Галицький фаховий коледж імені В'ячеслава Чорновола
відділення комп'ютерних технологій
циклова комісія інформатики та комп'ютерних дисциплін

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач відділенням
комп'ютерних технологій
Наталія СТЕФУРАК _____
(підпис)
«____» _____ 2025р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи
освітньо-професійного ступеня «фаховий молодший бакалавр»
зі спеціальності 123 «Комп'ютерна інженерія»

на тему:
«Система керування дверним замком на основі розпізнавання відбитків пальців»

Студент групи КІ-41	Богдан ТАЗЮК	_____ (підпис)
Керівник роботи	Василь ПАВЛЮС	_____ (підпис)
Консультанти:		
з техніко-економічного обґрунтування	Любов МЕЛЕНЧУК	_____ (підпис)
нормоконтролер	Ольга СЛЄПЦОВА	_____ (підпис)

Тернопіль – 2025

Галицький фаховий коледж імені В'ячеслава Чорновола
відділення комп'ютерних технологій
циклова комісія інформатики та комп'ютерних дисциплін

ЗАТВЕРДЖУЮ
Завідувач відділення
комп'ютерних технологій
Наталія СТЕФУРАК / _____/
підпис
«___»_____2024р

ЗАВДАННЯ

на кваліфікаційну роботу
на здобуття освітньо-кваліфікаційного рівня «фаховий молодший бакалавр»
студенту Тазюку Богдану Олександровичу
(прізвище, ім'я та по-батькові студента)

1. Тема кваліфікаційної роботи: «Система керування дверним замком на основі розпізнавання відбитків пальців», затверджено наказом по коледжу
Від "25" листопада 2024р., №253а-н
2. Термін здачі студентом завершеної роботи "26" червня 2025р.
3. Вихідні дані до роботи: *сучасні технології біометричної ідентифікації, принципи роботи мікроконтролерів ESP8266, серводвигунів і сканерів відбитків пальців, існуючі рішення у сфері безконтактного доступу, технічне завдання на створення системи керування замком з Telegram-сповіщенням.*
4. Перелік питань, які повинні бути розроблені в роботі:
а) основна частина: *аналіз предметної області систем контролю доступу, опис апаратної та програмної реалізації проєкту, вибір компонентів, побудова логіки роботи системи, реалізація алгоритму зчитування та обробки відбитків пальців, створення Telegram-сповіщення, тестування працездатності.*
б) техніко-економічне обґрунтування: *огляд ринку подібних біометричних систем, аналіз вартості окремих компонентів, оцінка загальної вартості проєкту, обґрунтування доцільності використання створеної системи*.

5. Перелік графічного матеріалу *структурна схема пристрою, блок-схема алгоритму роботи, схема з'єднання компонентів, фото компонентів, фотографії макета пристрою в зібраному вигляді, скріншоти роботи Telegram-бота.*

6. Консультанти роботи:

Розділ	Консультанти	Підпис, дата	
		Завдання видано	Завдання прийнято
з техніко-економічного обґрунтування	Меленчук Л.І. вчена ступінь, звання П.І.П. консультанта		

КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ п/п	Найменування етапу	Терміни	
		початку	завершення
1	Вибір теми, ознайомлення з вимогами до кваліфікаційної роботи.	25.11.2024	01.12.2024
2	Аналіз предметної області та прикладів рішень.	02.12.2024	05.02.2025
3	Вивчення апаратних та програмних засобів реалізації.	29.01.2025	07.02.2025
4	Формування функціональних вимог та розробка структури системи.	08.02.2025	01.03.2025
5	Проєктування алгоритмів, електричних схем і візуальних ілюстрацій.	03.03.2025	05.04.2025
6	Налаштування середовища Arduino IDE, підключення бібліотек та тестових скетчів.	18.03.2025	08.04.2025
7	Реалізація основної логіки системи доступу.	09.04.2025	09.05.2025
8	Збірка та налагодження пристрою.	10.05.2025	16.05.2025
9	Розробка економічного розділу та спеціальної частини кваліфікаційної роботи.	11.03.2025	03.05.2025
10	Тестування роботи пристрою, виправлення помилок.	13.05.2025	28.05.2025
11	Оформлення пояснювальної записки.	29.05.2025	15.06.2025
12	Попередній захист, врахування зауважень, коригування.	16.06.2025	16.06.2025
13	Підготовка до захисту кваліфікаційної роботи.	17.06.2025	25.06.2025
14	Захист кваліфікаційної роботи.	26.06.2025	26.06.2025

Дата видачі "25" листопада 2024 р. Керівник _____/ Василь ПАВЛЮС

Завдання прийняв до виконання_____/Богдан ТАЗЮК

Реферат

Кваліфікаційна робота. Система керування дверним замком на основі розпізнавання відбитків пальців. 53 с., 23 рисунки, 3 додатки, 6 джерел.

Об'єктом розробки є інтелектуальна система доступу, що забезпечує відкривання або закривання дверного замка на основі біометричної ідентифікації користувача за відбитком пальця.

Метою роботи є створення надійної та зручної в користуванні системи, яка дозволяє здійснювати контроль доступу до приміщення шляхом перевірки відбитка пальця, а також надсилати сповіщення про події (успішні чи неуспішні спроби входу) у Telegram-бот адміністратора системи.

Технічною основою реалізації системи виступає мікроконтролер NodeMCU на базі ESP8266, до якого підключено сканер відбитків пальців DY50, сервопривід для механічного керування замком, світлодіоди для візуальної індикації стану, а також бузер для звукових сигналів. Комунікація з Telegram здійснюється через захищені HTTPS-запити. Інформаційні повідомлення надсилаються у чат Telegram-бота одразу після кожної взаємодії з системою: у разі розпізнавання зареєстрованого користувача або фіксації неуспішної спроби доступу.

Програмна реалізація створена мовою програмування C++ в середовищі Arduino IDE із використанням бібліотек для обробки біометричних даних, керування периферійними пристроями та надсилання запитів до Telegram API.

Результатом проєкту є функціональна та адаптивна система, придатна для встановлення в житлових або комерційних приміщеннях з метою підвищення безпеки та автоматизації контролю доступу.

СИСТЕМА КЕРУВАННЯ ЗАМКОМ, ESP8266, БІОМЕТРІЯ, ВІДБИТОК ПАЛЬЦЯ, TELEGRAM-БОТ, ІНТЕРНЕТ РЕЧЕЙ, ARDUINO, БЕЗПЕКА.

Abstract

Graduation Project. Fingerprint-Based Door Lock Control System. 54 pages, 23 figures, 3 appendices, 6 references.

The object of the development is an intelligent access control system designed to unlock or lock a door based on biometric fingerprint identification.

The aim of this work is to develop a reliable and user-friendly system that enables secure access to premises by verifying a registered fingerprint and sending event notifications (successful or unsuccessful access attempts) to the administrator via a Telegram bot.

The system is built on a NodeMCU microcontroller based on the ESP8266 platform. It incorporates a DY50 fingerprint scanner, a servo motor for mechanical lock control, LEDs for visual status indication, and a buzzer for audible alerts. Communication with Telegram is performed through secure HTTPS requests. Informational messages are sent directly to a Telegram bot chat after each interaction with the system, either when a registered user is recognized or when an unauthorized attempt is detected.

The software is developed in C++ using the Arduino IDE and includes libraries for biometric data processing, peripheral device control, and interaction with the Telegram API.

As a result, a fully functional and adaptable access control system has been implemented, suitable for installation in residential or commercial environments to improve security and automate access management.

LOCK CONTROL SYSTEM, ESP8266, BIOMETRICS, FINGERPRINT, TELEGRAM BOT, INTERNET OF THINGS, ARDUINO, SECURITY.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

API – Application Programming Interface

DY50 – Biometric Fingerprint Sensor DY50

GPIO – General Purpose Input/Output

HTTPS – HyperText Transfer Protocol Secure

IDE – Integrated Development Environment

IoT – Internet of Things

LED – Light Emitting Diode

UART – Universal Asynchronous Receiver-Transmitter

ВСТУП

Система контролю доступу на основі розпізнавання відбитків пальців є сучасним технологічним рішенням, що забезпечує високий рівень безпеки та комфорту при доступі до приміщень. У сучасних умовах інформаційної безпеки та автоматизації подібні системи набувають дедалі більшого значення для захисту приватних, комерційних і державних об'єктів.

Останнім часом провідні наукові установи та компанії, такі як Google, Apple та Samsung, активно розробляють біометричні системи для ідентифікації користувачів у смартфонах, системах контролю доступу та фінансових операціях. Світові тенденції свідчать про зростання популярності біометричних технологій, оскільки вони забезпечують високий рівень безпеки та мінімізують ризики несанкціонованого доступу.

Актуальність цієї роботи полягає у необхідності розробки доступних та ефективних систем контролю доступу для побутових та комерційних приміщень. Основні проблеми, які вирішує система, включають зниження ймовірності несанкціонованого проникнення, спрощення процесу доступу та можливість віддаленого керування.

Основною ціллю роботи є розробка системи керування дверним замком на основі розпізнавання відбитків пальців, яка забезпечує безпечний доступ до приміщення та дистанційне керування через Telegram-бот. Система може бути застосована в системах розумного будинку, офісних приміщеннях та інших об'єктах, де необхідно забезпечити високий рівень безпеки.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАВДАНЬ

1.1 Опис предметної області

В сучасному світі системи контролю доступу відіграють важливу роль у забезпеченні безпеки житлових, комерційних та промислових приміщень. Одним із сучасних напрямків розвитку таких систем є біометрична ідентифікація, зокрема використання відбитків пальців для аутентифікації користувачів. Біометричні замки набувають все більшої популярності завдяки високому рівню безпеки, зручності використання та відсутності необхідності у фізичних ключах або паролях, які можуть бути втрачені чи скомпрометовані.

Більшість сучасних систем керування дверними замками на основі відбитків пальців використовують оптичні, ємнісні або ультразвукові сенсори для сканування та розпізнавання унікальних біометричних даних користувача. Після сканування відбиток пальця порівнюється з базою даних авторизованих користувачів, і у разі збігу замок розблокується.

Проте, незважаючи на розвиток технологій, існують певні проблеми, пов'язані з біометричною автентифікацією. Наприклад, неякісні або забруднені сенсори можуть знижувати точність розпізнавання, що призводить до помилок при доступі. Крім того, деякі системи не підтримують віддалене керування або журналювання подій, що може бути важливим у певних сценаріях використання.

Впровадження біометричних систем контролю доступу пов'язане з питаннями конфіденційності та захисту персональних даних користувачів. Оскільки відбиток пальця є унікальною та незмінною характеристикою особи, необхідно забезпечити безпечне збереження та обробку біометричних даних, щоб уникнути їхнього несанкціонованого використання.

Незважаючи на ці виклики, системи керування дверними замками на основі відбитків пальців мають значні переваги у порівнянні з традиційними методами контролю доступу. Вони дозволяють підвищити рівень безпеки, мінімізувати ризик несанкціонованого доступу та значно спростити процес аутентифікації користувачів. Завдяки інтеграції з мобільними застосунками та іншими

розумними пристроями, такі системи можуть забезпечувати додаткові можливості, включаючи віддалене керування, сповіщення про спроби доступу та налаштування рівнів авторизації для різних користувачів.

Типова структура роботи системи керування дверним замком на основі відбитків пальців наведена на рисунку 1.1.

Рисунок 1.1 – Типова структура роботи системи керування дверним замком

Аналізуючи цю сферу, можна виділити кілька ключових аспектів:

– Технічна складова включає апаратні компоненти (біометричний сканер, мікроконтролер, електрозамок, модулі зв'язку, індикатори стану), програмні рішення (алгоритми біометричної ідентифікації, база користувачів, протоколи обміну даними), а також способи збору, обробки, передачі та збереження інформації.

– Функціональні можливості охоплюють основні операції системи, такі як реєстрація та розпізнавання користувачів за біометричними даними, керування доступом через мобільні платформи або чат-бот, ведення журналів відвідувань,

синхронізація з іншими безпековими системами, а також підтримка автономного режиму роботи у випадку втрати зв'язку з мережею.

– Інтеграція та взаємодія передбачає можливість підключення до локальних чи віддалених серверів для збереження логів, використання мобільних додатків для дистанційного керування, а також підтримку альтернативних методів автентифікації, таких як RFID-карти чи PIN-коди.

– Економічні аспекти системи сприяють скороченню витрат на традиційні ключі та механічні замки, підвищенню рівня захисту, зменшенню ризику несанкціонованого проникнення, а також дозволяють здійснювати дистанційне керування без необхідності фізичної присутності.

Загалом, дослідження предметної області системи контролю доступу на основі відбитків пальців охоплює широкий спектр технічних, функціональних, економічних та безпекових чинників. Запровадження такої технології сприяє покращенню контролю доступу та забезпеченню зручності для користувачів.

1.2 Аналіз існуючих рішень

Огляд існуючих рішень у галузі систем керування дверними замками дозволяє оцінити різноманітність доступних продуктів, їхні функціональні можливості та обмеження. Сучасні системи контролю доступу можуть працювати на основі механічних, електронних, біометричних чи хмарних технологій. Нижче представлено декілька прикладів існуючих рішень на ринку:

- August Smart Lock.
- Yale Assure Lock.
- Samsung Smart Door Lock.

August Smart Lock (рис. 1.1) – це розумний замок для дверей, розроблений компанією August Home. Вперше представлений у 2013 році, цей пристрій надає користувачам можливість дистанційного керування доступом до їхніх осель за допомогою мобільного додатка. Замок інтегрується з різними розумними платформами, такими як Amazon Alexa, Google Assistant та Apple HomeKit, що робить його універсальним рішенням для сучасних систем безпеки.

Основною перевагою August Smart Lock є можливість дистанційного керування замком через спеціальний мобільний додаток, що дозволяє користувачам відкривати або закривати двері незалежно від свого місцезнаходження. Функція автоматичного блокування та розблокування забезпечує додатковий рівень комфорту: пристрій автоматично закриває двері після виходу користувача та розблоковує їх при поверненні завдяки технології Bluetooth та геолокації.

Пристрій підтримує функцію віртуальних ключів, яка дозволяє надавати тимчасовий або постійний доступ іншим особам без використання фізичних ключів. Налаштування доступу та його відкликання здійснюється через додаток. Інтеграція з системами розумного будинку дозволяє August Smart Lock працювати разом із системами безпеки, відеодомофонами та іншими пристроями, підвищуючи рівень контролю та зручності для користувачів.

Додаток веде журнал активності, де фіксується інформація про те, хто і коли відкривав або закривав двері. Пристрій також підтримує голосове керування через голосових асистентів, що робить процес користування ще зручнішим. August Smart Lock є одним із найпопулярніших пристроїв у сфері розумного дому, забезпечуючи зручність, безпеку та гнучкість у керуванні доступом до оселі.

Рисунок 1.2 – Система August Smart Lock

Yale Assure Lock (рис. 1.3) – це сучасний розумний дверний замок, розроблений компанією Yale, одним із провідних світових виробників систем безпеки. Ця серія замків забезпечує надійний контроль доступу до оселі, поєднуючи передові технології безпеки з інтуїтивно зрозумілим інтерфейсом. Yale Assure Lock підтримує різні бездротові стандарти, такі як Wi-Fi, Bluetooth, Z-Wave та Zigbee, що дозволяє легко інтегрувати замок з популярними екосистемами розумного дому, включаючи Amazon Alexa, Google Assistant та Apple HomeKit.

Основні характеристики Yale Assure Lock включають керування без ключів, що дозволяє відчиняти та зачиняти двері за допомогою цифрової клавіатури, мобільного додатку або голосових команд. Завдяки підключенню до Wi-Fi або Bluetooth, користувачі можуть керувати замком з будь-якої точки світу через мобільний додаток Yale Access. Замок також має функцію автоматичного блокування, що знижує ризик залишити двері відчиненими після виходу користувача.

Крім того, Yale Assure Lock дозволяє створювати віртуальні ключі, що дає змогу надавати тимчасовий або постійний доступ іншим людям. Це ідеальне рішення для гостей, орендарів або домогосподарів. Інтеграція з розумним будинком забезпечується завдяки підтримці стандартів Z-Wave, Zigbee та Wi-Fi, що дозволяє легко підключити замок до систем безпеки та автоматизації будинку. Мобільний додаток також надає журнал активності, який дозволяє власникам відстежувати, хто і коли користувався замком.

Для забезпечення додаткової безпеки Yale Assure Lock оснащений резервним механізмом, зокрема механічним ключем або аварійним живленням через батарею на випадок розрядження основного джерела живлення.

Завдяки гнучким можливостям налаштувань і широкій інтеграції з іншими розумними пристроями, Yale Assure Lock є одним із найбільш зручних і безпечних рішень для сучасного дому. Він доступний у різних варіаціях, що дозволяє користувачам обрати модель відповідно до своїх потреб та рівня безпеки.

Рисунок 1.3 – Система Yale Assure Lock

Samsung Smart Door Lock – це інноваційна серія розумних дверних замків, розроблена компанією Samsung для забезпечення високого рівня безпеки та зручності в житлових і комерційних приміщеннях. Завдяки сучасним технологіям замки цієї серії підтримують кілька способів автентифікації, що робить систему контролю доступу надійною та гнучкою.

Однією з головних переваг є використання біометричних технологій. Вбудований сканер відбитків пальців дозволяє швидко і точно ідентифікувати користувача, що значно підвищує рівень захисту. Окрім цього, замок підтримує альтернативні методи доступу, зокрема введення персонального PIN-коду та використання RFID-карток, що розширює можливості його використання.

Додаткову зручність забезпечує функція дистанційного керування. Підключення через Bluetooth або Wi-Fi дозволяє власнику контролювати стан замка за допомогою мобільного додатка. Користувач може переглядати історію відкриттів, отримувати миттєві сповіщення про доступ та навіть надавати тимчасові коди для гостей.

Замки Samsung Smart Door Lock легко інтегруються в систему розумного будинку Samsung SmartThings, що дозволяє автоматизувати різні процеси.

Наприклад, після розблокування дверей можуть автоматично вмикатися освітлення або охоронна система змінювати режим роботи.

Безпека також посилюється завдяки додатковим захисним механізмам. Замки оснащені сенсорами, які реагують на спроби злому або механічного впливу, активуючи вбудовану сигналізацію. Крім того, передбачена функція автоматичного блокування, яка замикає двері після їх закриття, мінімізуючи ризик залишити приміщення незахищеним.

Також в даній системі присутня корисна функція аварійного живлення. У випадку розрядження батарей користувач може тимчасово підключити замок до зовнішнього джерела живлення через мікро-USB, що дозволяє уникнути блокування дверей.

Таким чином, Samsung Smart Door Lock (рис. 1.4) – це багатофункціональне рішення для безпеки та зручного доступу до приміщень. Поєднання біометричних технологій, мобільного керування та інтеграції в розумний будинок робить ці замки ефективним інструментом для сучасного користувача, який цінує комфорт і надійний захист.

Рисунок 1.4 – Система Samsung Smart Door Lock

Отримані результати аналізу допоможуть сформувати вимоги до проєкту та визначити оптимальні технічні рішення для реалізації системи.

1.3 Постановка завдання

Система керування дверним замком на основі розпізнавання відбитків пальців повинна забезпечити високий рівень безпеки, зручність використання та можливість інтеграції з іншими розумними пристроями. Основне завдання полягає в розробці замка, який використовує біометричні дані для підтвердження особи та надання доступу до приміщення лише авторизованим користувачам.

За допомогою розпізнавання відбитків пальців система повинна мати датчик, який сканує та зберігає відбитки пальців користувачів. Датчик має забезпечити точне та швидке розпізнавання відбитків, навіть при зміні кута сканування або умов освітлення.

Крім того, система повинна надавати можливість авторизації користувачів, що передбачає додавання нових осіб до бази даних, а також зміну або видалення їхніх даних при необхідності.

Керування доступом передбачає автоматичне відкриття замка для авторизованих користувачів після успішного розпізнавання їх відбитка пальця. Крім того, система повинна фіксувати спроби несанкціонованого доступу, забезпечуючи таким чином безпеку приміщення.

Ще однією важливою функцією є дистанційне керування замком. Завдяки підключенню до Wi-Fi або Bluetooth користувачі мають можливість керувати замком через мобільний застосунок або Інтернет з будь-якої точки світу. Мобільний застосунок також має функцію перегляду журналу подій, де власники можуть бачити, хто і коли користувався замком.

Автоматичне блокування передбачає, автоматичне закриття замка дверей після певного часу або після виходу користувача. Це допомагає зменшити ризик забути зачинити двері та підвищує рівень безпеки.

Нефункціональні вимоги до системи включають високу швидкість роботи. За допомогою технологій розпізнавання відбитків пальців, система повинна

здійснювати розпізнавання протягом кількох секунд, щоб забезпечити зручність та оперативний доступ.

Надійність системи є ще однією важливою вимогою. Вона повинна бути стійкою до збоїв та несанкціонованого доступу. У разі проблем з основним джерелом живлення або біометричними даними, система має бути оснащена резервними механізмами, такими як введення пароля та аварійне живлення.

Для безпеки всі дані про відбитки пальців повинні зберігатися в зашифрованому вигляді для запобігання витоку інформації та несанкціонованому доступу.

Енергоспоживання є важливим аспектом, оскільки система повинна бути енергоефективною, зокрема при використанні бездротових технологій, що дозволить знизити витрати на електроенергію.

Інтеграція з іншими розумними пристроями також є важливою складовою. Система повинна забезпечити легку інтеграцію з іншими компонентами розумного дому, такими як камери спостереження або датчики руху, для покращення контролю доступу та загальної безпеки.

Завдяки виконанню цих функціональних та нефункціональних вимог система керування дверним замком на основі розпізнавання відбитків пальців стане ефективним та надійним рішенням для забезпечення безпеки в сучасному житті.

2 ПРОЄКТУВАННЯ СИСТЕМИ

У попередньому розділі буде визначено загальні принципи роботи системи керування дверним замком, що базується на мікроконтролері ESP8266. Розглянуто особливості використання біометричних даних та інтеграції з Telegram-ботом для ідентифікації користувачів. Крім того, проаналізовано потенційну роль сервера у забезпеченні централізованого управління доступом.

Також було сформульовано список основних функцій, які повинна виконувати система, а саме:

- реєстрація користувачів та їхніх біометричних даних;
- перевірка та авторизація доступу через Telegram-бот;
- управління замком на основі отриманих даних;
- можливість віддаленого управління через мобільний застосунок або вебінтерфейс.

Наступним етапом роботи є процес проєктування системи, що включає визначення ключових компонентів та їх взаємодії, вибір загальної архітектури та розробку структурної схеми. Розглянемо ці аспекти детальніше.

2.1 Визначення компонентів системи

Беручи до уваги проведений аналіз, було прийнято рішення використовувати в даному проєкті мікроконтролер ESP8266, оскільки він має достатню обчислювальну потужність, вбудований Wi-Fi модуль для підключення до мережі та можливість взаємодії з периферійними пристроями. Основним елементом ідентифікації користувачів у системі буде біометричний датчик відбитків пальців, який дозволяє зчитувати, зберігати та порівнювати відбитки для перевірки особи. Саме цей тип аутентифікації обрано через його високий рівень безпеки та зручність використання.

Для фізичного управління дверним механізмом застосовуватиметься серводвигун, який забезпечуватиме відкривання та закривання замка залежно від результатів перевірки користувача. Оскільки система повинна мати додаткові

засоби сповіщення, до її складу ввійдуть світлодіоди різних кольорів, що сигналізуватимуть про статус доступу: зелений вказує на успішну авторизацію, а червоний – на заборонений доступ. Додатково, для аудіовізуального сповіщення використовуватиметься бузер, який видаватиме звукові сигнали у разі успішного або невдалого зчитування відбитка пальця.

Для обробки та збереження інформації про користувачів передбачена база даних, яка міститиме записи про зареєстровані відбитки пальців та історію спроб входу. З метою розширення можливостей керування та моніторингу роботи системи використовуватиметься Telegram-бот, який забезпечить можливість віддаленого контролю, надсилання повідомлення про спроби доступу та дозволить адміністратору керувати списком користувачів.

Живлення всіх компонентів здійснюватиметься за допомогою блока живлення на 5В або 12В залежно від вимог окремих пристроїв. Взаємодія між усіма елементами системи відбуватиметься через мікроконтролер, який координує їхню роботу, аналізує отримані дані та приймає рішення щодо надання або відмови у доступі.

2.2 Проєктування структури системи

Визначившись із компонентами, можна перейти до розробки загальної структури системи, яка включатиме кілька функціональних підсистем.

Основою проєкту є підсистема керування, яка забезпечує координацію роботи всіх інших компонентів. Вона отримує дані від підсистеми ідентифікації користувачів, обробляє їх і ухвалює рішення про надання або заборону доступу.

Однією з важливих складових системи є підсистема контролю замка, яка реалізує фізичне відкривання або закривання дверей на основі отриманих команд. Для цього використовується сервопривід, керований мікроконтролером. Додатково передбачена підсистема сповіщення, що складається зі світлодіодних індикаторів та бузера. Вона сигналізує про статус системи та результат аутентифікації.

Система також містить підсистему моніторингу та віддаленого керування, яка реалізується через Telegram-бот. Вона дозволяє власнику отримувати повідомлення про спроби доступу, переглядати історію входів і в разі потреби додавати або видаляти користувачів. Завдяки цьому підхід до контролю доступу є не лише безпечним, а й зручним для адміністратора.

Структурна схема системи представлена на рисунку 2.1.

Рисунок 2.1 – Структурна схема системи

Як видно з рисунка, підсистема керування є центральним елементом, який взаємодіє з іншими функціональними блоками. Підсистема ідентифікації отримує та обробляє біометричні дані, після чого передає результати в керуючий модуль. У разі успішної аутентифікації активується підсистема контролю замка, яка змінює його стан. Одночасно підсистема сповіщення надає візуальні та звукові сигнали про виконані дії. Якщо виявляються підозрілі спроби доступу або система потребує адміністративного втручання, підсистема моніторингу передає відповідні дані через Telegram-бот.

Загалом, розроблена структура дозволяє створити ефективну систему контролю доступу, яка поєднує апаратні та програмні засоби для забезпечення безпеки, зручності та гнучкості в управлінні.

2.3 Алгоритм роботи системи

Після визначення архітектури системи та її функціональних підсистем, наступним кроком є опис логіки її роботи. Для цього було розроблено алгоритм, який демонструє послідовність дій мікроконтролера під час процесу ідентифікації користувача та керування електронним замком. Алгоритм дозволяє краще зрозуміти, як відбувається обробка введених даних, прийняття рішень та виконання керуючих дій на основі біометричної інформації.

Робота системи розпочинається з ініціалізації всіх необхідних компонентів, включаючи модуль зчитування відбитків пальців, сервопривід, світлодіодні індикатори, бузер та модуль зв'язку з Telegram-ботом. Після цього система переходить у режим очікування користувача, при якому зчитувач відбитків пальців готовий приймати запити.

Як тільки користувач прикладає палець до сенсора, система здійснює спробу зчитування та порівняння отриманого відбитка з тими, що вже збережені в базі даних пристрою. У разі успішного розпізнавання, керуючий модуль надсилає команду на відкривання дверей, що реалізується через привід замка. Додатково активуються звукові та візуальні сигнали, які інформують про дозвіл доступу. Після цього система витримує коротку затримку тривалістю 5 секунд аби користувач встиг відкрити двері, після чого автоматично виконується закривання замка.

Якщо ж відбиток не розпізнано, система подає сигнал про заборону доступу і повертається у вихідний стан не відкриваючи замок. В обох випадках інформація про спробу входу може бути передана через Telegram-бот, що забезпечує віддалений моніторинг ситуації.

Алгоритм роботи системи у вигляді блок-схеми представлено в додатку А. Він включає основні етапи роботи системи: запуск, очікування введення, перевірку доступу, виконання дій відповідно до результату аутентифікації, і повернення у початковий стан. Завдяки такій логіці забезпечується безперервна робота пристрою з високим рівнем автономності та зручністю для користувача.

У цьому розділі було здійснено детальне проєктування системи керування дверним замком на базі мікроконтролера ESP. Визначено ключові компоненти, їх функціональність та принципи взаємодії. Сформовано логічну структуру системи з підсистемами ідентифікації, керування замком, сповіщення та віддаленого моніторингу. Побудовано алгоритм роботи пристрою, що забезпечує надійну, безпечну та зручну взаємодію з користувачем. Представлене рішення дозволяє ефективно поєднати апаратні та програмні засоби для реалізації сучасної системи контролю доступу.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ

Наступним етапом роботи є безпосередня реалізація та тестування системи. Цей процес охоплює вибір конкретних апаратних компонентів відповідно до функціональних вимог, створення електричної принципової схеми, монтаж системи на макетній платі, а також розробку програмного забезпечення згідно з раніше визначеною логікою. Завершальним кроком є перевірка працездатності системи та усунення можливих недоліків.

3.1 Вибір компонентів системи

Як було зазначено раніше, система складається з таких основних елементів: мікроконтролера ESP, біометричного датчика відбитків пальців для ідентифікації користувачів, сервопривода для фізичного управління замком, реле або транзистора для комутації, світлодіодів для візуальної індикації, бузера для звукових сповіщень, а також модуля зв'язку з Telegram-ботом через Wi-Fi. У цьому підрозділі буде детально розглянуто обрані компоненти, обґрунтовано доцільність їх використання та наведено їхні основні технічні характеристики.

Мікроконтролер

Першим та основним компонентом цього проєкту є плата мікроконтролера ESP8266 (рис. 3.1).

Рисунок 3.1 – Плата мікроконтролера ESP8266 Lolin

ESP8266 Lolin – це популярна мікроконтролерна плата, створена для простого та ефективного впровадження IoT-рішень. Вона побудована на базі модуля ESP8266, який має вбудований Wi-Fi, що дозволяє підключати пристрої до інтернету без додаткових модулів.

ESP8266 Lolin може живитися як від micro-USB, так і від зовнішнього джерела живлення через спеціальний пін VIN. Це забезпечує зручність у використанні як для стаціонарних, так і для портативних проєктів. Завдяки вбудованому стабілізатору напруги, плата може працювати з джерелами живлення в діапазоні від 4.5 В до 10 В.

Всі характеристики контролера ESP показано в таблиці в додатку В.

Наступним важливим компонентом, використаним у реалізації системи, є біометричний датчик відбитків пальців DY50_MAIN_V3 (рис. 3.2). Цей модуль призначений для зчитування, обробки, збереження та ідентифікації відбитків пальців. Завдяки вбудованому процесору, датчик здатен автономно обробляти дані та приймати рішення про автентифікацію без необхідності зовнішньої обробки сигналу мікроконтролером.

Датчик підключається до мікроконтролера ESP8266 через UART-інтерфейс (Universal Asynchronous Receiver-Transmitter) – універсальний асинхронний передавач-приймач, який забезпечує послідовну передачу даних між двома пристроями за допомогою всього двох ліній: TX (передача) і RX (прийом). Такий підхід дозволяє мінімізувати кількість використовуваних виводів і забезпечує надійний обмін даними. Важливо дотримуватися правильного підключення: вивід TX датчика підключається до RX мікроконтролера, а RX датчика – до TX мікроконтролера, тобто передача й прийом перехрещуються.

Для підключення було використано апаратний UART ESP8266, що дозволило уникнути типових проблем, пов'язаних із бібліотекою SoftwareSerial, зокрема втратою даних на високих швидкостях. Апаратний UART ESP8266 працює стабільніше, швидше реагує на вхідні сигнали та не перевантажує мікроконтролер зайвим програмним опрацюванням. Комунікація з датчиком

здійснюється на стандартній швидкості 57600 бод, яка підтримується обома пристроями.

Окрім сигнальних ліній для стабільної роботи модуля необхідно забезпечити живлення в діапазоні 3.3-5 В, а також надійне підключення до GND. DY50_MAIN_V3 широко використовується в проєктах безпеки, таких як електронні замки, системи контролю доступу та ідентифікації персоналу. Він дозволяє зберігати в пам'яті до кількох сотень відбитків (типово – 1000), що робить його зручним для багатокористувацьких систем. Його компактність, сумісність з багатьма платформами та надійність забезпечують просту інтеграцію в малі пристрої керування доступом.

Рисунок 3.2 – Біометричний датчик відбитків пальців DY50_MAIN_V3

Основні особливості датчика DY50_MAIN_V3:

– Підтримка зчитування, запису та пошуку відбитків пальців;

– UART-інтерфейс для зв'язку з мікроконтролером (рекомендована швидкість 57600 біт/с);

– вбудована пам'ять для збереження зареєстрованих шаблонів;

– автономна обробка даних (не потребує постійної участі контролера для верифікації);

– LED-підсвітка для підказок користувачеві (активується при торканні сканера);

– компактний розмір і просте підключення через 6-піновий роз'єм;

– рекомендована напруга живлення – 3.3-5 В;

– надійність зчитування навіть при незначному забрудненні пальців.

Одним із ключових компонентів у системі є серво-двигун MG90S (рис. 3.3), який відповідає за фізичну імітацію відкриття та закриття дверного замка. Сервопривід є незамінним елементом у проєктах, де потрібно забезпечити точне позиціонування або обмежене обертання елемента у певному кутовому діапазоні. На відміну від звичайних електродвигунів, він не обертається безперервно, а лише повертається на заданий кут, що робить його оптимальним для керування механічними елементами замикання.

MG90S має вбудований редуктор та механізм зворотного зв'язку, який дозволяє контролювати положення вала з високою точністю. Управління здійснюється за допомогою PWM-сигналу з мікроконтролера, де ширина імпульсу визначає кінцевий кут повороту. Наприклад, імпульс тривалістю 1 мс відповідає положенню 0°, а 2 мс – 180° (діапазон може трохи відрізнятись залежно від моделі).

У системі керування дверним замком сервопривід виконує функцію виконавчого пристрою, що безпосередньо змінює стан замка. У разі успішної автентифікації за допомогою біометричного датчика, ESP8266 генерує PWM-сигнал, який призводить до повороту вала сервопривода на заданий кут – наприклад, 90° для імітації відкриття замка. Після короткої затримки система повертає вал у початкове положення, таким чином замикаючи двері.

Рисунок 3.3 – Сервопривід MG90S

Технічні характеристики MG90S:

- напруга живлення: 4.8–6.0 В;
- крутний момент: до 2.5 кг·см при 4.8 В, до 3.0 кг·см при 6.0 В;
- швидкість обертання: 0.1 сек/60° (при 4.8 В), 0.08 сек/60° (при 6.0 В);
- робочий діапазон температур: від -30°C до +60°C;
- тип управління: PWM (широтно-імпульсна модуляція);
- кут повороту: приблизно 180° (обмежується конструкцією);
- інтерфейс: 3-контактний (сигнал, живлення, земля);
- матеріал шестерень: метал (на відміну від популярного SG90 з пластиковими шестернями);
- вага: 13.4 г;
- розміри: 22.8 x 12.0 x 29.5 мм.

Одним із елементів звукової індикації у системі є активний п'єзокерамічний бузер (рис. 3.4). Його основна функція – аудіосповіщення користувача про результат аутентифікації або іншу подію в системі. Акустичний сигнал є додатковим інтерфейсом взаємодії між користувачем і системою, який дозволяє

навіть без перегляду світлодіодів чи екрана швидко зрозуміти, чи було надано доступ.

На відміну від пасивного бузера, активний зумер має вбудований генератор частоти. Це означає, що для його роботи не потрібно генерувати сигнал PWM – достатньо подати логічну «1» або живлення на вхід. Завдяки цьому його підключення до мікроконтролера надзвичайно просте: лише один керуючий пін, який можна керувати через digitalWrite().

У даній системі активний зумер використовується для подачі короткого звукового сигналу при успішному розпізнаванні відбитка пальця, для генерації тривалого або повторного звуку у випадку невдалої спроби доступу, а також як додаткове звукове сповіщення про зміну стану замка (відкриття або закриття).

Рисунок 3.4 – Активний бузер

Технічні характеристики активного бузера:

- робоча напруга: 5 В;
- середній робочий струм: близько 30–35 мА;
- частота звуку: ~2300 Гц (± 300 Гц);
- рівень звукового тиску: ~85–90 дБ на відстані 10 см;
- розміри корпусу: Ø12 мм, висота 9.2 мм;
- довжина виводів: 6.5 мм і 5 мм (відстань між пін-наконечниками ~7 мм);
- вага: близько 1.6 г.

У системі керування дверним замком важливу роль відіграють світлодіодні індикатори – зелений і червоний (рис. 3.5). Вони слугують простим та наочним засобом інформування користувача про поточний стан системи, результат автентифікації або події, що відбуваються в процесі взаємодії з замком.

Зелений світлодіод використовується як індикатор успішної аутентифікації. Він засвічується на кілька секунд після того, як користувача впізнано за відбитком пальця, і замок відкрито. Натомість червоний світлодіод сигналізує про відмову в доступі – наприклад, якщо відбиток не знайдено в базі даних або якщо спроба входу була здійснена невідомим користувачем. Така форма індикації дозволяє миттєво зрозуміти результат авторизації без потреби взаємодії з іншими елементами системи (екраном, мобільним застосунком тощо).

Кожен світлодіод підключений до окремого GPIO-піна мікроконтролера через токообмежувальний резистор (220–330 Ом), що дозволяє уникнути перевантаження виходу ESP8266. Керування світлодіодами реалізовано програмно через функції digitalWrite(), що дозволяє вмикати або вимикати їх у відповідь на події в системі.

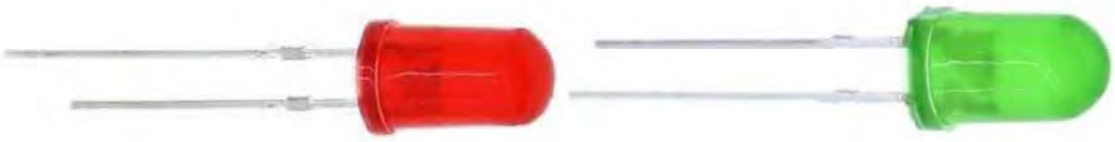


Рисунок 3.5 – Червоний та зелений світлодіоди

Основні характеристики стандартних 5мм світлодіодів:

- напруга живлення: 1.8–2.2 В (червоний), 2.0–3.2 В (зелений);
- робочий струм: 10–20 мА;
- колір світіння: червоний та зелений;
- діаметр корпусу: 5 мм;
- кут огляду: ~30–60°;
- тип виводів: анод (довший пін), катод (коротший пін, зазвичай зі скошеним краєм).

3.2 Реалізація принципової електричної схеми та монтаж пристрою

Після детального аналізу обраних компонентів та визначення логіки роботи системи наступним кроком є реалізація принципової електричної схеми та

фізичне збирання прототипу пристрою на макетній платі. Електрична схема дає змогу візуалізувати взаємозв'язки між усіма елементами системи, зрозуміти спосіб підключення та забезпечити коректну роботу всієї конструкції.

Для проєктування схеми було використано середовище Fritzing – програму з інтуїтивно зрозумілим інтерфейсом, яка дозволяє створювати прототипи електронних схем із використанням віртуальних компонентів. Вона також дає змогу формувати вигляд монтажу на макетній платі (breadboard), а при необхідності – експортувати файли для виготовлення друкованої плати. Таке середовище є особливо зручним у навчальних і дослідницьких цілях, оскільки поєднує графічну простоту з достатнім рівнем технічної деталізації.

На принциповій електричній схемі (рис. 3.6) зображено всі основні з'єднання між ESP8266 та периферійними пристроями – датчиком відбитків пальців DY50_MAIN_V3, сервоприводом MG90S, активним бузером і двома світлодіодами. Особливу увагу приділено підключенню UART-інтерфейсу до ESP8266, оскільки саме через нього відбувається комунікація з біометричним сенсором.

На монтажній схемі пристрою (рис. 3.7) представлено візуальну реалізацію компонування всіх елементів на макетній платі. Тут зображено розміщення проводів, розташування елементів, резисторів до світлодіодів та правильне підключення живлення, зокрема використання виводу Vin для живлення 5В модулів (датчика та сервопривода), а також спільного заземлення.

Фотографія змонтованого пристрою наведена на рисунку 3.8. Вона демонструє як фізично реалізовано проєкт на макетній платі з усіма компонентами в робочому стані. Монтаж було виконано з дотриманням правил ергономіки та безпеки: використано кольорове маркування проводів, мінімізовано перехрещення контактів, а також забезпечено легкий доступ до елементів для тестування й обслуговування.

Таким чином, електрична та монтажна схеми слугують основою для подальшої реалізації програмної частини та проведення тестування системи.

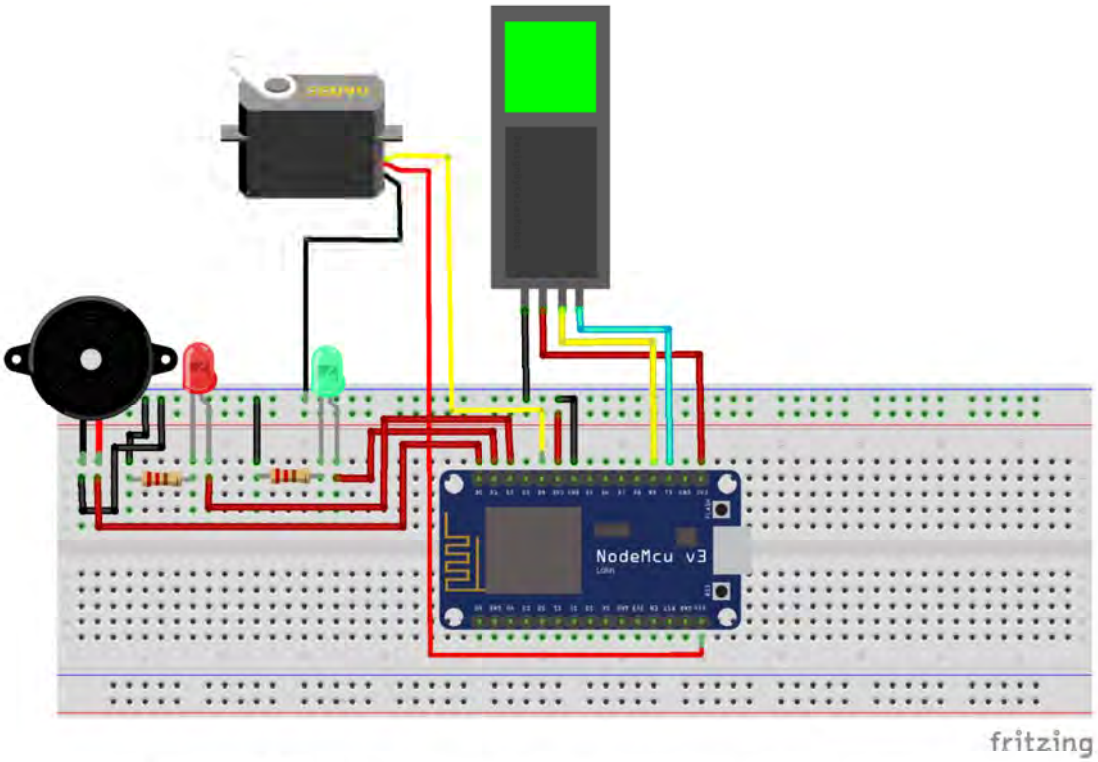


Рисунок 3.6 – Принципова електрична схема системи

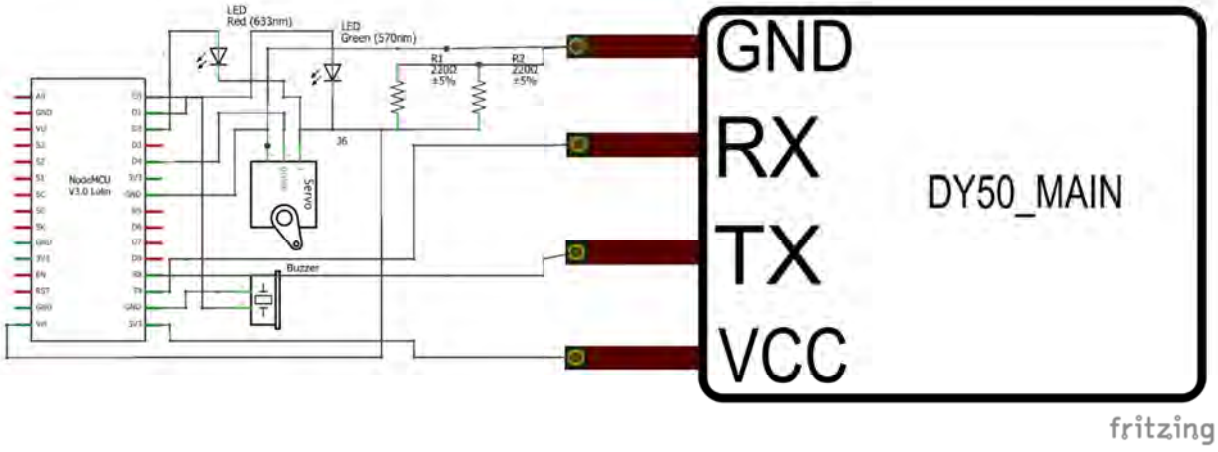


Рисунок 3.7 – Монтажна схема на макетній платі

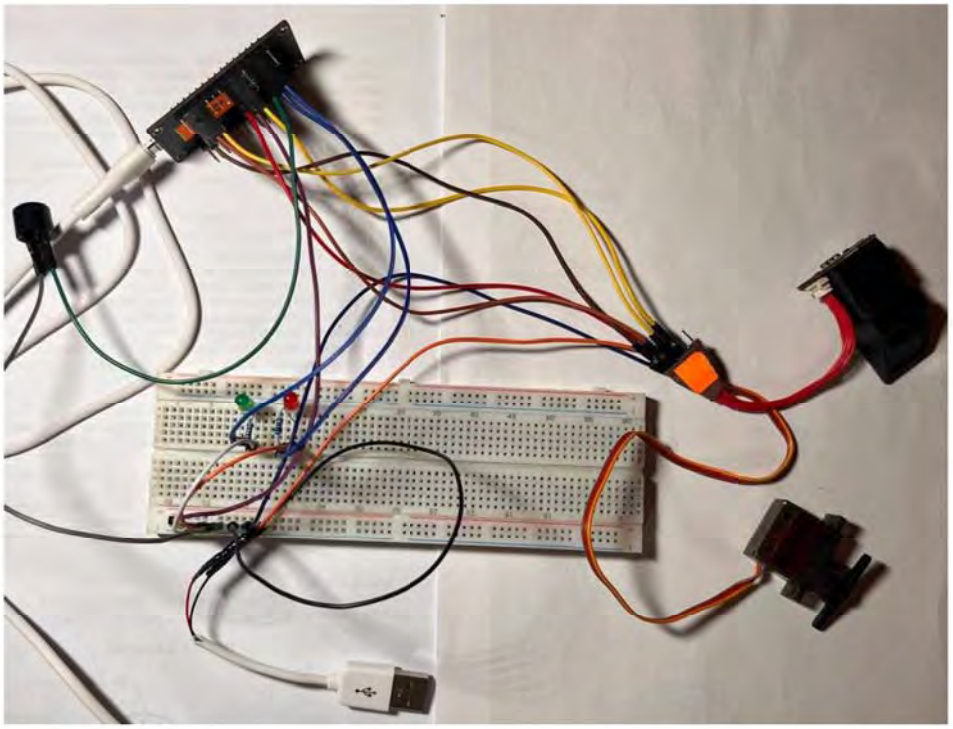


Рисунок 3.8 – Змонтований пристрій у зібраному вигляді

3.3 Реалізація програмного забезпечення

Програмна частина системи була реалізована у середовищі Arduino IDE із застосуванням мови програмування C++ та бібліотек, орієнтованих на роботу з мікроконтролерами ESP8266, сканером відбитків пальців та сервісом Telegram. Основна задача полягає у зчитуванні біометричних даних, керуванні виконавчими пристроями та надсиланні повідомлень через мережу Wi-Fi.

На початку програми здійснюється підключення необхідних бібліотек, серед яких `Adafruit_Fingerprint.h` – для повноцінної взаємодії з біометричним модулем DY50_MAIN_V3, `Servo.h` – для керування положенням сервоприводу, `ESP8266W-` – для реалізації HTTPS-запитів до Telegram API. Безпосередньо перед початком компіляції середовище Arduino IDE виглядає, як показано на рисунку 3.9.

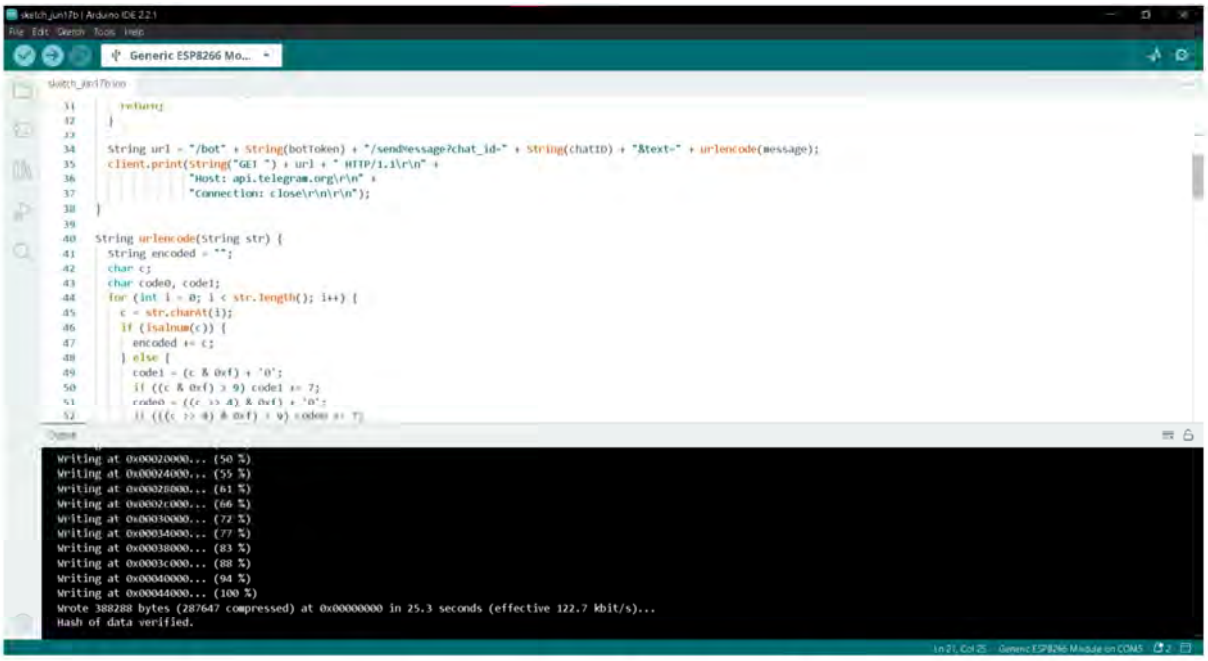


Рисунок 3.9 – Інтерфейс середовища Arduino IDE під час компіляції та завантаження коду на ESP8266

У функції `setup()` здійснюється первинна ініціалізація: починається серійний зв'язок для діагностики, запускається сканер відбитків з швидкістю 57600 бод, встановлюється підключення до Wi-Fi мережі. Саме тут важливим є виклик функції `finger.begin(57600)`, який задає коректну швидкість обміну даними через UART між сенсором і мікроконтролером, забезпечуючи точність передачі даних. У разі невдалої ініціалізації система переходить у режим очікування або повідомляє про помилку.

У програмі реалізовано зв'язок з Telegram через webhook – URL-адресу із вказаним токеном бота та текстом повідомлення. Вся передача даних у бот здійснюється через об'єкт `WiFiClientSecure`, що забезпечує безпечне з'єднання з API Telegram без необхідності проксі або сторонніх сервісів. Повідомлення формуються динамічно, залежно від того, чи був користувач авторизований, і надсилаються відразу після події. Приклад успішного повідомлення у Telegram показано на рисунку 3.10.

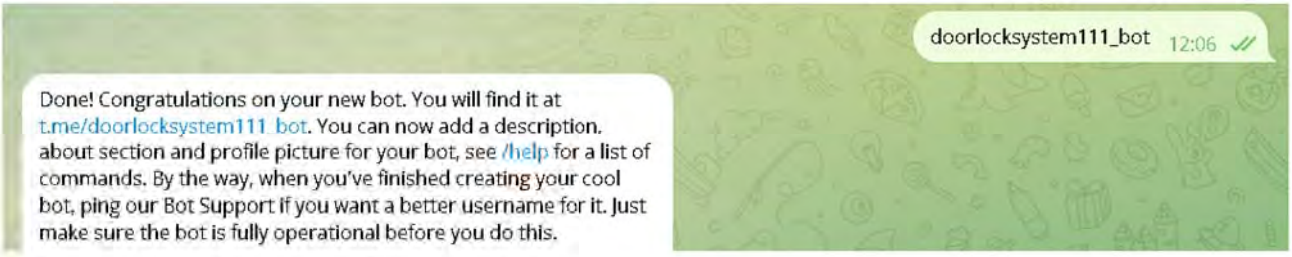


Рисунок 3.10 – Повідомлення у Telegram про успішну авторизацію користувача через бот

Основна логіка програми реалізована у нескінченному циклі `loop()`. У цьому блоці реалізовано очікування події прикладання пальця, зчитування відбитка через функцію `getFingerprintID()` та подальше виконання дій залежно від результату. Якщо відбиток знайдено – викликається послідовність функцій `unlockDoor()`, `indicateSuccess()` та `sendTelegramMessage()`, кожна з яких відповідає за конкретну частину процесу: фізичне відкриття замка, активацію зеленої індикації та надсилання звіту адміністратору.

У випадку невдалої спроби сканування система виконує блок з функціями `indicateError()` та `sendTelegramMessage()` із відповідним текстом. Таким чином, система повідомляє користувача світлом та звуком про помилку, а також адміністратору – про потенційну підозрілу активність.

Діагностика під час роботи здійснюється через серійний монітор, що дає змогу бачити результат зчитування, помилки обміну або повідомлення про з'єднання з Telegram.

Окремої уваги заслуговує реалізація затримок – наприклад, функція `delay(5000)` після успішного відкриття дозволяє фізично дочекатися, поки користувач відчинить двері, перш ніж автоматично повернути сервопривід у початкове положення. Це рішення спрощує взаємодію з замком і робить систему зручнішою у повсякденному користуванні.

У коді використовуються умовні оператори для обробки результатів `finger.getImage()` та `finger.image2Tz()` – ці рядки дозволяють контролювати якість зображення, верифікацію та пошук у пам'яті пристрою. Їх правильне

застосування гарантує, що навіть при повторних спробах або некоректному прикладанні пальця система не зависне, а повернеться до стабільного стану очікування.

Ще однією важливою особливістю є реалізація підключення сканера через апаратний UART, а не програмний, що критично для ESP8266. Такий підхід не лише забезпечив стійкість роботи пристрою під навантаженням, а й дозволив уникнути проблем із втратами сигналу, які часто виникають при використанні `SoftwareSerial`.

Повний програмний код системи подано у додатку Б. Він побудований у вигляді окремих логічних блоків із коментарями, що дозволяє не тільки зручно підтримувати систему, а й легко адаптувати її до нових функцій у майбутньому, таких як PIN-авторизація тощо.

3.4 Підключення та налаштування Telegram-бота

Одним із ключових елементів функціональності системи є можливість дистанційного моніторингу та повідомлення про події через Telegram. Така інтеграція дозволяє в режимі реального часу отримувати інформацію про відкриття дверей, невдалі спроби авторизації або технічні збої. Для цього в системі реалізовано механізм взаємодії з Telegram-ботом, створеним спеціально для даного проєкту.

Процес налаштування розпочинається зі створення Telegram-бота через офіційний сервіс @BotFather. Це спеціальний бот, який надає можливість створювати інших ботів, а також керувати їхніми налаштуваннями. Після запуску @BotFather та введення команди /newbot користувачеві пропонується задати ім’я та унікальне ім’я користувача (username) для нового бота. У відповідь Telegram автоматично генерує токен доступу, який слід зберегти – саме він дозволяє здійснювати запити до Telegram API зі сторони ESP8266.

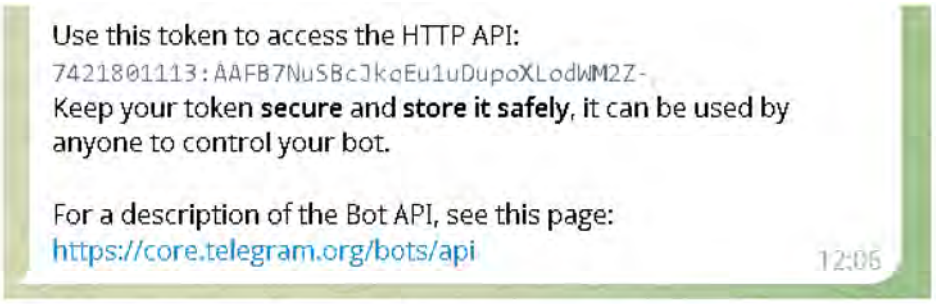


Рисунок 3.11 – Створення Telegram-бота через @BotFather та отримання токену доступу

Наступним кроком є отримання Chat ID – унікального ідентифікатора користувача або групи, куди бот надсилатиме повідомлення. Найпростіший спосіб – надіслати будь-яке повідомлення до створеного бота, а потім використати спеціальний сервіс (наприклад, https://api.telegram.org/bot<token>/getUpdates), щоб отримати ID зі структури відповіді JSON. В Chat ID автоматично прив'язується канал, група або конкретний аккаунт, що забезпечує правильну маршрутизацію повідомлень.

Рисунок 3.12 – Визначення Chat ID через API Telegram після відправки тестового повідомлення

У коді ESP8266 було реалізовано функцію `sendTelegramMessage(String message)`, яка виконує HTTPS-запит до Telegram API з параметрами токена, ID чату та тексту повідомлення. Для цього використовується бібліотека `WiFiClientSecure`, що дозволяє надсилати запити через зашифроване з'єднання. URL формується у вигляді:

https://api.telegram.org/bot<TOKEN>/sendMessage?chat_id=<CHAT_ID>&text=<ТЕКСТ_ПОВІДОМЛЕННЯ>

Таким чином, після кожної події в системі (наприклад, успішна ідентифікація або невдала спроба входу) відбувається формування тексту повідомлення та передача його через Wi-Fi у вигляді POST-запиту на Telegram-сервер. Це забезпечує оперативне інформування адміністратора або користувача, незалежно від його місцезнаходження.

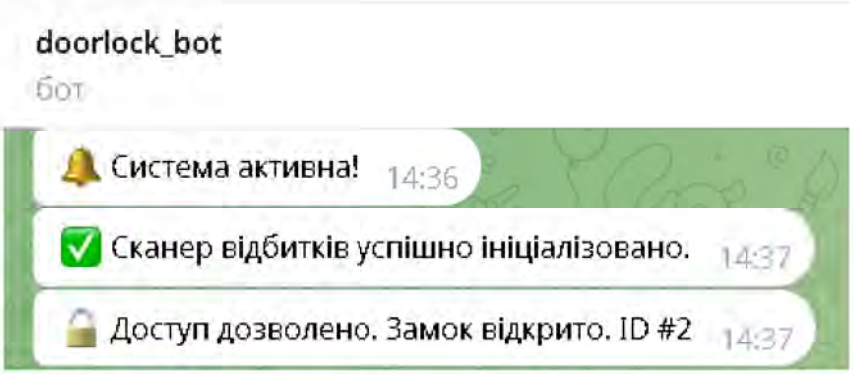


Рисунок 3.13 – Повідомлення в Telegram-боті після успішного сканування відбитка пальця

Перевагою такого підходу є простота реалізації та висока надійність з'єднання. Водночас, для безпечної роботи з API застосовано HTTPS-запити, що дозволяє уникнути передачі важливої інформації у відкритому вигляді. У випадку відсутності з'єднання або помилки авторизації, система фіксує проблему в серійному моніторі, дозволяючи здійснити діагностику.

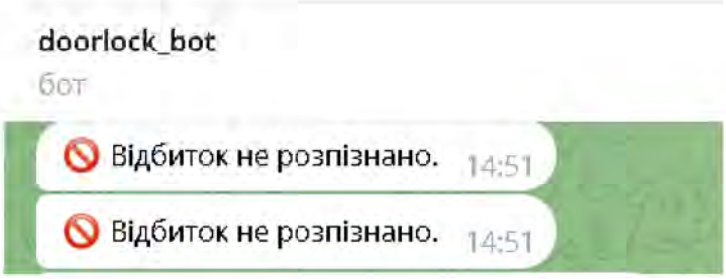


Рисунок 3.14 – Повідомлення про несанкціоновану спробу доступу з виводом у Telegram

Завдяки використанню Telegram-бота, система стала не лише локальним інструментом контролю, але й частиною IoT-екосистеми з можливістю

дистанційного моніторингу в режимі реального часу. Це розширює її функціональність, підвищує безпеку та зручність для кінцевого користувача.

3.5 Тестування роботи системи

Після завершення реалізації апаратної та програмної частин системи було проведено всебічне тестування її функціональності. Основна мета цього етапу – переконатися, що всі компоненти працюють згідно з розробленою логікою, взаємодіють між собою стабільно, а також своєчасно реагують на події, ініційовані користувачем.

Передусім було здійснено апаратне тестування: перевірено підключення датчика відбитків пальців DY50_MAIN_V3 через UART, працездатність сервоприводу MG90S, активного бузера та світлодіодів. Датчик був підключений через апаратні виводи RX/TX мікроконтролера ESP8266. На цьому етапі виник перший важливий нюанс: під час першої спроби комунікації сканера з ESP8266 було використано Serial-порт, що за замовчуванням використовується Arduino IDE для моніторингу (Serial Monitor). У результаті виник конфлікт – сканер не функціонував належним чином. Це було вирішено переходом до апаратного UART (GPIO1 – TX та GPIO3 – RX), відмовившись від одночасного використання Serial Monitor, що суттєво стабілізувало з'єднання між контролером і сканером.

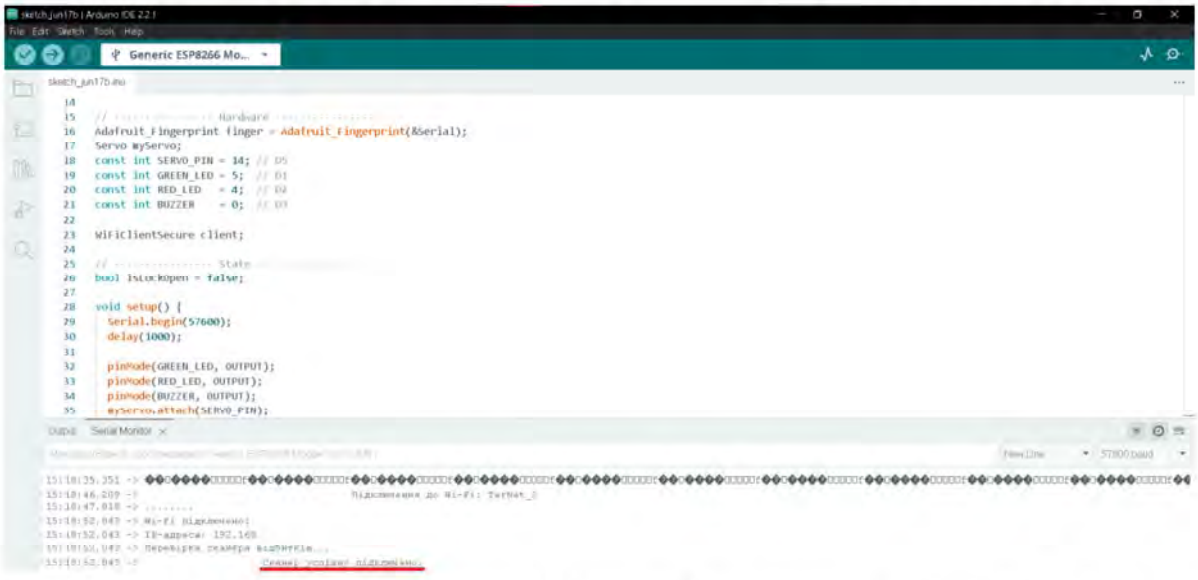


Рисунок 3.15 – Серійний монітор Arduino IDE із повідомленням про успішне зчитування відбитка пальця

Під час програмного тестування виникла друга проблема – складність у реалізації коду запису нового відбитка в пам'ять сканера. Спершу сенсор не реагував на введене ID для реєстрації пальця, і виявити причину було непросто. Згодом з'ясувалося, що сенсор перебував у неініціалізованому стані або був обраний неправильний `baud rate` (швидкість передачі даних). Встановлення стандартної швидкості 57600 бод через `finger.begin(57600)` і додавання перевірки статусу повернення (`FINGERPRINT_OK`) дозволило успішно записувати нові шаблони в пам'ять пристрою.

На етапі тестування Telegram-бота також виник третій нюанс – проблема з відправленням повідомлень під час тестів на різних Wi-Fi мережах. У деяких мережах (наприклад, з обмеженим NAT або фільтрацією портів) ESP8266 не міг виконати HTTPS-запит до Telegram API. Це було вирішено шляхом додавання `client.setInsecure();`, що дозволяє працювати з TLS-з'єднанням без перевірки сертифіката. У фінальній реалізації було обрано стабільну мережу з відкритим доступом до інтернету, що забезпечило надійне надсилання повідомлень у чат.

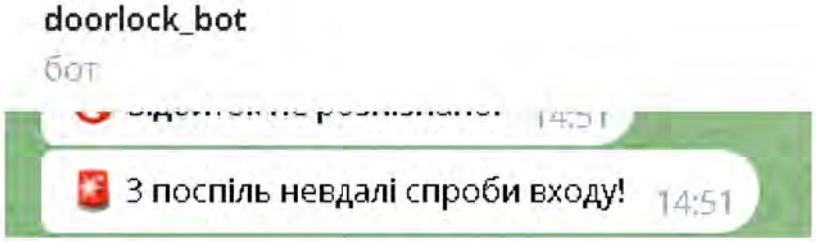


Рисунок 3.16 – Повідомлення в Telegram про невдалу спробу входу з невідомим відбитком

З технічної точки зору, система показала себе надійною. Після прикладання пальця до сенсора система за 1-2 секунди проводить біометричну перевірку. У разі позитивного результату активується зелений світлодіод, відкривається замок, а в Telegram надходить повідомлення. Якщо ж користувача не ідентифіковано – червоний світлодіод подає сигнал про відмову, зумер звучить двічі або довше, і в Telegram надсилається сповіщення про несанкціонований доступ.

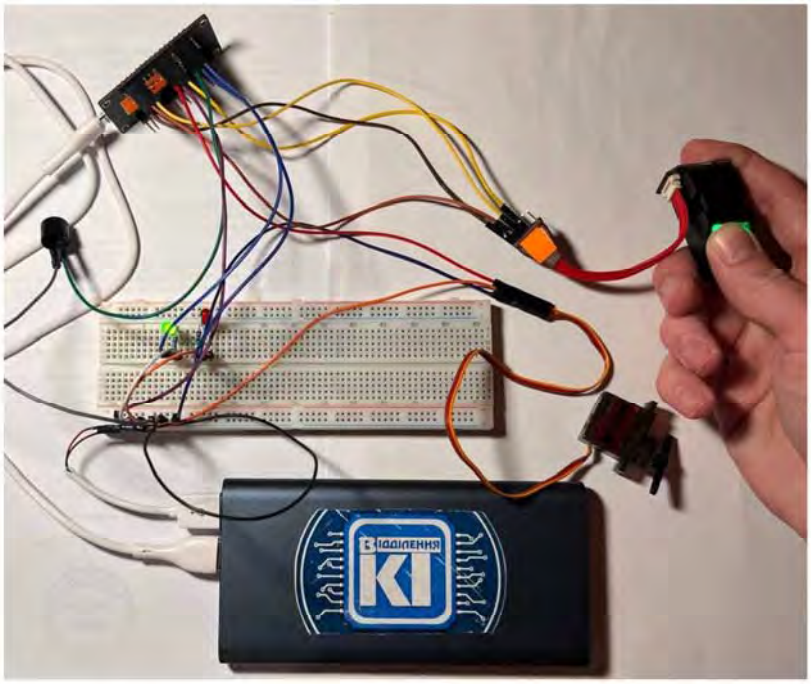


Рисунок 3.17 – Візуальна індикація відкриття дверей: зелений світлодіод активний, замок відкрито

Було протестовано також затримки в логіці. Наприклад, після успішної авторизації активується `delay(5000)`, яка дає користувачу 5 секунд для відкриття дверей перед тим, як сервопривід автоматично повертає замок у закрите положення. Це дозволяє уникнути залишення дверей відкритими, навіть якщо користувач не зреагував одразу.

Загалом у процесі тестування було перевірено коректність зчитування відбитків пальців, стабільність передачі повідомлень до Telegram, точність реакції сервопривода на керуючі команди, а також функціонування світлодіодної індикації й звукової сигналізації за допомогою бузера. Особливу увагу було приділено стабільності Wi-Fi з'єднання, що є критично важливим для надсилання повідомлень у Telegram. Час спрацювання системи, тобто від прикладання пальця до моменту відкриття дверей, у середньому складав 2-3 секунди, що відповідає вимогам до швидкості роботи побутових систем доступу.

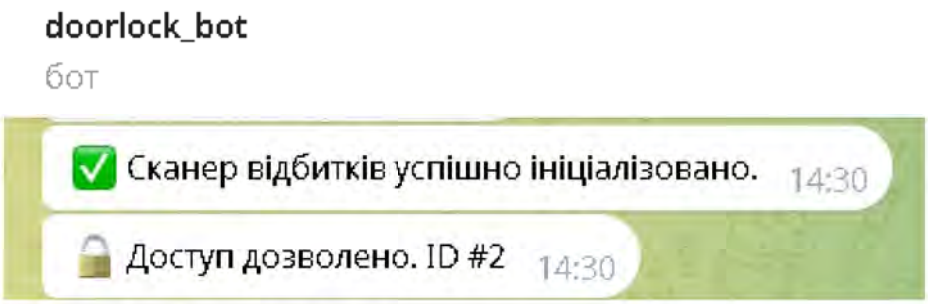


Рисунок 3.18 – Повідомлення в Telegram про успішну авторизацію користувача

Усі виявлені помилки були усунуті в процесі поетапного тестування, а система на фінальному етапі продемонструвала стабільну та передбачувану роботу. Завдяки використанню апаратного UART, правильно підібраному таймінгу та надійному Telegram API, пристрій вийшов не лише функціональним, але й зручним для користувача.

4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ

4.1 Аналіз ринку

Сучасні системи контролю доступу, зокрема ті, що базуються на біометричній автентифікації, дедалі активніше використовуються як у побутових, так і в комерційних умовах. Їх популярність зумовлена високим рівнем безпеки, простотою у використанні та можливістю інтеграції в екосистеми розумного дому. На українському ринку представлені різні рішення, які відрізняються функціональністю, способом встановлення та, звичайно ж, вартістю.

Комерційні біометричні замки відомих виробників, як-от ZKTeco чи Yale, мають вартість від 5 000 до 9 000 грн залежно від наявності таких функцій, як Wi-Fi керування, віртуальні ключі, підтримка Bluetooth або RFID. Наприклад, модель ZKTeco ML10B з підтримкою сканера та RFID карт коштує близько 5 000 грн, а більш функціональний GL300W із підтримкою мережевого доступу – вже понад 6 700 грн. Рішення преміум класу, зокрема Aqara Smart Lock або аналоги від Samsung, можуть досягати вартості 9 000–12 000 грн, оскільки забезпечують голосове керування, повну інтеграцію з системами безпеки та детальний журнал подій.

На тлі таких рішень самостійно зібрана система виглядає економічно доцільнішою. Наприклад, модуль сканера DY50_MAIN_V3 обійдеться в середньому в 400–450 грн, контролер ESP8266 – ще близько 150–180 грн, серводвигун MG90S – орієнтовно 100 грн, інші компоненти, такі як бузер, світлодіоди, резистори та провідники – у межах 150–200 грн. Загальна вартість реалізації всієї системи разом із макетною платою становить приблизно 900–1 000 грн, що є більш ніж у 5 разів дешевше за готові продукти з аналогічним функціоналом.

Варто зазначити, що попри нижчу ціну, запропонована система не поступається базовим комерційним рішенням у плані функціональності. Вона підтримує ідентифікацію за відбитками, керування замком через Telegram-бот, фіксацію подій та візуально-звукову індикацію. Це дає змогу ефективно

використовувати її як в умовах побуту, так і для організації обмеженого доступу в офісах, лабораторіях чи навчальних закладах.

Таким чином, створення системи керування дверним замком на основі біометричної автентифікації в межах навчального проєкту не лише технічно доцільне, а й економічно виправдане. В умовах обмеженого бюджету та необхідності адаптації під конкретні потреби, такий підхід має перевагу перед готовими комерційними рішеннями.

4.2 Розрахунок витрат на реалізацію

Розрахунок витрат на розробку та впровадження системи керування дверним замком на основі біометричної автентифікації здійснено з урахуванням вартості основних компонентів, допоміжних матеріалів, а також витрат на програмне забезпечення та підключення до мережі.

Таблиця 4.1 – Вартість компонентів системи

№	Назва компонента	К-сть, шт.	Ціна за одиницю, грн.
1	Контролер ESP8266	1	170
2	Біометричний сканер відбитків DY50_MAIN_V3	1	440
3	Серводвигун MG90S	1	100
4	Активний бузер	1	30
5	Світлодіоди (зелений і червоний)	2	30
6	Резистори, провідники, кнопки, корпус	-	150
7	Макетна плата / плата для монтажу	1	80
	Разом		1000

Здійснимо розрахунок витрат на оплату праці.

Для розробки системи в ідеальних умовах залучаються кілька спеціалістів: проєктувальник, інженер-програміст та фахівець з налаштування. Втім, з огляду на масштаби проєкту, усі функції може виконувати одна особа – інженер-програміст.

Середня місячна заробітна плата інженера-програміста в Україні становить близько 30 000 грн. Розробка системи за розрахунками триває не більше одного місяця.

Вирахуємо податкові відрахування із заробітної плати:

– Податок на доходи фізичних осіб (ПДФО) – 18%:

30 000 грн × 18% = 5 400 грн

– Військовий збір – 1,5%:

30 000 грн × 1,5% = 450 грн

– Єдиний соціальний внесок – 22%:

30 000 грн × 22% = 6 600 грн

– Загальна сума відрахувань:

5 400 грн + 450 грн + 6 600 грн = 12 450 грн

– Чиста заробітна плата:

30 000 грн − 12 450 грн = 17 550 грн

Отже, загальна вартість реалізації системи складається з вартості компонентів і витрат на оплату праці:

1 000 грн + 30 000 грн = 31 000 грн

Загалом, витрати на розробку та впровадження системи залишаються значно нижчими за вартість комерційних аналогів, які стартують приблизно з 5 000 грн і можуть перевищувати 9 000 грн, враховуючи додаткові функції.

Цей кошторис підтверджує економічну доцільність розробки власної системи керування дверним замком на основі біометричної автентифікації у межах навчального проекту.

4.3 Обґрунтування доцільності розробки

Розробка власної системи керування дверним замком на основі біометричної автентифікації є доцільною з кількох причин. По-перше, власне рішення дозволяє максимально адаптувати функціонал під конкретні потреби користувача, що часто важко реалізувати за допомогою готових комерційних продуктів. Це особливо актуально для специфічних умов використання,

наприклад, у житлових будинках, офісах або навчальних лабораторіях, де вимоги до безпеки та зручності можуть суттєво відрізнятися. По-друге, розроблена система вирізняється високою гнучкістю – її можна легко модернізувати та розширювати, додаючи нові модулі або функції без необхідності повної заміни обладнання. Це забезпечує довгострокову перспективу ефективного використання пристрою.

Ще одним важливим аргументом на користь власної розробки є зниження загальних витрат у процесі експлуатації. Відсутність необхідності сплачувати ліцензійні збори, абонентську плату за сторонні сервіси або витрати на регулярне сервісне обслуговування робить систему економічно вигіднішою порівняно з комерційними аналогами. Крім того, створення власного рішення гарантує повний контроль над збереженням і обробкою біометричних даних, що особливо важливо для забезпечення конфіденційності та безпеки інформації користувачів. Власна система уникає ризиків, пов'язаних із передачею персональних даних у хмарні сервіси сторонніх розробників.

Окрім практичної користі, розробка такої системи має важливе освітнє значення. Проєкт дає можливість отримати цінний досвід у сфері апаратного забезпечення та програмування, що сприяє підвищенню кваліфікації та професійному зростанню. Загалом, створення власної системи керування дверним замком на основі біометрії є раціональним рішенням, яке поєднує в собі економічну доцільність, технічну гнучкість та високий рівень безпеки, що робить її привабливою альтернативою готовим продуктам на ринку.

ВИСНОВКИ

У межах даної кваліфікаційної роботи було розроблено, реалізовано та протестовано систему керування дверним замком, що базується на використанні біометричного датчика відбитків пальців та мікроконтролера ESP8266. Основною метою проєкту стало створення доступного, безпечного та функціонального рішення для обмеження доступу до приміщення з можливістю дистанційного моніторингу та автоматизації.

На початковому етапі було проведено аналіз сучасного ринку систем контролю доступу, в ході якого встановлено, що переважна більшість готових комерційних рішень мають високу вартість і часто не дозволяють гнучко адаптувати систему під індивідуальні потреби користувача. Це стало підставою для вибору самостійної розробки як більш економічно вигідного і технологічно гнучкого варіанту.

В процесі розробки було здійснено підбір необхідних компонентів, серед яких: біометричний сенсор DY50_MAIN_V3, сервопривід MG90S, ESP8266 як основний контролер, активний бузер, індикатори (світлодіоди), а також допоміжні елементи. Усі модулі були з'єднані відповідно до технічних вимог, враховуючи особливості UART-зв'язку та обмеження ESP8266 щодо одночасної роботи з декількома пристроями. Для покращення роботи було реалізовано обхід програмної бібліотеки SoftwareSerial, надаючи перевагу апаратному UART.

Програмне забезпечення системи забезпечує зчитування відбитків пальців, їх ідентифікацію в пам'яті сенсора, активацію механізму замка, візуальну й звукову індикацію, а також надсилання повідомлень у Telegram за допомогою інтеграції з Google Таблицями через Webhook. Такий підхід дозволив реалізувати систему, що не лише виконує свої основні функції, а й надає зручний спосіб фіксації спроб доступу.

Проведений техніко-економічний аналіз показав, що вартість реалізації самостійно зібраної системи становить близько 1000 грн, що значно нижче за ринкову вартість аналогічних пристроїв, яка часто перевищує 5000–7000 грн.

Розрахунок витрат на оплату праці та податкові зобов'язання підтвердив економічну доцільність такої реалізації в умовах обмеженого бюджету.

В результаті тестування система показала стабільну роботу: коректно розпізнавала зареєстровані відбитки, своєчасно активувала замок та надсилала сповіщення про доступ. Система може бути використана як у побутових, так і в малих комерційних умовах, з можливістю подальшого розширення функціоналу – зокрема, інтеграції з хмарними сервісами, мобільними застосунками або іншими модулями «розумного дому».

Таким чином, поставлені завдання були успішно реалізовані. Створена система продемонструвала технічну ефективність, доступність у впровадженні, гнучкість для подальшого розвитку та високу практичну цінність як для реального використання, так і в освітньому процесі.

СПИСОК ДЖЕРЕЛ ПОСИЛАННЯ

1. Характеристики мікроконтролера ESP8266. Вебсайт: URL: https://uk.wikipedia.org/wiki/ESP8266 (дата звернення: 11.03.2025).

2. Біометричний сканер відбитків пальців DY50_MAIN_V3. Вебсайт: URL: https://robopeak.com/product/fingerprint-sensor (дата звернення: 10.04.2025).

3. Серводвигун MG90S: технічні характеристики. Вебсайт: URL: https://www.electropeak.com/servo-motor-mg90s (дата звернення: 11.04.2025).

4. Підключення ESP8266 до Telegram-бота. Вебсайт: URL: https://randomnerdtutorials.com/telegram-control-esp8266-nodemcu (дата звернення: 14.04.2025).

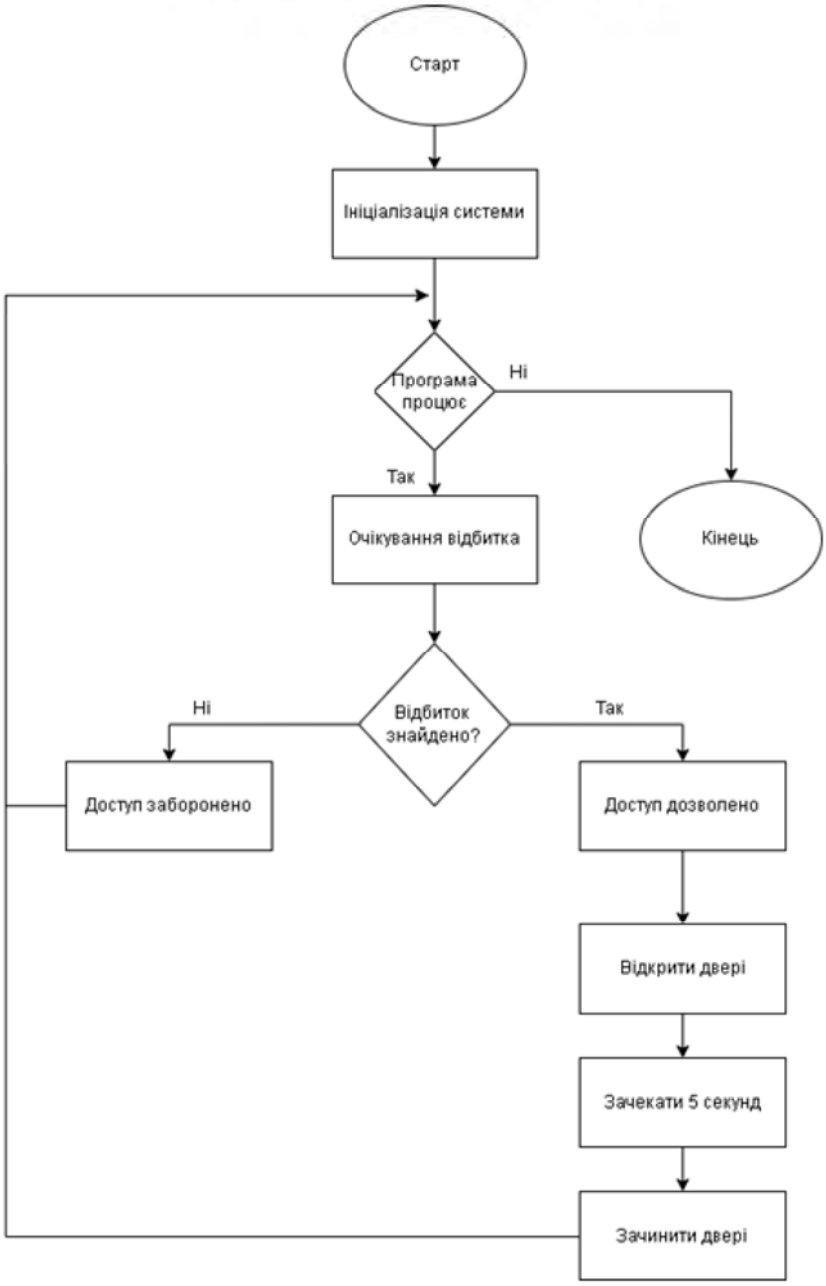
5. Бібліотека Adafruit Fingerprint Sensor. Вебсайт: URL: https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library (дата звернення: 15.04.2025).

6. Методичні рекомендації до виконання кваліфікаційної роботи для студентів спеціальності 123 «Комп'ютерна інженерія» / Павлюс В.П., Посвятовська О.Б., Кульчинська Н.З. – Галицький фаховий коледж імені В'ячеслава Чорновола, Тернопіль, 2023. – 52 с.

ДОДАТКИ

Додаток А

Блок-схема роботи прототипу



Додаток Б

Лістинг програмного коду

```
#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <Adafruit_Fingerprint.h>
#include <Servo.h>

// Параметри Wi-Fi
const char* ssid = "TerNet_2";
const char* password = "88888888";

// Дані Telegram
const char* botToken = "7421801113:AAFB7NuSBcJkoEu1uDupoXLodWM2Z-
pY8eo";
const char* chatID = "886730048";

WiFiClientSecure client;

// Сканер та серво
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&Serial);
Servo myServo;

// Піни
const int SERVO_PIN = 14;
const int GREEN_LED = 5;
const int RED_LED = 4;
const int BUZZER = 0;

int failCounter = 0;
bool isLockOpen = false;

void sendTelegram(String message) {
  if (!client.connect("api.telegram.org", 443)) {
    Serial.println("Telegram connection failed");
    return;
  }
  String url = "/bot" + String(botToken) + "/sendMessage?chat_id=" +
String(chatID) + "&text=" + urlencode(message);
  client.print(String("GET ") + url + " HTTP/1.1\r\n" +
               "Host: api.telegram.org\r\n" +
               "Connection: close\r\n\r\n");
}

String urlencode(String str) {
  String encoded = "";
  char c, code0, code1;
  for (int i = 0; i < str.length(); i++) {
    c = str.charAt(i);
    if (isalnum(c)) {
      encoded += c;
    } else {
```

```
      code1 = (c & 0xf) + '0';
      if ((c & 0xf) > 9) code1 += 7;
      code0 = ((c >> 4) & 0xf) + '0';
      if (((c >> 4) & 0xf) > 9) code0 += 7;
      encoded += '%';
      encoded += code0;
      encoded += code1;
    }
  }
  return encoded;
}

void setup() {
  Serial.begin(57600);
  delay(1000);

  pinMode(GREEN_LED, OUTPUT);
  pinMode(RED_LED, OUTPUT);
  pinMode(BUZZER, OUTPUT);

  myServo.attach(SERVO_PIN);
  myServo.write(0); // Замок зачинено

  WiFi.begin(ssid, password);
  Serial.print("Connecting to WiFi...");
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println(" connected.");
  client.setInsecure();
  sendTelegram("Система активна");

  if (finger.verifyPassword()) {
    Serial.println("Fingerprint scanner found.");
    signalSuccess();
    sendTelegram("Сканер відбитків успішно ініціалізовано");
  } else {
    signalError();
    sendTelegram("Помилка ініціалізації сканера відбитків");
    while (true);
  }
}

void loop() {
  uint8_t result2 = getFingerprintID();

  if (result2 == FINGERPRINT_OK) {
    if (!isLockOpen) {
      signalSuccess();
      sendTelegram("Доступ дозволено. Замок відкрито. ID #" +
String(finger.fingerID));
```

```
      myServo.write(90);
      isLockOpen = true;
    } else {
      signalSuccess();
      sendTelegram("Замок зачинено. ID #" + String(finger.fingerID));
      myServo.write(0);
      isLockOpen = false;
    }
    failCounter = 0;
  } else if (result2 == FINGERPRINT_NOTFOUND) {
    signalError();
    failCounter++;
    sendTelegram("Відбиток не розпізнано");
    if (failCounter >= 3) {
      sendTelegram("3 поспіль невдалі спроби входу");
      failCounter = 0;
    }
  } else if (result2 == FINGERPRINT_PACKETRECIEVEERR ||
             result2 == FINGERPRINT_IMAGEFAIL ||
             result2 == FINGERPRINT_IMAGEMESS) {
    signalError();
    sendTelegram("Помилка сканера відбитків: код " +
String(result2));
  }

  delay(500);
}

void signalSuccess() {
  digitalWrite(GREEN_LED, HIGH);
  digitalWrite(RED_LED, LOW);
  tone(BUZZER, 1000, 100);
  delay(150);
  tone(BUZZER, 1600, 150);
  delay(200);
  tone(BUZZER, 2000, 200);
  delay(250);
  digitalWrite(GREEN_LED, LOW);
}

void signalError() {
  digitalWrite(RED_LED, HIGH);
  digitalWrite(GREEN_LED, LOW);
  tone(BUZZER, 200, 500);
  delay(500);
  digitalWrite(RED_LED, LOW);
}

uint8_t getFingerprintID() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK) return p;
  p = finger.image2Tz();
```

```
  if (p != FINGERPRINT_OK) return p;
  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK) return p;
  Serial.print("Found ID #");
  Serial.print(finger.fingerID);
  return FINGERPRINT_OK;
}
```

Додаток В

Характеристики мікроконтролера ESP8266

Основні критерії	Значення
Максимальний вихідний струм 3.3V	500мА
Flash-пам’ять	4МБ
Тактова частота	80МГц
Цифрові піни / виходи	11 GPIO (деякі підтримують PWM, I2C, SPI)
Напруга живлення	5 В (через micro-USB) або 3.3 В (напряму)
Інтерфейси зв’язку	Wi-Fi, UART, SPI, I2C
Рівень споживання (глибокий сон)	~10 мкА
Роз’єм живлення	Micro-USB
Інтегрований модуль живлення	ШІМ-конвертер 5 В → 3.3 В
Мікроконтролер	ESP8266EX
Максимальний вихідний струм 3.3V	500мА
Flash-пам’ять	4МБ
Тактова частота	80МГц
Цифрові піни / виходи	11 GPIO (деякі підтримують PWM, I2C, SPI)
Напруга живлення	5 В (через micro-USB) або 3.3 В (напряму)
Інтерфейси зв’язку	Wi-Fi, UART, SPI, I2C
Рівень споживання (глибокий сон)	~10 мкА
Роз’єм живлення	Micro-USB