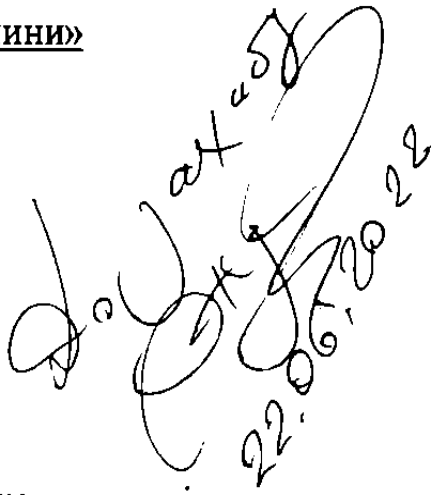
Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет «Комп'ютерні технології і системи»
(назва факультету)

Кафедра «Електронні обчислювальні машини»
(повна назва кафедри)

Пояснювальна записка

до кваліфікаційної роботи
бакалавра
(ступінь вищої освіти)



на тему: Розробка засобів ідентифікації та аутентифікації користувачів автоматизованих систем з використанням бездротових технологій
за освітньою програмою Кібербезпека
зі спеціальності: 125 Кібербезпека
(шифр і назва спеціальності)

Виконала: групи: КБ1811
студентка

(підпис студента) / Анастасія ВИСОЧИНА /
(Ім'я ПРІЗВИЩЕ)

Керівник: (підпис) / доцент, Денис ОСТАПЕЦЬ /
(посада, Ім'я ПРІЗВИЩЕ)

Нормоконтролер: (підпис) / ст. викладач, Володимир ДЗЮБА /
(посада, Ім'я ПРІЗВИЩЕ)

Консультанти:

(назва розділу) (підпис) / /
(посада, Ім'я ПРІЗВИЩЕ)

(назва розділу) (підпис) / /
(посада, Ім'я ПРІЗВИЩЕ)

(назва розділу) (підпис) / /
(посада, Ім'я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент (підпис)

Дніпро –2022 рік

Ministry of Education and Science of Ukraine
Ukrainian State University of Science and Technologies

Faculty «Computer technologies and systems»
(faculty)

Department «Electronic computers»
(department)

Explanatory Note
to Bachelor's Thesis
bachelor's
(higher education degree)

on the topic: Development of means for identification and authentication of users of automated systems using wireless technologies

in the Speciality: 125 Cybersecurity
(speciality and its code)

Done by the student of the group: KB1811 / Vysochina Anastasiya /
(name, surname)

Scientific Supervisor: / Associate Professor, Denis Ostapets /
(position, name, surname)

Normative controller : / Senior lecturer, Volodymyr Dziuba /
(position, name, surname)

Supervisors

(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)

Dnipro – 2022

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи
Кафедра: ЕОМ
Рівень вищої освіти: Перший (бакалаврський)
Освітня програма: Кібербезпека
Спеціальність: 125 Кібербезпека
(шифр та назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри _____
_____ _____
(підпис) (Ім'я ПРІЗВИЩЕ)
Дата _____

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра
(ступінь вищої освіти)

студенту Височиній Анастасії Сергіївні
(Прізвище, Ім'я По батькові)

1. Тема роботи: Розробка засобів ідентифікації та аутентифікації користувачів автоматизованих систем з використанням бездротових технологій

Керівник роботи: Остапець Денис Олександрович, к.т.н., доцент
(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від "07" 12 2021 р. № 67ст

2. Строк подання студентом роботи: 13.06.2022 р.
3. Вихідні дані до роботи: Методи ідентифікації та аутентифікації користувача. Характеристики технологій бездротового зв'язку
4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):
4.1 Аналітична частина:
Аналіз бездротових технологій
4.2Основна частина:
- Огляд та порівняльний аналіз засобів ідентифікації та аутентифікації користувачів;
- Функціонування, основні процедури та інформаційна структура комплексу;
- Розробка програмного забезпечення комплексу
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
- Аналіз бездротових технологій;
- Склад та функції комплексу;
- Структура даних;
- Основні алгоритми програм;
- Приклади роботи комплексу

6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав: (підпис консультанта, дата)	Завдання прийняв (підпис студента, дата)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Прим.
1	Огляд та порівняльний аналіз засобів ідентифікації користувачів	25.04.22	20
2	Функціонування, основні процедури та інформаційна структура комплексу	11.05.22	30
3	Розробка та налагодження програмного забезпечення комплексу	06.06.22	45
4	Реферат, вступ, висновки	13.06.22	5
5	Подання кваліфікаційної роботи до кафедри	13.06.22	
6	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	23.06.22	

Студент _____ (підпис) Анастасія ВИСО (Ім'я ПРІЗВИ

Керівник роботи _____ (підпис) Денис ОСТАП (Ім'я ПРІЗВИЩ

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи бакалавра:

58 с., 27 рис., 1 табл., 2 додатка, 12 джерел.

Об'єкт розробки – програмні засоби демонстрації ідентифікації та аутентифікації з використанням бездротових технологій.

Мета роботи – розробка програмних засобів майнової ідентифікації та аутентифікації з використанням смартфону та бездротового з’єднання.

Представлено аналіз факторів, методів та засобів ідентифікації та аутентифікації, алгоритму визначення відстані по силі сигналу. Обрано передачу закодованого токену зі смартфону.

Наведені узагальнені алгоритми роботи засобів в різних режимах, розроблено програмне забезпечення засобів та перевірена його працездатність, створено інструкцію з використання.

Розроблене програмне забезпечення може використовуватися для демонстрації процесу ідентифікації та аутентифікації та може бути масштабоване для подальшого використання у інших проектах

Ключові слова: BLUETOOTH, СМАРТФОН, АУТЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, ВИЗНАЧЕННЯ ВІДСТАНІ, ТОКЕН, JWT, JAVA, C#

ЗМІСТ

ВСТУП

Вимоги до забезпечення захисту з часом лише збільшуються і потребують безперервного вдосконалення. Механізми забезпечення санкціонованого доступу до використання інформації є вкрай важливими, але не менш важливою є зручність користувача. Захистити дані так, щоб отримати до них несанкціонований доступ було б практично неможливо – це основне, але не єдине завдання розробника системи аутентифікації. Важливо також не переускладнити систему для користувача

У сучасних системах часто виставляються надто суворі вимоги до паролів, які користувачі не можуть легко виконати, що призводить до записування паролів, що негативно впливає на безпеку, тому доцільно удосконалювати безпарольні системи входу. Ця робота присвячена розробці системи майнової безпарольної аутентифікації, тому тема роботи є актуальною.

Тема роботи затверджена наказом № 67 ст від 07.12.2021.

Головна мета цієї роботи – розробка програмних засобів майнової ідентифікації та аутентифікації з використанням смартфону та бездротового з’єднання.

Представлена кваліфікаційна робота складається зі вступу, 3 розділів та висновків.

У розділі 1 представлений огляд засобів ідентифікації та аутентифікації. Розглянуті різні фактори аутентифікації, виділено переваги та недоліки того чи іншого фактору. Оглянуті різні засоби майнової аутентифікації. Порівняні різні бездротові технології

У розділі 2 наведено функціональну структуру розроблюваного комплексу. Наведено опис процесу визначення відстані до користувача, та обміну аутентифікаційною інформацією.

У розділі 3 здійснено вибір засобів розробки для обох частин комплексу (мови програмування, середовища), наведені основні алгоритми роботи комплексу, на основі яких розроблено програмне забезпечення. Наведено методику використання розробленого комплексу та подана інструкція з використання.

У додатках А, Б наведено код програм.

1 ОГЛЯД ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСОБІВ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

1.1 Загальні відомості

Ідентифікація – процедура розпізнавання користувача за його ідентифікатором (ім'я, логін, е-мейл) та перевірки, чи перебуває він у списку системи. Основними засобами ідентифікації є штрих-кодові та радіочастотні (RFID – Radio Frequency Identification Device) мітки, картки з магнітною смугою, у побуті – бейджі, ім'я, опис зовнішності [1].

Аутентифікація – процедура встановлення, чи є користувач, який надає той чи інший ідентифікатор тим суб'єктом, якому належать ці дані та чи легітимно він їх використовує. Для цього використовується якась інформація або об'єкт, який має виключно справжній користувач або додаток. Зазвичай застосовуються одноразові, багаторазові паролі, графічні паролі, ключі доступу, біометричні дані [1].

1.2 Класифікація факторів аутентифікації

Виділяють три фактори аутентифікації [2]

Щось, нам відоме (фактор знання) Ідентифікаційна характеристика користувача містить секретну інформацію, недоступну іншим суб'єктам – слово-пароль, фразу, пін-код. Плюси цього фактора – простота розробки та впровадження, інтуїтивне розуміння системи користувачем. Найбільший мінус паролів – вони залежать від збереження секретності самим користувачем. Існує безліч способів перехопити пароль або вивідати його, часто паролі просто записують і залишають на видному місці, полегшуючи зламування.

Щось, що у нас є (майновий фактор) Ідентифікаційною характеристикою є володіння авторизованим користувачем певним предметом, до появи комп'ютерів це міг бути підпис чи ключ від замка. В АС це зазвичай файл даних, який вбудовується в пристрій (карту з магнітною смугою, RFID-мітку, сім-карту або будь-якого роду токен, в якому обчислюється одноразовий пароль). Аутентифікацію на основі пристрою найскладніше обійти, так як

використовується унікальний фізичний об'єкт, також, на відміну від пароля, про розкриття якого користувач може ніколи не дізнатися, користувач дуже швидко розуміє, що пристрій аутентифікації був викрадений або іншим чином скомпрометований. Основними слабкими місцями є більш висока вартість, можливість відмови обладнання та ризик втрати. На рисунку 1.1 наведені найбільш розповсюджені пристрої аутентифікації.

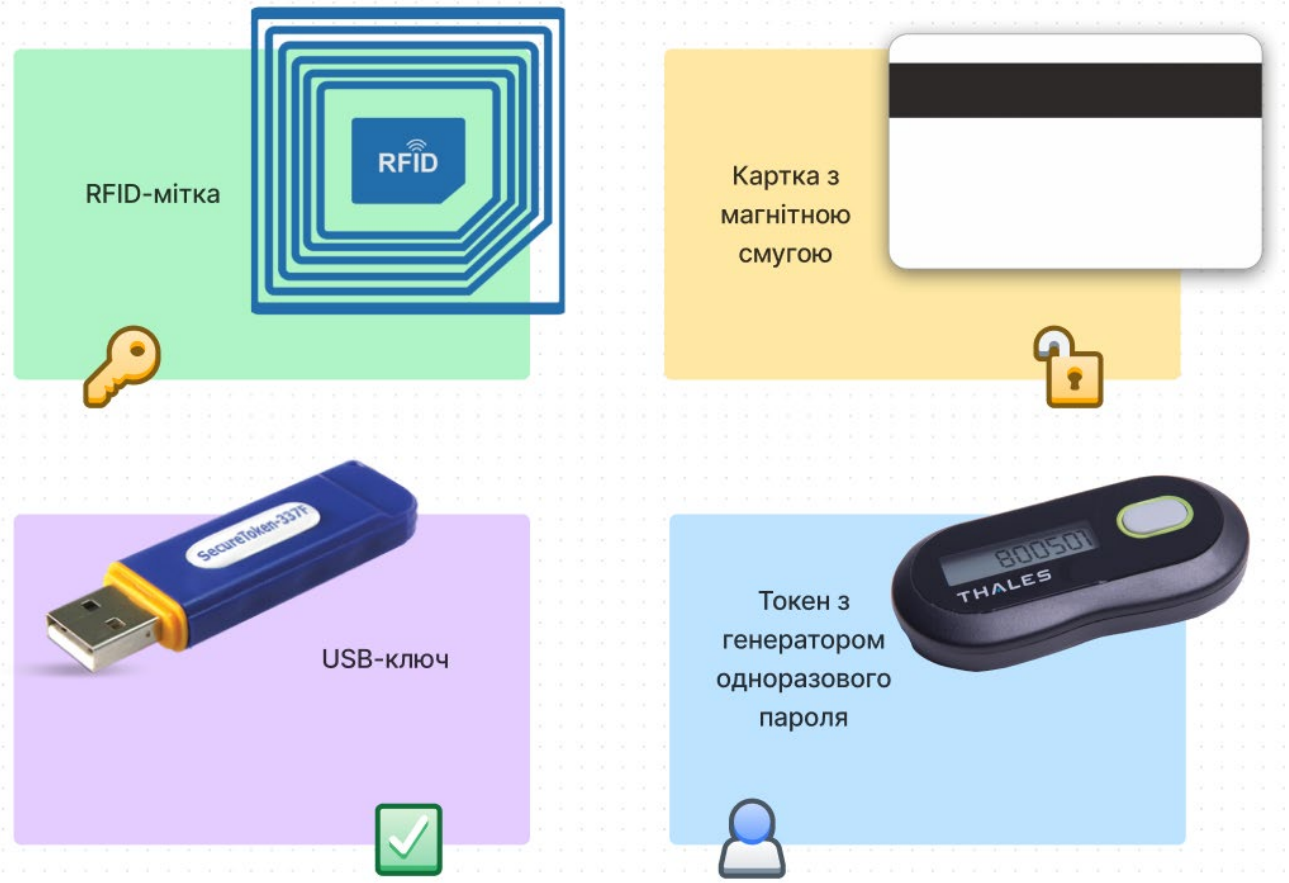


Рисунок 1.1 – Основні засоби майнової аутентифікації

Щось, властиве нам (біометричний фактор) Ідентифікаційною характеристикою є фізична особливість, унікальна для особи, що аутентифікується - голос, відбиток пальця, скан руки, обличчя, сітківки, клавіатурний почерк та інші поведінкові характеристики. Біометрична аутентифікація є найпростішим способом для суб'єкта перевірки, оскільки його участь є мінімальною. Однак цей фактор має значний недолік - обладнання для біометричної ідентифікації набагато дорожче, а його впровадження складніше, біометричні фактори також можна перехопити, наприклад записати голос поза

процесом аутентифікації і використовувати його для злому. Але на відміну від пароля, якщо біометричні показники все ж потрапили зловмиснику, власник не має способу заповнити збитки через незмінність біометричних характеристик. На рисунку 1.1 наведені найбільш розповсюджені пристрої аутентифікації.

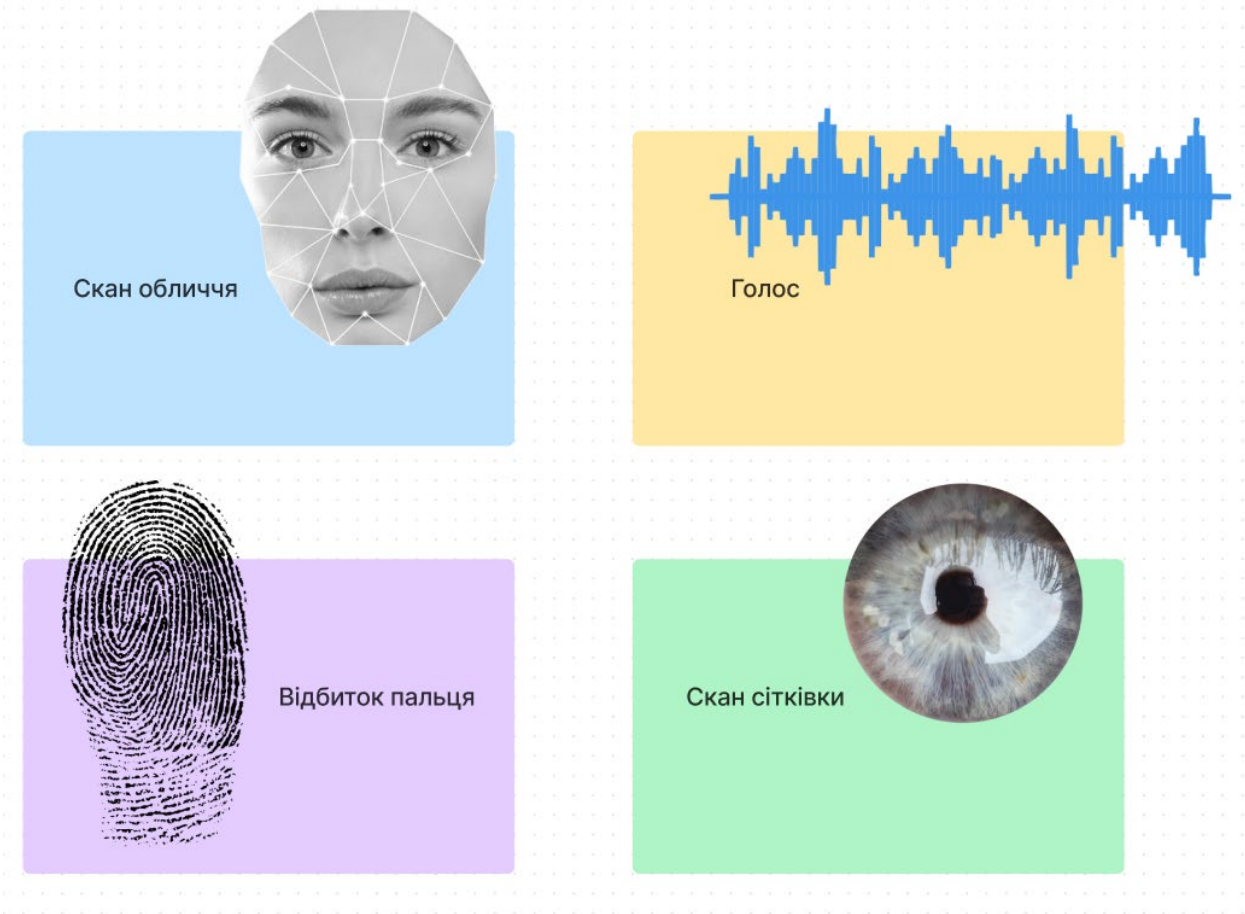


Рисунок 1.2 – Основні критерії біометричної аутентифікації

У разі потреби у підвищеній захищеності доцільно вдатися до використання багатофакторної аутентифікації. За звітом корпорації "Google" від лютого поточного року [3] запровадження обов'язкової двофакторної (парольної + майнової) автентифікації на 150 мільйонів користувачів підвищило їхню безпеку в два рази.

У цій роботі використаний майновий фактор, як прийнятний за вартістю, простотою впровадження та зручністю для користувача.

1.3 Огляд засобів майнової аутентифікації

Засоби майнової аутентифікації поділяються на два основних типи, що відображено на рисунку 1.3

Залежно від типу пристроїв, які використовуються для аутентифікації користувачів АС вони поділяються на пасивні (пристрої для зберігання аутентифікатора) та активні (у різних ситуаціях можуть створювати різні аутентифікатори). [4]

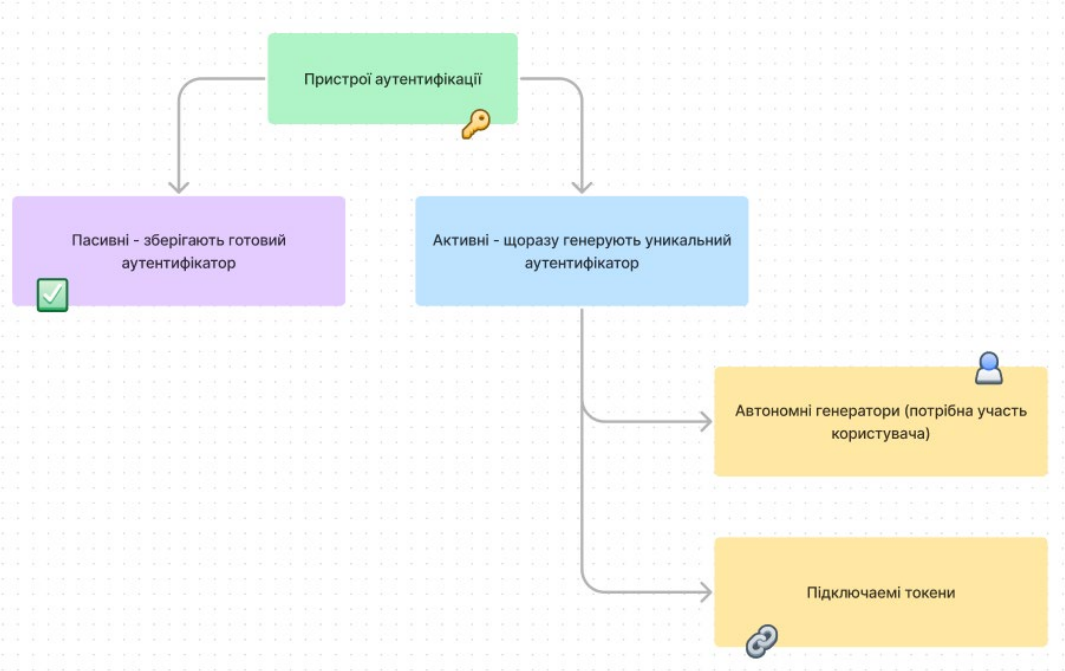


Рисунок 1.3 – Класифікація пристроїв аутентифікації

До пасивних пристроїв належать юсб-накопичувачі, RFID-мітки та карти з магнітною стрічкою. Зараз вони використовуються значно рідше, незважаючи на те, що вони дешевші у виробництві та впровадженні - ці продукти схильні до копіювання при отриманні доступу або перехопленні інформації, що передається по відкритому каналу зв'язку.

Активні пристрої аутентифікації не мають таких проблем, адже на пристрої встановлено мікрочіп з обчисленням одноразового пароля/пін коду, що по-перше ускладнює процедуру копіювання та підробки; по-друге – робить марним перехоплення інформації на певному сеансі авторизації.

Залежно від функціональності пристрою аутентифікації їх поділяють на дві групи:

- Автономні генератори одноразових паролів (не вимагають спеціальної апаратної підтримки, мають кнопки взаємодії з АС). Але існує обмеження складності протоколів аутентифікації, оскільки користувач бере участь у передачі даних.

- Смарт-карти та токени, що підключаються до комп'ютера (потрібен спеціальний сканер, порт). Для застосування таких пристроїв у системах аутентифікації може знадобитися використання асиметричної криптографії.

Бездротові токени є гібридом цих двох типів, оскільки не вимагають фізичного підключення і при цьому стійко зв'язуються з АС.

Як активний бездротовий токен можна використовувати смартфон, що й реалізовано в цьому проекті, це підвищує зручність для користувача, а також безпеку, оскільки використовуючи розроблені виробником засоби він має змогу віддалено заблокувати його при втраті.

1.4 Аналіз основних бездротових технологій

У якості протоколу, придатного до передачі даних авторизації можна розглянути такі варіанти: RFID, IrDA, Bluetooth, Wi-fi. У таблиці 1.1 наведені основні показники цих технологій

Таблиця 1.1 – Порівняльна характеристика бездротових технологій

Технологія / Характе-ристики	RFID	IrDA	Bluetooth	Wi-fi
Відстань передачі	від 10 см до кількох метрів	до кількох метрів (при знаходженні приймача і передавача на одній лінії)	від 10 до 100 метрів	близько 100-300 метрів
Топологія	«точка–точка»	«точка–точка»	«точка–точка», «зірка», мережа	«точка–точка», зірка
Швидкість передачі	424 Кбіт\с	От 2,4Кбіт\с До 16Мбіт\с	721 Кбіт\с	от 300 Мбіт/с
Робоча частота	13.56МГц	3.4*10^(14)Гц (світло)	2,4-2,48 ГГц	2412–2484 МГц
Зручність використання	Середня (малий радіус дії)	Низька (необхідність точно позиціонувати приймач та передавач)	Висока	Висока
Поширеність у сучасних пристроях	Середня (присутня у середньо-високому ціновому сегменті)	Вкрай низька, практично не використовується для передачі даних, в основному включена як ПДУ	Повсюдно розповсюджений	Повсюдно розповсюджений
Відносний ступінь захищеності	Середня	Низька	Висока	Висока
Відносна складність інтеграції	Низька	Висока	Низька	Середня
Можливість оцінки відстані	Не потрібна через малий радіус дії	Практично неможлива	Наявна у специфікації 4.0 та вище, можлива з прийнятною точністю	Можлива з прийнятною точністю

Виходячи з глобальної поширеності, та зручності використання, високого ступеня захищеності, низької складності реалізації та можливості оцінки відстані, у даному проекті використовується технологія Bluetooth.

1.5 Висновки за розділом

У розділі розглянуто поняття ідентифікації та аутентифікації, класифікацію факторів та засобів майнової аутентифікації, проведено порівняльний аналіз патернів аутентифікації та бездротових технологій, які можна застосувати для передачі аутентифікаційних даних.

Результати показують, що найкращим варіантом є система заснована на майновому факторі, у вигляді активного токена – смартфона.

Передача сформованого токена відбувається бездротовим каналом передачі даних, протоколом Bluetooth, такий вибір пов'язаний зі співвідношенням переваг і недоліків різних систем та його якісної оцінкою.

У першу чергу така конфігурація системи дозволяє скоротити витрати на впровадження (оскільки вона базується на апаратному пристрої, що є у користувача) і мінімізувати участь користувача. Система відповідає сучасним стандартам безпеки, базується на загальноприйнятих стандартах формування та передачі даних, що спрощує інтеграцію у різноманітні системи.

2 ФУНКЦІОНУВАННЯ, ОСНОВІ ПРОЦЕДУРИ ТА ІНФОРМАЦІЙНА СТРУКТУРА КОМПЛЕКСУ

2.1 Узагальнена схема роботи комплексу

Систему аутентифікації було вирішено реалізувати наступним чином: дві незалежні одна від одної програми, основна - мобільний додаток “Authentication Server” формує токен і визначає присутність пристрою в зоні дозволеної авторизації та службова програма на ПК, що демонструє процес авторизації. В рамках подальшого розвитку системи як “Application Server” може виступати веб-додаток, сервіс, веб-сайт або будь-яка інша програма, оскільки для системи авторкою обрано стандартний протокол формування та обміну аутентифікаційними даними - JWT токени. Перевагою цих токенів є відкритість стандарту, простота реалізації (для більшості мов/фреймворків розроблені інструменти автоматизації генерації), відсутність необхідності зберігати поточні сесії та можливість передавати всередині токена довільну додаткову інформацію.

На рисунку 2.1 покроково показано процес генерації та обміну токеном

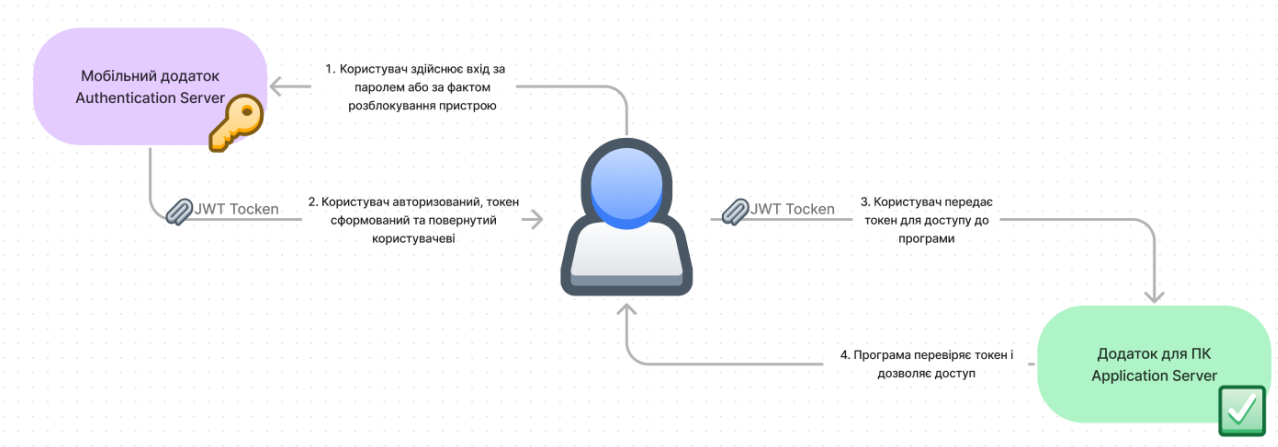


Рисунок 2.1 – Узагальнена схема роботи комплексу

Передача сформованого токена відбувається бездротовим каналом передачі даних, за протоколом Bluetooth, такий вибір пов'язаний з відносною простотою реалізації, достатньою захищеністю каналу передачі даних, повсюдною

поширеністю в мобільних пристроях (що знижує матеріальні витрати на реалізацію системи), простою та зрозумілістю для користувача.

2.2 Процес ідентифікації та аутентифікації користувача

На першому етапі користувачеві необхідно сполучити пристрої по Bluetooth. Після успішного поєднання починається основний цикл системи, першим кроком якого є створення токена на мобільному пристрої. Після цього відбувається процедура визначення присутності, якщо користувач знаходиться досить близько до ПК, відбувається передача токена. Останній етап - прийом та обробка токена комп'ютером. Далі, після того як сплине час життя старого токена на мобільному пристрої відбувається формування нового. Якщо ПК не отримає у відведений час новий токен (тобто користувач перестане перебувати в зоні присутності), авторизація скидається. На рисунку 2.2 відображено цикл формування токена

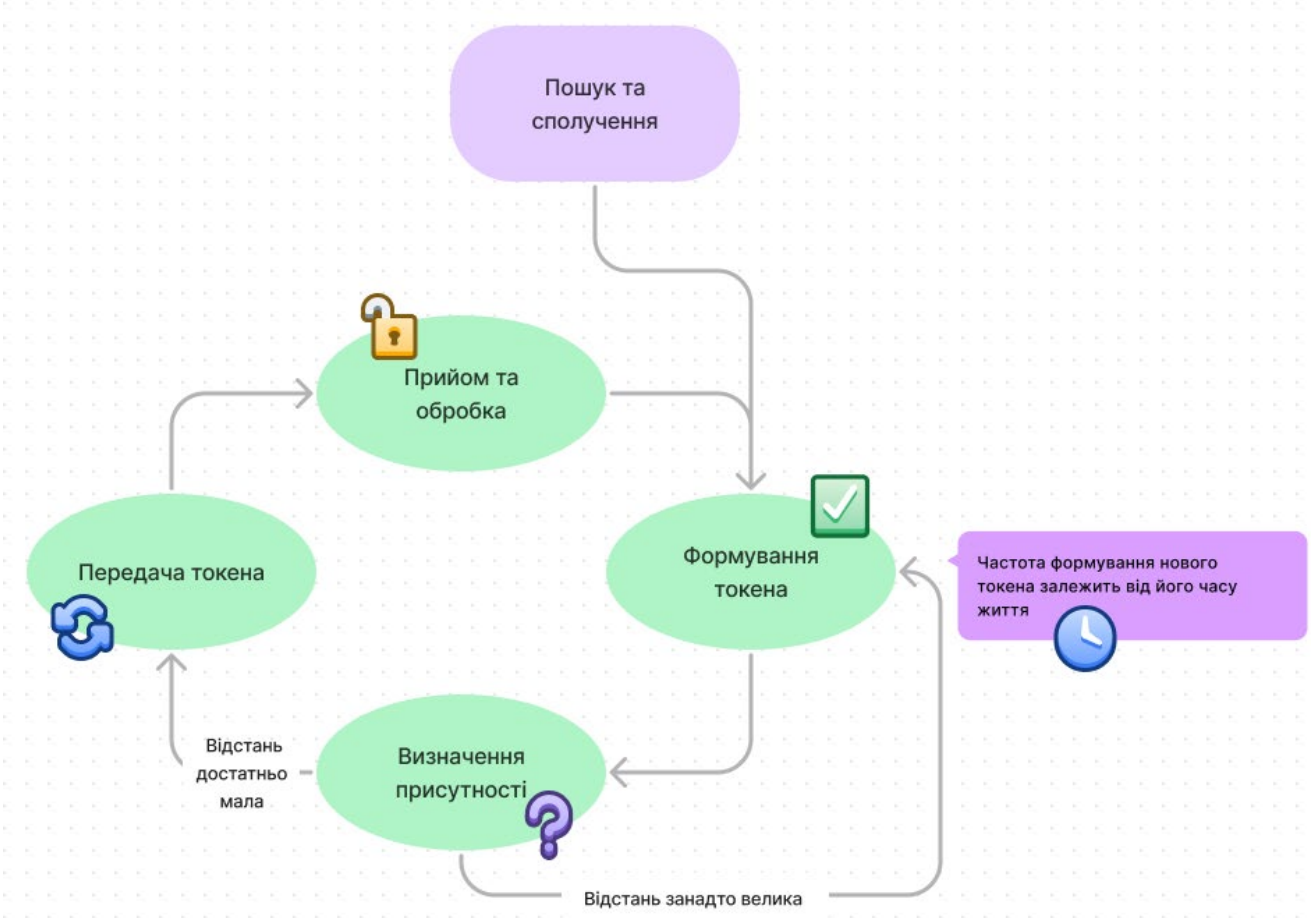


Рисунок 2.2 – Послідовність процедур при формуванні та обміні токеном

2.3 Структура мобільного додатку

Мобільний додаток реалізує функції формування токена та визначення відстані до ПК. Структура мобільного додатка зображено рисунку 2.3

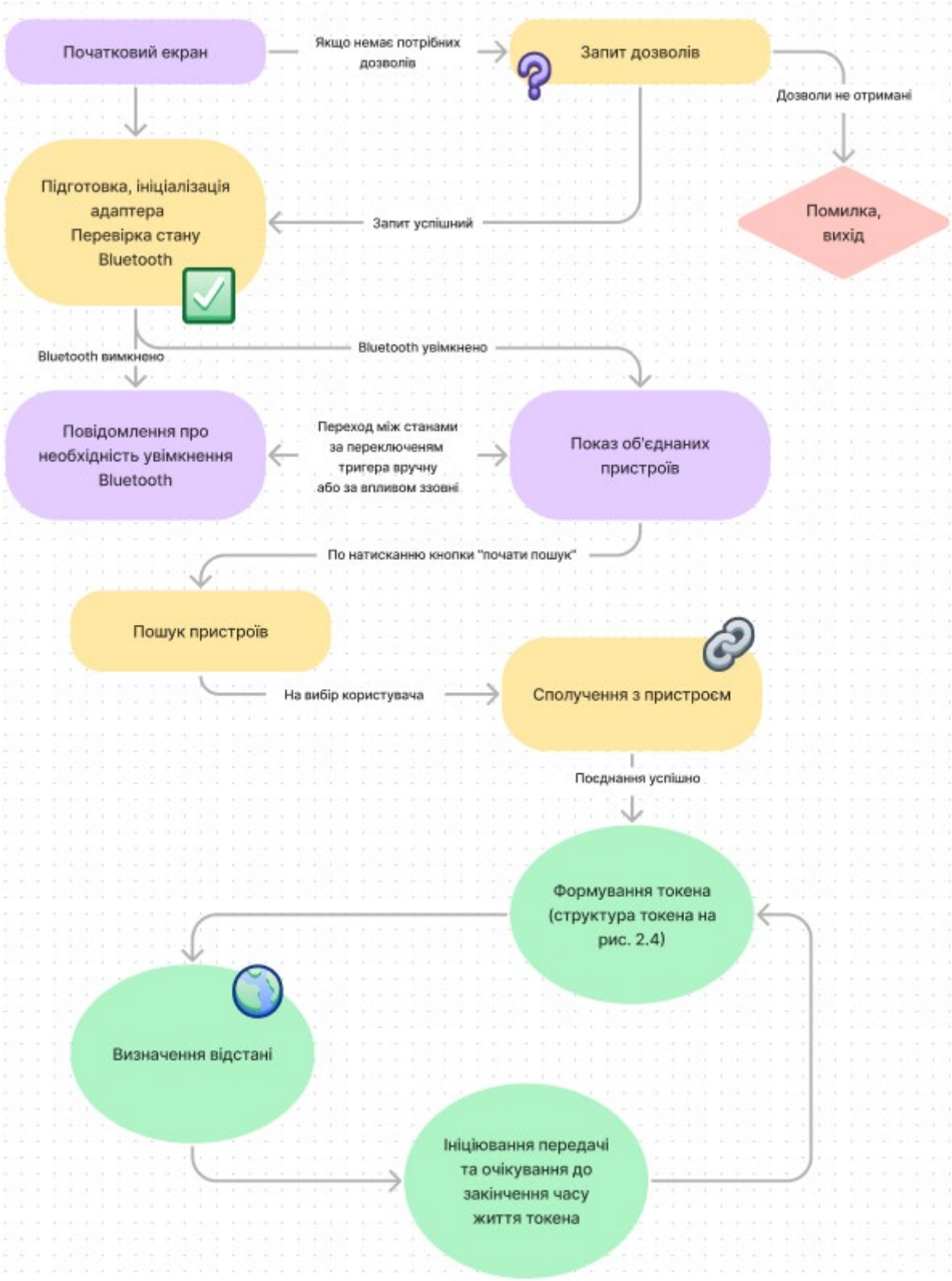


Рисунок 2.3 – Узагальнена послідовність виконання мобільної частини комплексу

Основні процедури програми наведені нижче.

Запит дозволів. Для коректної роботи програми необхідно стандартними засобами ОС Android запитати у користувача згоду на використання деяких ресурсів системи, які ОС вважає чутливими з безпеки;

Підготовка, ініціалізація адаптера, перевірка стану Bluetooth. Тому що для роботи необхідно використовувати бездротове з'єднання - перший крок - визначити, чи воно доступне і включений Bluetooth, якщо ні - потрібно надати користувачеві можливість його включити, якщо він хоче використати систему у даний момент;

Пошук пристроїв. Для відображення списку пристроїв для підключення відбувається сканування всіх пристроїв, які мають сумісний Bluetooth адаптер неподалік користувача

Сполучення з пристроєм. Запит обробляється стандартними засобами ОС

Формування токена. Для створення використовується бібліотека Java JWT

Визначення відстані. Для визначення відстані використовується рівень сигналу RSSI (received signal strength indicator). Детальний розгляд методів визначення відстані див. розділ 2.5

Ініціювання передачі та очікування до закінчення часу життя токена. Токен передається пристрою, зв'язок з яким був організований раніше. Токен має кінцевий час життя, тому для того, щоб користувач весь необхідний час був авторизований необхідно періодично оновлювати токен. Для цього незадовго до закінчення часу життя використаного токена потрібно розпочати формування нового.

2.4 Структура JWT токену

JSON Web Token (JWT) — це відкритий стандарт для створення токенів доступу на основі формату JSON. [5] Зазвичай використовується для передачі даних авторизації в клієнт-серверних додатках. Токени створюються сервером, підписуються секретним ключем і передаються клієнту для того, щоб він міг підтвердити свою особистість. Токен JWT складається з заголовка (header),

корисного навантаження (payload) і підпису. Перші два елементи – це JSON об'єкти, які відповідають визначеній стандартом структурі. Третій елемент обчислюється на основі перших і залежить від обраного алгоритму, потребує паролю, у цьому проекті у якості пароля для підпису використовується ідентифікатор пристрою. Токени можуть бути представлені компактніше (JWS/JWE Compact Serialization): заголовок та корисне навантаження кодується алгоритмом Base64-URL, після чого додається підпис та розділові крапки («.»). Структура токену наведена на рисунку 2.4.

Рисунок 2.4 – Основні структурні одиниці токену

2.5 Визначення відстані між пристроями Bluetooth

Специфікації Bluetooth версій 3.0 і нижче не надавали жодних засобів визначення відстані. Ґрунтуючись на наявності чи відсутності стабільного сигналу можна оцінити лише перебуває користувач у зоні покриття чи ні (радіус

близько 5-10 м у приміщеннях), тому пристрої зі стандартом Bluetooth нижче ніж 4.0 не можуть використовуватися у проектуємій системі.

Починаючи зі специфікації версії 4.0, крім класичної реалізації у стандарті з'явилася версія з низьким енергоспоживанням “BLE”, яка передає в широкомовних рекламних пакетах показник RSSI, який можна використовувати для визначення відстані з допустимою для цього завдання похибкою. Згідно з дослідженням [6] показник RSSI (рисунок 2.5) змінюється набагато плавніше ніж при використанні XBee і незначно плавніше ніж при використанні Wi-Fi, тобто, якщо розглянути величину RSSI як плавно спадаючу можна оцінити відстань з прийнятною точністю.

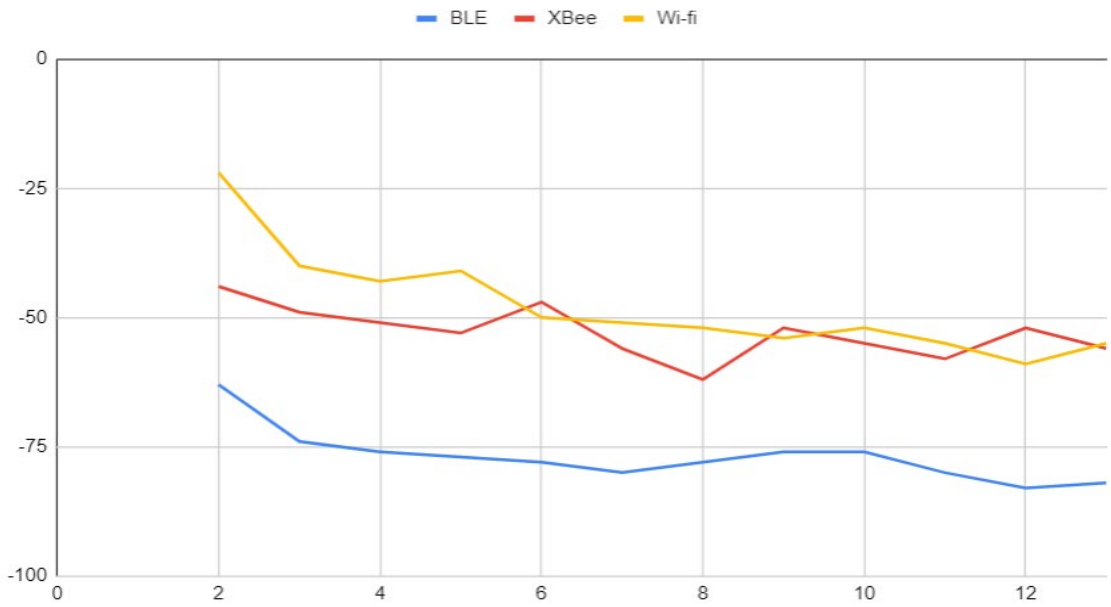


Рисунок 2.5 – Графік залежності RSSI від відстані

Для визначення відстані використовується формула 2.1

$$D = 10^{\frac{Pm-RSSI}{10*N}} \quad (2.1)$$

де: D - відстань

Pm - потужність на відстані 1 метр (зазвичай приймається за -69)

RSSI - значення RSSI передане пристроєм

N - фактор оточення (в діапазоні від 2 до 4, для приміщень ~3)

2.6 Структура програми, що реалізує аутентифікацію на ПК

У програмі передбачена функція трансляції даних у режимі Bluetooth-маячка, зв’язування з мобільним додатком, перевірку токену та авторизацію користувача. Структура програми зображена на рисунку 2.6.

Для успішної авторизації програма виконує кроки, опис яких наведено нижче:

Ініціалізація Bluetooth. Потрібно перевірити чи підключений відповідний пристрій, а також провести підготовчі заходи для подальшого використання його в програмі.

Запуск мовлення в режимі маячка. Якщо в комп'ютері встановлено BLE-сумісний пристрій, то програма почне посилати рекламні пакети в широкомовному режимі, для того, щоб телефон міг його виявити, тобто починає працювати як маячок.

Рекламні пакети це короткі повідомлення, що транслюються на виділених каналах. Структура рекламного повідомлення показана рисунку 2.7.

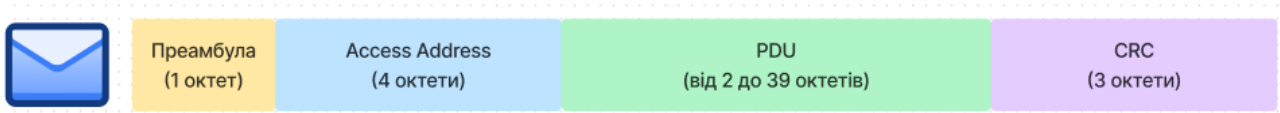


Рисунок 2.7 – Складові рекламного пакету

Преамбула складається з послідовності 10101010, яка служить для синхронізації передавача та приймача.

Access Address - призначений для того, щоб пристрої розуміли, кому направлений BLE пакет. Це можна порівняти з кодом доступу, якщо цей код не знайомий – пакет ігнорується. На всіх рекламних каналах він однаковий (0x8E89BED6), тому всі пристрої на каналі бачать один одного.

PDU - пакет даних довжиною від 2 до 39 октетів (довжина відображена в заголовку пакета, перші 16 біт PDU)

CRC – контрольна сума

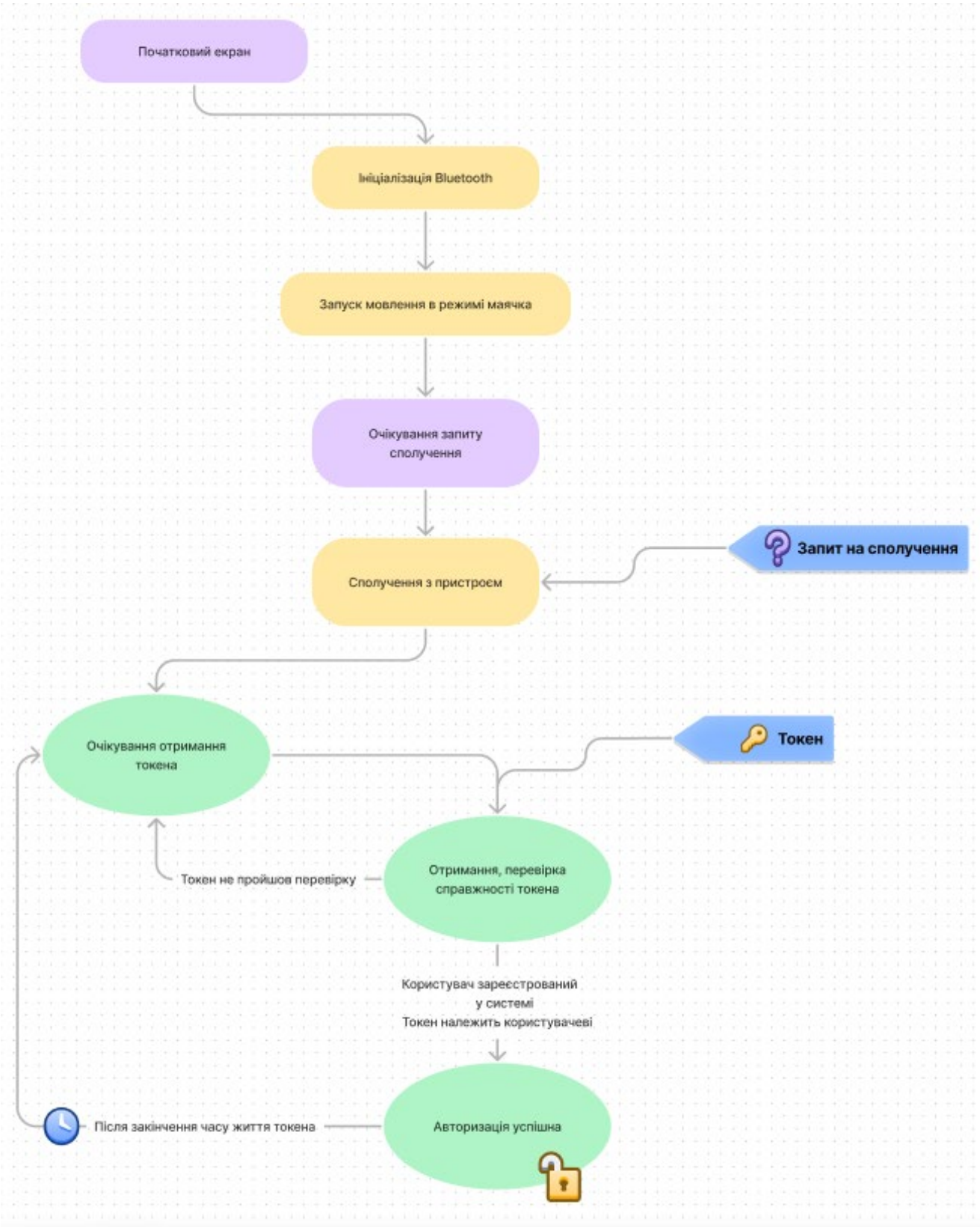


Рисунок 2.6 – Узагальнена послідовність виконання програми на ПК

Сполучення з пристроєм. Комп'ютер отримує від смартфона запит на сполучення. Якщо сполучення виконується вперше користувачеві потрібно ввести або звірити PIN-коди на пристроях. Якщо сполучення відбулося успішно програма переходить у стан очікування отримання токену

Отримання, перевірка справжності токена. Для перевірки дійсності токена необхідно, щоб сервер аутентифікації та програма мали спільний ключ (генерується під час первинної конфігурації системи). Коли користувач передає токен, програма може створити для відкритої частини токена свій підпис за тим же алгоритмом, яка, у випадку, якщо токен валідний збігається з підписом токена переданого користувачем. Якщо підписи не збігаються, це може бути ознакою потенційної атаки.

Авторизація. Якщо перевірка токена пройшла успішно, користувач є в базі, то він отримує доступ до системи, що захищається (у цій демонстраційній програмі отримує можливість вводити текст у поле)

2.7 Можливі загрози системі

У протоколі Bluetooth на сеансовому рівні реалізований менеджер безпеки з'єднання, яке встановлюється при передачі токена (внутрішнього токена для авторизації каналу передачі). Проте протоколи безпеки Bluetooth мають опції, які не виключають всіх факторів ризику, що несе із собою канал передачі. Зловмисник може не тільки прослуховувати трафік, але й здійснювати так звану атаку Man in the Middle (атака "людина посередині") [7], у випадку, якщо в процесі розробки системи було обрано неправильний рівень безпеки. Усього їх чотири, від рівня 1, який взагалі не підтримує жодного захисту, до рівня 4, що забезпечує авторизоване з'єднання зашифроване за протоколом ECDHE (Elliptic Curve Diffie-Hellman), але не всі рівні підтримуються старішими специфікаціями Bluetooth, тому для кожного конкретного випадку потрібно вибирати найвищий рівень захисту, який забезпечує сполучення (для сполучення обов'язковий авторизований канал зв'язку). Атака на такий канал значно складніша і канал можна вважати захищеним. У розробленій авторкою системі сполучення є

обов'язковим для обміну токеном, а вибором підтримуваного рівня безпеки займається ОС, тому канал зв’язку можна вважати достатньо безпечним.

Стандарт JWT токенів сам не забезпечує належного захисту від MITM атак. Наприклад типовий MITM атакою є заміна алгоритму підпису на “none” і тоді непідписаний токен вважається валідним, отже зловмисник може довільно його міняти. Для того, щоб запобігти такій атаці, необхідно вибирати такі засоби розробки (бібліотеки/фреймворки), в яких реалізовано відкидання токенів без підпису, або реалізувати цю функцію вручну. Але типовим способом забезпечення безпеки токенів є захищене з'єднання, що реалізує Bluetooth.

2.8 Висновки за розділом

У розділі представлена структура системи ідентифікації та аутентифікації, що розробляється. Вона складається з двох незалежних програм - сервера аутентифікації (мобільний додаток) і сервера програми (базова реалізація для ПК).

Розглянуто структуру використовуваного токена, процедури його формування та перевірки та наведено алгоритм визначення присутності.

Наведені рекомендації для підвищення безпечності використання токену.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСУ

3.1 Вибір інструментів для розробки

Для розробки сервера аутентифікації обрано мову Java [8], оскільки в основі цільової ОС Android лежить реалізація віртуальної машини Java [9], тобто ця мова буде виконуватися максимально нативно, без трансляції, ще одного шару віртуалізації або портування засобами Android Native Development Kit.

Як середовище розробки було обрано Android Studio [10] як найбільш підтримувана IDE, тому що її розробником є Google, який також розробляє ОС. Її основні переваги

- Візуальний редактор дизайну програми
- Вбудований швидкий емулятор для налагодження
- Наявність системи IntelliSense, яка підсвічує код та доповнює його під час введення, а також дає рекомендації щодо оптимізації та відповідності стандартам останніх версій ОС

Для розробки програми для ПК авторкою роботи вибрана середа розробки Visual Studio 2022, мова програмування C#, тип проекту Universal Windows Platform [11]. Метою платформи є створення універсальних програм, що запускаються на Windows для ПК та мобільних платформ або Windows IoT. Кросплатформеність та орієнтованість на IoT забезпечують просту інтеграцію технології Bluetooth та BLE, а також через вимоги мобільних платформ підвищується безпека, тому що для доступу до ресурсів пристрою (наприклад, доступ до мікрофону, геоданих, веб-камери, Bluetooth) здійснюється тільки із запитом дозволу від користувача. Середовище та мова розробки обрано за кількома критеріями:

- Підтримка розробки UWP додатків
- Інтуїтивно зрозумілий інтерфейс IDE
- Підтримка IntelliSense
- Проста реалізація необхідних можливостей мовою
- Простота налагодження

Всі ці критерії відповідають мові C# з Visual Studio 2022 IDE.

3.2 Розробка мобільного додатку

Програмний код серверу аутентифікації знаходиться у додатку А.

Робота додатку передбачає наступний ряд функцій:

- Отримання дозволів на використання апаратних ресурсів
- Пошук доступних для сполучення пристроїв
- Забезпечення сполучення з ПК
- Визначення присутності смартфона у зоні дозволеної аутентифікації
- Формування JWT токена
- Передача токена
- Формування нового токена за таймером часу життя

Інтерфейс додатку наведено на рисунку 3.1.

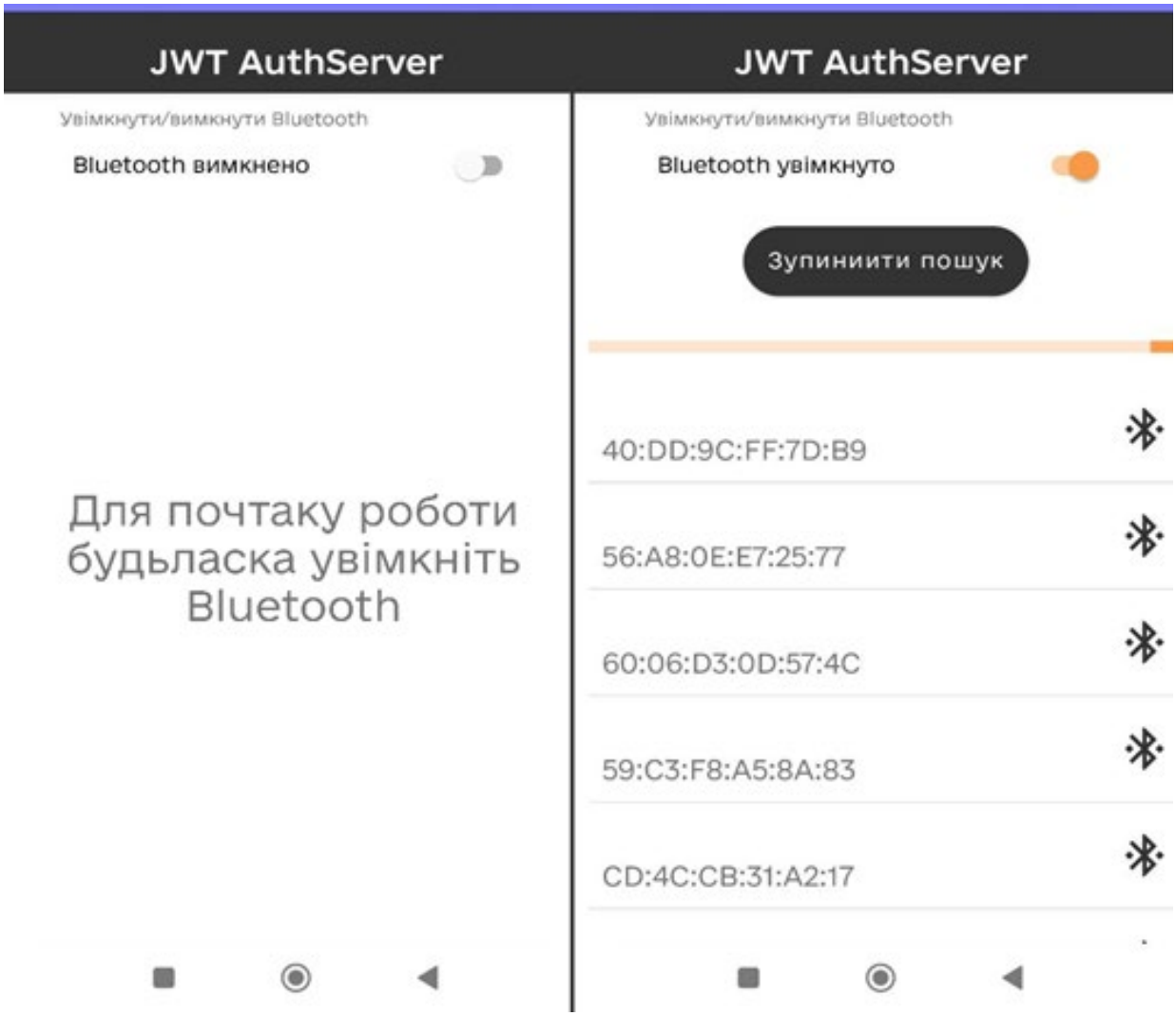


Рисунок 3.1. – Інтерфейс мобільної частини системи

Основний екран додатку залежить від того, чи увімкнутий Bluetooth на початку роботи додатка. Якщо Bluetooth вимкнено, то користувач повинен побачити допоміжне повідомлення і увімкнути Bluetooth. Якщо Bluetooth увімкнено на екрані відображаються раніше прив'язані пристрої, та кнопка для початку пошуку. Для реалізації роботи з BLE використовується бібліотека blessed-android [12] тому що вона реалізує високий рівень абстракції, правильно використовує потоки без додаткової участі розробника та робить програмування для BLE максимально прозорим.

Також для узгодження виконання програми в часі та забезпечення більш структурованого та ясного коду використовуються базові засоби RxAndroid, реалізації реактивного програмування на базі Android Java.

Основні процедури та функції програми представляють собою переважно лінійні алгоритми, які виконуються асинхронно, тому авторка роботи віддала перевагу текстовим описам функціонування, а не блок-схемам. Далі наведений перелік та опис цих процедур.

Отримання дозволів на використання апаратних ресурсів. Для цього насамперед потрібно створити перелік необхідних дозволів «neededPermissions». А згодом, використовуючи стандартні засоби ОС виконати запит на отримання дозволів. У випадку вдалого отримання дозволів відбувається перехід до наступного кроку.

Пошук доступних для сполучення пристроїв. Сканер шукає пристрої відповідно при виявленні нові пристрої виводяться на екран у вигляді списку. З цього списку користувач може вибрати потрібний пристрій по кліку на необхідний.

Забезпечення сполучення з ПК. Насамперед відбувається запит на підключення. Якщо підключення вдале додаток продовжує свою роботу, якщо ні, користувач може спробувати виконати сполучення знову.

Визначення присутності смартфона у зоні дозволеної аутентифікації. По-перше необхідно просканувати необхідний пристрій. Коли сканування завершиться вдало буде отримано об'єкт «ScanResult» у якому нам цікаве поле

.rssi, коли ми отримали показник RSSI ми можемо визначити відстань за формулою (див. формула 2.1)

Формування JWT токена. У процесі формування токена до нього додається два поля у payload токену – поля username з визначеним для користувача ім’ям та deviceType із значенням android, потім токен підписується паролем з deviceID та представляється в компактному виді.

Передача токена. Токен передається у відповідний BLE сервіс на ПК.

Формування нового токена за таймером часу життя. За узгодження виконання у часі відповідає таймер, він починає відлік при успішній передачі токена. Кожні 30000 мс (30с) починається формування нового токена (це трохи менше за час життя токену, бо потрібен додатковий час для відправки та прийому). Якщо за 2000000 мс (33,3 хв) не сталося успішної передачі токена програма переходить у стан очікування.

3.3 Розробка демонстраційної програми для ПК

Програмний код наведено у додатку Б.

Робота додатку передбачає наступний ряд функцій:

- Широкомовна трансляція рекламних повідомлень
- Отримання токену
- Аутентифікація користувача за списком

Інтерфейс додатку наведено на рисунку 3.2.

Рисунок 3.2 – Інтерфейс програми для ПК

Основний екран додатку демонструє необхідну інформацію та відображає поле текстового вводу, яке являє собою модель будь якої дії, яка потребує аутентифікації, у подальшій розробці прототипа може бути замінена захищеною базою даних, веб-додатком, тощо. Для початку роботи користувач повинен дозволити виявлення пристрою, що увімкне широкомовне транслювання пакетів.

Якщо комп’ютер користувача не має BLE- сумісного пристрою кнопка буде неактивною і статус виявлення зміниться на «BLE» не підтримується.

Для реалізації роботи з BLE використовується бібліотека ble.net.

Далі подано детальний опис найбільш значущих модулів та їх спрощена програмна реалізація (усі фрагменти коду у підрозділі наведені з додатку Б)

Широкомовна трансляція рекламних повідомлень. Для ініціалізації широкомовного режиму необхідно створити об’єкт «GattServiceProvider». Коли службу буде визначено, наступний крок – публікація служби. Це інформує ОС про те, що служба має бути повернена у разі запиту на виявлення віддаленими пристроями.

Отримання токену. Коли віддалений пристрій намагається записати значення характеристики, виникає подія «ReadRequested» з подробицями про віддалений пристрій, характеристику та її значення.

Відразу після отримання токена зводиться таймер на 40000 мс (40с) (на 10 секунд більше, ніж таймер відправки) після закінчення якого виконується вихід користувача із системи. Якщо раніше був отриманий новий токен – виходу з системи не відбувається

Аутентифікація користувача за списком. Для прототипу, як база користувачів виступає xml файл в який у відкритому вигляді записано ім'я кожного користувача та ІД його пристрою. У реальній системі потрібна реалізація кешування ІД або шифрування бази даних.

Для обробки токена використовується бібліотека jose-jwt

Після отримання токена необхідно виділити з нього корисне навантаження.

Після виділити з корисного навантаження ім'я користувача. Коли рядок ім'я користувача буде отримано необхідно перевірити, чи це ім'я користувача в базі

На малюнку 3.3 відображено структуру бази користувачів

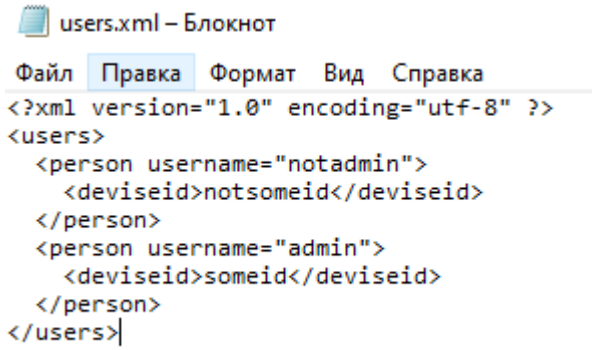


Рисунок 3.3 – База з двома демонстраційними користувачами

Якщо користувач є в базі строка deviseid набуде значення ідентифікатора пристрою, а якщо користувача в базі немає – буде пустою і статус авторизації зміниться на «Помилка, користувач не знайдений»

Наступний крок для існуючого користувача – розкодувати його токен.

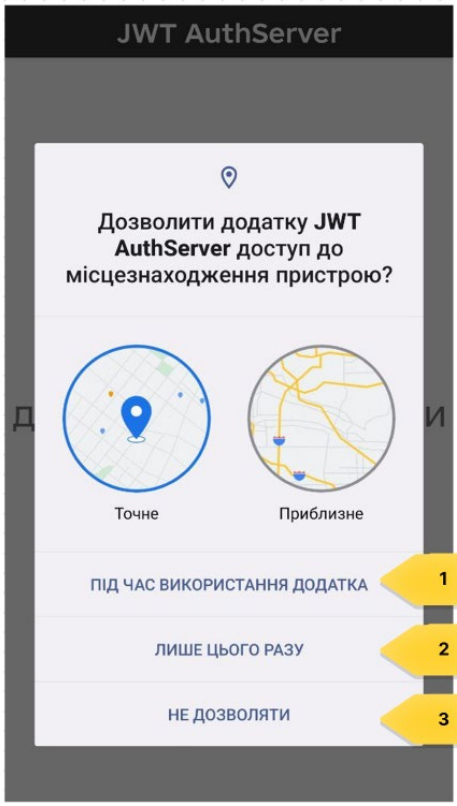
Якщо не виникла помилка – токен справжній, і після процедури перевірки часу життя можна аутентифікувати користувача.

3.4 Перевірка працездатності комплексу та інструкція користувача

Мобільний додаток повинен реалізовувати наступні функції

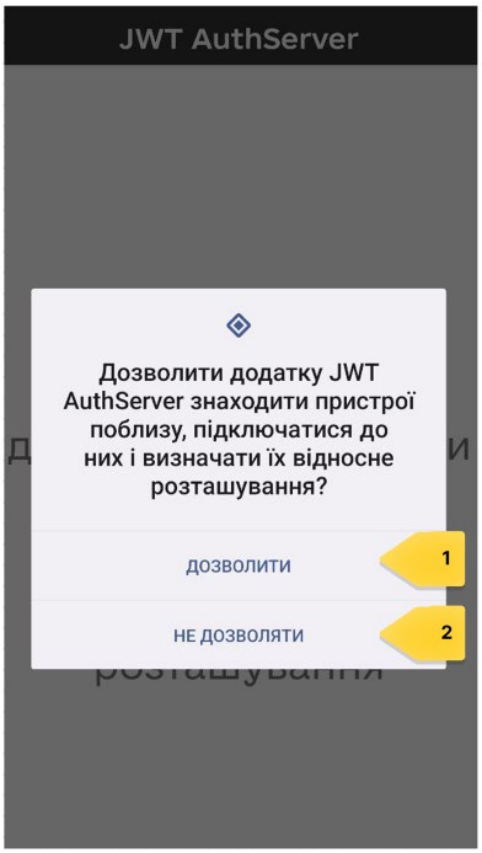
- Отримання дозволів
- Пошук пристроїв
- Підключення до пристрою та передача токену

Перший крок для користувача при встановлені системи – дозволити використання системних ресурсів, інтерфейс наведено на рисунках 3.4 та 3.5.



кнопка дозволу використання локації весь час(1); кнопка дозволу використання локації одноразово(2); кнопка відхилення запиту дозволу(3)

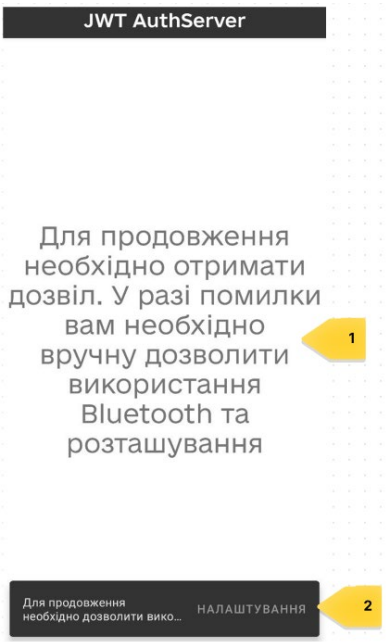
Рисунок 3.4 – Діалог запиту дозволу на використання локації



кнопка дозволу(1); кнопка відхилення запиту дозволу(2)

Рисунок 3.5 – Діалог запиту дозволу на знаходження пристроїв поблизу

Якщо користувач відхилив дозвіл йому буде продемонстроване повідомлення з поясненням, що дозвіл дійсно необхідний, повідомлення показане на рисунку 3.6.



повідомлення про необхідність дозволу(1); кнопка повторного запиту дозволів(2)

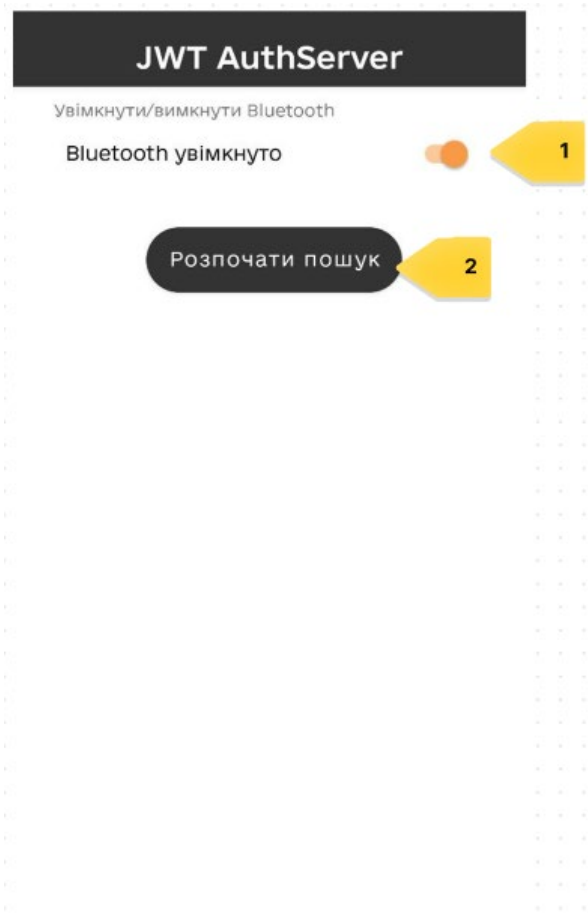
Рисунок 3.6 – Повідомлення про необхідність дозволу

Після отримання необхідних ресурсів додаток переходить до основного режиму роботи, якщо Bluetooth вимкнено додаток демонструє екран наведений на рисунку 3.7

перемикач стану Bluetooth(1)

Рисунок 3.6 – Стан роботи «Очікування вмикання Bluetooth»

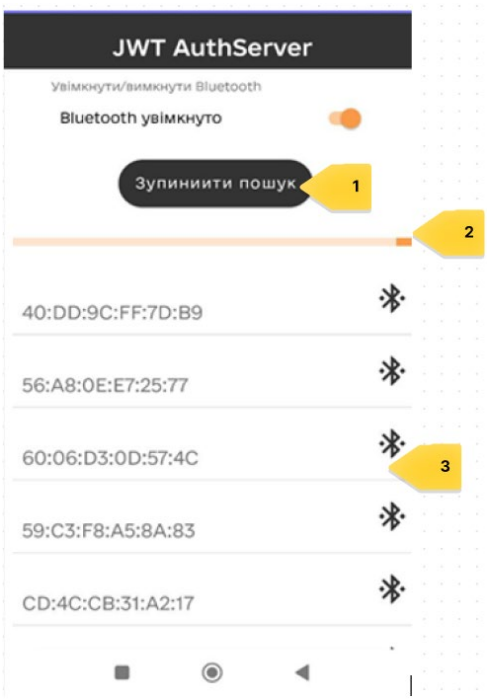
Коли користувач вмикає Bluetooth (із додатку, або із інтерфейса системи, або якщо додаток вмикається коли Bluetooth вже увімкнено) програма демонструє екран наведений на рисунку 3.8



перемикач стану Bluetooth(1); кнопка пошуку пристроїв(2)

Рисунок 3.6 – Стан роботи «Bluetooth увімкнуто»

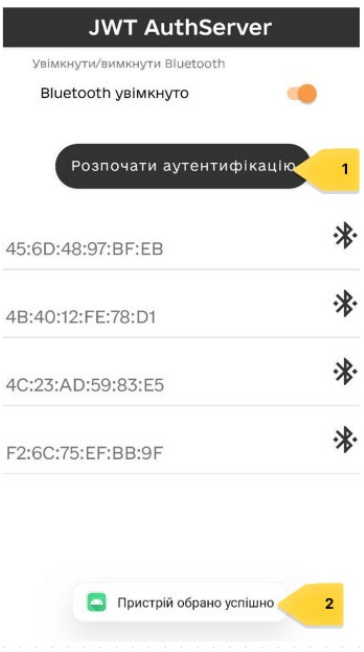
Якщо цільового пристрою немає у списку потрібно провести сканування. По натисненню кнопки «Розпочати пошук» додаток починає сканувати пристрої поблизу. Зовнішній вигляд та опис сканування наведено на рисунку 3.7.



кнопка зупинити пошук(1); індикатор сканування(2); знайдені пристрої(3)

Рисунок 3.7 – Стан роботи «Сканування пристроїв»

Коли сканування було завершено, користувач повинен натиснути на рядок, де представлений потрібний пристрій. Коли він це зробить він отримає повідомлення наведене на рисунку 3.8 та кнопка змінить свій стан.



кнопка аутентифікації(1); повідомлення(2)

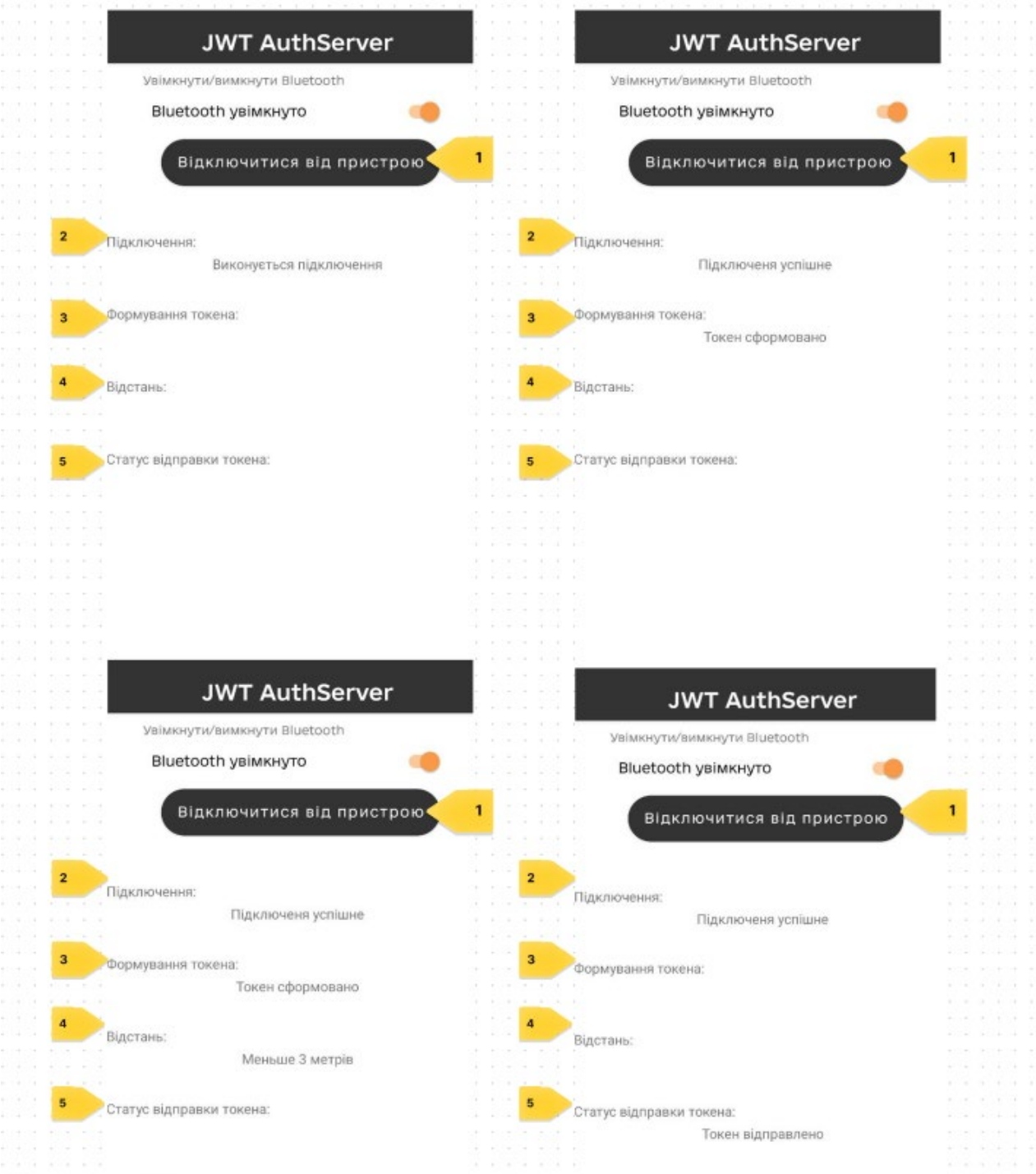
Рисунок 3.8 – Інформаційне повідомлення

По натисненню кнопки «Розпочати аутентифікацію» додаток ініціює сполучення з обраним пристроєм. Якщо в процесі сполучення виникла помилка користувач отримає відповідне повідомлення, як показано на рисунку 3.9

спливаюче повідомлення(1)

Рисунок 3.9 – Помилка сполучення

Якщо ж сполучення виконано успішно розпочинається цикл формування та передачі токену. На кожному етапі користувачеві демонструється нині виконувана операція. Демонстрація циклу роботи наведено на рисунку 3.10. Якщо користувач натисне кнопку «Від’єднатися від пристрою» додаток проведе від’єднання та перейде у стан «Bluetooth увімкнуто»



кнопка від’єднання від пристрою(1); стан підключення(2); стан формування токена(3); стан визначення відстані(4); стан передачі токена(5)

Рисунок 3.10 – Робота з токеном

Програма для ПК повинна реалізовувати наступні функції

- Перевірка адаптера на сумісність
- Широкомовний режим
- Отримання токену

- Дозвіл аутентифікованому користувачеві використовувати поле вводу

Після запуску програми виконується перевірка наявності сумісного з технологією BLE адаптеру, якщо адаптер не знайдено, або він не сумісний з використанням BLE користувач отримає повідомлення наведене на рисунку 3.11.

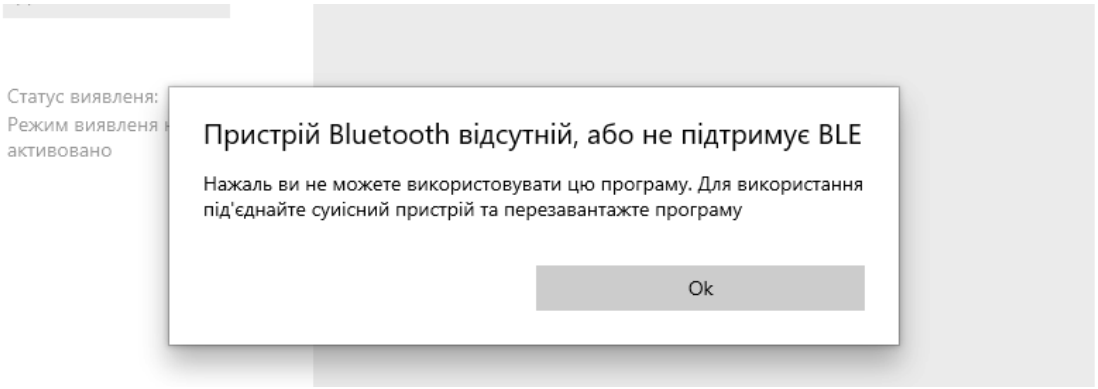
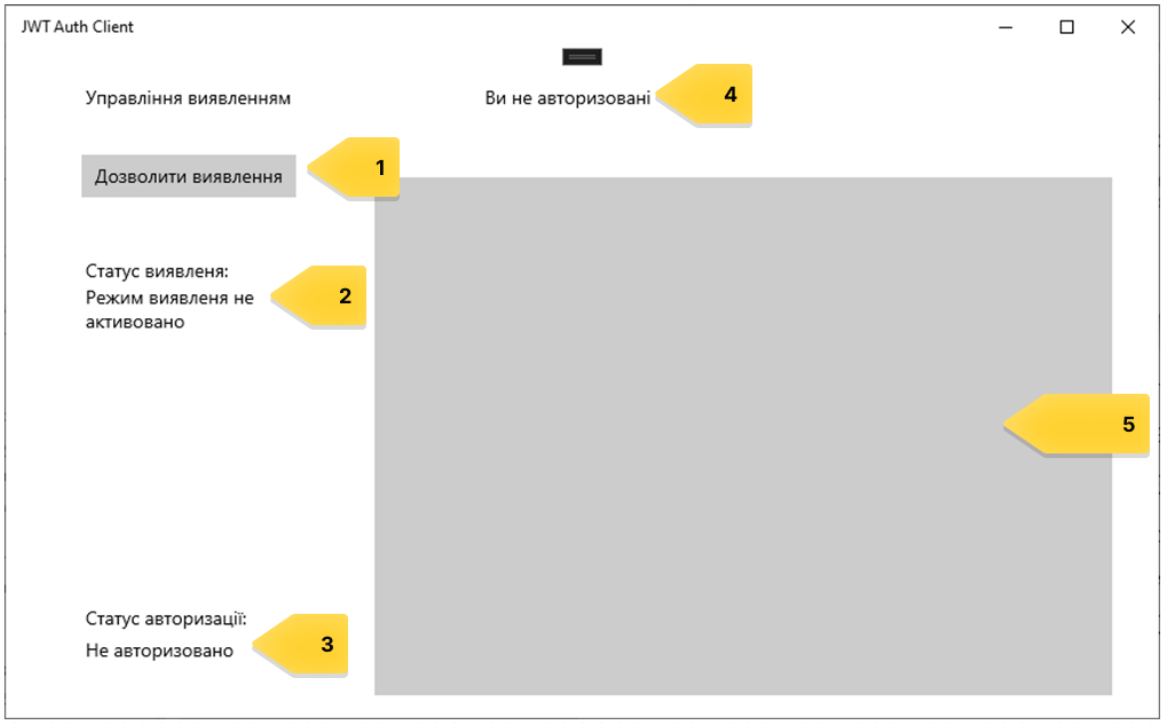


Рисунок 3.11 – Не вдалося знайти сумісний адаптер

У випадку, коли адаптер знайдено користувачу пропонується початковий екран програми, як на рисунку 3.12.



кнопка запуску широкомовного режиму(1); статус виявлення(2); статут авторизації(3); повідомлення для користувача(4); неактивне поле вводу(5)

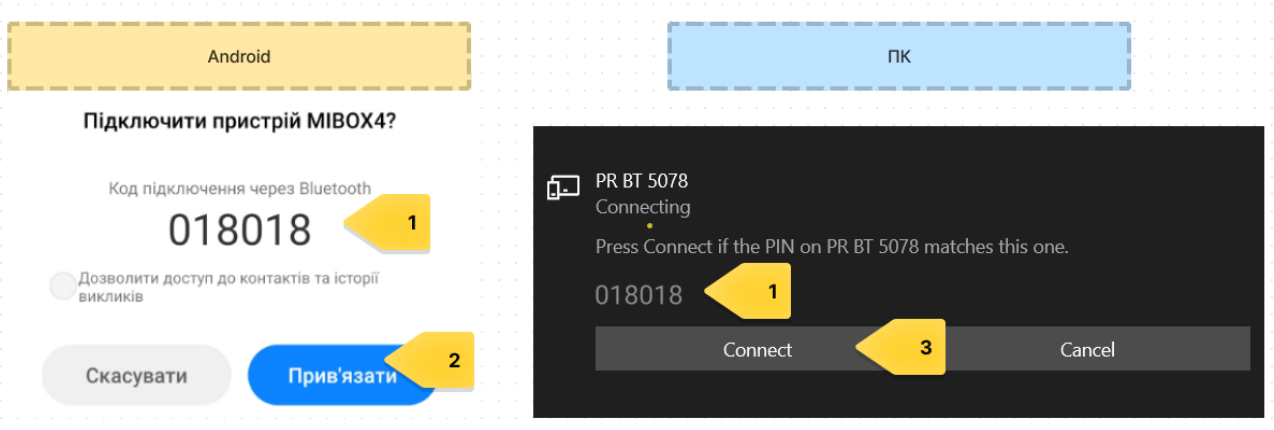
Рисунок 3.12 – Основний екран програми

Наступний крок – увімкнення широкомовного режиму, для цього користувачеві потрібно клікнути по кнопці «Дозволити виявлення». Коли широкомовне розповсюдження рекламних пакетів розпочнеться програма набуде вигляду відображеного на рисунку 3.13.

кнопка вимкнення широкомовного режиму(1); статус виявлення(2);

Рисунок 3.13 – Широкомовна відправка повідомлень увімкнена

Коли мобільний додаток ініціює сполучення у перший раз (якщо ПК і мобільний пристрій не були спарені раніше) ви побачите стандартний діалог сполучення який наведено на рисунку 3.14



ПІН-код, повинен співпадати для успішного сполучення(1); кнопка сполучення(2,3);

Рисунок 3.14 – Вигляд діалогу запиту сполучення на смартфоні та ПК

Після встановлення з’єднання ПК повинен отримати токен і перевірити його. Якщо токен має некоректний підпис, або сплинув статус авторизації зміниться як на рисунку 3.15.

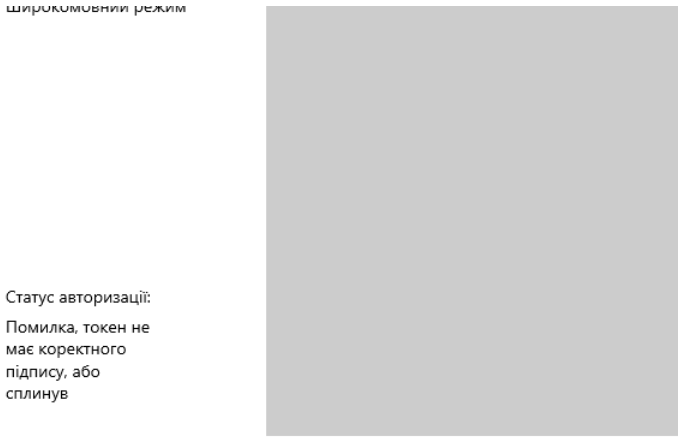


Рисунок 3.15 – Помилка обробки токена

Після отримання коректного токену відбувається аутентифікація та користувачеві дозволяється використовувати програму у повному обсязі, що відображено на рисунку 3.16

вітальне повідомлення(1); статус авторизації(2); активоване поле вводу(3);

Рисунок 3.16 – Користувач аутентифікований

3.5 Висновки за розділом

У даному розділі був зроблений вибір інструментів розробки, за допомогою яких розроблений мобільний додаток, реалізуючий серверну частину комплексу аутентифікації, визначення відстані до ПК, формування та обміну токеном. Також розроблено демонстраційну програму для ПК, яка відображає базові функціональні елементи клієнту комплексу, отримує токен, перевіряє його, та проводить аутентифікацію користувача за наявності у базі.

Наведено інструкцію із використання розробленої системи аутентифікації. Також була перевірена працездатність обох частин системи у різних випадках, наведені описи та ілюстрації усіх станів додатків.

ВИСНОВКИ

У роботі розроблений комплекс програмних засобів майнової ідентифікації та аутентифікації з використанням смартфону та бездротового з’єднання.

Під час виконання роботи було розглянуто та впроваджено до системи спосіб визначення відстані при використанні бездротових пристроїв.

Розроблений прототип системи може бути масштабовано для забезпечення процедури аутентифікації у різних системах, пристроях, веб-апплікаціях.

Розглянуті різні бездротові технології та порівняно їх між собою за основними ознаками та характеристиками, включаючи можливість отримання інформації про відстань до користувача.

Описано структуру та організацію розроблюваної системи. Наведено складові елементи та їх призначення. Розроблено принципи взаємодії додатків. Визначено функції android-додатку та ПК програми.

Обрано інструменти для розробки: середовища та мови програмування, бібліотеки, за допомогою яких реалізовано деяку частину функціоналу.

Розроблено програмне забезпечення, виконано перевірку його працездатності та наведено інструкцію для користувача.

ПЕРЕЛІК ПОСИЛАНЬ

1. Turner, "Digital Authentication: The Basics" [Електронний ресурс] – Режим доступу: https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics

2. Authentication: From Passwords to Public Keys First Edition. [Текст] – Richard E. Smith, — 2002.

3. SAFETY & SECURITY Making you safer with 2SV [Електронний ресурс] – Режим доступу: https://blog.google/technology/safety-security/reducing-account-hijacking/

4. Хорев П.Б. Методы и средства защиты информации в компьютерных системах [Текст] – Учеб. пособие для студ. высш. учеб. заведений. — М.: Академия, 2005

5. Sebastián Peyrott JWT Handbook [Текст] – Sebastián Peyrott, Auth0 — 2019.

6. Radio Frequency-Based Indoor Localization in Ad-Hoc Networks [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/317150846_Radio_Frequency-Based_Indoor_Localization_in_Ad-Hoc_Networks

7. An active man-in-the-middle attack on bluetooth smart devices [Текст] – February 2018 International Journal of Safety and Security Engineering

8. Oracle Java [Електронний ресурс] – Режим доступу: https://www.oracle.com/cis/java/

9. Android Runtime (ART) and Dalvik [Електронний ресурс] – Режим доступу: https://source.android.com/devices/tech/dalvik

10. Android studio [Електронний ресурс] – Режим доступу: https://developer.android.com/studio

11. Что такое приложение UWP? [Електронний ресурс] – Режим доступу: https://docs.microsoft.com/ru-ru/windows/uwp/get-started/universal-application-platform-guide

12. Weliem/blessed-android [Електронний ресурс] – Режим доступу: https://github.com/weliem/blessed-android