, що підвищило швидкість автентифікації та не погіршило точність автентифікації клієнта.

2.3 Структура інформаційної технології автентифікації клієнтів в режимі реального часу

Для реалізації удосконаленого методу автентифікації клієнтів в режимі реального часу, інформаційна технологія повинна містити такі складові: модуль збору даних, модуль обробки даних, модуль зберігання даних та модуль автентифікації (рис. 2.3).

До функцій модулю збору даних входить збір бінарних даних, перетворення їх в пакети та подступове їх надсилання в модуль обробки даних. Модуль виступає окремим сервісом, який отримує дані (голос клієнта) за протоколом TCP під час розмови агента з клієнтом. Модуль отримує ці дані, групує їх в блоки, накладає деякі метадані, наприклад, ідентифікатор блоку, для того, щоб модуль обробки даних зміг

їх відсортувати в такому ж порядку та продовжити роботу з ним, та відсилає блоки в модуль обробки даних - сервіс, який працює через HTTP протокол. Ідентифікатор блоку потрібний для того, щоб впорядкувати їх, так як сервіс відправляє їх асинхронно, не очікуючи відповіді від попереднього перед відправкою наступного, тому це потрібно для синхронізації.

Послідовність дій при функціонуванні модулю наведена на рисунку 2.3.

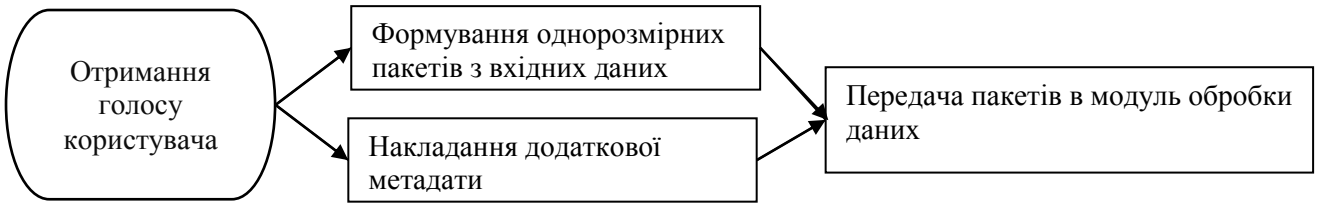


Рисунок 2.3 – Послідовність дій функціонування модулю збору даних

Модуль обробки даних відповідає за сортування отриманих пакетів, перетворення масиву пакетів, тренування заданого голосу, перетворення його в один голосовий відбиток та передача його в модуль зберігання даних. Відбиток голосу клієнта ділиться на вирази певної довжини. З кожного виразу отримується вектор мел-кепстральних коефієнтів та передається у класифікатор K-NN.

Послідовність дій функціонування модулю обробки даних зображена на рисунку 2.4.

Рисунок 2.4 – Послідовність дій функціонування модулю обробки даних

Модуль зберігання даних відповідає за зберігання голосових відбитків клієнтів

отриманих від модулю обробки даних та видачу існуючих голосових відбитків при виклику запиту від модулю прийняття рішення.Під час автентифікації запитується необхідний голосовий відбиток за допомогою ідентифікатора в модулі зберігання даних та порівнюється з голосом клієнта в режимі реального часу.

Послідовність дій функціонування модулю зберігання даних зображена на рисунку 2.5.

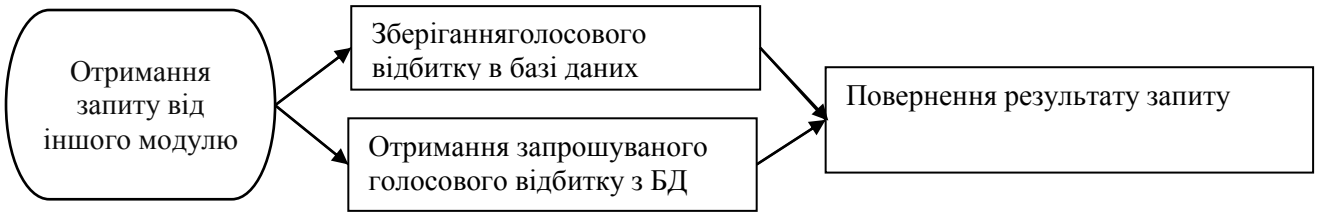


Рисунок 2.5 – Послідовність дій функціонування модулю зберігання даних

Головна мета модулю автентифікації – це порівняти існуючий голосовий відбиток, який отримано з модулю зберігання даних з голосом клієнта в режимі реального часу та сформувати певний результат на основі цього порівняння. Тобто, якщо голосові відбитки будуть мати великий відсоток схожості – клієнт автентифікувався успішно та може виконувати чи запитувати якусь конфіденційну інформацію. В іншому випадку він буде позначений як шахрай.

Модуль автентифікації має часткову ідентичність з модулем обробки даних. Схожість полягає у декількох етапів, таких як: запис голосу клієнта, поділ на вирази певної довжини і відокремлення з кожного виразу відбитку голосу клієнта. Проте відмінність модулю обробки даних полягає у використанні індивідуального ім’я об’єкта на основі голосового зразка. Інформаційна технологія співвідносить такі характеристики, як ймовірність прогнозу клієнта з найвищим шансом автентифікації до ймовірності іншої. Отже, коли ці співвідношення мають достатньо великий розрив між двома заданими характеристиками - стверджуємо, що об’єкт знаходиться у фазі автентифікації. Отже, при умові, що клієнт зареєстрований в інформаційній технології, то можна досягти повної автентифікації об’єкта та відповідно алгоритму дій, який розроблена технологія матиме застосувати до автентифікованої особи. Наприклад, це можуть бути такі дії, як відхилення чи підтвердження допуску, тощо.

Послідовність дій функціонування модулю автентифікації зображена на

рисунку 2.7.

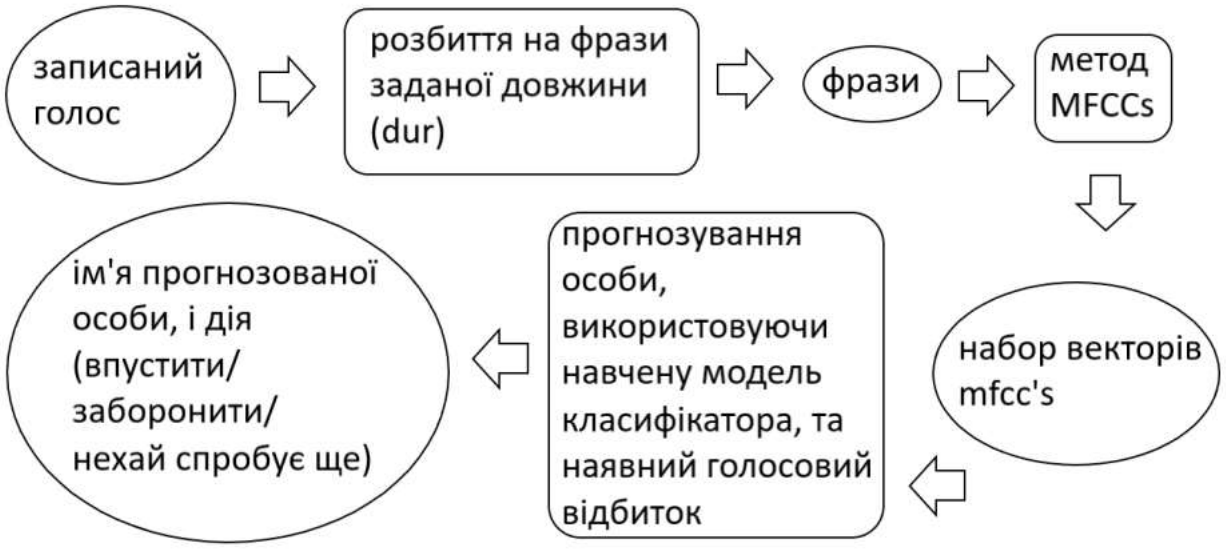


Рисунок 2.7 – Послідовність дій функціонування модулю автентифікації клієнта

Загалом процес автентифікації в інформаційній технології автентифікації клієнтів в режимі реального часу є таким: голос користувача фіксується у модулі збору даних, відбувається його конвертація, тобто перетворення в пакети, та їх відправлення в модуль обробки даних. Відбувається формування голосового відбитку методом MFCCs та тренування інформаційної технології голосовими відбитками, які передаються в модуль зберігання даних, що зберігає їх в базі голосових моделей з подальшим процесом ідентифікації. Модуль автентифікації отримує існуючий голосовий відбиток від модуля зберігання даних, порівнює його з отриманим від модулю обробки даних та приймає рішення – чи клієнт автентифікований успішно.

На рисунку 2.3 представлено структуру інформаційної технології автентифікації клієнтів в режимі реального часу.

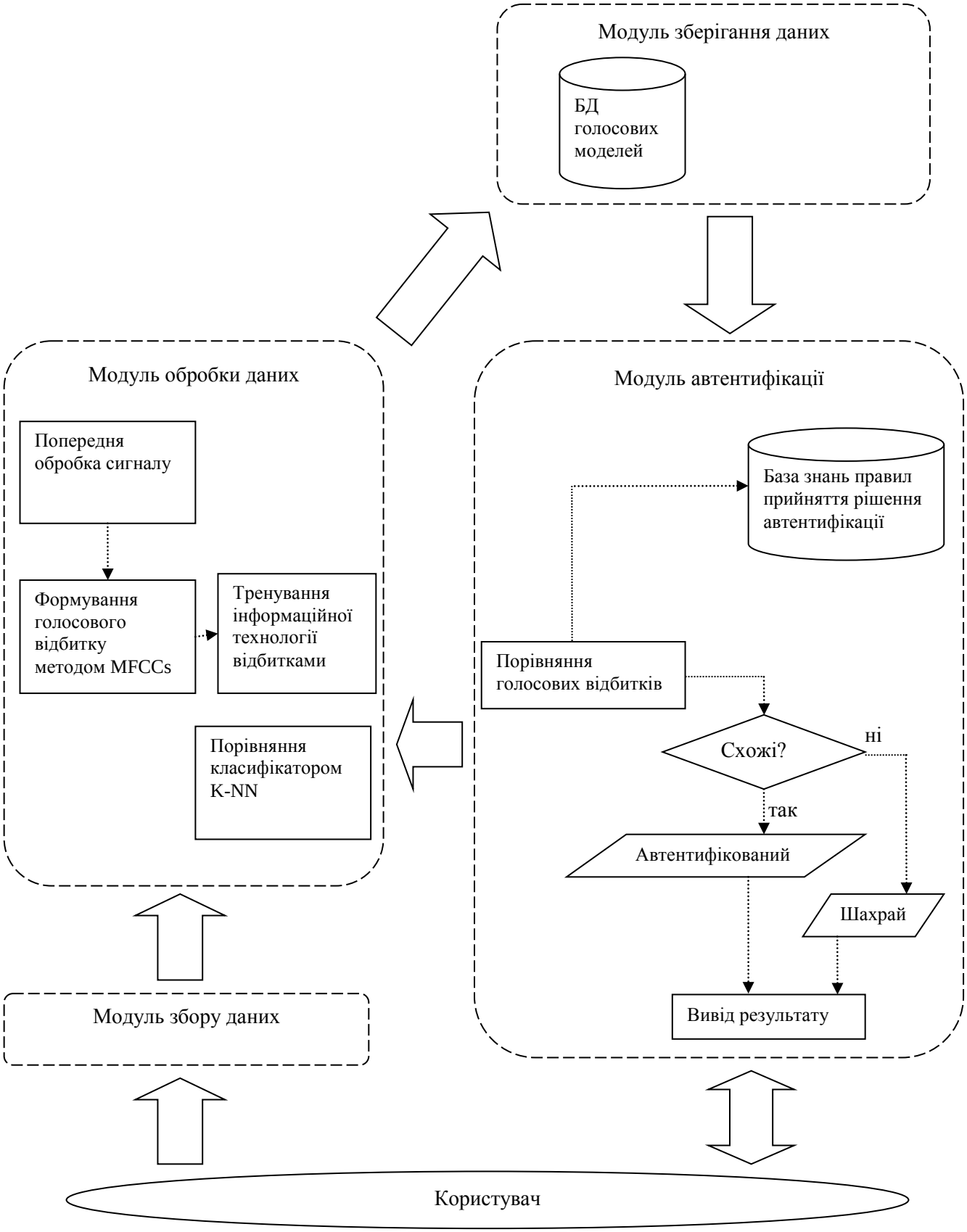


Рисунок 2.3 – Структура інформаційної технології автентифікації клієнтів в режимі реального часу

Отже, розроблена структура інформаційної технології автентифікації клієнтів в режимі реального часу, забезпечить швидкий та достатньо точний процес автентифікації.

2.4 Висновок

Отже, запропонована математична модель автентифікації клієнтів в режимі реального часу, що є основою математичного методу MFCCs, дозволить швидко автентифікувати клієнтів за рахунок введення коефіцієнту автентифікації, а використання класифікатора K-NN забезпечить високу точність процесу розпізнавання голосу. Метод процесу автентифікації клієнтів в режимі реального часу удосконалено за рахунок поєднанні математичного методу MFCCs щодо голосових відбитків та класифікатора K-NN голосових відбитків, що дозволило підвищити швидкість автентифікації та не погіршити точність автентифікації клієнта. Запропонована структура інформаційної технології автентифікації клієнтів забезпечить реалізацію удосконаленого методу процесу автентифікації клієнтів в режимі реального часу.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ АВТЕНТИФІКАЦІЇ КЛІЄНТІВ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

3.1 Обгрунтування вибору мови та середовища програмування інформаційної технології автентифікації клієнтів в режимі реального часу

Об'єктно-орієнтована мова програмування C# використовується для розробки інформаційної технології автентифікації клієнтів в режимі реального часу.

Щоб краще зрозуміти вибір цієї мови, пропонується опис найбільш популярних мов програмування.

C – це універсальний процедурний імперативний мова програмування загального призначення, розроблений в 1972 році Денисом Річі з Bell Telephone Laboratories для написання операційної системи UNIX [18].

Хоча C був розроблений для написання системного програмного забезпечення, в даний час він широко використовується для написання прикладного програмного забезпечення.

C, ймовірно, є найпопулярнішою мовою програмування в світі з точки зору кількості програмного забезпечення, яке він уже написав, коду, доступного під безкоштовними ліцензіями, і кількості програмістів, які його знають. Версії компілятора C існують для багатьох операційних систем і апаратних архітектур. C справив великий вплив на інші мови програмування, особливо C++, який спочатку був розроблений як розширення для C, а також на Java і C#, які запозичили синтаксис C [19].

Мова програмування ++ був розроблений на основі C і був отриманий в результаті додавання Бьорном Страуструпом об'єктно-орієнтованої функціональності з синтаксисом, подібним C.

Objective-C – це дуже «тонка» надбудова над C, яка дозволяє об'єктно-орієнтоване програмування з використанням гібридної парадигми динамічного / статичного типу. Основою синтаксису Objective-C був синтаксис C, проте синтаксис для його об'єктно-орієнтованих можливостей був запозичений з Smalltalk.

Мова програмування C# заснований на суворої компонентної архітектури і реалізує розширені механізми захисту коду. C# поєднує в собі кращі можливості ряду попередників. Крім згаданого раніше мови C++, необхідно вказати ще кілька

значущих для нашого часу мов програмування, а саме Java і Visual Basic. C# схожий на Java, C++ і Visual Basic, але орієнтований на компоненти. Доданий ряд нових функцій (делегати, індексатори, механізм (un) боксу і т. Д.).

C# був розроблений як мова програмування прикладного рівня для середовища CLR і тому залежить в першу чергу від можливостей самого середовища CLR. В першу чергу це відноситься до системи типів C#. Наявність або відсутність певних виразних особливостей мови диктується тим, чи може конкретна мовна функція бути переведена у відповідні конструкції CLR. Таким чином, з розвитком середовища CLR з версії 1.1 до 2.0 сам C# став значно багатшими; аналогічного взаємодії слід очікувати в майбутньому. (Однак цей шаблон буде порушений з випуском C# 3.0, який представляє собою мовні розширення, які базуються на розширеннях платформи .NET.) CLR надає C#, як і всі інші .NET-орієнтовані мови, безліч функцій, які "відсутні класичні" мови програмування ".. Наприклад, прибирання сміття не реалізована в самому C#, але виконується CLR для програм, написаних на C# так само, як це робиться для програм на VB.NET, J# і т. Д [20].

Java - мова програмування загального призначення. Відноситься до об'єктно-орієнтованим мовам програмування, до мов зі строгою типізацією. В Java реалізований механізм управління пам'яттю, який називається складальником сміття або garbage collector. Розробник створює об'єкти, а JRE за допомогою збирача сміття очищає пам'ять, коли об'єкти перестають використовуватися. Мінусом Java є відсутність інструменту для створення нативного дизайну.

Python ідеально підходить для знайомства з розробкою. Python простіше і зрозуміліше більш складних мов. Для роботи з Python пропонується велика кількість середовищ розробки. Крім цього, пропонується велика кількість бібліотек і фреймворків, які суттєво спрощують процес створення додатків. Python затребуваний на ринку. Незважаючи на зростаючу кількість програмістів, які працюють на цій мові, попит на нього теж зростає. Розробка на Python йде значно швидше, ніж на інших мовах програмування. Програми, написані за допомогою Python, вважаються одними з найбільш повільних. Дана мова програмування не підходить для тих завдань, які вимагають великого обсягу пам'яті.

В таблиці 3.1 наведено порівняння основних мов програмування.

Таблиця 3.1 — Порівняння різних мов програмування

№	Парадигми / Мови	Функціональна	Логічна	Процедурна	Об'єктно-орієнтована
1	Ada	-	-	+	+
2	C	-	-	+	-
3	C++		-	+	+
4	C#		-	+	+
5	Java	-	-	+	+
6	Haskell	+		+	-
7	Common LISP	+		+	+
8	Python		-	+	+
9	Smalltalk	+		+	+
10	Delphi		-	+	+
11	Prolog		+	-	-

Переваги мови C#:

- C # розроблявся разом з новим каркасним фреймворком Framework.Net і тому може використовуватися на усіх платформах;
- необмежені можливості успадкування та універсалізації;
- як нащадок C / C ++, він простий в освоєнні для будь-якого, знайомого з попередником, що полегшує перехід з однієї мови на іншу;
- C # помітно надійніше і простіше;
- потужна база даних каркасного фреймворка: десктопний WPF, сервісний WCF і веб MVC. А .NET 4.5;
- полегшення роботи з паралельним та асинхронним програмуванням.

Недоліки C#:

- прив'язка до MS-сервера;
- роскомпіляція до назви змінних;

– продуктивність компілятора нижча, ніж у самого C [21].

Microsoft Visual Studio - це серія продуктів Microsoft, що включає інтегровану середу розробки програмного забезпечення і ряд інших інструментів. Ці продукти дозволяють розробляти як консольні, так і графічні додатки, включаючи підтримку технології Windows Forms, а також веб-сайти, веб-додатки, веб-сервіси як у власному, так і в керованому коді для всіх платформ, підтримуваних Microsoft Windows, Windows Mobile , Windows Phone, Windows CE, .NET Framework, .NET Compact Framework і Microsoft Silverlight [22].

Visual Studio включає декілька з наступних компонентів:

– Visual Basic .NET, а до його появи — Visual Basic;
– Visual C++;
– Visual C#;
– Visual F# (входить до складу Visual Studio 2010);
– Visual Studio Debugger.

Багато варіантів постачання також включають:

– Microsoft SQL Server;
– MSDE Visual Source Safe.

У минулому, до складу Visual Studio також входили продукти:

– Visual InterDev;
– Visual J++;
– Visual J#;
– Visual FoxPro;
– Visual Source Safe – файл-серверна система управління версіями.

Істотною зміною в Microsoft Visual Studio 2017 стала підтримка багатьох цільових платформ: крім базової Windows тепер можна створювати проекти для iOS і Android. Додана підтримка фреймворку Unity для розробників комп'ютерних ігор. Оновлений механізм автентифікації: клієнт синхронізується з одним обліковим записом Microsoft при запуску Visual Studio.

Версія включає .NET Framework 4.7 і підтримку універсальної платформи Windows 10. Розробники на C++ залишилися задоволені новою функціональністю стандарту C++ 14 і навіть деякими поліпшеннями в C++ 17.

Отже, мова C# має ряд значних переваг, які перекривають її недоліки.

Використання цієї мови є доцільним для розробки інформаційної технології автентифікації клієнтів в режимі реального часу. За допомогою цієї мови програмування можна легко описати необхідно логіку та побудувати інтерфейс програми. Середовище програмування Visual Studio теж має ряд позитивних характеристик і великий функціонал, що дозволяє легко працювати над обраним проектом, тому воно буде використано під час розробки програмного забезпечення автентифікації клієнтів в режимі реального часу.

3.2 Розробка алгоритму роботи програмного забезпечення автентифікації клієнтів в режимі реального часу

При проектуванні програмного забезпечення автентифікації клієнтів в режимі реального часу було прийнято рішення використати метод мел-частотних кепстральных коефіцієнтів (MFCC) для отримання значущих ознак у аудіоданих клієнтів і алгоритм класифікації даних на основі моделей k-найближчих (KNN), так як MFCC порівняно з іншими методами володіє хорошим співвідношенням швидкості роботи до продуктивності, а KNN добре себе зарекомендував у задачі класифікації даних, які виділені із звукових висловлювань відрізняються не тільки варіаціями у вимові фрази, але і самими фразами. Іншими словами, даний програмний продукт є текстонезалежною підсистемою розпізнавання особистості клієнта. Нижче описується її робота. На схемі алгоритму (рисунок 3.2) зображено роботу інформаційної технології автентифікації клієнтів в режимі реального часу.

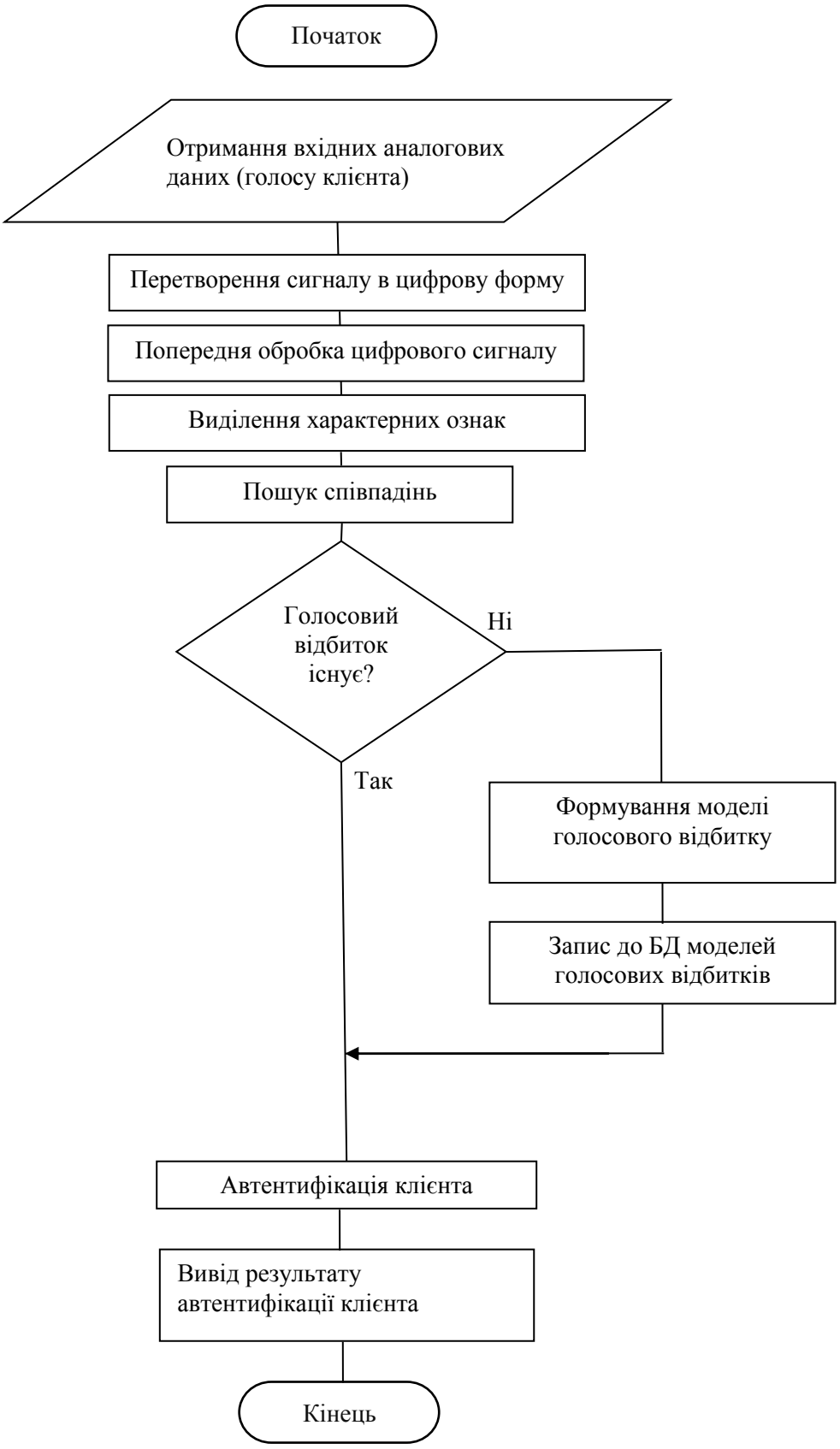


Рисунок 3.2 – Схема алгоритму функціонування інформаційної технології автентифікації клієнтів в режимі реального часу

Відповідно до схеми алгоритму (рисунок 3.2) спочатку на вхід подається аналоговий мовний сигнал, який в ході перетворень перетворюється в оброблений

цифровий сигнал. Після чого відбувається перевірка на співпадіння записаного голосу вже з існуючими голосами в БД, та в разі його наявності в базі даних відбувається автентифікація клієнта та виведення результату автентифікації. Якщо ж співпадінь не знайдено, то формується модель голосового відбитку та записується до БД задля проходження автентифікації в майбутньому.

Також розглянемо функціональну схему розроблювальної інформаційної технології автентифікації клієнтів в режимі реального часу (рисунок 3.3).

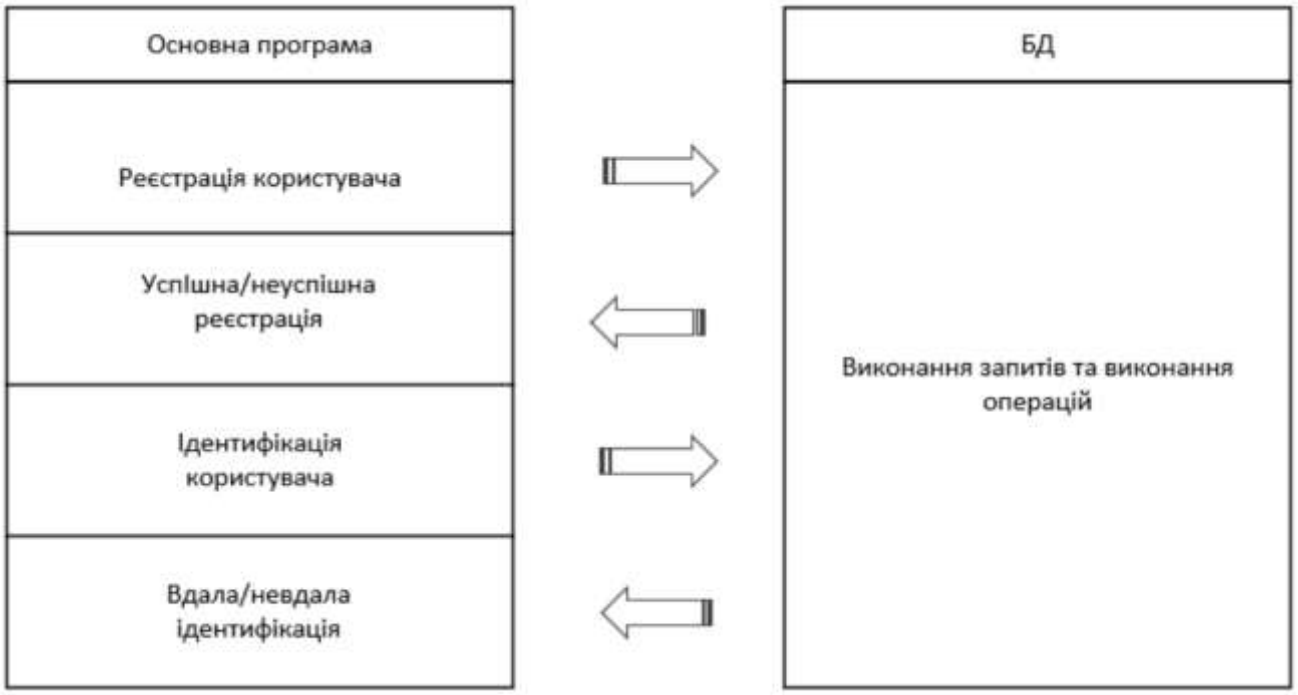


Рисунок 3.3 – Функціональна схема інформаційної технології автентифікації клієнтів в режимі реального часу

На функціональній схемі зображені всі виклики до бази даних. Під час реєстрації нам потрібно зберегти голосовий відбиток та отримати відповідь про успішну/неуспішну реєстрацію. Також для автентифікації клієнта нам потрібно отримати існуючий голосовий відбиток та отримати відповідь – вдала/невдала автентифікація.

Отже, запропонований алгоритм забезпечить збільшення швидкості процесу автентифікації клієнтів в режимі реального часу.

3.3 Програмна реалізація інформаційної технології автентифікації клієнтів в режимі реального часу

Структура інформаційної технологія автентифікації клієнтів в режимі реального часу базується на таких основних модулях: модуль збору даних, модуль обробки даних, модуль зберігання даних та модуль автентифікації, які описані в попередньому розділу. Опишемо їх з точки зору програмної реалізації.

Для кожного модулю буде створений окремий проект та програмний код буде написаний на мові програмування C#. Для розробки буде використовуватись середовище Visual Studio.

Модуль, який відповідає за збір даних, містить таку сукупність класів:

- InputBuffer;
- InputData;
- InputHandler;
- InputConvertor;
- PacketData;
- UserData.

Клас InputBuffer тримає в собі буферизовані вхідні дані клієнта, тобто його голос в бінарному вигляді без додаткової інформації.

Клас InputHandler відповідає за перетворення бінарних даних в пакети, тобто конвертацію об’єктів класу InputBuffer в PacketData. Для конвертації він використовує методи класу InputConvertor. Дані розбивається на блоки визначеного розміру з додатковими метаданими та поміщуються в об’єкти класу PacketData.

Клас InputHandler є окремим сервісом з описаними контрактами та методами, які отримують вхідні дані клієнта (його голос та ідентифікатор) за протоколом TCP та формують об’єкти InputBuffer. Клас містить також унікальний ідентифікатор для того, щоб при передачі блоків в модуль обробки, вони могли бути відсортовані, так як сервіс відправляє їх асинхронно, не очікуючи відповіді від попереднього перед відправкою наступного, тому це потрібно для синхронізації. Після їх збору модуль групує їх, накладає певну додаткову інформацію, включаючи UserData для присвоєння певного унікального значення клієнта, щоб модуль обробки даних зміг їх присвоїти певного клієнту, зареєстрованому в інформаційній технології, та передає в

модуль обробки через протокол HTTP.

Під час будь-якого дзвінку клієнта до інформаційної технології відбувається також його ідентифікацію, тобто приходить ще запит з інформацією, яку представив цей клієнт, для її зв’язку з даними (голосом), які збираються в режимі реального часу.

Модуль обробки даних, який містить в собі основні алгоритми та методи для процесу автентифікації (математичний метод MFCCs та класифікатор K-NN) реалізовує такі класи:

– MFCCsHandler;
– KNNHandler;
– Voiceprint;
– Phrase;
– RecognitionManager;
– RecognitionResult;
– InputService.

Робота модулю починається з класу InputService, який отримує дані з модулю збору даних у вигляді об’єктів PacketData. Далі відбувається їх сортування по отриманих ідентифікаторам та виклик методів класу RecognitionManager, який займається процесом розпізнавання голосу клієнта. Він містить методи SplitOnPhrases, ExecuteMFCCs, TrainClassificator.

Метод SplitOnPhrases відповідає за розбиття на окремі фрази записаних даних результатом якого виступають об’єкти класу Phrase. Далі викликається метод ExecuteMFCCs в якому інкапсульований алгоритм математичного методу MFCCs, результатом якого є набір векторів кепстральних коефіцієнт, тобто повертається двомірний масив з об’єктами класу RecognitionResult. Наступним етапом роботи модулю є виклик методу Execute MFCCs, який забезпечує тренування заданим класифікатором KNN. Використання при цьому KNNHandler класа є необхідним. Відбиток голосу клієнта ділить на відразки певнох довжини.

Отриманий голосовий відбиток, який виступає об’єктом класу Voiceprint повинен бути збережений в базі даних, відповідно кінцевим етапом роботи модулю є передача голосових відбитків в модуль зберігання даних, по протоколу HTTP.

Модуль зберігання даних використовує такі класи:

– VoiceprintData;

– CustomerData.

Модуль приймає голосовий відбиток від модулю обробки даних, перетворює його в простішу структуру VoiceprintData без надлишкової інформації та зберігає в базі даних MS SQL.

Клас CustomerData виступає в якості ідентифікатора клієнта та містить всю інформацію про нього та ідентифікатори голосових відбитків для нього.

Модуль також виконує запити на отримання даних при виклику відповідних методів його сервісу (GetVoiceprint. GetCustomerInformation), які викликаються модулем автентифікації.

Модуль автентифікації, який є ядром інформаційної технології та працює з іншими модулями містить такі класи:

– AuthenticationResult;
– VoiceprintDTO;
– VoiceprintComparer;
– Utilities;
– VoiceprintDB;

Модуль автентифікації частково містить аналогічні етапи модулю обробки такі як: запис голосу клієнта та його поділ на фрази, але відмінний в тому, що використовує створену модуль, яка генерує індивідуальний ідентифікатор об’єкта на основі голосового відбитку.

Клас Utilities саме займається цими схожими етапами та використовує аналогічні класи до методу обробки даних.

Клас VoiceprintDB займається відправкою запитів до бази даних та отримання існуючого голосового відбитку VoiceprintDTO по певному переданому ідентифікатору CustomerData.

Основна логіка порівняння голосових відбитків знаходиться в класі VoiceprintComparer, який визначає коефіцієнт автентифікації R та порівнює його з еталонним Re, яке було визначено в попередньому розділі як 0.8.

Результатом роботи методу Compare класу VoiceprintComparer буде об’єкт класу AuthenticationResult, який містить в собі отриманий коефіцієнт автентифікації R та результат у вигляді таких значень як “Успішно автентифікований” та “Шахрай”.

Отже, запропонована реалізація інформаційної технології базується на таких

сучасних технологіях як: мова програмування C# та середовище розробки Visual Studio, які в поєднання надають можливість реалізації розробленої інформаційної технології. Програмна реалізації інформаційної технології автентифікації клієнтів в режимі реального часу виконує всі поставлені задачі та коректно працює. Голос клієнту записується, формується голосовий відбиток, який зберігається в базі даних, порівняння голосових відбитків відбувається точно та процес автентифікації швидкий та зрозумілий для кінцевого користувача.

3.4 Тестування та аналіз результатів роботи інформаційної технології

Перед аналізом результатів роботи програмного забезпечення автентифікації клієнтів в режимі реального часу та перевірки чи виконана поставлена мета: підвищення швидкості та збереження точності автентифікації клієнтів в режимі реального часу, розглянемо та протестуємо основний функціонал роботи програми.

З метою дослідження коректності функціонування інформаційної технології було виконано такі кроки:

1. Ідентифікація агента за логіном та паролем, яка виконується з метою отримання конкретного ідентифікатора агента, по якому можливо буде дізнатись з яким саме агентом спілкувався конкретний клієнт.
2. Отримання вхідного дзвінку від клієнта на номер телефону Cisco, який прив’язаний до інформаційної системи.
3. Відображення інформації про вхідний дзвінок та вікна з полем для введення певного ідентифікатора клієнта по якому можливо буде отримувати існуючі голосові відбитки в системі та здійснювати процес ідентифікації (порівнювати їх з отриманим голосовим відбитком).
4. Після введення ідентифікатора клієнта з’являється ще одне вікно, для підтвердження того, що клієнт не проти використання його даних, тобто записаного голосу. Якщо клієнт погоджується – інформаційна технологія почне процес автентифікації, інакше – процес автентифікації буде відбуватись в ручному режимі без розпізнавання голосу та порівняння з існуючими в режимі реального часу.

5. Процес автентифікації займає приблизно 3 хвилини після якого буде відображено вікно про результат автентифікації:
    a. Клієнт автентифікований успішно, тобто сформований голосовий відбиток в режимі реального часу має схожість з існуючим в інформаційній технології;
    b. Автентифікації клієнта не пройшла успішно – сформований голосовий відбиток в режимі реального часу не схожий до існуючого в інформаційній технології;
    c. Особа, яка проходила процес автентифікації виявилась шахраєм, тобто сформований голосовий відбиток в режимі реального часу має схожість з існуючими голосовими відбитками шахраїв збережених в інформаційній технології;
6. Також при виникненні будь-якої помилки з’єднання інформаційної технології з використовуваними системами – з’являється відповідне вікно з повідомленням. Для вирішення потрібно перевірити та налаштувати з’єднання між модулями та продовжити процес автентифікації.

Інформаційна технологія встановлена, запускаємо її та вводимо дані менеджера, який буде приймати дзвінки (рисунок 3.4).

Рисунок 3.4 – Вікно введення даних менеджера

Після цього інформаційна технологія очікує вхідні дзвінки, тобто коли певний клієнт зателефонує на номер, який прив’язаний до інформаційної технології – з’явився повідомлення про новий дзвінок. Зробимо тестовий дзвінок за допомогою Cisco телефону (рисунок 3.5). Для цього потрібно інсталювати та запустити Cisco Communication додаток, ввести відповідний номер телефону, який зареєстрований в інформаційній системі, як певний агент, та здійснити дзвінок.

Рисунок 3.5 – Дзвінок за допомогою Cisco телефону

У спливаючому вікні інформаційної технології зможемо побачити те, що дзвінок почався та потрібно ідентифікувати клієнта (рисунок 3.6), тобто ввести ідентифікатор, який називає клієнт на дзвінку, для подальшого проведення процесу автентифікації цього клієнта.

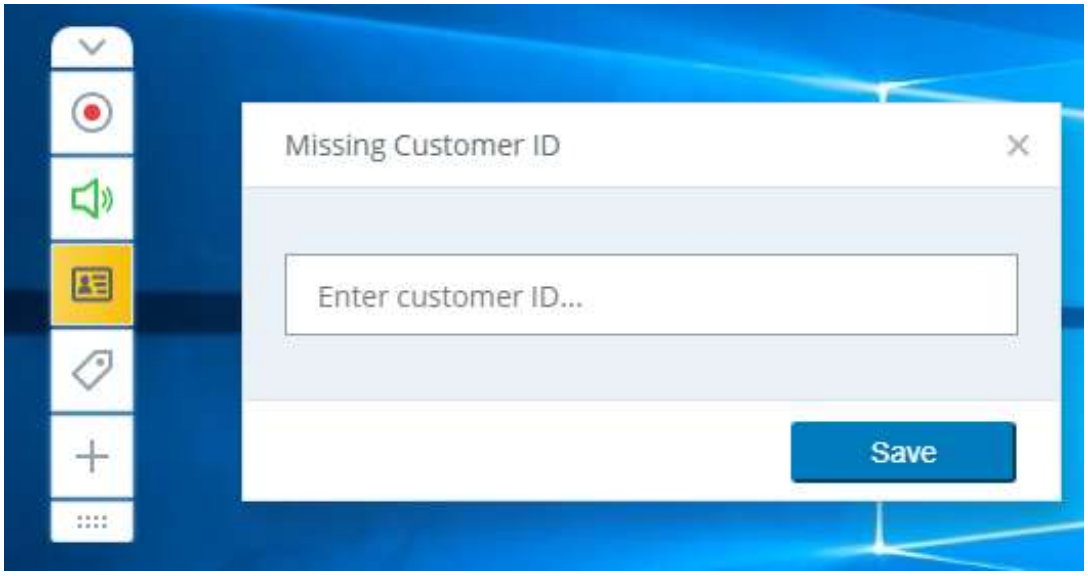


Рисунок 3.6 – Вікно вводу даних для ідентифікації клієнта

Після введення ідентифікатора клієнта потрібно також підтвердити те, що клієнт не забороняє записувати та використовувати його голос для подальших процесів автентифікації. Вікно погодження зображено на рисунку 3.7.

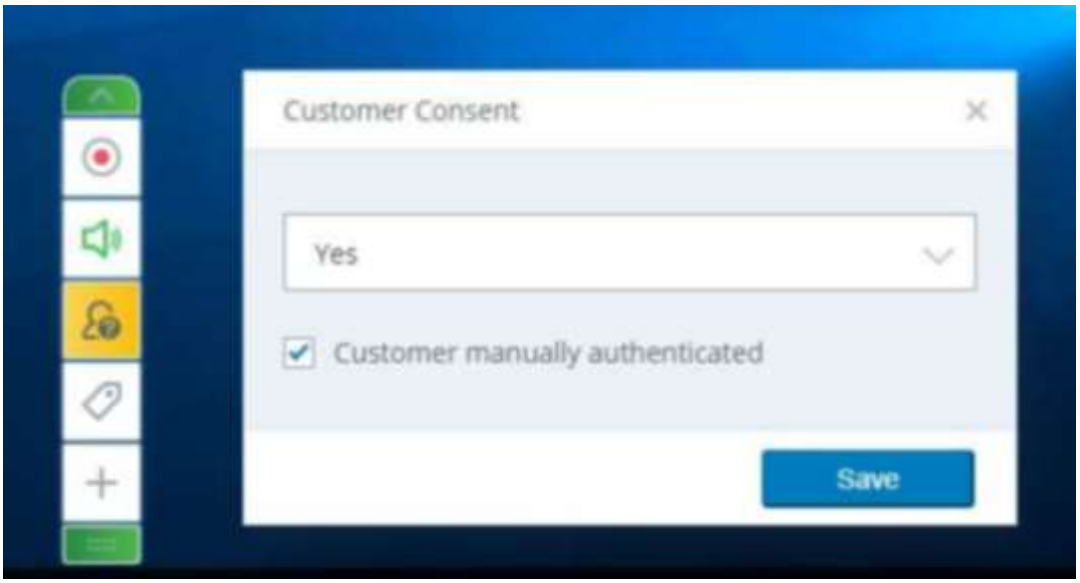


Рисунок 3.7 – Вікно погодження клієнта на процес автентифікації

Якщо введений ідентифікатор клієнта вже є в інформаційній технології, тобто клієнт вже був раніше зареєстрований та містить голосовий відбиткок – інформаційна технологія почне процес автентифікації (рисунок 3.8).

Рисунок 3.8 – Процес автентифікації клієнта

Якщо клієнт буде автентифікований успішно – з’явиться відповідне повідомлення (рисунок 3.9).

Рисунок 3.9 – Клієнт автентифікований успішно

Якщо клієнта не вдасться автентифікувати, тобто його голос не буде відповідати дійсності – буде відображено відповідне повідомлення (рисунок 3.10).

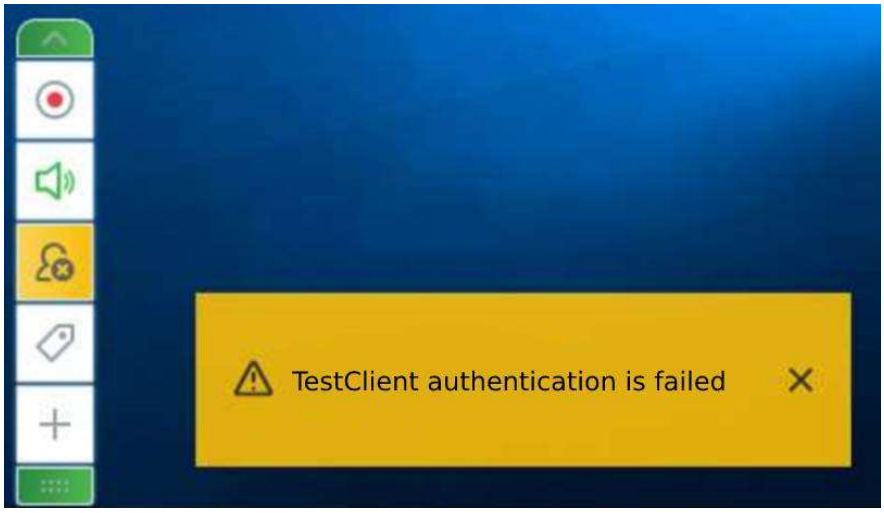


Рисунок 3.10 – Клієнт не зміг автентифікуватись коректно

Якщо клієнт виявиться шахраєм, тобто сформований голосовий відбиток буде порівняно з існуючими голосовими відбитками шахраїв та виявлено схожість – буде відображено відповідне повідомлення (рисунок 3.11).

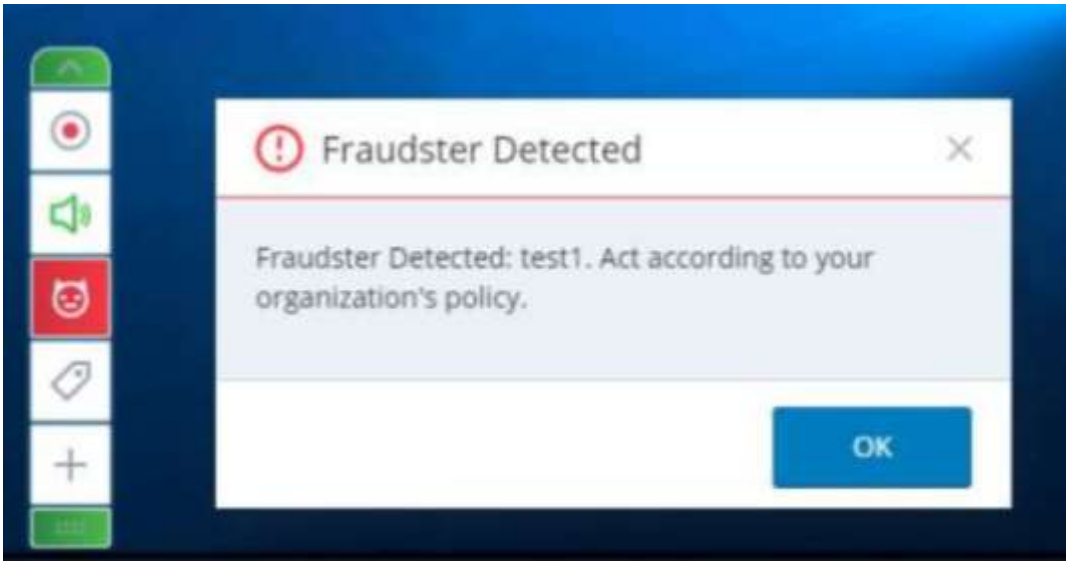


Рисунок 3.11 – Клієнт виявився шахраєм

Також інформаційна технологія здатна відображувати будь-які проблеми зі сторони її підключення до системи певної фінансової установи, тобто додатку, який взаємодіє з інформаційною технологією (рисунок 3.12).

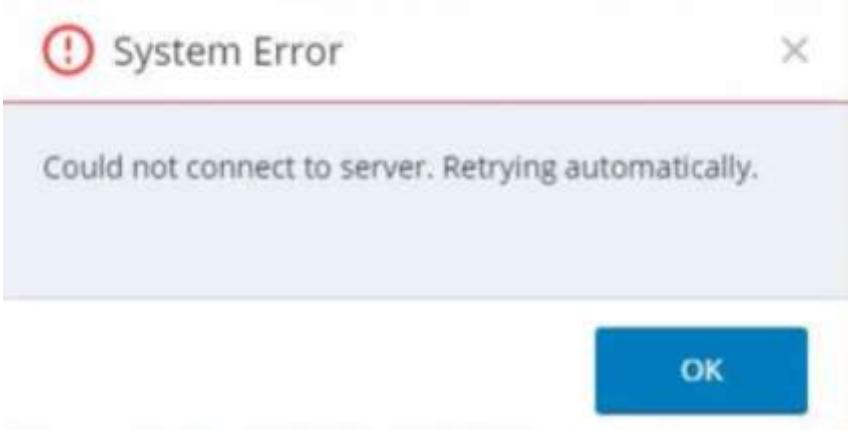


Рисунок 3.12 – Помилка з’єднання з сервером

Отже, програма працює коректно та задовільняє поставлені задачі.

З метою перевірки досягнення мети дослідження було проведено низку експериментів, що виконувались запропонованою інформаційною технологію та аналогами (VocalPassword, Voice Key, AMIS Biolink).

Експериментальні дослідження зводились до використання тестового симулятора дзвінків з метою сформувати потужну базу вибірки аби генерувати голосові відбитки.

Після проведення тестування (1000 тестових дзвінків тривалістю в 2 хвилини) визначимо середній час автентифікації клієнта та точність автентифікації голосового відбитку клієнта. Приклад роботи тестового симулятору з часом виконання наведено на рисунку 3.12. На таблиці 3.4 наведені та оцінено час, що витрачається на цей процес часові результати в середньому (вибірка – 1000 тестових дзвінків тривалістю 2 хвилини).

Таблиця 3.4 – Результати аналізу швидкості при автентифікації клієнтів в режимі реального часу з використанням запропонованої інформаційної технології та її аналогів

	VocalPassword (Nuance)	Voice Key	AMIS (Biolink)	Інформаційна технологія автентифікації клієнтів в режимі реального часу
t, мс	15 602	19 927	14 602	13 235

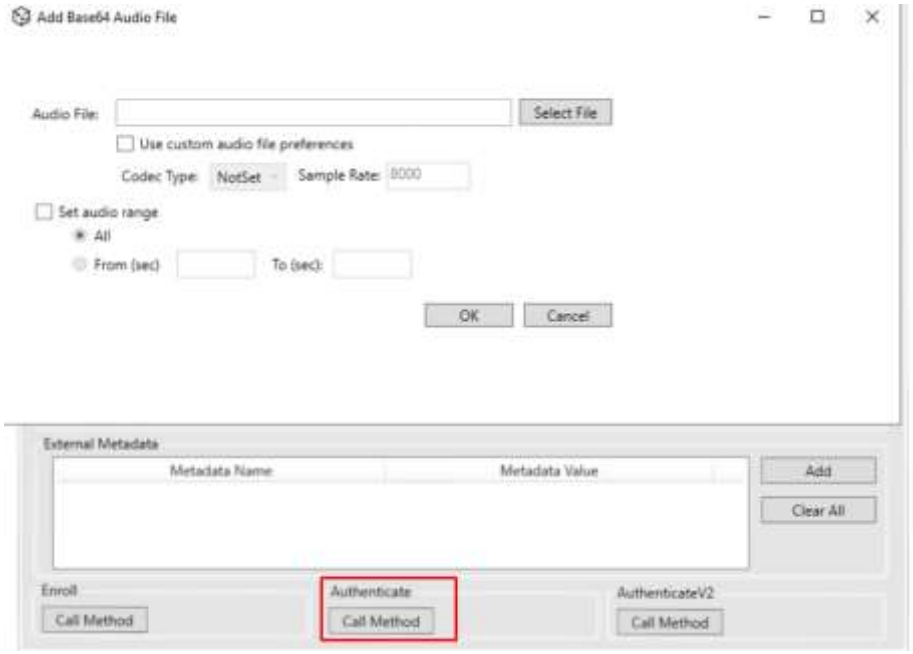


Рисунок 3.12 – Тестовий симулятор дзвінків

Сутність кожного експерименту полягала у обрані 10 різних записаних голосів тривалістю в 2 хвилини та проведенні процесу автентифікації для кожного з понад 100 разів.

Отже, як показали дослідження, швидкість процесу автентифікації клієнтів підвищиться, в середньому, не менш як на 9 відсотків.

Для аналізу точності було взято за результат відсоткове відношення кількості точної автентифікації (збережений голосовий відбиток та новоутворенний – голос однієї людини) до загальної кількості тестових дзвінків в процесі автентифікації.

Результати роботи інформаційної технології автентифікації клієнтів в режимі реального часу та її аналогів наведені в таблиці 3.5.

Таблиця 3.5 – Результати аналізу точності при автентифікації клієнтів в режимі реального часу з використанням запропонованої інформаційної технології автентифікації та її аналогів

	VocalPassword (Nuance)	Voice Key	AMIS (Biolink)	Інформаційна технологія автентифікації клієнтів в режимі реального часу
Точність, %	97	98	95	99

За результатами проведених досліджень, проведене тестування удосконаленої інформаційної технології автентифікації клієнтів в режимі реального часу на основі математичного методу MFCCs та класифікатора KNN забезпечує аналіз голосових відбитків клієнта та реалізує удосконалений метод автентифікації клієнтів в режимі реального часу, що дозволило підвищити швидкість процесу автентифікації, в середньому, не менш як на 9 відсотків та не погіршити точність порівняння голосових відбитків.

3.5 Висновок

У ході виконання третього розділу було розроблено структуру та алгоритм роботи програмного забезпечення автентифікації клієнтів в режимі реального часу, проаналізовано мови програмування та обрано C# з відповідним середовищем програмування – Visual Studio 2017. Розроблено основні програмні модулі інформаційної технології: модуль збору даних, модуль обробки даних, модуль зберігання даних та модуль автентифікації. Для кожного модулю побудовано алгоритм та описаного покроково функціонал його роботи. Проведено тестування та аналіз результатів роботи програмного забезпечення для автентифікації клієнтів в режимі реального часу, яке показало, що інформаційна технологія автентифікації клієнтів в режимі реального часу задовільняє поставлену мету та процес автенттифікації клієнтів відбувається швидше за існуючі аналоги, а точність порівняння голосових відбитків не погіршилась.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність результатів виконаної роботи.

Магістерська кваліфікаційна робота «Інформаційна технологія автентифікації клієнтів в режимі реального часу» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок (або рішення про виведення науково-технічної розробки на ринок може бути прийнято у процесі проведення самої роботи), тобто коли відбувається так звана комерціалізація науково-технічної розробки. Цей напрямок є пріоритетним, оскільки результатами розробки можуть користуватися інші споживачі, отримуючи при цьому певний економічний ефект. Але для цього потрібно знайти потенційного інвестора, який би взявся за реалізацію цього проекту і переконати його в економічній доцільності такого кроку.

Для наведеного випадку нами мають бути виконані такі етапи робіт:

1. проведено комерційний аудит науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;
2. розраховано витрати на здійснення науково-технічної розробки;
3. розрахована економічна ефективність науково-технічної розробки у випадку її впровадження і комерціалізації потенційним інвестором і проведено обґрунтування економічної доцільності комерціалізації потенційним інвестором.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Інформаційна технологія автентифікації клієнтів в режимі реального часу» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за

12-ма критеріями, наведеними в табл. 4.1 [24].

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою

7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкуренті в немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін	Термін реалізації ідеї від 3-х до 5-ти років. Термін	Термін реалізації ідеї менше 3-х років. Термін окупності	Термін реалізації ідеї менше 3-х років. Термін окупності

1 2	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	5	5	5
2. Ринкові переваги (наявність аналогів)	3	3	3
3. Ринкові переваги (ціна продукту)	4	4	4
4. Ринкові переваги (технічні властивості)	3	4	3
5. Ринкові переваги (експлуатаційні витрати)	2	2	2
6. Ринкові перспективи (розмір ринку)	3	2	3
7. Ринкові перспективи (конкуренція)	3	2	3
8. Практична здійсненність (наявність фахівців)	4	4	4
9. Практична здійсненність (наявність фінансів)	4	4	3
10. Практична здійсненність (необхідність нових матеріалів)	5	5	5
11. Практична здійсненність (термін реалізації)	5	4	4
12. Практична здійсненність (розробка документів)	5	4	5
Сума балів	46	43	44
Середньоарифметична сума балів $СБ_c$	44,3		

За результатами розрахунків, наведених в таблиці 4.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 4.3 [24].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Інформаційна технологія автентифікації клієнтів в режимі реального часу» становить 44,3 бала, що, відповідно до таблиці 4.3, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

4.2 Розрахунок узагальненого коефіцієнта якості розробки

Окрім комерційного аудиту розробки доцільно також розглянути технічний рівень якості розробки, розглянувши її основні технічні показники. Ці показники по-різному впливають на загальну якість проектної розробки.

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення розрахуємо за формулою [23]:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i , \qquad (4.1)$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

α_i – коефіцієнт, який враховує питому вагу *i-го* технічного показника в загальній якості розробки. Коефіцієнт α_i визначається експертним шляхом і при цьому має виконуватись умова $\sum_{i=1}^{k} \alpha_i = 1$;

β_i – відносне значення *i-го* технічного показника якості нової розробки.

Відносні значення β_i для різних випадків розраховуємо за такими формулами:

для показників, зростання яких вказує на підвищення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{ні}}{I_{аі}}, \quad (4.2)$$

де $I_{ні}$ та $I_{на}$ – чисельні значення конкретного i-го технічного показника якості відповідно для нової розробки та аналога;

для показників, зростання яких вказує на погіршення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{аі}}{I_{ні}}; \quad (4.3)$$

Використовуючи наведені залежності можемо проаналізувати та порівняти техніко-економічні характеристики аналогу та розробки на основі отриманих наявних та проектних показників, а результати порівняння зведемо до таблиці 4.4.

Таблиця 4.4 – Порівняння основних параметрів розробки та аналога.

Показники (параметри)	Одиниця вимірювання	Аналог	Проектований пристрій	Відношення параметрі в нової розробки до аналога	Питома вага показника
Точність процесу автентифікації	%	97	99	1,02	0,25
Час здійснення процесу автентифікації (в режимі реального часу)	мс	14602	13235	1,11	0,3
Доступність інтерфейсу автентифікації	бал	6	8	1,33	0,1
Завантаженість блоків системи автентифікації в процесі роботи	%	75	87	0,86	0,25
Захищеність	бал	7	7	1	0,1

БД					

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення складе:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i = 1{,}02 \cdot 0{,}25 + 1{,}11 \cdot 0{,}3 + 1{,}33 \cdot 0{,}1 + 0{,}86 \cdot 0{,}25 + 1 \cdot 0{,}1 = 1{,}04.$$

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,04 рази.

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов'язані з проведенням науково-дослідної роботи на тему «Інформаційна технологія автентифікації клієнтів в режимі реального часу», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.3.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [24]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.4)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=24 дні.

$$З_о = 15530{,}00 \cdot 56 / 24 = 36236{,}67 \ грн.$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.5 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник дослідження	15530,00	647,08	56	36236,67
Науковий співробітник	14520,00	605,00	52	31460,00
Інженер-розробник програмного забезпечення	14200,00	591,67	48	28400,00
Технік	7150,00	297,92	20	5958,33
Всього				102055,00

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Інформаційна технологія автентифікації клієнтів в режимі реального часу» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \qquad (4.5)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} , \qquad (4.6)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо *Мм*=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [24];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок

робітників першого розряду з нормальними умовами праці виробничих об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$T_р$ – середнє число робочих днів в місяці, приблизно $T_р$ = 24 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}7 / (24 \cdot 8) = 65{,}26$ *грн.*
$З_{р1} = 65{,}26 \cdot 6{,}20 = 404{,}58$ *грн.*

Таблиця 4.6 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Підготовка автоматизованого робочого місця розробника програмного забезпечення	6,20	2	1,10	65,26	404,58
Підготовка комп'ютерного обладнання	8,00	4	1,50	88,98	711,88
Інсталяція програмного забезпечення розробки технології автентифікації клієнтів	5,60	5	1,70	100,85	564,75
Компіляція програмних блоків автентифікації	4,30	5	1,70	100,85	433,65
Формування бази даних дослідження	20,00	3	1,35	80,09	1601,72
Всього					3716,58

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \qquad (4.7)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (102055,00 + 3716,58) · 11 / 100% = 11634,87 грн.

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.8)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (102055,00 + 3716,58 + 11634,87) · 22 / 100% = 25829,42 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Інформаційна технологія автентифікації клієнтів в режимі реального часу».

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{вj}, \quad (4.9)$$

де $Н_j$ – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 ... 1,15*);

$В_j$ – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$М_1$ = 4,0 · 280,00 · 1,1 - 0 · 0 = 1232,00 грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн

Офісний папір	280,00	4,0	0	0	1232,00
Папір для записів	135,00	3,0	0	0	445,50
Органайзер офісний	195,00	4,0	0	0	858,00
Канцелярське приладдя (набір офісного працівника)	210,00	4,0	0	0	924,00
Картридж для принтера	985,00	1,0	0	0	1083,50
Диск оптичний	22,50	3,0	0	0	74,25
Flesh-пам'ять 32 GB	340,00	1,0	0	0	374,00
Тека для паперів	120,00	3,0	0	0	396,00
Всього					5387,25

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Інформаційна технологія автентифікації клієнтів в режимі реального часу» відсутні.

4.3.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення. Витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення відсутні.

4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для

проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 8560,00 \cdot 1 \cdot 1,11 = 9501,60$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.8 – Витрати на придбання програмних засобів за кожним видом

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
ОС Windows	1	8560,00	9501,60
Прикладний пакет Microsoft Office	1	7730,00	8580,30
Забезпечення бази даних Rabbit MQ	1	11460,00	12720,60
Прикладний пакет мови програмування C#	1	8650,00	9601,50
.NET Framework4.8	1	5280,00	5860,80
Всього			46264,80

4.3.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування за кожним видом обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12} \ , \qquad (4.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час

досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (31250,00 \cdot 2) / (3 \cdot 12) = 1736,11$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.9 – Амортизаційні відрахування за кожним видом обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Персональний комп'ютер розробника програмного забезпечення	31250,00	3	2	1736,11
Комплекс пристроїв передачі даних мережі Internet	8460,00	3	2	470,00
Робоче місце інженера-програміста	10200,00	5	2	340,00
Пристрій виводу інформації	6890,00	5	2	229,67
Оргтехніка	10670,00	5	2	355,67
Лабораторія	345600,00	25	2	2304,00
Всього				5435,44

4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e = 6,20$ грн;

$K_{вп і}$ – коефіцієнт, що враховує використання потужності, $K_{вп і} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,50 \cdot 408,0 \cdot 6,20 \cdot 0,95 / 0,97 = 1264,80$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Персональний комп'ютер розробника програмного забезпечення	0,50	408,0	1264,80
Комплекс пристроїв передачі даних мережі Internet	0,04	408,0	101,18
Робоче місце інженера-програміста	0,12	360,0	267,84
Пристрій виводу інформації	0,50	10,0	31,00
Оргтехніка	0,50	6,5	20,15
Всього			1684,97

4.3.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Інформаційна технологія автентифікації клієнтів в режимі реального часу» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{H_{св}}{100\%}, \qquad (4.13)$$

де $H_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св} = 20\%$.

$B_{св} = (102055,00 + 3716,58) \cdot 20 / 100\% = 21154,32$ *грн.*

4.3.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.14)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 45%.

$B_{сп}$ = (102055,00 + 3716,58) · 45 / 100% = 47597,21 грн.

4.3.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.15)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 90%.

$І_в$ = (102055,00 + 3716,58) · 90 / 100% = 95194,42 грн.

4.3.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.16)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 145%.

$B_{нзв} = (102055{,}00 + 3716{,}58) \cdot 145 / 100\% = 153368{,}79$ *грн.*

Витрати на проведення науково-дослідної роботи на тему «Інформаційна технологія автентифікації клієнтів в режимі реального часу» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + M + К_в + B_{спец} + B_{прг} + A_{обл} + B_е + B_{св} + B_{сп} + I_в + B_{нзв}. \quad (4.17)$$

$B_{заг}$= 102055,00 +3716,58 +11634,87 +25829,42001 +5387,25 +0,00 +0,00 + 46264,80 + 5435,44 +1684,97 +21154,32 +47597,21 +95194,42 +153368,79 = 519323,09 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.18)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,9.

ЗВ = 519323,09 / 0,9 = 577025,65 грн.

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Інформаційна технологія автентифікації клієнтів в режимі реального часу» передбачають комерціалізацію протягом 4-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик;

Показник	1-й рік	2-й рік	3-й рік	4-й рік
Збільшення кількості споживачів, осіб	500	950	1000	820

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 9600 осіб;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 8120,00 грн;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 112,32 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 4-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [23]:

$$\Delta П_i = (\pm\Delta Ц_о \cdot N + Ц_о \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.19)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2022 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0{,}8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо ρ =40%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2022 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1$ =(112,32·9600,00+8232,32·500)·0,83·0,4·(1-0,18/100%)=1414132,17 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2$ =(112,32·9600,00+8232,32·1450)·0,83·0,4·(1-0,18/100%)=3543240,62 грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3$ =(112,32·9600,00+8232,32·2450)·0,83·0,4·(1-0,18/100%)=5784407,42 грн.

Збільшення чистого прибутку 4-го року:

$\Delta П_4$ =(112,32·9600,00+8232,32·3270)·0,83·0,4·(1-0,18/100%)=7622164,19 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати

потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.20)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ=0,17;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$ПП = 1414132,17/(1+0,17)^1+3543240,62/(1+0,17)^2+5784407,42/(1+0,17)^3+$$
$$+7622164,19/(1+0,17)^4=1208659,97+2588385,29+3611613,68+4067568,29=$$
$$=11476227,23 \text{ грн.}$$

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \quad (4.21)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 577025,65 грн.

$PV = k_{інв} \cdot ЗВ = 2 \cdot 577025,65 = 1154051,30$ грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \quad (4.22)$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 11476227,23 грн;

PV – теперішня вартість початкових інвестицій, 1154051,30 грн.

$E_{абс} = ПП - PV$ = 11476227,23 - 1154051,30 = 10322175,93 грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Тж]{1 + \frac{E_{абс}}{PV}} - 1, \quad (4.23)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 10322175,93 грн;

PV – теперішня вартість початкових інвестицій, 1154051,30 грн;

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$E_в = \sqrt[Тж]{1 + \frac{E_{абс}}{PV}} - 1$ = (1+10322175,93/1154051,30)$^{1/4}$= 0,78.

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (4.24)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2022 році в Україні d =0,15;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,4.

$\tau_{мін}$= 0,15+0,4 = 0,55 < 0,78 свідчить про те, що внутрішня економічна

дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Інформаційна технологія автентифікації клієнтів в режимі реального часу» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \tag{4.25}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 0,78 = 1,29 р.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

4.4 Висновок

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Інформаційна технологія автентифікації клієнтів в режимі реального часу» становить 44,3 бала, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий). При оцінюванні за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,04 рази. Також термін окупності становить 1,29 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок. Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Інформаційна технологія автентифікації клієнтів в режимі реального часу».

ВИСНОВОК

Під час над виконання досліджень за темою магістерської кваліфікаційної роботи було визначено актуальність задачі розробки інформаційної технології автентифікації клієнтів в режимі реального часу.

Поставлені задачі перед магістерською кваліфікаційною роботою виконані в повному обсязі, а саме:

- проведено аналіз сучасних підходів автентифікації клієнтів в режимі реального часу та обрано текстонезалежний підхід автентифікації по голосу як……;
- проведено аналіз сучасних інформаційних технологій автентифікації клієнтів в режимі реального часу (BioLink AMIS, Voice Key та VocalPassword) та визначено їх основний недолік - недостатню швидкість процесу автентифікації, що не дозволяє автентифікацію клієнта в режимі реального часу та обмежує область використання;
- проведено аналіз класифікаторів для проведення автентифікації клієнтів в режимі реального часу та обрано K-NN (k – найближчих сусідів), як найбільш точний серед проаналізованих;
- обгрунтовано вибір математичного методу MFCCs для автентифікації клієнта за голосом, який підвищить швидкість процесу автентифікації в поєднанні з обраним K-NN класифікатором;
- удосконалено математичну модель процесу автентифікації клієнтів в режимі реального часу за рахунок введення коефіцієнту автентифікації при кепстральному аналізі голосових відбитків;
- удосконалено метод процесу автентифікації клієнтів в режимі реального часу, який базується на поєднанні математичного методу MFCCs щодо голосових відбитків та класифікатора K-NN голосових відбитків, що дозволило підвищити швидкість автентифікації та не погіршити точність автентифікації клієнта.
- розроблено структуру інформаційної технології автентифікації клієнтів в режимі реального часу;
- обгрунтовано вибір мови C# та середовища програмування Visual Studio для реалізації інформаційної технології автентифікації клієнтів в режимі реального часу;
- розроблено алгоритм роботи програмного забезпечення автентифікації клієнтів в

режимі реального часу;

- реалізовано інформаційну технологію автентифікації клієнтів в режимі реального часу;
- проведено тестування інформаційної технології та виконано аналіз отриманих результатів, який показав, що інформаційна технологія автентифікації клієнтів в режимі реального часу виконує поставлену задачу, процес автентифікації клієнтів відбувається швидше на 9%, а точність автентифікації клієнта за голосовим відбитком не погіршилась.

Розроблена інформаційна технологія реалізована з використанням об’єктно орієнтованої мови програмування C# в середовищі розробки Visual Studio. При цьому, мова клієнта – англійська або українська, кількість одночасних клієнтських дзвінків не більше 200, кількість голосових відбитків збережених в БД не більше 2500, процес зберігання голосового відбитку займає не більше 30 секунд, що відповідає завданню на магістерську кваліфікаційну роботу.

Удосконалено інформаційну технологію автентифікації клієнтів в режимі реального часу, яка забезпечує аналіз голосових відбитків клієнта та реалізує удосконалений метод автентифікації клієнтів в режимі реального часу, що дозволило підвищити швидкість процесу автентифікації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Савчук Т. О., Магльона В. В., Програмний модуль автентифікації користувача в режимі реального часу, КОНФЕРЕНЦІЇ ВНТУ електронні наукові видання, LI Науково-технічна конференція факультету інтелектуальних інформаційних технологій та автоматизації (2022) [Електронний ресурс] – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2022/paper/view/15483

2. Савчук Т. О., Магльона В. В., Аналіз класифікаторів для процесу автентифікації клієнтів в режимі реального часу, III Міжнародна науково-практична конференція. SCIENTIFIC PROGRESS: INNOVATIONS, ACHIEVEMENTS AND PROSPECTS, 4-6.12.2022 Мюнхен, Німеччина [Електронний ресурс] – Режим доступу: https://sci-conf.com.ua/iii-mizhnarodna-naukovo-praktichna-konferentsiya-scientific-progress-innovations-achievements-and-prospects-4-6-12-2022-myunhen-nimechchina/

3. Савчук Т. О., Магльона В. В., Автентифікації клієнтів за голосовим відбитком в режимі реального часу, Таврійський науковий вісник [Електронний ресурс] – Режим доступу: http://journals.ksauniv.ks.ua/index.php/tech/execution

4. Заявка на свідоцтво на отримання авторського права на комп'ютерну програму "Інформаційна технологія автентифікації клієнтів в режимі реального часу" (номер 115600 від 02.11.2022)

5. В.Н.Сорокін, В.В.Вьюгін, А.А.Тананикін Розпізнавання особистості за голосом, аналітичний огляд [Електронний ресурс] – Режим доступу: http://www.jip.ua/2012/1-30-2012.pdf

6. AMIS – система голосовоі біометрії [Електронний ресурс] – Режим доступу: https://www.biolink.ua/products/software/AMIS/

7. VoiceKey Засоби автентифікації за голосом [Електронний ресурс] – Режим доступу: https://sites.google.com/site/identifikaciapogolosu/home/biometria-pogolosu/programmnye-sredstva-biometrii-po-golosu/

8. My voice is my password [Електронний ресурс] – Режим доступу: https://www.nuance.com/en-gb/omnichannel-customer-engagement/security/multi-modal-biometrics/vocalpassword.html

9. Hasan M. R., Jamil M., Rabbani M .G, Speaker identification using mel frequency cepstral coefficients. 3rd International Conference on Electrical & Computer Engineering. 2018. Vol. 1, No 1. P. 230-232.

10. Classifier comparison. [Електронний ресурс] – Режим доступу: https://scikitlearn.org/stable/auto_examples/classification/plot_classifier_comparison.html

11. Метод k-найближчих сусідів (K-nearest neighbor) [Електронний ресурс] – Режим доступу:

12. Difference Between C# and C++ [Електронний ресурс] – Режим доступу: https://wiki.loginom.ua/articles/k-nearest-neighbor.html

13. Hasan M. R., Jamil M., Rabbani M .G, Speaker identification using mel frequency cepstral coefficients. 3 rd International Conference on Electrical & Computer Engineering. 2019. Vol. 1, No 1. P. 230-232.

14. Mel Frequency Cepstral Coefficient (MFCC) tutorial [Електронний ресурс] – Режим доступу: http://practicalcryptography.com/miscellaneous/machine-learning/guide-mel-frequency-cepstral-coefficients-mfccs/

15. Машини опорних векторів (Support vector machines) [Електронний ресурс] – Режим доступу: https://wiki.loginom.ua/articles/support-vector-machines.html

16. Наївний байєсовський класифікатор [Електронний ресурс] – Режим доступу: http://bazhenov.me/blog/2012/06/11/naive-bayes.html

17. Дерева рішень: загальні принципи [Електронний ресурс] – Режим доступу: https://loginom.ua/blog/decisiontree-p1

18. Lof: визначення локальних викидів на основі плотності. [Електронний ресурс] – Режим доступу: https://dl.acm.org/citation.cfm?id=335388

19. Isolation forest. [Електронний ресурс] – Режим доступу: https://cs.nju.edu.cn/zhouzh/zhouzh.files/publication/icdm08b.pdf

20. Про прості однокласові методи класифікації. [Електронний ресурс] – Режим доступу: https://dblp.org/pers/hd/n/Noumir:Zineb

21. Comparing MLP, SVM and KNN [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/document/6682864

22. Багатошаровий персептрон (Multilayered perceptron) [Електронний ресурс] – Режим доступу: https://wiki.loginom.ua/articles/multilayered-perceptron.html#mnogosloynyyperseptron-multilayered-perceptron

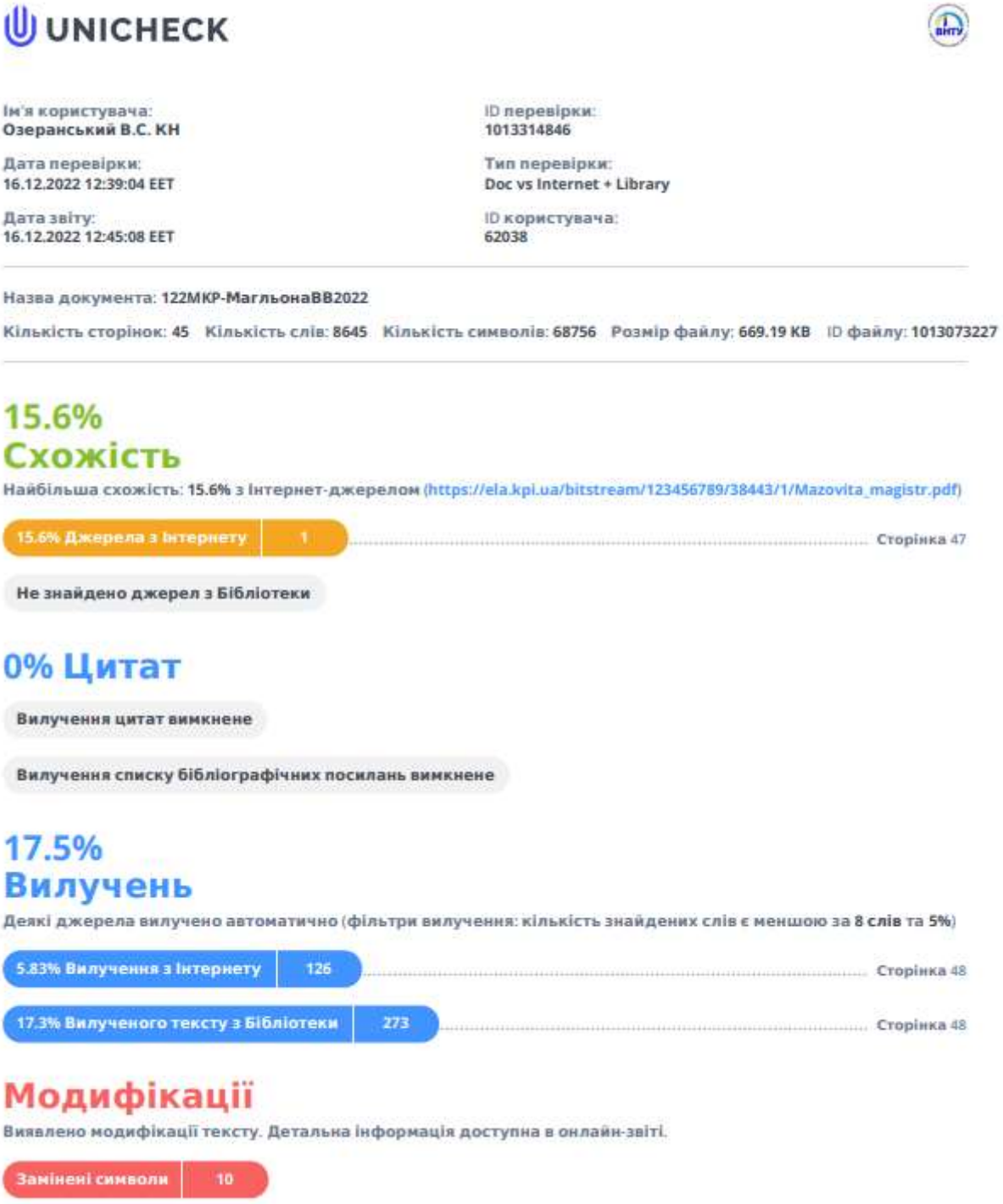
23. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : **В. О. Козловський, О. Й. Лесько, В. В. Кавецький**. – Вінниця : ВНТУ, 2021. – 42 с.

24. **Кавецький В. В.** Економічне обґрунтування інноваційних рішень: **практикум** / В. В. Кавецький, В. О. Козловський, І. В. Причепа – Вінниця : ВНТУ, **2016**. – 113 с.

ДОДАТКИ

Додаток А (обов'язковий)

Результат перевірки на плагіат в онлайн системі UNICHECK



UNICHECK

Ім'я користувача:
Озеранський В.С. КН

ID перевірки:
1013314846

Дата перевірки:
16.12.2022 12:39:04 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
16.12.2022 12:45:08 EET

ID користувача:
62038

Назва документа: 122МКР-МагльонаВВ2022

Кількість сторінок: 45 Кількість слів: 8645 Кількість символів: 68756 Розмір файлу: 669.19 KB ID файлу: 1013073227

15.6%
Схожість

Найбільша схожість: 15.6% з Інтернет-джерелом (https://ela.kpi.ua/bitstream/123456789/38443/1/Mazovita_magistr.pdf)

15.6% Джерела з Інтернету | 1 ..... Сторінка 47

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

17.5%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 5%)

5.83% Вилучення з Інтернету | 126 ..... Сторінка 48

17.3% Вилученого тексту з Бібліотеки | 273 ..... Сторінка 48

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 10

Додаток Б (обов'язковий)

Лістинг програми

```
using System;
using System.Text;
using RabbitMQ.Client;
using RabbitMQ.Client.Events;

namespace MessagingPublisher
{
    /// <summary>
    /// RabbitMQ client for recording commands publishing
    /// </summary>
    public class RabbitMQClient : IMessagingClient
    {
        #region Private Members

        private ConnectionFactory _factory = null;
        private IConnection _connection = null;
        private IModel _channel = null;
        private readonly ILog _logger = null;
        private readonly CommunicationParams _communicationParams;

        private readonly object _connectLock = new object();

        #endregion

        #region Event Handlers

        /// <summary>
        /// Event handler for returned RMQ messages
        /// </summary>
        public EventHandler<RabbitMQEventArgs> MessageReturned { get; set; }

        #endregion

        #region Constructors

        /// <summary>
        /// Initialize RabbitMQ client
        /// </summary>
        /// <param name="log"> Instance of ILog for logging </param>
        /// <param name="communicationParams"> Communication parameters for connection to RabbitMQ service </param>
        public RabbitMQClient(ILog log, CommunicationParams communicationParams)
        {
            _logger = log;
            _communicationParams = communicationParams;
        }

        #endregion

        #region Public Methods

        /// <summary>
        /// Connect to RabbitMQ service
        /// </summary>
        /// <returns> If client is connected successfully - true, otherwise - false </returns>
        public bool Connect()
        {
            lock (_connectLock)
            {
                if (!_communicationParams.IsValid())
                {
                    _logger.WriteExt("RabbitMQClient.Connect", LogLevel.Error, "Communication parameters is not valid.");
                    return false;
                }
```

```
            SetConnectionConfiguration();

            try
            {
                if (_connection == null || !_connection.IsOpen)
                {
                    _connection = _factory.CreateConnection();
                    _connection.ConnectionShutdown += Connection_ConnectionShutdown;
                    _channel = _connection.CreateModel();
                    _channel.ConfirmSelect();
                    _channel.BasicReturn += (sender, dataReturned) => OnMessageReturned(this, dataReturned);

                    _logger.WriteExt("RabbitMQClient.Connect", LogLevel.Info, "Connection created successfully.");
                }
                else
                {
                    _logger.WriteExt("RabbitMQClient.Connect", LogLevel.Info, "The connection is already open.");
                }

                return true;
            }
            catch (Exception e)
            {
                _logger.WriteExt("RabbitMQClient.Connect", LogLevel.Error, "Failed to connect. Will try to reconnect. {0}", e);
                return false;
            }
        }
    }

    /// <summary>
    /// Disconnect from RabbitMQ service
    /// </summary>
    public void Disconnect()
    {
        lock (_connectLock)
        {
            _channel?.Close();
            _channel = null;

            _connection?.Close();
            _connection = null;

            _logger.WriteExt("RabbitMQClient.Disconnect", LogLevel.Info, "The connection is closed.");
        }
    }

    /// <summary>
    /// Check if client is connected to RabbitMQ service
    /// </summary>
    /// <returns> If client is connected - true, otherwise - false </returns>
    public bool IsConnected()
    {
        lock (_connectLock)
        {
            return _connection?.IsOpen == true && _channel?.IsOpen == true;
        }
    }

    /// <summary>
    /// Publish recording command to RabbitMQ service
    /// </summary>
    /// <param name="exchange"> Exchange name for the queue </param>
    /// <param name="routingKey"> Queue name (UserId) for getting the command </param>
    /// <param name="message"> String representation of recording command and details </param>
    /// <param name="isMandatory"> If true - failed message will be returned, otherwise - ignored </param>
    /// <returns> If recording command is published successfully - true, otherwise - false </returns>
    public bool Publish(string exchange, string routingKey, string message, bool isMandatory)
    {
        return Publish(exchange, routingKey, Encoding.UTF8.GetBytes(message), isMandatory);
    }
```

```
        #endregion

        #region Private Methods

        private bool Publish(string exchange, string routingKey, byte[] message, bool isMandatory)
        {
            try
            {
                lock (_connectLock)
                {
                    _channel.BasicPublish(exchange: exchange,
                                          routingKey: routingKey,
                                          mandatory: isMandatory,
                                          basicProperties: GetDefaultProperties(),
                                          body: message);

                    _logger.WriteExt("RabbitMQClient.Publish", LogLevel.Info, "RabbitMQ message published successfully for routing key:
{0}", routingKey);
                }
            }
            catch (Exception e)
            {
                _logger.WriteExt("RabbitMQClient.Publish", LogLevel.Error, "Failed to publish RabbitMQ message: {0}", e);
                return false;
            }

            return true;
        }

        private void Connection_ConnectionShutdown(object sender, ShutdownEventArgs e)
        {
            _logger.WriteExt("RabbitMQClient.Connection_ConnectionShutdown", LogLevel.Error, "Connection is interrupted.");
            Disconnect();
        }

        private void SetConnectionConfiguration()
        {
            _factory = new ConnectionFactory();

            _factory.UserName = _communicationParams.username;
            _factory.Password = _communicationParams.password;
            _factory.HostName = new Uri(_communicationParams.endpoint).Host;
            _factory.Port = new Uri(_communicationParams.endpoint).Port;
            _factory.AutomaticRecoveryEnabled = true;
            _factory.NetworkRecoveryInterval = TimeSpan.FromSeconds(3);
        }

        private IBasicProperties GetDefaultProperties()
        {
            IBasicProperties props = _channel.CreateBasicProperties();
            props.Expiration = "36000000";
            props.Persistent = true;

            return props;
        }

        private void OnMessageReturned(object sender, BasicReturnEventArgs eventArgs)
        {
            try
            {
                var rmqResponse = new RabbitMQEventArgs()
                {
                    Body = eventArgs.Body.ToArray(),
                    ResponseCode = eventArgs.ReplyCode
                };

                MessageReturned?.Invoke(sender, rmqResponse);
            }
            catch(Exception e)
            {
                _logger.WriteExt("RabbitMQClient.OnMessageReturned", LogLevel.Error, "Failed to handle returned message {0}", e);
```

```
            }
        }

        #endregion
    }
}
using System;

namespace MessagingPublisher
{
    /// <summary>
    /// RabbitMQ Messaging Publisher for recording commands
    /// </summary>
    public class RabbitMQPublisher : IMessagingPublisher
    {
        #region Private Members

        private readonly IMessagingClient _client = null;
        private readonly ILog _logger = null;

        #endregion

        #region Event Handlers

        /// <summary>
        /// Event handler for returned RMQ messages
        /// </summary>
        public EventHandler<RabbitMQEventArgs> MessageReturned { get; set; }

        #endregion

        #region Constructors

        /// <summary>
        /// Initialize RabbitMQ Publisher
        /// </summary>
        /// <param name="log"> Instance of ILog for logging </param>
        /// <param name="communicationParams"> Communication parameters for connection to RabbitMQ service </param>
        /// <param name="messagingClient"> Instance of specific Messaging Client (RabbitMQClient by default) </param>
        public RabbitMQPublisher(ILog log, CommunicationParams communicationParams, IMessagingClient messagingClient = null)
        {
            _logger = log;
            _client = messagingClient ?? new RabbitMQClient(log, communicationParams);
            _client.MessageReturned += MessageReturned;
        }

        #endregion

        #region Public Methods

        /// <summary>
        /// Start connection to provided RabbitMQ client
        /// </summary>
        /// <returns> If publisher created the connection successfully - true, otherwise - false </returns>
        public bool Start()
        {
            if (!Connect())
            {
                Disconnect();
                return false;
            }

            return true;
        }

        /// <summary>
        /// Stop connection to provided RabbitMQ client
        /// </summary>
        public void Stop()
        {
            Disconnect();
```

```
            _logger.WriteExt("RabbitMQPublisher.Stop", LogLevel.Info, "The connection is stopped.");
        }

        /// <summary>
        /// Check if publisher is connected to provided RabbitMQ client
        /// </summary>
        /// <returns> If publisher is connected - true, otherwise - false </returns>
        public bool IsConnected()
        {
            return _client.IsConnected();
        }

        /// <summary>
        /// Send recording command to provided RabbitMQ client
        /// </summary>
        /// <param name="exchange"> Exchange name for the queue </param>
        /// <param name="routingKey"> Queue name (UserId) for getting the command </param>
        /// <param name="message"> String representation of recording command and details </param>
        /// <param name="isMandatory"> If true - failed message will be returned, otherwise - ignored </param>
        /// <returns> If recording command is sent successfully - true, otherwise - false </returns>
        public bool SendMessage(string exchange, string routingKey, string message, bool isMandatory)
        {
            return _client.Publish(exchange, routingKey, message, isMandatory);
        }

        #endregion

        #region Private Methods

        private bool Connect()
        {
            if (_client.IsConnected())
            {
                _logger.WriteExt("RabbitMQPublisher.Connect", LogLevel.Info, $"Connection already exists.");
                return true;
            }

            return _client.Connect();
        }

        private void Disconnect()
        {
            _client.Disconnect();
        }

        #endregion
    }
}
using System;

namespace Common
{
    /// <summary>
    /// Event arguments for RMQ data returned
    /// </summary>
    public class RabbitMQEventArgs : EventArgs
    {
        /// <summary>
        /// Message data in binary format
        /// </summary>
        public byte[] Body { get; set; }

        /// <summary>
        /// Response code of unsent RMQ message
        /// </summary>
        public ushort ResponseCode { get; set; }
    }
}
```

Додаток В (обов'язковий)

Додаток В (обов'язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ АВТЕНТИФІКАЦІЇ КЛІЄНТІВ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Виконав: студент 2-го курсу,
групи КН-21м
спеціальності 122 – «Комп`ютерні науки»
Магльона В. В.
(прізвище та ініціали)

Керівник: професор кафедри комп'ютерних науки
Савчук Т. О. (прізвище та ініціали)
«__»_____2022 р.

Таблиця В.1 Порівняльна таблиця інформаційних технологій автентифікації клієнтів в режимі реального часу

Назва інф. технології	BioLink AMIS	Voice Key	VocalPassword
Витяг ознак	MFCC	PLP, voicedness	MFCC, PLP
Розпізнавання голосового відбитку	Алгоритм bushderby	Алгоритм Витерби	Алгоритм Витерби
Точність	95%	98%	97%
Час розпізнавання	5 сек	12 сек	30 сек
Переваги	Великий відсоток точності розпізнавання	Велика швидкість розпізнавання голосового відбитку	Надійна інф. технологія розпізнавання голосового відбитку
Недоліки	В якості розпізнавального алгоритму використовується нейронна мережа	Велика кількість функцій, тому важкий в налаштуванні	Мала швидкість розпізнавання голосового відбитку

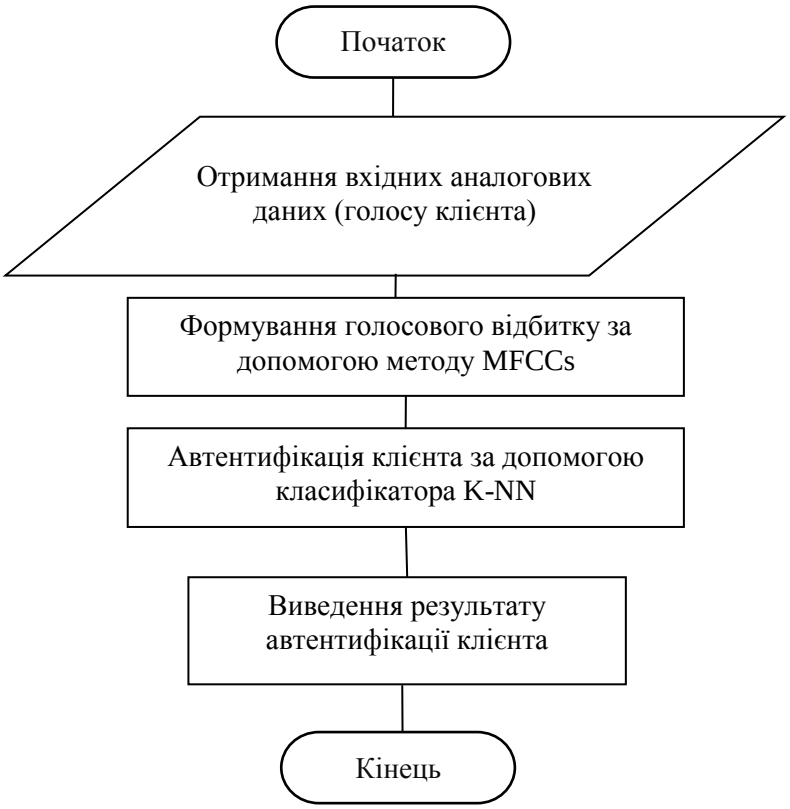


Рисунок В.1 – Основні етапи методу автентифікації клієнтів в режимі реального часу

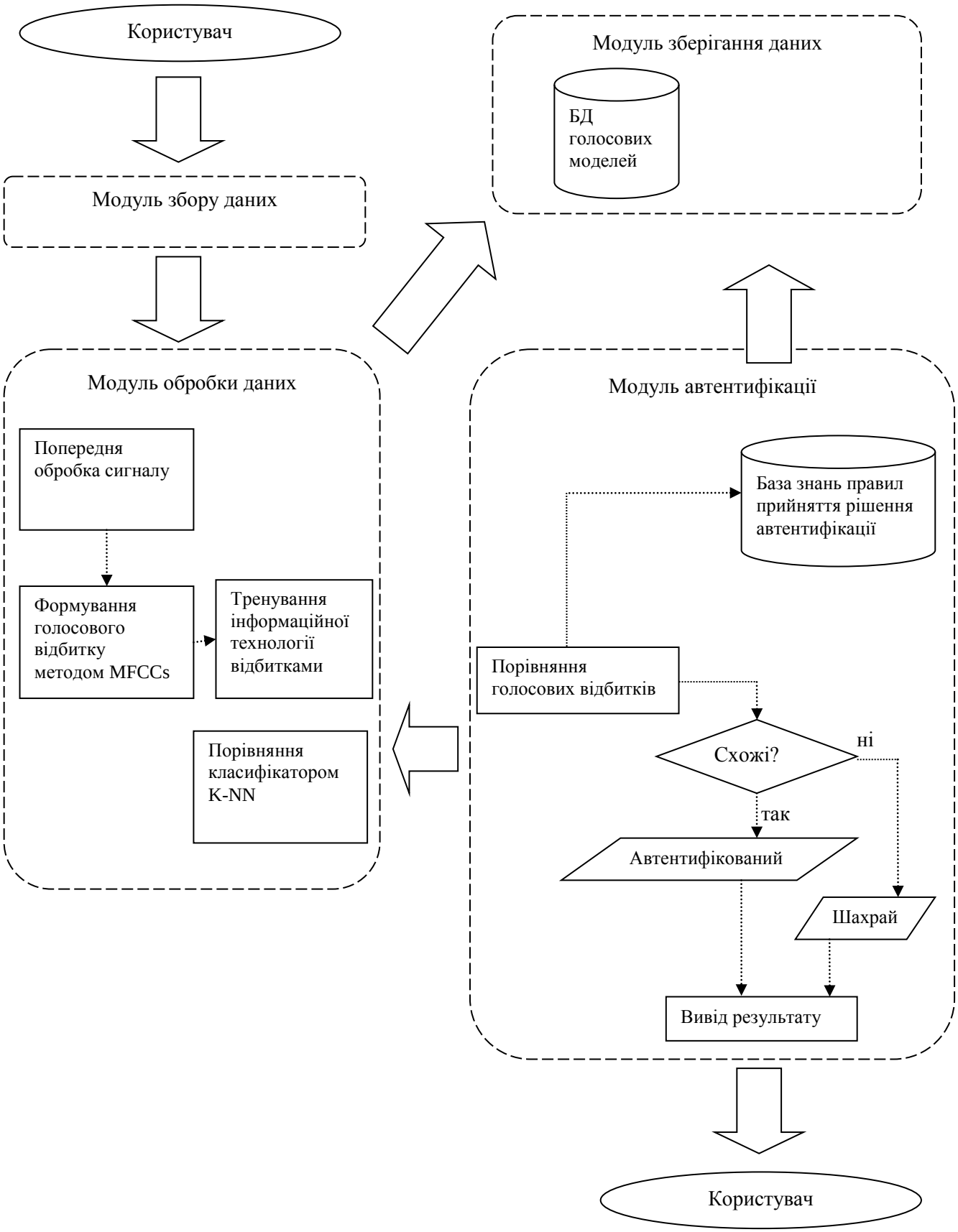


Рисунок В.2 – Структура інформаційної технології автентифікації клієнтів в режимі реального часу

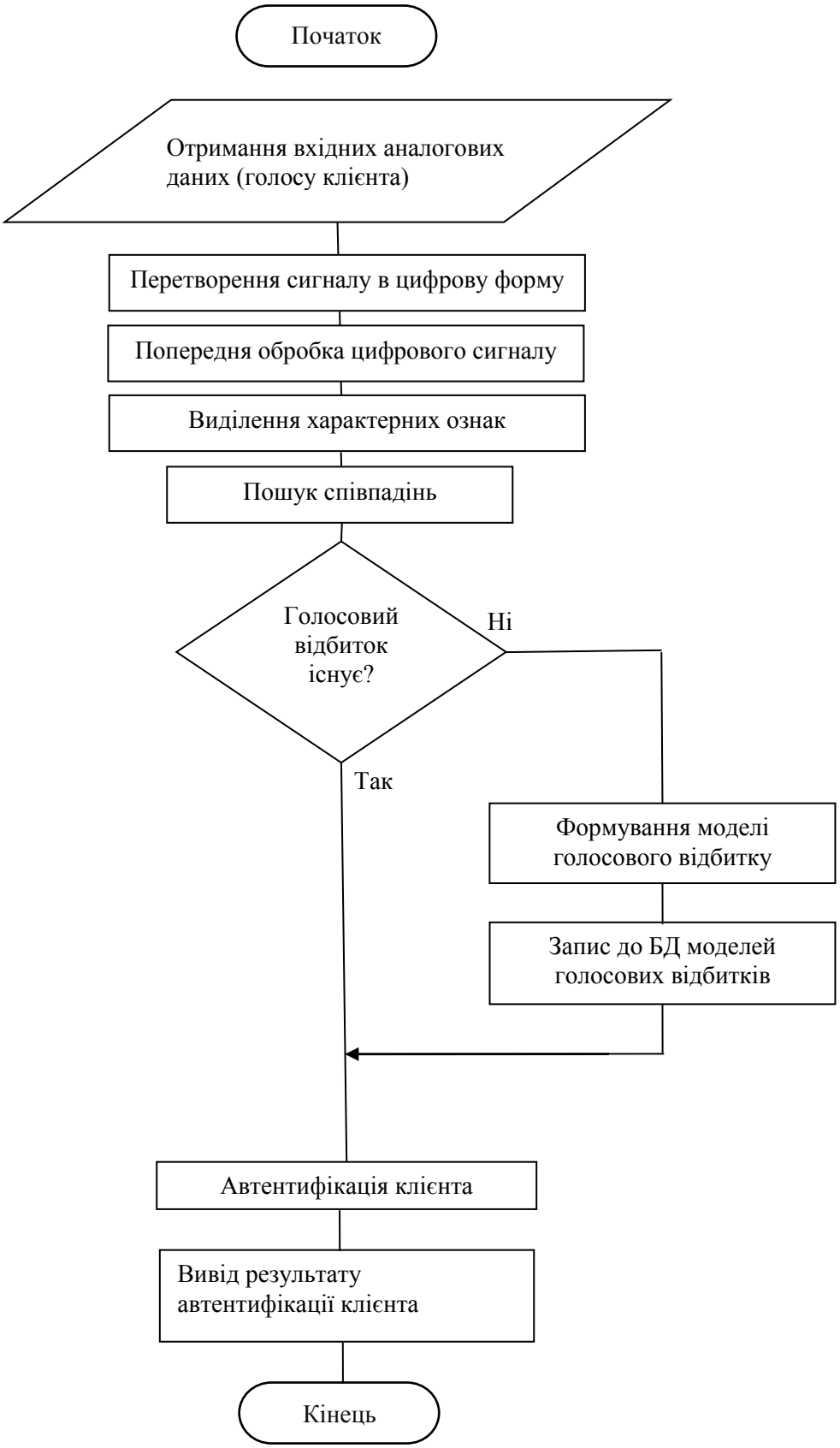


Рисунок В.3 – Схема алгоритму функціонування інформаційної технології автентифікації клієнтів в режимі реального часу

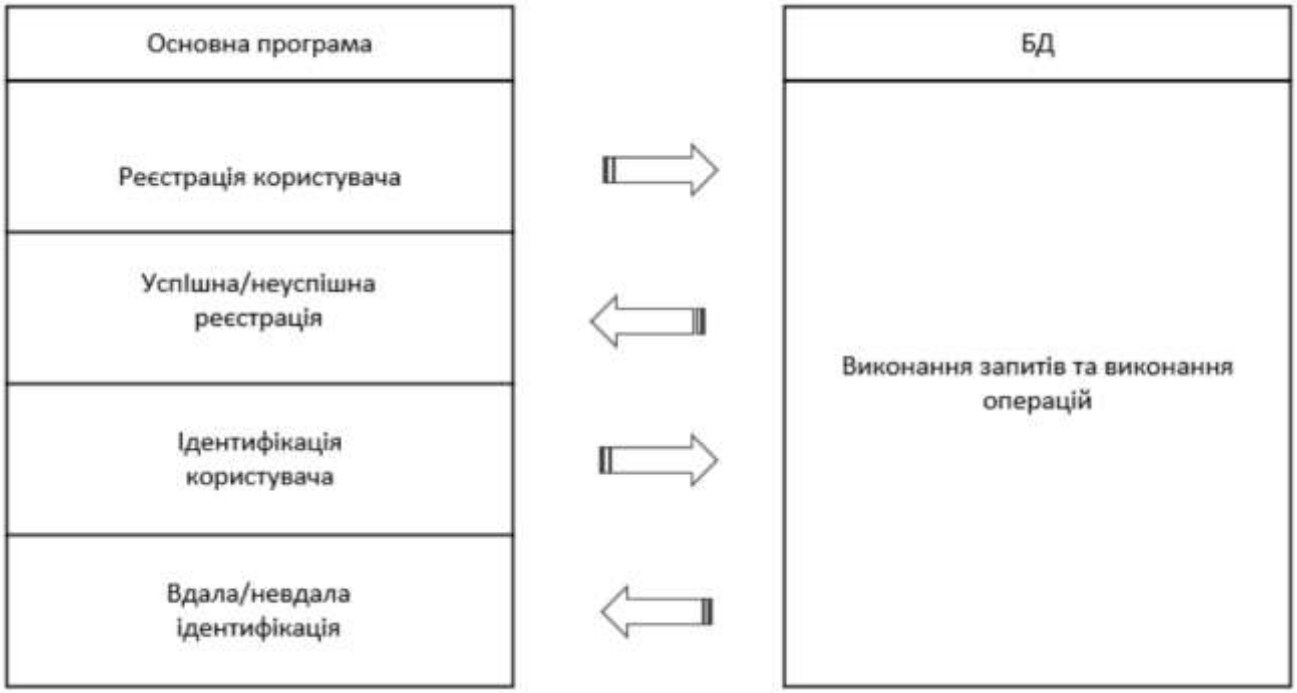


Рисунок В.4 – Функціональна схема інформаційної технології автентифікації клієнтів в режимі реального часу

	VocalPassword (Nuance)	Voice Key	AMIS (Biolink)	Інформаційна технологія автентифікації клієнтів в режимі реального часу
Час в мс роботи процесу автентифікації	15 602	19 927	14 602	13 235

	VocalPassword (Nuance)	Voice Key	AMIS (Biolink)	Інформаційна технологія автентифікації клієнтів в режимі реального часу
Точність, %	97	98	95	99

Рисунок В.5 – Результати тестування програмного забезпечення автентифікації клієнтів в режимі реального часу

Додаток Г (довідниковий)

Інструкція користувача

Для використання комп'ютерної програми користувачеві потрібно виконати наступні кроки:

1. Перейти до місця, де знаходиться встановлювач додатку "AuthenticationClients" (рисунок Г.1).

Рисунок Г.1 – Встановлювач додатку для автентифікації клієнтів в режимі реального часу

2. Встановити додаток для автентифікації клієнтів в режимі реального часу (рисунок Г.2).

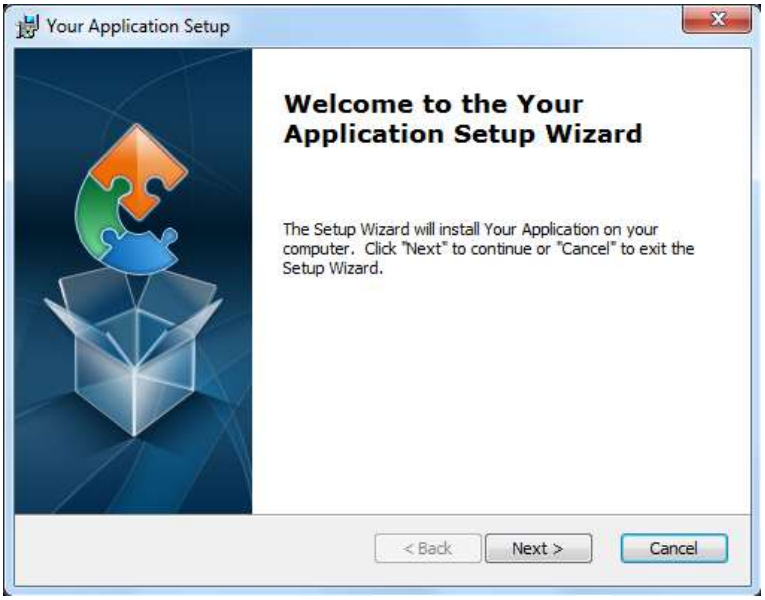


Рисунок Г.2 – Вікно встановлення додатку для автентифікації клієнтів в режимі реального часу

3. Додаток встановлений, запускаємо його та вводимо дані менеджера, який буде приймати дзвінки (рисунок Г.3).

Рисунок Г.3 – Вікно введення даних менеджера

4. Після цього додаток очікує вхідні дзвінки. Зробимо тестовий дзвінок за допомогою Cisco телефону (рисунок Г.4).

Рисунок Г.4 – Дзвінок за допомогою Cisco телефону

5. У сливаючому вікні додатку зможемо побачити те, що дзвінок почався та нам потрібно ідентифікувати клієнта (рисунок Г.5).

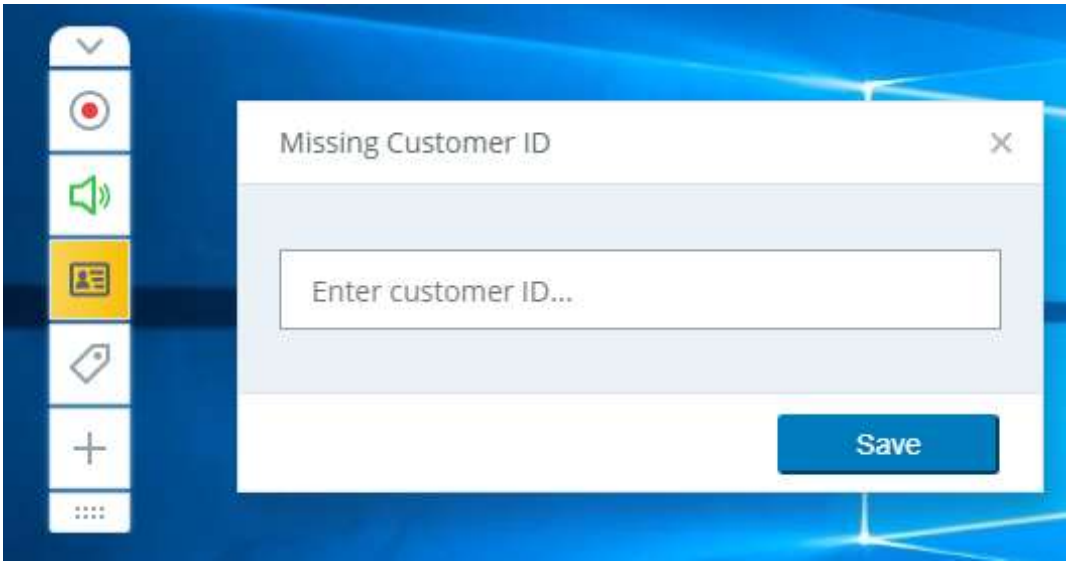


Рисунок Г.5 – Вікно вводу даних для ідентифікації клієнта

6. Якщо введений ідентифікатор клієнта вже є в інформаційній технології, тобто клієнт вже був раніше зареєстрований та містить голосовий відбиткок – почнеться процес автентифікації (рисунок Г.6).

Рисунок Г.6 – Процес автентифікації клієнта

7. Якщо клієнт буде автентифікований успішно ми побачимо відповідне повідомлення (рисунок Г.7).

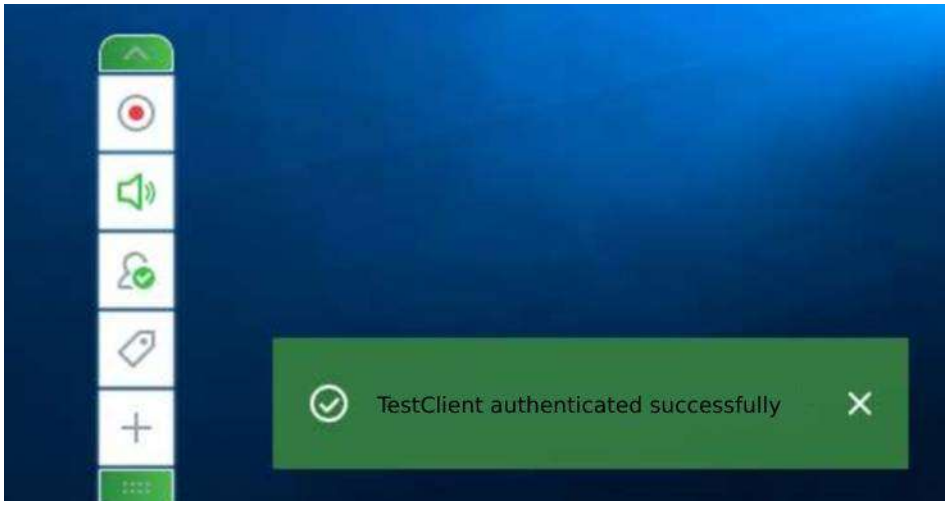


Рисунок Г.7 – Клієнт автентифікований успішно

8. Якщо клієнт виявиться шахраєм, тобто його голос не буде відповідати дійсності – буде відображено відповідне повідомлення (рисунок Г.8).

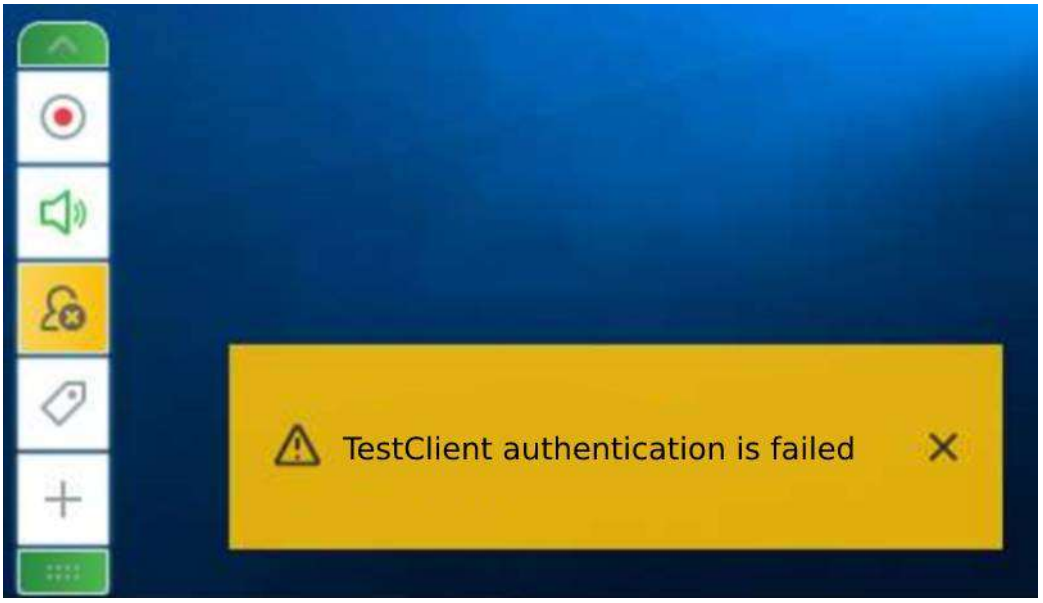


Рисунок Г.8 – Клієнт не зміг автентифікуватись коректно