**Міністерство освіти і науки України**

**Луцький національний технічний університет**
(повне найменування закладу вищої освіти)

**Факультет комп'ютерних та інформаційних технологій**
(повне найменування факультету)

**Кафедра комп'ютерної інженерії та безпеки**
(повне найменування кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

## СИСТЕМА БЕЗПЕКИ З ВИКОРИСТАННЯМ RFID ТА МОБІЛЬНИХ ПРИСТРОЇВ

## SECURITY SYSTEM USING RFID AND MOBILE DEVICES

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Іщук Даниїл Вікторович

(підпис)

Керівник:
к.т.н., доцент
Костючко Сергій Миколайович

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 06 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Тарас ТЕРЛЕЦЬКИЙ
« 10 » 01 2025 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

*Іщуку Даниїлу Вікторовичу*
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Система безпеки з використанням RFID та мобільних пристроїв*

Керівник роботи *к.т.н., доц. Костючко Сергій Миколайович*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

3. Вихідні дані до роботи *джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
*Вступ*
*Теоретичні основи побудови систем безпеки з використанням RFID та мобільних технологій*
*Проєктування та обгрунтування апаратних і програмних засобів систем безпеки*
*Практична реалізація системи безпеки на основі RFID та мобільних технологій*
*Висновки*

5. Перелік графічного (ілюстративного) матеріалу:
*Існуючі рішення*
*Використані технології*
*Архітектура системи*
*Схема роботи програмного продукту*

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| *Теоретичні основи побудови систем безпеки з використанням RFID та мобільних технологій* | *Костючко С.М., доцент* | | |
| *Проєктування та обгрунтування апаратних і програмних засобів систем безпеки* | *Костючко С.М., доцент* | | |
| *Практична реалізація системи безпеки на основі RFID та мобільних технологій* | *Костючко С.М., доцент* | | |
| *Нормоконтроль* | *Багнюк Н.В., доцент* | | |
| *Гарант ОП* | *Лавренчук С.В., доцент* | | |
| *Показник запозичень тексту* | ***___%*** | | |
| *Академічна доброчесність* | *Міскевич О.І.,ст.викладач* | | |

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | *Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень* | до 10.02.2025 р. | Виконано |
| 2. | *Теоретичні основи побудови систем безпеки з використанням RFID та мобільних технологій* | до 02.03.2025 р. | Виконано |
| 3. | *Практична реалізація системи безпеки на основі RFID та мобільних технологій* | до 02.04.2025 р. | Виконано |
| 4. | *Висновки та пропозиції* | до 10.04.2025 р. | Виконано |
| 5. | *Формування списку використаних джерел* | до 15.04.2025 р. | Виконано |
| 6. | *Формування додатків* | до 02.05.2025 р. | Виконано |
| 7. | *Оформлення ілюстративного матеріалу* | до 10.05.2025 р. | Виконано |
| 8. | *Представлення остаточного варіанту кваліфікаційної роботи керівникові* | до 15.05.2025 р. | Виконано |
| 9. | *Нормоконтроль* | до 30.05.2025 р. | Виконано |
| 10 | *Інструментальна перевірка на академічний плагіат* | до 03.06.2025 р | Виконано |
| 11. | *Здача кваліфікаційної роботи та всіх супровідних документів на кафедру* | до 10.06.2025 р. | Виконано |

**Здобувач вищої освіти** _____ (підпис) Іщук Д.В. (прізвище, ініціали)

**Керівник кваліфікаційної роботи** _____ (підпис) Костючко С.М. (прізвище, ініціали)

# АНОТАЦІЯ

Іщук Д. В. Система безпеки з використанням RFID та мобільних пристроїв. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків.

Мета роботи – розробити інтегровану систему безпеки, яка забезпечує контроль доступу за допомогою RFID-технологій та мобільного застосунку через Bluetooth.

Об'єкт дослідження – процес контролю доступу до фізичних об'єктів із використанням електронних технологій.

Предмет дослідження – технічні та програмні засоби побудови системи безпеки на основі RFID та мобільного керування.

Перший розділ, в якому розглянуто теоретичні основи побудови систем безпеки з використанням технології RFID та мобільних пристроїв. Проведено аналіз літературних джерел, визначено принципи роботи систем, а також сформульовано основні завдання дослідження.

Другий розділ присвячено обґрунтуванню вибору апаратного та програмного забезпечення. Розглянуто особливості компонентів. Запропоновано архітектуру системи, описано методи інтеграції та розробки, розглянуто питання інформаційної безпеки.

У третьому розділі подано практичну реалізацію проєкту. Описано процес збирання, налаштування та тестування системи. Проаналізовано роботу пристрою, перевірено відповідність отриманих результатів поставленим вимогам. Проведено аналіз ефективності, надійності та стабільності системи.

Ключові слова: система безпеки, RFID, Arduino, Bluetooth, доступ, ідентифікація, контроль доступу.

# ANNOTATION

Ishchuk D. Security system using RFID and mobile devices. Manuscript.

Qualification work for bachelor's degree in Computer Engineering, specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The goal is to develop an integrated security system that provides access control using RFID technology and a mobile application via Bluetooth.

The object of research is the process of controlling access to physical objects using electronic technologies.

The subject of the research is the technical and software tools for building a security system based on RFID and mobile control.

The first chapter discusses the theoretical foundations of building security systems using RFID technology and mobile devices. The author analyzes the literature, defines the principles of operation of the systems and the current state of development of the relevant technologies, and formulates the main objectives of the study.

The second section is devoted to justifying the choice of hardware and software. The features of the components are considered: Arduino Uno, RC522 RFID module, HC-05 Bluetooth module, MG90S servo, buzzer, and others. The system architecture is proposed, integration and development methods are described, and information security issues are considered.

The third section presents the practical implementation of the project. The process of assembling, configuring, and testing the system is described. Code fragments are presented, the operation of the device is analyzed, and the compliance of the results with the requirements is checked. The efficiency, reliability and stability of the developed system are analyzed.

Keywords: security system, RFID, Arduino, Bluetooth, access, identification, access control.

# ЗМІСТ

# ВСТУП

У сучасних умовах питання безпеки об’єктів, майна та доступу до інформації набуває все більшої актуальності. Зі зростанням популярності інтелектуальних систем, інтеграція електронних пристроїв з мобільними технологіями відкриває нові можливості для створення ефективних рішень у сфері контролю доступу. Одним із найбільш перспективних напрямів є застосування технології радіочастотної ідентифікації RFID у поєднанні з мобільними пристроями, що дозволяє підвищити рівень автоматизації, зручності та безпеки. Актуальність дослідження зумовлена необхідністю розробки надійної, недорогої та функціональної системи безпеки, яка легко інтегрується в побутові, освітні або комерційні середовища. Широке використання мікроконтролерів Arduino та сумісних з ними модулів робить можливим створення таких систем навіть без глибоких технічних знань, що сприяє їхній популяризації. При цьому існує потреба в адаптації цих рішень до конкретних умов та сценаріїв використання. Проблематика безконтактного керування доступом активно досліджується упродовж останніх років. Аналізуються аспекти побудови RFID-систем на основі мікроконтролерів, Bluetooth-комунікацій та засобів захисту даних. Вивчаються моделі шифрування даних, а також взаємодія між мікроконтролерами й мобільними додатками. Однак більшість наявних рішень орієнтована на промислові або великі корпоративні системи, тоді як потреби малих об’єктів залишаються менш дослідженими. Це обумовлює доцільність подальшої розробки доступних та простих систем безпеки.

Мета роботи – розробка та реалізація інтегрованої системи безпеки з використанням RFID-технології, яка забезпечує авторизований доступ через RFID-картку або мобільний пристрій.

Завдання дослідження:

– розглянути принципи роботи RFID-системи на базі модуля RC522;

– вивчити особливості роботи мікроконтролера Arduino Uno у контексті системи безпеки;

– визначити методику реалізації бездротового доступу через Bluetooth-модуль HC-05;

– обґрунтувати вибір та реалізувати функціональну схему управління сервоприводом;

– опрацювати програмне забезпечення для взаємодії між RFID-зчитувачем, Bluetooth-модулем та виконавчими елементами;

– протестувати розроблену систему в умовах, наближених до реальних.

Об’єкт дослідження – система контролю доступу на основі електронних компонентів.

Предмет дослідження – програмно-апаратні засоби керування доступом з використанням RFID-технології та мобільних пристроїв.

Методика дослідження включає методи моделювання електронних схем, програмування мікроконтролерів, експериментального тестування, логічного аналізу та системного підходу.

Інформаційна база дослідження сформована на основі технічної документації компонентів (RC522, HC-05, MG90S), довідкових матеріалів з програмування Arduino, даних з офіційних ресурсів, матеріалів наукових конференцій, спеціалізованих форумів, нормативних документів та електронних джерел, пов’язаних із безпекою IoT-систем.

Результати роботи доповідалися на міжнародній науково-практичній конференції молодих вчених та студентів «Програмне та апаратне забезпечення в інформаційних технологіях», Луцьк, 6 травня 2025 року [1].

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ БЕЗПЕКИ З ВИКОРИСТАННЯМ RFID ТА МОБІЛЬНИХ ТЕХНОЛОГІЙ

## 1.1 Поняття та класифікація систем безпеки

Сучасні системи безпеки є невід'ємним інструментом захисту критичних об'єктів, даних та персональної інформації. Завдяки стрімкому розвитку цифрових технологій зростають вимоги до цих систем: вони повинні не лише перешкоджати несанкціонованому доступу, а й бути здатними адаптуватися до сучасних загроз, інтегруватися з іншими системами, забезпечувати централізоване управління, віддалений моніторинг та автоматизоване реагування на події.

Система безпеки – це сукупність технічних, програмних та організаційних засобів, які призначені для виявлення, попередження або усунення загроз безпеці об'єкта чи інформації. Вона виконує функції захисту від несанкціонованого доступу, контролю за переміщенням осіб, ідентифікації користувачів, фіксації подій, реагування на небезпеки тощо.

Залежно від сфери застосування, системи безпеки поділяються на:

– фізичні системи безпеки, які забезпечують охорону територій, будівель, приміщень, технічних засобів;

– інформаційні системи безпеки, що спрямовані на захист комп'ютерних мереж, даних, цифрових ресурсів;

– комбіновані системи, які включають як фізичні, так і інформаційні компоненти, наприклад, системи контролю доступу з біометричними параметрами.

Іншою ознакою класифікації є принцип дії: активні системи, які впливають на об'єкт або загрозу (наприклад, автоматичне блокування дверей), та пасивні, що лише сповіщають про загрозу або фіксують події.

Крім того, важливим параметром є рівень автоматизації та керування. Автономні системи діють самостійно, інтегровані – взаємодіють з іншими

системами (наприклад, пожежною сигналізацією), централізовані – керуються з єдиного пульта або програмного комплексу.

З розвитком технологій інтеграція інтелектуальних систем безпеки, побудованих на мікроконтролерах, датчиках, RFID, біометричних рішеннях, мобільних додатках та хмарних сервісах, набуває все більшої популярності. Такі системи забезпечують високу гнучкість, можливість масштабування та ефективну адаптацію до різних умов експлуатації.

## 1.2 Історія розвитку та еволюція RFID-технологій

Радіочастотна ідентифікація (RFID) – це технологія, що дозволяє здійснювати автоматичну ідентифікацію об’єктів на основі передачі даних через радіохвилі. Її витоки сягають середини XX століття, коли вперше були реалізовані прототипи пристроїв для розпізнавання об’єктів за допомогою електромагнітного випромінювання.

Технологія, найближча до даної припадає на часи Другої світової війни, коли британські військові використовували подібні технології для розпізнавання своїх літаків. Протягом наступних десятиліть відбувався поступовий розвиток цієї технології: зменшувалися габарити міток, підвищувалась швидкість передачі даних, збільшувалася надійність зчитування. У 1980-х роках RFID почала знаходити застосування в логістиці, контролі доступу, виробничих процесах.

У 1990-х роках з появою стандартів і здешевленням виробництва міток, RFID стала масово впроваджуватися в торгівлі, охороні, транспорті. У XXI столітті технологія стала невід’ємною складовою сучасних систем автоматизації й безпеки. Водночас відбулося подальше вдосконалення RFID-систем: з’явилися безконтактні смарт-картки, багаторазові мітки, мітки з можливістю запису інформації, мікросхеми з шифруванням.

На сьогодні RFID-технології поділяються за частотними діапазонами (низькочастотні, високочастотні, ультрависокочастотні) та способом живлення

(пасивні, активні, напівпасивні). Кожен варіант має свої переваги й обмеження залежно від сфери використання.

Системи безпеки з використанням RFID нині успішно застосовуються в офісах, навчальних закладах, промислових підприємствах, лікарнях, а також у побуті – наприклад, для відкриття вхідних дверей чи керування гаражними воротами. Простота, надійність, невисока вартість та можливість інтеграції з іншими технологіями роблять RFID незамінним інструментом у багатьох сферах.

## 1.3 Технічні засоби реалізації систем безпеки з використанням RFID

Побудова ефективної системи безпеки з використанням RFID неможлива без відповідного технічного забезпечення. Основними складовими є RFID-мітки, зчитувачі, контролери, а також допоміжні пристрої для керування доступом – серводвигуни, електромагнітні замки, зумери тощо.

RFID-мітки – це носії інформації, які мають вбудовану антену та мікросхему, що зберігає унікальний ідентифікаційний номер. У побутових системах зазвичай використовують пасивні мітки, які не потребують живлення і активуються під дією зчитувача. Вони можуть бути у вигляді карток, брелоків, наліпок тощо.

Зчитувач RFID (наприклад, модуль RC522) виконує функцію активації мітки та прийому сигналу з неї. Він з'єднується з контролером, який обробляє отримані дані, приймає рішення про допуск чи заборону доступу, а також може передавати інформацію на зовнішні пристрої або в мобільний додаток.

Контролером у багатьох DIY-проєктах виступає плата Arduino Uno – доступна та зручна для розробки. Вона дозволяє реалізувати базову логіку роботи системи, обробку введення/виведення, а також взаємодію з іншими пристроями (наприклад, модулем Bluetooth HC-05 для зв'язку зі смартфоном).

Серводвигун MG90S застосовується для фізичного керування механізмом замка. У разі успішної ідентифікації, мікроконтролер подає сигнал на серво, що повертає замок у відчинене положення.

Для підвищення зручності користування системою застосовуються мобільні додатки. Вони дозволяють реалізувати дистанційне відкриття замка, перегляд логів доступу, зміну налаштувань системи. У випадку використання Bluetooth-зв'язку необхідна наявність відповідного модуля на платі Arduino та на смартфоні.

## 1.4 Мобільні технології як інструмент керування доступом

Мобільні технології суттєво розширили функціональні можливості систем безпеки. Завдяки широкому розповсюдженню смартфонів і планшетів, користувачі можуть керувати системою практично з будь-якого місця. Сучасні мобільні додатки дозволяють не лише відкривати замок, а й налаштовувати систему, додавати нові RFID-картки, перевіряти історію доступу тощо.

Однією з переваг мобільних рішень є можливість реалізації багаторівневої авторизації. Наприклад, навіть після проходження RFID-ідентифікації система може вимагати підтвердження з мобільного пристрою або біометричної перевірки (відбитка пальця, розпізнавання обличчя).

Мобільні додатки для систем безпеки можуть працювати з використанням різних протоколів зв'язку – Bluetooth, Wi-Fi, GSM. Bluetooth-модулі забезпечують пряме з'єднання між смартфоном та контролером, тоді як Wi-Fi або GSM дозволяють керувати системою віддалено, навіть перебуваючи поза межами об'єкта.

В реаліях сьогодення існує велика кількість мобільних додатків для Android та iOS, які підтримують взаємодію з Arduino та RFID. Деякі з них мають відкритий вихідний код, що дозволяє адаптувати програму під власні потреби. У рамках даної роботи планується створення власного мобільного додатку з

можливістю керування замком, авторизацією користувачів та веденням журналу подій.

## 1.5 Перспективи використання RFID та мобільних технологій у системах безпеки

У сучасних умовах стрімкого розвитку інформаційних технологій та зростання потреби у забезпеченні надійного захисту ресурсів, системи безпеки зазнають значних трансформацій. Традиційні методи контролю доступу, такі як механічні замки або навіть кодові панелі, поступово втрачають свою ефективність через зростаючі вимоги до гнучкості, масштабованості та зручності у користуванні. Саме тому на перший план виходять технології, що поєднують апаратні та програмні засоби, зокрема RFID-технології та мобільні додатки.

RFID відкриває можливості не лише для простого контролю доступу, а й для повноцінного моніторингу пересування осіб, автоматизації процесів обліку ресурсів, управління робочими процесами в офісах та на підприємствах. Це дозволяє значно підвищити рівень внутрішньої безпеки об'єкта та забезпечити ефективне управління персоналом.

У поєднанні з мобільними пристроями RFID-технології набувають ще більшої універсальності. Смартфони, обладнані Bluetooth-модулями або NFC, можуть виступати як ключі доступу, пристрої аутентифікації чи інструменти адміністрування системи безпеки. Це, зокрема, забезпечує зручне керування доступом у реальному часі, навіть віддалено, через інтернет або захищене Bluetooth-з'єднання. Застосування мобільних додатків у таких системах дозволяє реалізовувати багаторівневу аутентифікацію, поєднуючи RFID-картку, біометричні дані (відбиток пальця) та пароль.

Крім того, важливо відзначити роль хмарних сервісів та IoT (Інтернету речей), які також тісно інтегруються в системи безпеки на базі RFID. Це дозволяє створювати розподілені системи з централізованим управлінням, де дані зчитування міток, логування подій або активація замків зберігаються в хмарі. Це

не тільки спрощує обслуговування, але й підвищує надійність у випадку локальних збоїв.

Таким чином, можна стверджувати, що технології RFID та мобільні рішення становлять важливу частину сучасної інфраструктури безпеки. Їх ефективна інтеграція дає змогу створювати адаптивні, масштабовані та зручні у використанні системи, що відповідають актуальним вимогам часу.

### 1.6 Дослідження літератури

Безпека є дуже важливим питанням у людському суспільстві. Забезпечення безпеки людей та їхніх цінних речей є дуже важливим для запобігання незаконному поводженню з ними. Забезпечення системи безпеки для будинків стало життєво важливим дослідженням, в якому застосовуються новітні технології для досягнення цієї мети. Бездротова мережа є однією з технологій, які використовуються для забезпечення віддаленого моніторингу та управління домашніми дверима або воротами, бездротові додатки, засновані на безпеці, стрімко зросли завдяки значному вдосконаленню сучасних технологій. Багато систем контролю доступу були розроблені та/або впроваджені на основі різних типів бездротових технологій зв'язку різними людьми [2].

Система безпеки відіграє важливу роль, щоб не допустити невідомих користувачів до несанкціонованого доступу до захищених фізичних та логічних місць. Основні типи систем безпеки – це звичайний дверний замок з ключем, а також електронно-автоматична система ідентифікації. Звичайні замки зазвичай є простими пристроями, які використовуються для вирішення безпосередньо для вирішення проблеми. Крім того, люди можуть зламати замки і отримати доступ до захищених місць. Отже, доводиться конструювати замки, до яких не так легко отримати доступ. У цьому випадку корисним рішенням є автоматичні дверні замки на основі пароля, які широко використовуються в офісах і будинках. Система безпеки застосовує кілька типів ідентифікації технологій, таких як штрих-код, магнітна смуга та радіочастотна ідентифікація (RFID). Одним з

найбільш швидко зростаючих сегментів виробництва автоматичних ідентифікаційних даних та нових технологій є радіочастотна ідентифікація (RFID) в наші дні. Системи автоматичної ідентифікації, які пропонують кращу продуктивність. З цієї причини RFID – це не те саме, що штрих-кодування, яке є оптичною технологією. Між зчитувачем і об'єктом, позначеним RFID-міткою, не потрібна видимість. Технологія RFID використовує радіохвилі для ідентифікації живого чи неживого [3].

RFID впроваджується в багатьох сферах, таких як логістика, ланцюги поставок, відстеження активів, охорона здоров'я, промислові підприємства та багато інших, полегшуючи наше життя і генеруючи величезні обсяги інформації на багатьох рівнях.

Цей оглядовий документ описує найбільш активні теми досліджень, що стосуються технології RFID. Ця інформація допоможе дослідникам виявити прогалини в дослідженнях і визначити актуальні теми. Крім того, вона може бути корисною для інших дисциплін і для тих, хто не належить до академічних кіл, оскільки містить короткий огляд найактивніших досліджень у сфері застосування RFID і питань безпеки.

Опубліковані численні огляди та дослідження, що вивчають RFID з різних точок зору. 2009 року, вчений Arun N. Nambiar зробив огляди про застосування цієї технології. Крім того, я натрапив на огляд, опублікований у 2010 році вченим Benjamin Khoo, про те, як RFID використовується для відстеження в Інтернеті речей (IoT). Огляд конкретних застосувань, наприклад, у поштових і кур'єрських службах, був опублікований у 2006 році вченими Zhang Xiao-dan, Yue Shu-jie, Wang Wei-min. Так само в 2010 році вченими Alok Mishra та Deepti Mishra була опублікована робота про її використання в авіаційній промисловості; робота про її використання в таких видах діяльності, як будівництво, була опублікована в 2015 році вченими Enrique Valero, Antonio Adán та Carlos Cerrada; з 2013 по 2018 рік були публікації, пов'язані з охороною здоров'я; роботи з управління ланцюгами поставок були опубліковані між 2010 і 2016 роками; робота про локалізацію в парадигмі «розумного будинку» була опублікована в 2018 році;

нарешті, в 2020 році був опублікований систематичний огляд літератури про застосування RFID в ланцюгах поставок і його вплив на конкурентні переваги організацій [4], проаналізований з корпоративної, клієнтської та вигідної точок зору. Також був проведений огляд ролі RFID в транспорті [5], в якому були визначені переваги і бар'єри на шляху її впровадження.

# РОЗДІЛ 2
# ПРОЄКТУВАННЯ ТА ОБҐРУНТУВАННЯ АПАРАТНИХ І ПРОГРАМНИХ ЗАСОБІВ СИСТЕМИ БЕЗПЕКИ

## 2.1 Постановка завдання та загальна архітектура системи

Питання забезпечення фізичної безпеки набуває все більшої актуальності як у побутовій, так і в промисловій сферах. Зокрема, зростає потреба у створенні інтелектуальних систем контролю доступу, які здатні забезпечити ефективний захист приміщень та територій від несанкціонованого проникнення. У цьому контексті особливу роль відіграють системи, побудовані на основі безконтактних технологій, таких як RFID (Radio Frequency Identification), а також мобільні пристрої, що слугують інтерфейсом для керування доступом.

Метою розробки цієї системи є створення інтегрованого комплексу безпеки, який поєднує в собі використання RFID-карт, Bluetooth-з'єднання та мобільного додатку для забезпечення доступу до об'єкта. У проєкті передбачається реалізація апаратно-програмного рішення, яке дозволить авторизованим користувачам відкривати замок за допомогою одного з трьох способів: RFID-карти, мобільного додатку через Bluetooth або спеціального коду.

Таким чином, основним завданням є проєктування системи, яка відповідала б наступним вимогам:

– забезпечення надійної ідентифікації користувача;

– можливість вибору методу доступу (RFID, Bluetooth, код);

– автономна робота без постійного підключення до мережі Інтернет;

– простота монтажу та обслуговування;

– енергоефективність та низький рівень споживання енергії;

– можливість модернізації та масштабування у майбутньому.

Для реалізації цього завдання обрано модульну архітектуру, яка включає апаратну частину (мікроконтролер Arduino Uno, RFID-модуль RC522, Bluetooth-модуль HC-05, сервопривід MG90S, зумер для звукової індикації, джерело

живлення) та програмне забезпечення (скетч Arduino, мобільний додаток, створений на базі MIT App Inventor або аналогічної платформи).

Загальна логіка роботи системи полягає в наступному. При наближенні RFID-карти до зчитувача, мікроконтролер зчитує унікальний код та порівнює його з попередньо записаними у пам'яті пристрою значеннями. У разі збігу здійснюється відкриття замка за допомогою сервоприводу, що обертає механізм. Альтернативно, користувач може скористатись мобільним додатком, який через Bluetooth надсилає команду на Arduino. Якщо авторизація проходить успішно – система активує сервопривід. Для ще більшої універсальності можлива реалізація функції введення цифрового коду у самому застосунку, що підвищує гнучкість використання.

Усі дії користувача супроводжуються звуковими сигналами зумера, які інформують про успішну або невдалу авторизацію. Наприклад, один короткий сигнал означає успішний вхід, два коротких – помилка зчитування, а довгий – відмову у доступі.

Основні компоненти системи взаємодіють між собою за такими інтерфейсами:

– SPI (Serial Peripheral Interface) – для комунікації між Arduino та RFID RC522;

– UART (Serial) – для зв'язку Arduino з Bluetooth-модулем HC-05;

– PWM (Pulse Width Modulation) – для керування сервоприводом;

– Digital I/O – для керування зумером та іншими компонентами.

Завдяки такій архітектурі забезпечується розділення функціональних модулів, що, у свою чергу, спрощує подальшу підтримку, модернізацію та масштабування системи.

## 2.2 Вибір апаратних компонентів системи

На етапі розробки апаратної частини системи контролю доступу особливу увагу було приділено підбору компонентів, які забезпечують не лише належний

рівень функціональності, але й простоту у використанні, економічність, доступність та надійність. При створенні системи безпеки з використанням RFID-технологій та мобільного пристрою важливо правильно обрати апаратні компоненти, які зможуть ефективно взаємодіяти один з одним та виконувати поставлені завдання.

У цьому підрозділі розглядається вибір ключових елементів, які формують основу системи, а саме: мікроконтролер Arduino Uno, зчитувач RFID RC522, Bluetooth-модуль HC-05, сервопривід MG90S та зумер. Крім того, аналізуються альтернативні рішення, що потенційно можуть бути використані замість обраних компонентів.

Arduino Uno (рис. 2.1) є одним із найпопулярніших мікроконтролерів серед розробників систем автоматизації, прототипування та IoT-рішень. Він заснований на мікроконтролері ATmega328P, має достатню кількість цифрових та аналогових входів/виходів, підтримує UART, SPI, I2C протоколи, а також володіє широкою базою готових бібліотек.

Однією з ключових переваг Arduino Uno є його відкритість та доступність. На відміну від багатьох комерційних платформ, Arduino має розвинену спільноту, велику кількість прикладів коду, документації та бібліотек, що значно пришвидшує процес розробки. Крім того, Uno підтримується в Arduino IDE, яка дозволяє швидко компілювати, завантажувати і тестувати скетчі без необхідності встановлення складних середовищ розробки.

Завдяки простоті підключення периферійних пристроїв, Arduino Uno стає ідеальним рішенням для проєктів, де важлива гнучкість і можливість швидкого налаштування. В нашій системі Arduino Uno виступає як центральний блок управління, що обробляє сигнали з RFID-зчитувача та Bluetooth-модуля, а також керує сервоприводом і зумером.

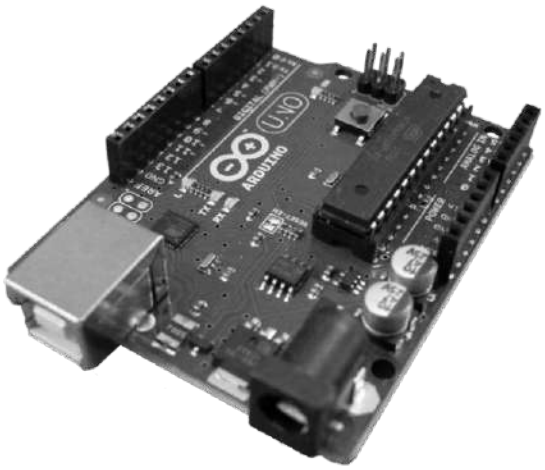

Рисунок 2.1 – Arduino Uno [6]

RFID (Radio Frequency Identification) – це технологія автоматичної ідентифікації об’єктів за допомогою радіохвиль. У цьому проєкті використовується модуль RC522, який працює на частоті 13,56 МГц і підтримує стандарт ISO/IEC 14443 A. Даний модуль дозволяє зчитувати дані з RFID-міток або карт на відстані до 5 см, що є достатнім для побутового використання.

Модуль RC522 (рис. 2.2) має вбудовану антену та забезпечує надійне зчитування UID (унікального ідентифікатора) карт. Він підключається до Arduino за допомогою інтерфейсу SPI, що забезпечує високу швидкість передачі даних.

Основними перевагами RC522 є:

– невеликий розмір та простота монтажу;

– низьке енергоспоживання;

– наявність широкої підтримки у вигляді бібліотек Arduino;

– доступна вартість.

Завдяки цим характеристикам модуль RC522 є доцільним вибором для створення системи доступу, де необхідне надійне зчитування RFID-карт без контакту.


Рисунок 2.2 – RFID RC522 [7]

HC-05 – це Bluetooth-модуль класу 2, який забезпечує бездротову передачу даних між мікроконтролером та мобільним пристроєм. Він підтримує Bluetooth 2.0 і має радіус дії до 10 метрів у стандартних умовах.

HC-05 (рис. 2.3) легко інтегрується з Arduino через UART-інтерфейс. Його налаштування здійснюється за допомогою AT-команд, що дозволяє змінювати параметри з'єднання, ім'я пристрою, пароль, швидкість передачі даних тощо. У нашій системі HC-05 дозволяє користувачеві за допомогою смартфона надсилати команди на Arduino, що значно підвищує зручність взаємодії.

До переваг модуля можна віднести:

– стабільне з'єднання з мобільними пристроями;

– можливість роботи в ролі відправника або приймача;

– підтримка широкого діапазону напруг живлення (від 3,3 В до 6 В);

– активна спільнота та багато прикладів реалізації на Arduino.

Завдяки цим характеристикам, модуль HC-05 є ідеальним вибором для реалізації бездротової взаємодії у проєкті.

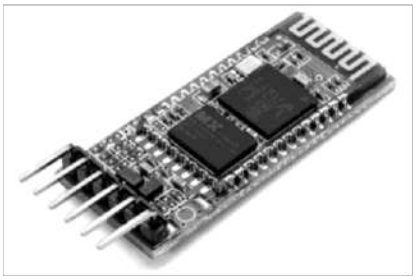

Рисунок 2.3 – Bluetooth HC-05 [8]

Серед ключових елементів системи фізичного доступу, важливу роль відіграє сервопривід, що відповідає за безпосереднє керування механічним замком. У межах цього проєкту було обрано сервопривід MG90S, який є вдосконаленою версією популярного SG90. Основною перевагою MG90S є металеві шестерні, які забезпечують більшу надійність, зносостійкість і збільшений крутний момент у порівнянні з аналогами на пластикових шестернях.

MG90S (рис. 2.4) має компактні розміри, працює у межах обертання від 0 до 180 градусів та сумісний з Arduino через стандартний PWM-сигнал. Це дозволяє інтегрувати його у систему без потреби в додаткових драйверах чи складних налаштуваннях. Такий сервопривід легко забезпечує необхідну силу для переміщення механізму замикання навіть при більшому навантаженні.

У контексті даної системи безпеки MG90S використовується для керування замком: він обертається в заданий напрям після успішної авторизації користувача за допомогою RFID-карти або мобільного додатку через Bluetooth. Стабільна робота, швидка реакція на команду та сумісність із різними джерелами живлення роблять цей компонент оптимальним вибором для задач такого типу.

До переваг MG90S належать:

– підвищена міцність завдяки металевим шестерням;

– крутний момент до 2.2 кг·см, що перевищує можливості SG90;

– просте керування за допомогою Arduino IDE;

– сумісність із широким спектром напруг живлення (4,8-6 В);

– швидкий відгук та точне позиціонування.

Таким чином, MG90S дозволяє підвищити надійність та довговічність системи, не ускладнюючи її реалізацію та залишаючись в межах розумної вартості.


Рисунок 2.4 – Сервопривід MG90S [9]

Зумер (рис. 2.5) використовується в системі для звукової індикації дій користувача. Наприклад, він подає короткий сигнал при успішному зчитуванні RFID-карти або надсиланні команди через Bluetooth, або довгий сигнал у випадку помилки.

Наявність звукового супроводу значно покращує зручність використання пристрою, адже користувач отримує миттєвий зворотний зв'язок. Для реалізації використано п'єзоелектричний зумер, який легко підключається до цифрового виходу Arduino і не вимагає додаткових модулів керування. За допомогою простого коду можна задавати тривалість і частоту сигналів, адаптуючи їх до різних ситуацій.

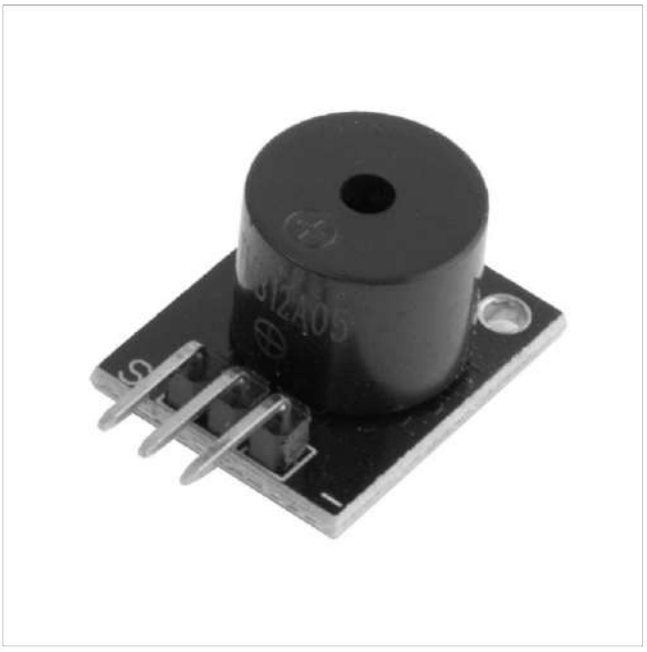

Рисунок 2.5 – Зумер [10]

Попри те, що в цьому проєкті були обрані компоненти Arduino Uno, RC522, HC-05, MG90S та п’єзоелектричний зумер, існує низка альтернативних рішень, які можуть бути використані у майбутніх модифікаціях системи.

ESP32 (рис. 2.6) – сучасний мікроконтролер із вбудованими модулями Wi-Fi та Bluetooth, який дозволяє створювати компактніші й функціональніші системи. Проте він вимагає більш глибокого розуміння мікроконтролерного програмування.

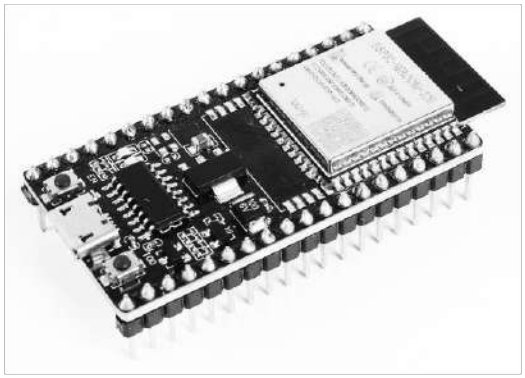

Рисунок 2.6 – ESP32 [11]

Wi-Fi модулі (ESP8266) (рис. 2.7) – дають змогу підключити систему до Інтернету, забезпечуючи віддалений доступ. Недоліком є менша стабільність зв’язку у порівнянні з Bluetooth у деяких умовах.

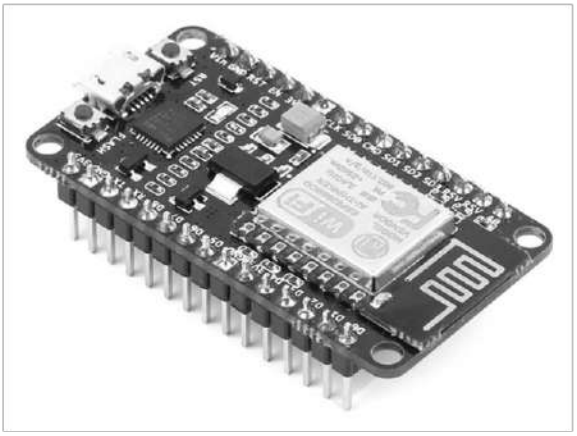

Рисунок 2.7 – ESP8266 [12]

NFC (PN532) (рис. 2.8) – працює на коротшій відстані, що зменшує ризик несанкціонованого зчитування, проте вимагає точного позиціонування пристрою та складнішої інтеграції.

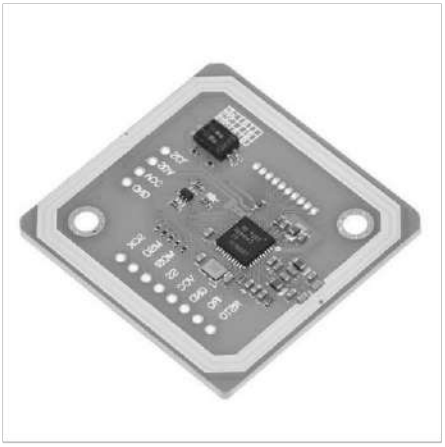

Рисунок 2.8 – PN532 [13]

Альтернативні Bluetooth-модулі (HC-06, HM-10) – забезпечують передачу даних, але не завжди підтримують зміну ролі пристрою або складніші протоколи. HC-05 залишається універсальним вибором завдяки гнучкості налаштувань.

Інші сервоприводи (SG90, MG996R) – можуть бути використані в залежності від потреб. SG90 дешевший, але менш потужний. MG996R забезпечує ще більшу силу, проте має більші габарити та споживання енергії.

Таким чином, обрані компоненти, зокрема MG90S, забезпечують надійність, простоту використання, сумісність із Arduino, а також можливість подальшого масштабування системи. Вони дозволяють розробити систему безпеки, яка є ефективною, доступною для реалізації та легко адаптується до нових вимог.

## 2.3 Інтеграція апаратної частини

Інтеграція апаратної частини є ключовим етапом у розробці будь-якої вбудованої системи, адже саме на цьому етапі всі обрані модулі та пристрої об’єднуються в єдину функціональну структуру. В контексті системи безпеки на

базі Arduino Uno інтеграція полягає у фізичному з'єднанні таких компонентів, як модуль RFID RC522, Bluetooth-модуль HC-05, сервопривід MG90S, зумер і додаткові живильні елементи. Кожен із цих компонентів має свої особливості підключення, які необхідно врахувати, щоб забезпечити стабільну та надійну роботу системи.

RFID RC522 працює через інтерфейс SPI (Serial Peripheral Interface). Для забезпечення коректної роботи з Arduino Uno використовуються наступні контакти:

– SDA → D10;

– SCK → D13;

– MOSI → D11;

– MISO → D12;

– RST → D9;

– VCC → 3.3V;

– GND → GND.

Особливу увагу слід приділити живленню цього модуля: він потребує 3.3V, а не 5V, оскільки в іншому випадку є ризик пошкодити мікросхему.

Bluetooth HC-05 підключається через послідовний інтерфейс UART. Зазвичай використовується програмна реалізація серійного порту, наприклад, за допомогою бібліотеки SoftwareSerial:

– TX → D2;

– RX → D3;

– VCC → 5V;

– GND → GND.

При підключенні слід врахувати, що рівень логіки на піні RX модуля не повинен перевищувати 3.3V, тому рекомендується використовувати дільник напруги.

Сервопривід MG90S підключається до одного з PWM-виходів плати Arduino Uno, зазвичай до D6 або D7. Він має три виводи:

– сигнальний (оранжевий) → D6;

– VCC (червоний) → 5V;

– GND (коричневий) → GND.

Сервоприводи можуть створювати пульсації напруги при роботі, тому важливо використовувати конденсатори для згладжування або додаткові джерела живлення при підключенні декількох сервоприводів.

Зумер (п'єзоелектричний або активний) підключається до цифрового виходу, наприклад, D8. Через Arduino він отримує сигнали високого або низького рівня, що викликає звук:

– VCC → D8;

– GND → GND.

Цей пристрій слугує як сигнал тривоги або індикації події, наприклад, доступу до системи.

Інтеграція всіх елементів потребує чіткого планування розміщення на макетній платі або монтажу на друкованій платі (PCB). Для прототипу найчастіше використовують макетну плату (breadboard), яка дозволяє швидко змінювати з'єднання без пайки.

Оскільки Arduino Uno має обмежену кількість цифрових входів/виходів, дуже важливо ефективно розпоряджатися доступними пін-ком. У деяких випадках можна застосовувати мультиплексори, логічні елементи або просто планувати схему так, щоб уникнути конфліктів у призначенні пінів.

Також необхідно враховувати можливі електричні перешкоди – особливо при роботі Bluetooth та RFID одночасно, оскільки обидва пристрої мають бездротову природу. Рекомендується використовувати екрановані дроти для чутливих сигналів і мінімізувати довжину проводів.

## 2.4 Вибір програмних засобів і логіка роботи системи

Програмне забезпечення є невід'ємною частиною будь-якої системи безпеки, побудованої на базі мікроконтролерів. Воно виконує роль інтелектуального ядра, яке забезпечує взаємодію між усіма апаратними

компонентами системи, приймає рішення на основі отриманих даних, а також реалізує логіку доступу й зворотного зв'язку з користувачем. У даному проєкті основним інструментом розробки прошивки для мікроконтролера є середовище Arduino IDE, а для створення мобільного застосунку – платформа візуального програмування MIT App Inventor. Вибір саме цих програмних засобів є обґрунтованим як з точки зору функціональності, так і з погляду зручності використання в умовах обмежених ресурсів.

Arduino IDE (Integrated Development Environment) – це офіційне середовище для розробки програмного коду (скетчів) для плат Arduino. Воно має набір інструментів, які дозволяють редагувати код, компілювати та налагоджувати все через графічний інтерфейс, а також дає нам можливість взаємодіяти з мікроконтролером, зберігаючи складені програми в його внутрішній пам'яті для запуску всього обладнання. Додаток IDE є вільним програмним забезпеченням, оскільки його вихідний код доступний і розміщений на GitHub і пропонує інструкції з компіляції [14].

Основні переваги Arduino IDE:

– підтримка великої кількості бібліотек для підключення модулів RFID, Bluetooth, сервоприводів, зумерів тощо;

– простий синтаксис, що дозволяє швидко почати роботу навіть початківцям;

– можливість моніторингу послідовного порту, що спрощує налагодження;

– кросплатформеність: підтримується Windows, Linux, macOS.

У межах проєкту була використана низка бібліотек, зокрема:

– MFRC522.h – для роботи з RFID RC522;

– SoftwareSerial.h – для створення віртуального UART для HC-05;

– Servo.h – для керування сервоприводом MG90S.

Код системи базується на простій логіці: при зчитуванні RFID-карти її ID порівнюється з попередньо збереженими значеннями. Якщо співпадіння є, активується сервопривід, який відкриває замок, а також подається сигнал на зумер. У випадку відмови – відтворюється відповідний звуковий сигнал.

У коді також реалізовано обробку команд, що надходять через Bluetooth-з'єднання з мобільного пристрою. Це дозволяє дублювати керування – як за допомогою RFID, так і через смартфон, що є зручним резервним варіантом.

Для створення застосунку, який керує системою з мобільного пристрою, обрано платформу MIT App Inventor. Цей інструмент дозволяє створювати Android-застосунки на основі блочного програмування, що значно спрощує процес розробки.

Середовище має візуальний інтерфейс, де кожен блок виконує певну функцію (з'єднання Bluetooth, надсилання команд, отримання відповідей тощо). Програма, створена за допомогою MIT App Inventor, дозволяє:

– підключатися до модуля HC-05 по Bluetooth;

– надсилати команди для відкриття/закриття замка;

– отримувати зворотний сигнал (наприклад, про успішний вхід);

– виводити статус з'єднання на екран користувача;

– реалізувати додаткові функції (запит на авторизацію, журнал доступу тощо).

Переваги платформи:

– простота використання – не потребує знання мов програмування;

– гнучкість – дозволяє додавати графіку, кнопки, текстові поля;

– швидкість розробки – прототип можна створити за кілька годин;

– онлайн-доступ – не потрібно встановлювати ПЗ на комп'ютер.

Застосунок можна встановити на будь-який смартфон з Android через файл .apk або QR-код. Система перевіряє команду, надіслану з додатку, та виконує відповідну дію через Arduino.

Уся логіка взаємодії в системі реалізується на рівні програмного коду. Послідовність дій така:

– мікроконтролер перебуває в режимі очікування сигналу від RFID-зчитувача або Bluetooth-модуля;

– якщо піднесено карту, зчитується її ID. Система порівнює його зі збереженими значеннями;

– у випадку збігу ID – сервопривід активується, зумер подає звуковий сигнал;

– у разі надходження команди з мобільного пристрою (наприклад, «відкрити замок»), Arduino також активує виконавчі пристрої;

– система може передати відповідь назад на мобільний застосунок – підтвердження дії або повідомлення про помилку.

Ця двоканальна модель управління дозволяє реалізувати резервний контроль доступу. Якщо з якоїсь причини RFID-карта не спрацювала (наприклад, пошкодження), користувач завжди може скористатись мобільним застосунком.

Альтернативно до MIT App Inventor можна було б використати:

– Kodular: платформа для створення мобільних застосунків без навичок програмування. Можливість застосування реклами для застосунку, покупки в додатку, та інші функції;

– Thunkable: навідміну від попередньої платформи, Thunkable підтримує розробку не тільки для Android, а ще й для iOS, та пропонує додаткові функції за підписку;

– Android Studio: офіційне середовище розробки, розроблене компанією Google, яке має підтримку Kotlin, Java та C++;

– Blynk: платформа, яка підтримує широкий спектр апаратних модулів, таких як ESP32, Arduino, Raspberry Pi та інші.

Однак, з урахуванням простоти реалізації, часу на розробку та навчання, MIT App Inventor є найбільш доцільним вибором у рамках даного проєкту.

## 2.5 Заходи інформаційної безпеки в системі

Інформаційна безпека – один із ключових аспектів, який потрібно враховувати при розробці будь-якої системи доступу, особливо коли мова йде про захист приміщень або об’єктів із обмеженим входом. Навіть якщо система побудована на недорогих компонентах і призначена для побутового або

навчального використання, вона повинна мати базовий захист від типових векторів атак і несанкціонованого доступу. Акцент зроблено на трьох напрямках: безпека RFID-ідентифікаторів, захист Bluetooth-з'єднання, а також загальна архітектурна стійкість системи до атак.

Ключова функція системи – контроль доступу. Для цього використовуються RFID-карти або мобільний застосунок, що передає команду через Bluetooth. Якщо зловмисник спробує отримати доступ до системи без належного ідентифікатора, вона не повинна виконати жодної дії.

Для забезпечення цього:

– у коді жорстко прописано дозволені UID RFID-карток. Усі інші ідентифікатори ігноруються;

– аналогічно, з боку Bluetooth передбачено прийом лише певних команд (наприклад, «OPEN», «LOCK»), які перевіряються на відповідність;

– система не виконує жодних дій, поки не отримано валідну команду або правильний UID;

– можна додати лічильник невдалих спроб доступу та блокування системи на певний час.

Ці заходи дозволяють уникнути простої підміни картки або випадкового підключення стороннього Bluetooth-пристрою.

RFID-технологія (зокрема, 13,56 МГц модуль RC522) має певні слабкі місця. Уразливість полягає в тому, що UID багатьох дешевих RFID-карт можна скопіювати за допомогою спеціального обладнання (наприклад, зчитувачів з функцією клонування). Це створює ризик несанкціонованого дублювання ключа доступу.

З метою зменшення ризику:

– використовуються не стандартні UID, а зашифровані команди або UID у зв'язці з секретним кодом;

– у перспективі можливо впровадити алгоритм шифрування UID або використовувати захищені RFID-картки з криптографічною автентифікацією (наприклад, MIFARE DESFire);

– користувачу рекомендується зберігати картки окремо від пристрою та не передавати їх третім особам.

Варто зазначити, що елементарна обфускація UID у програмному коді (скажімо, у вигляді хешування) суттєво ускладнює процес клонування, особливо для тих, хто не має відповідної підготовки з боку зловмисників.

Bluetooth-модуль HC-05 працює через протокол UART, який не має вбудованого шифрування, проте деякі заходи безпеки можна реалізувати на логічному рівні. Основні ризики Bluetooth-з'єднання – це можливість несанкціонованого підключення до модуля та прослуховування переданої інформації.

Для підвищення безпеки можлива подальша реалізація:

– HC-05 переведено у режим «приймача», тобто він лише приймає підключення, але сам не ініціює їх;

– змінено стандартний PIN-код (1234 або 0000) на власний, складніший, що ускладнює з'єднання сторонніх пристроїв;

– додано програмну перевірку команд. Наприклад, навіть якщо хтось підключиться до модуля, він не зможе активувати замок без правильної структури команди;

– Bluetooth-з'єднання можна обмежити у часі – модуль активується лише після зчитування RFID або у певні години;

– у разі підозрілих дій можна реалізувати логування спроб з'єднання для подальшого аналізу.

Також доцільним є оновлення Bluetooth-модуля на більш сучасну версію (наприклад, HC-05 з підтримкою AT-команд або модуль HM-10 з BLE), які підтримують додаткові функції безпеки.

Попри заходи безпеки, жодна система не є повністю захищеною. Потенційні вектори атак включають:

– можливість перепідключення проводів або заміна RFID-зчитувача. Для уникнення – усі з'єднання зафіксовані та заховані в корпусі;

– сканування, підключення, надсилання шкідливих команд. Вирішується зміною PIN, обмеженням команд, логічною перевіркою;

– підбір UID або послідовностей команд. Обмежується кількістю спроб і запровадженням пауз після невдалих спроб;

– у деяких випадках зчитувач може приймати картки з відстані до 5-10 см.

# РОЗДІЛ 3
# ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ НА ОСНОВІ RFID ТА МОБІЛЬНИХ ТЕХНОЛОГІЙ

## 3.1 Архітектура та структура системи

Розроблена система безпеки з використанням RFID-технології та мобільних пристроїв базується на інтеграції апаратного та програмного забезпечення, об'єднаних у єдину функціональну структуру. Архітектура системи була сформована з урахуванням вимог до надійності, простоти реалізації, гнучкості, а також можливості подальшої модифікації. У процесі проєктування особливу увагу приділено забезпеченню ефективної взаємодії між апаратною частиною – фізичними компонентами системи – та програмним забезпеченням, яке забезпечує логіку їхньої роботи.

Загальна архітектура системи передбачає централізоване керування всіма ключовими процесами через мікроконтролер Arduino Uno. Саме цей елемент виконує роль «центру управління», який координує всі сигнали, отримані від зовнішніх пристроїв, та приймає рішення щодо надання або відмови в доступі. Взаємодія між користувачем і системою може здійснюватися двома основними способами: через RFID-картку або через мобільний додаток, що з'єднується із системою по Bluetooth. Таке поєднання двох каналів доступу дозволяє підвищити зручність використання системи, а також забезпечує додаткову гнучкість – наприклад, можливість використання смартфона як альтернативного ідентифікатора.

Основна функція системи полягає у здійсненні перевірки прав доступу та, у разі успішної аутентифікації, керуванні виконавчим елементом – у цьому випадку сервоприводом, який імітує механізм замка. Вся логіка функціонування системи полягає в тому, що мікроконтролер після зчитування даних з RFID-картки або мобільного додатку порівнює отриману інформацію з попередньо записаними значеннями. На рисунку 3.1 зображено блок схему пристрою.

Якщо збіг підтверджено, система подає сигнал на виконавчий елемент і зумер, що підтверджує дію зворотним звуковим сигналом. У разі помилки – наприклад, при використанні недійсної картки або неправильного коду – система залишається заблокованою, і зумер видає звук іншої тональності, по зрівнянню з дійсною карткою, що є базовим механізмом забезпечення безпеки.

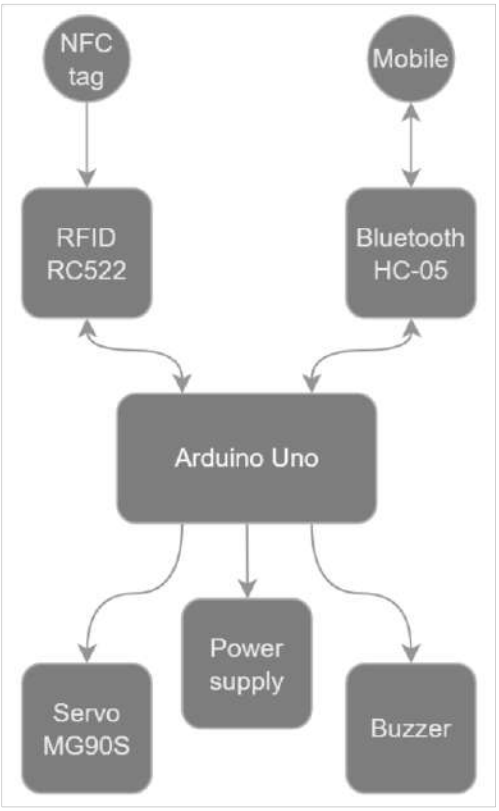


Рисунок 3.1 – Блок схема пристрою

З погляду структурної організації, система включає декілька апаратних вузлів, з'єднаних між собою відповідно до заданої логіки. RFID-зчитувач підключається до мікроконтролера та забезпечує отримання унікального ідентифікаційного номера з картки користувача. Bluetooth-модуль HC-05 дає змогу встановити бездротове з'єднання з мобільним пристроєм та обробляти команди, які надходять від користувача через додаток. Сервопривід виконує фізичну дію – наприклад, імітує відкривання дверного замка – тоді як зумер слугує для подачі звукових сигналів, що підвищує зручність взаємодії з пристроєм.

Для кращого розуміння загальної архітектури системи доцільно уявити її у вигляді взаємопов'язаних функціональних блоків. На вхід подаються команди від RFID або Bluetooth-модуля, далі Arduino обробляє їх, після чого система реагує відповідним чином – або відкриває замок, або залишає систему заблокованою. Для відстеження об'ємних активів мітка місцезнаходження повинна бути доступною за ціною і мати тривалий час автономної роботи. Мітки NFC не використовують батарейки, але вимагають, щоб приймач знаходився в межах 20 см від мітки, що обмежує їхню корисність. GPS-трекери не є надійними в приміщеннях, оскільки сигнали супутникового стеження можуть бути заблоковані, особливо сталевими та залізобетонними конструкціями [15]. Популярне рішення для відстеження активів базується на функції визначення місцезнаходження Bluetooth-маячка. Цей метод відстежує положення мітки, порівнюючи потужність опорного сигналу, закодованого в повідомленні маяка, з потужністю прийнятого сигналу. Потім позиція маяка тріангулюється за допомогою трьох або більше приймачів, щоб наближено визначити його місцезнаходження. Тим не менш, такий підхід не забезпечує точності, необхідної для систем управління запасами. Крім того, на точність визначення місцезнаходження можуть впливати зміни вологості та рухомі об'єкти, такі як навантажувачі, працівники та двері [16]. Хоча для вимірювання дальності від розпізнаної позиції можна використовувати індикатор сили сигналу Bluetooth (RSSI), часто ця методика не є точною для таких цілей, як система визначення місцезнаходження в приміщенні (ILS) та відстеження ресурсів [17]. Потрібне надійне, економічно ефективне і точне рішення з живленням від батареї для бездротового відстеження активів, яке можна використовувати в приміщеннях, а також з тривалим терміном служби батареї [18]. Усі процеси відбуваються у реальному часі, що забезпечує швидкий відгук та зручність використання [19].

Отже, запропонована архітектура є досить простою, але водночас функціонально завершеною. Вона забезпечує як базові вимоги до систем безпеки, так і дозволяє легко масштабувати систему – наприклад, додавши

можливість керування через інтернет або підключення нових методів автентифікації, таких як біометричні дані.

### 3.2 Реалізація апаратної частини системи

Побудова апаратної частини системи безпеки є одним із найважливіших етапів практичної реалізації проєкту. Від коректного вибору, налаштування та взаємодії між фізичними компонентами залежить стабільність і функціональність усієї системи. У даній роботі використано доступні, надійні й добре документовані апаратні елементи, які забезпечують ефективну взаємодію між собою та з програмною частиною. Метою цього етапу стало створення працездатної схеми, здатної виконувати функції ідентифікації користувача, обробки сигналів доступу та керування виконавчим механізмом.

Центральним елементом системи є мікроконтролер Arduino Uno, який виступає в ролі головного обчислювального модуля. Завдяки широкій підтримці серед розробників, відкритій архітектурі та численним бібліотекам для роботи з різними пристроями, Arduino Uno став зручним і надійним вибором для розробки прототипу. Його достатньо для обробки сигналів від периферійних пристроїв і реалізації основної логіки системи доступу.

Органічна електроніка пропонується як потенційний кандидат для задоволення таких потреб, зокрема для повсюдного використання радіочастот. Проте, обмеження з точки зору продуктивності пристроїв в радіочастотному діапазоні, особливо серйозні, коли застосовуються великі площі і масштабовані технології виготовлення, значною мірою перешкоджають досягненню такого привабливого сценарію [20]. Для забезпечення функції безконтактної ідентифікації в системі використано модуль RFID RC522, який працює на частоті 13,56 МГц. Його основне завдання – зчитування унікального ідентифікатора з RFID-картки, що передається до Arduino для подальшої перевірки. RC522 є відносно компактним і енергоефективним модулем, що легко інтегрується через SPI-інтерфейс, що забезпечує високу швидкість обміну даними між ним і

мікроконтролером. Підключення цього модуля здійснюється через стандартні піни: MOSI, MISO, SCK, SDA та GND, що полегшує його інсталяцію навіть для новачків у мікроелектроніці.

HC-05 – це бездротовий модуль Bluetooth з протоколом послідовного порту (SPP), що працює на частоті 2,4 ГГц, цей модуль може використовуватися як ведений (приймач), а також може бути ведучим (відправником) [21]. Для реалізації можливості керування системою з мобільного пристрою використовується модуль Bluetooth HC-05. Його основна функція – встановлення бездротового зв'язку зі смартфоном, через який користувач може надсилати сигнали для авторизації або відкриття замка. HC-05 є серійним модулем, що підтримує класичний Bluetooth-протокол, має просту схему підключення через UART-інтерфейс і дозволяє здійснювати двосторонній обмін даними з Arduino. За рахунок цього користувач може взаємодіяти з системою у зручний спосіб, навіть не маючи фізичного доступу до RFID-картки.

Фізичне керування замком реалізується за допомогою сервоприводу MG90S, який виконує обертальний рух в межах заданого кута. Цей сервомотор обрано завдяки його компактності, надійності та достатній потужності для приводу простого замкового механізму або імітації його роботи. Сервопривід підключається до PWM-виходу мікроконтролера і реагує на команду, яка надходить після успішної перевірки ідентифікатора. Рух сервоприводу є візуальним і функціональним підтвердженням дії системи.

Для покращення взаємодії з користувачем і зручності експлуатації до системи було додано зумер, який слугує для подачі звукових сигналів у разі успішного або невдалого доступу. Завдяки цьому компоненту користувач отримує миттєвий звуковий відгук, що підвищує інформативність роботи пристрою. Зумер активується коротким сигналом з Arduino у відповідь на певну подію, наприклад, після розпізнавання RFID-картки або при помилці доступу.

Збірка апаратної частини передбачала послідовне з'єднання всіх компонентів згідно з електричною схемою. Особливу увагу було приділено правильному підключенню живлення, щоб уникнути перевантаження лінії

живлення мікроконтролера. Застосовано додаткові резистори, що захищають сигнальні лінії, а також було враховано рівні напруги між модулями. Усі компоненти змонтовано на макетній платі, що дає змогу легко тестувати систему, вносити зміни та усувати помилки під час налаштування.

Таким чином, апаратна частина системи є результатом ретельного підбору та гармонійного поєднання електронних компонентів, які забезпечують основні функціональні можливості розробленого прототипу. Вона виконує всі поставлені завдання, зберігаючи при цьому простоту конструкції, що є перевагою на етапі створення, тестування й подальшого вдосконалення системи безпеки.

### 3.3 Розробка програмного забезпечення та логіки системи

Розробка програмного забезпечення є одним з ключових етапів побудови системи безпеки з використанням RFID та мобільних пристроїв, адже саме програмна частина забезпечує логіку функціонування пристрою, його реакцію на дії користувача та обробку сигналів від різних датчиків і модулів. Від якості написаного коду, його оптимізації та стійкості до помилок залежить надійність і безперервність роботи всієї системи.

У процесі розробки враховувалася необхідність створення надійної, стабільної та легко модифікованої програми. Вибір був зроблений на користь мови програмування C/C++, яка є стандартною для розробки під платформу Arduino. Ця мова дозволяє працювати безпосередньо з апаратними ресурсами плати, а також забезпечує достатній контроль над обробкою сигналів, затримками та взаємодією з підключеними модулями.

Для написання, компіляції та завантаження коду в мікроконтролер Arduino Uno використовувалося середовище розробки Arduino IDE, зображене на рисунку 3.2.


Рисунок 3.2 – Інтерфейс Arduino IDE

Це офіційне середовище для програмування плат Arduino, яке забезпечує простий і зручний інтерфейс, підтримує автоматичну компіляцію, монітор порту, бібліотеки сторонніх виробників та плагіни. Робота з Arduino IDE дозволила швидко розпочати розробку, а також без зайвих зусиль налагоджувати з'єднання з контролером, перевіряти помилки компіляції та тестувати роботу коду у реальному часі.

Середовище підтримує використання численних бібліотек, таких як MFRC522 для роботи з RFID RC522, Servo для управління сервомеханізмом MG90S, а також стандартну бібліотеку SoftwareSerial для створення додаткового серійного порту, необхідного для спілкування з Bluetooth-модулем HC-05. Використання Arduino IDE дозволило легко підключати ці бібліотеки, налаштовувати порти введення/виведення та реалізовувати логіку обробки сигналів у структурованій формі.

Програмна логіка реалізовувалася поступово – спершу було написано базовий код, що дозволяє зчитувати RFID-мітки з модуля RC522 та виводити їхній унікальний ідентифікатор у серійну консоль. Це дозволило перевірити працездатність самого модуля й наявність зв'язку з Arduino Uno. Після цього було реалізовано збереження авторизованих UID (унікальних ідентифікаторів) у масиві, щоб система могла порівнювати зчитані значення з дозволеними. На

рисунку 3.3 зображена блок схема логіки. У разі відповідності – система переходить до фази виконання дій, зокрема відкривання замка.

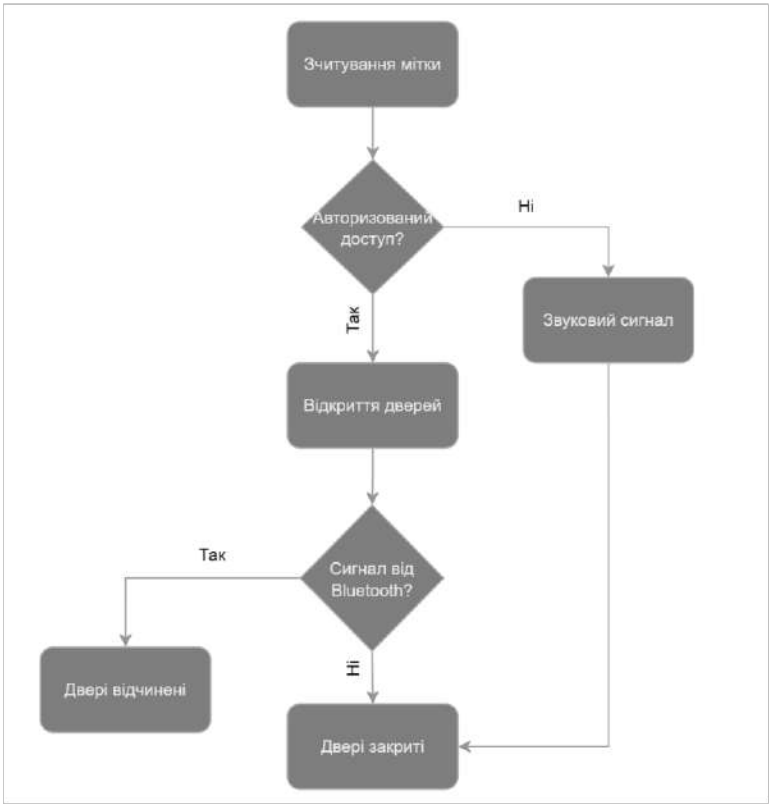


Рисунок 3.3 – Блок схема логіки

На наступному етапі відбувалася інтеграція Bluetooth-модуля HC-05, що забезпечує бездротовий зв’язок між мікроконтролером Arduino та мобільним пристроєм користувача. Програмний код був розширений можливістю приймати команди з мобільного додатку, наприклад, для відкривання замка, додавання або видалення RFID-міток, а також для оновлення параметрів роботи. Цей функціонал значно розширив можливості системи, зробивши її більш гнучкою та зручною у користуванні.

Одним із найважливіших аспектів реалізації логіки роботи було забезпечення правильного порядку дій у залежності від типу сигналу, що надходить: чи то сигнал зі сканера RFID, чи то команда з мобільного пристрою. Наприклад, при зчитуванні авторизованої RFID-мітки спочатку відбувається короткий звуковий сигнал з зумера, який інформує про успішне зчитування,

після чого активується сервомотор MG90S, який повертається на певний кут, відкриваючи механічний замок. Через кілька секунд сервомотор повертається у вихідне положення, фіксуючи замок.

Для обробки різних подій та оптимізації логіки роботи було використано структуроване програмування з виділенням окремих функцій для зчитування RFID, управління Bluetooth, керування сервомотором та генерації звукових сигналів. Це значно покращило читаність коду і спростило його налагодження.

Крім того, була реалізована логіка обробки невірних міток – при зчитуванні неавторизованої карти система подає кілька коротких сигналів з зумера, не відкриваючи замок. Також у разі кількох невдалих спроб поспіль передбачається блокування пристрою на певний час, що є елементом додаткового захисту від несанкціонованого доступу.

Мобільний додаток, з яким взаємодіє система, був створений з використанням інструментів для швидкої розробки інтерфейсів – зокрема застосовано платформи, які дозволяють створювати Bluetooth-з'єднання та передавати прості команди через вбудовану консоль або за допомогою кнопок. Це дозволяє користувачу не лише відкривати замок на відстані, але й здійснювати базову адміністрацію системи.

Отже, програмне забезпечення системи виконує ключову функцію – поєднує апаратні компоненти в єдину узгоджену систему, забезпечуючи логіку взаємодії між RFID-зчитувачем, Bluetooth-модулем, сервомеханізмом і зумером, а також реалізує необхідні умови доступу до об'єкта. Його розробка вимагала чіткого планування, поетапного тестування та багаторазового вдосконалення. Arduino IDE стала зручною, ефективною платформою для розробки і налагодження коду, дозволяючи сконцентруватися на логіці системи та якості її роботи, а не на технічних складностях програмування.

### 3.4 Інтеграція системи та її тестування

Завершальним і водночас найвідповідальнішим етапом у розробці проєкту стало об'єднання всіх окремих елементів – як апаратних, так і програмних – в одну узгоджену, працездатну систему. Саме інтеграція дозволяє перевірити, наскільки ефективно взаємодіють між собою компоненти та чи відповідає кінцева система початковим задумам і очікуванням. Важливо було не просто зібрати систему фізично, а забезпечити її стабільну роботу в умовах, наближених до реального середовища експлуатації.

Процес інтеграції почався зі збирання всіх апаратних частин на одній макетній платі. Було забезпечено живлення для контролера Arduino Uno, а також належне підключення всіх периферійних пристроїв: RFID-модуля RC522, Bluetooth-модуля HC-05, сервоприводу та зумера. Особливу увагу було приділено якості з'єднань, правильності підключення сигналів SPI та UART, а також уникненню потенційних перешкод, які могли б вплинути на роботу модуля зв'язку або точність зчитування RFID-карток.

Після фізичного збирання відбулося завантаження програмного забезпечення на мікроконтролер, що дозволило перейти безпосередньо до тестування інтегрованої системи. У цьому процесі були задіяні різні методи перевірки – від базових функціональних тестів до більш складних сценаріїв, які імітували дії кінцевого користувача. Тестування здійснювалося у середовищі, наближеному до умов реального використання – із застосуванням живлення від зовнішнього джерела, у присутності фізичних перешкод, змін температури й інших змінних, які могли вплинути на стабільність роботи.

Одним із перших тестів було перевірено здатність системи реагувати на RFID-картки. Система демонструвала стабільне зчитування UID з мінімальними затримками, а також коректно реагувала на невірні або незареєстровані картки. Була зафіксована висока точність і швидкість зчитування, що підтвердило правильність підключення модуля та коректність написаного коду.

Не менш важливою була перевірка каналу Bluetooth-зв'язку. Для цього використовувався звичайний мобільний пристрій із встановленим додатком, який надсилав коди доступу до системи. Перевірялася здатність контролера отримувати дані, обробляти їх і відповідати відповідно до логіки: активувати або блокувати доступ. Було виявлено, що передача даних відбувається стабільно, без затримок чи втрат, а сама система успішно відрізняє коректні та некоректні коди.

Тестування сервоприводу й зумера здійснювалося в різних режимах – при короткочасному спрацюванні, тривалому використанні, а також в умовах зміни живлення. Сервопривід чітко реагував на команди, повертаючись у задане положення без ривків і надмірного навантаження, а звуковий сигнал чітко інформував користувача про стан системи. Усі ці фактори свідчили про ефективну інтеграцію як апаратної, так і програмної частини.

Окремо проводилося інтеграційне тестування – етап, на якому перевірялась робота системи в цілому. Метою було встановити, наскільки коректно взаємодіють компоненти між собою, чи не виникає конфліктів між пристроями, особливо під час одночасної роботи декількох модулів. Наприклад, одночасне зчитування RFID-картки та надходження Bluetooth-команди не призводили до збоїв, що підтверджувало правильну організацію роботи з перериваннями та обробки подій.

У рамках оцінки ефективності реалізованого рішення також було здійснено порівняння початкових очікувань з реальними результатами. Було встановлено, що практично всі поставлені цілі були досягнуті. Система працює стабільно, реагує швидко, підтримує кілька методів авторизації та забезпечує надійний рівень безпеки на фізичному рівні. Єдиною проблемою, що виникла в процесі, було короткочасне зниження чутливості RFID-модуля при надто великій довжині SPI-з'єднань. Це питання було оперативно вирішено шляхом скорочення довжини проводів і покращення заземлення.

Таким чином, процес інтеграції та тестування продемонстрував високу надійність запропонованого технічного рішення. Усі компоненти системи вдало

поєдналися в єдине функціональне ціле, що підтверджує обґрунтованість обраної архітектури й ефективність розроблених алгоритмів керування.

### 3.5 Порівняння результатів з очікуваннями та демонстрація роботи системи

Після завершення розробки та всебічного тестування системи безпеки з використанням RFID та мобільних пристроїв постала необхідність провести детальний аналіз відповідності отриманих результатів тим очікуванням, які були визначені на етапі постановки завдання. Такий аналіз не лише підтверджує успішність реалізації проєкту, а й дозволяє виявити потенційні напрямки для подальшого вдосконалення.

На початку роботи було сформульовано низку ключових функціональних та технічних вимог: підтримка безконтактної ідентифікації за допомогою RFID-карток, можливість альтернативного керування через мобільний додаток (Bluetooth), оперативна реакція на події, стабільна робота в реальних умовах та зручний інтерфейс для користувача.

У процесі практичної реалізації ці цілі були досягнуті. Нижче подано порівняльну таблицю 3.1 очікуваних і фактичних результатів за основними критеріями:

Таблиця 3.1 – Результати тестування системи безпеки з використанням RFID та мобільних пристроїв

| Показник | Очікуване значення | Результат тестування | Коментар |
|---|---|---|---|
| Час зчитування RFID-картки | ≤ 1 с | ≈0,7 с | В межах очікувань |
| Час відповіді на команду Bluetooth | ≤ 2 с | ≈1,2 с | В межах норми, стабільна робота модуля |

Продовження таблиці 3.1

| Показник | Очікуване значення | Результат тестування | Коментар |
|---|---|---|---|
| Радіус дії Bluetooth | ≥ 8 м (в межах приміщення) | ≈10 м | Покращений результат |
| Надійність авторизації (точність) | ≥ 98% | 100% при тестуванні з 10 зчитувань | Жодного помилкового спрацьовування |
| Стабільність при тривалій роботі | Не менше 1 години | Протестовано 1,5 години | Високий рівень стабільності |
| Інтуїтивність взаємодії | Простий мобільний інтерфейс, сигнал | Реалізовано повністю | Простий у використанні |

Ці результати свідчать про відповідність реалізованої системи сформульованим критеріям. Особливо варто відзначити високу стабільність, низький час затримки реакції та зручний інтерфейс, що є критично важливими факторами для будь-якої системи контролю доступу.

У ході тестування було виявлено лише незначні особливості, що можуть бути враховані при майбутньому вдосконаленні. Наприклад, рівень сигналу Bluetooth може змінюватися залежно від наявності фізичних перешкод, що є стандартною особливістю радіозв’язку. Також рекомендується ізолювати проводку RFID та Bluetooth-модулів у готовому корпусі для уникнення перешкод.

Щодо демонстрації – у реальних умовах взаємодія виглядає наступним чином: користувач підносить RFID-картку до зчитувача або використовує мобільний застосунок для відправки команди. У разі успішної авторизації сервопривід виконує відкриття замка, а зумер подає короткий звуковий сигнал. Усі дії відбуваються протягом 1-2 секунд.

Таким чином, отримані результати повністю узгоджуються з поставленими на етапі проєктування вимогами. Система виявилася працездатною, стабільною, ефективною та зручною для користувача. З огляду на це, можна впевнено стверджувати, що обрані архітектурні рішення та підхід до реалізації виявилися вдалими, і проєкт має потенціал для подальшого розвитку, зокрема шляхом додавання функцій моніторингу через Wi-Fi або впровадження багатофакторної автентифікації.

# ВИСНОВКИ

У ході виконання кваліфікаційної роботи було реалізовано проєкт створення сучасної системи безпеки, яка поєднує технології RFID-ідентифікації та мобільного керування доступом. Проведене дослідження, обґрунтування вибору компонентів, розробка програмного забезпечення та практична реалізація дозволили досягти поставленої мети й виконати всі основні завдання.

По-перше, було розглянуто принципи роботи RFID-системи на базі модуля RC522. У теоретичному розділі та на етапі реалізації докладно описано архітектуру модуля, особливості його підключення до мікроконтролера, використання SPI-протоколу, а також реалізацію функції зчитування UID RFID-міток. Проведені експерименти показали високу надійність зчитування даних.

По-друге, вивчено особливості мікроконтролера Arduino Uno. Було доведено його ефективність як центрального керуючого елемента у системі. Завдяки доступності, підтримці великої кількості бібліотек і простоті програмування Arduino Uno виявився оптимальним вибором для проєкту.

Третє завдання – визначити методику реалізації бездротового доступу через Bluetooth-модуль HC-05 – також було успішно виконане. В роботі описано апаратне підключення модуля, налаштування за допомогою AT-команд, створення зв'язку зі смартфоном, а також реалізацію логіки прийому команд з мобільного застосунку.

У межах наступного завдання було обґрунтовано вибір і реалізовано функціональну схему управління сервоприводом MG90S, який слугує виконавчим елементом. Проведено тестування сервоприводу на відповідність умовам задачі (кут повороту, швидкість, стабільність).

Також було розроблено програмне забезпечення, яке забезпечує взаємодію між RFID-зчитувачем, Bluetooth-модулем та виконавчими елементами. Програмна частина охоплює обробку зчитаного UID, логіку авторизації, роботу з командним інтерфейсом Bluetooth та звукове сповіщення через зумер.

Протестовано систему в умовах, наближених до реальних – реалізовано шляхом симуляції сценаріїв доступу в побутових умовах. Результати тестування, викладені у відповідному підрозділі, підтверджують працездатність системи, її надійність, зручність у користуванні та готовність до подальшого впровадження.

Таким чином, усі поставлені завдання виконані. Запропонована система є ефективною, гнучкою та придатною для масштабування. Вона може бути використана як у побутових умовах, так і в малих комерційних об’єктах. Крім того, проєкт має потенціал подальшого розвитку, зокрема – розширення функціоналу за рахунок додаткових сенсорів, резервного живлення або впровадження Wi-Fi-комунікації.

Результати кваліфікаційної роботи підтверджують практичну значущість обраної теми та демонструють здатність автора до комплексного вирішення інженерної задачі із застосуванням сучасних апаратно-програмних засобів.

# ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Іщук Д., Нестеровський А., Костючко С., Кайдик О., Терлецький Т. Система безпеки з використанням RFID та мобільних пристроїв. *Програмне та апаратне забезпечення в інформаційних технологіях*: матер. міжнар. наук.-практ. конф. (м. Луцьк, 6 травня 2025 р.). Луцьк, 2025. С. 72-73.

2. Design and Implementation of a Smart Sensor and RFID Door Lock Security System with Email Notification / E. Edozie et al. *International Journal of Engineering and Information Systems*. 2020. P. 5. URL: https://www.academia.edu/100554265/Design_and_Implementation_of_a_Smart_Sensor_and_RFID_Door_Lock_Security_System_with_Email_Notification (date of access: 12.02.2025).

3. Locker Security System Using Keypad and RFID / S. Mohammed et al. *Conference: The 2nd international conference of Computer Science and Renewable Energies*. 2020. P. 4. URL: https://www.researchgate.net/profile/Salma-Mohammed-10/publication/334576905_Locker_security_system_using_keypad_and_RFID/links/5ef24254299bf1031f1bf69d/Locker-security-system-using-keypad-and-RFID.pdf (date of access: 15.02.2025).

4. Chanchaichujit J., Balasubramanian S., Charmaine N. S. M. A systematic literature review on the benefit-drivers of RFID implementation in supply chains and its impact on organizational competitive advantage. *Cogent Business & Management*. 2020. Vol. 7, no. 1. P. 1818408. URL: https://doi.org/10.1080/23311975.2020.1818408 (date of access: 22.02.2025).

5. Role of RFID technologies in transportation projects: a review / D. K. Sharma et al. *International Journal of Technology Intelligence and Planning*. 2020. Vol. 12, no. 4. P. 349. URL: https://www.inderscience.com/offers.php?id=109772 (date of access: 25.02.2025).

6. File:Arduino-uno-perspective-transparent.png. Wikimedia Commons. *Wikimedia Commons*. URL: https://commons.wikimedia.org/wiki/File:Arduino-uno-perspective-transparent.png (date of access: 07.03.2025).

7. File:RFID-RC522.jpg. Wikimedia Commons. *Wikimedia Commons*. URL: https://commons.wikimedia.org/wiki/File:RFID-RC522.jpg (date of access: 09.03.2025).

8. Bluetooth модуль HC-05. *Arduino в Україні*. URL: https://arduino.ua/prod999-bluetooth-modyl-hc-05 (дата звернення: 14.03.2025).

9. Сервопривід Tower Pro MG90S Servo 14G 2.5кг/см 180град (10750) electricbike Arduino робототехніка. electricbike. URL: https://electricbike.com.ua/arduino-robototekhnika/61432-servoprivod-tower-pro-mg90s-servo-14g-25kg-sm-180grad-10750.html (дата звернення: 18.03.2025).

10. Шилд активний зумер. РКС Компоненти - Радіомаг. URL: https://www.rcscomponents.kiev.ua/product/shyld-aktyvnyi-zumer_165685.html (дата звернення: 24.03.2025).

11. ESP32 Wroom 32E - SunFounder ESP32 Starter Kit documentation. Welcome to SunFounder's Documentations! - SunFounder Documents documentation. URL: https://docs.sunfounder.com/projects/esp32-starter-kit/en/latest/components/component_esp32_extension.html (date of access: 27.03.2025).

12. NodeMCU ESP8266 WebServer Tutorial - Electronics-Lab.com. Electronics-Lab.com. URL: https://www.electronics-lab.com/nodemcu-esp8266-webserver-tutorial/ (date of access: 30.03.2025).

13. Модуль RFID PN532 NFC V3. URL: https://voron.ua/uk/catalog/039845--modul-rfid-pn532-nfc-v3 (дата звернення: 05.04.2025).

14. Vista de Arduino IDE. *Repositorio Digital*. URL: https://repository.uaeh.edu.mx/revistas/index.php/prepa4/article/view/10474/10019 (date of access: 08.04.2025).

15. Comparative Study of Seamless Asset Location and Tracking Technologies / F. Ahmed et al. *Procedia Manufacturing*. 2020. Vol. 51. P. 1138-1145. URL: https://doi.org/10.1016/j.promfg.2020.10.160 (date of access: 13.04.2025).

16. Subedi S., Pyun J.-Y. A Survey of Smartphone-Based Indoor Positioning System Using RF-Based Wireless Technologies. *Sensors*. 2020. Vol. 20, no. 24. P. 7230. URL: https://doi.org/10.3390/s20247230 (date of access: 19.04.2025).

17. Ho Y. H., Chan H. C. B. Decentralized adaptive indoor positioning protocol using Bluetooth Low Energy. *Computer Communications*. 2020. Vol. 159. P. 231-244. URL: https://doi.org/10.1016/j.comcom.2020.04.041 (date of access: 24.04.2025).

18. Darroudi S. M., Gomez C., Crowcroft J. Bluetooth Low Energy Mesh Networks: A Standards Perspective. *IEEE Communications Magazine*. 2020. Vol. 58, no. 4. P. 95-101. URL: https://doi.org/10.1109/mcom.001.1900523 (date of access: 28.04.2025).

19. Bluetooth 5.1: An Analysis of Direction Finding Capability for High-Precision Location Services / G. Pau et al. *Sensors*. 2021. Vol. 21, no. 11. P. 3589. URL: https://doi.org/10.3390/s21113589 (date of access: 01.05.2025).

20. A 13.56 MHz Rectifier Based on Fully Inkjet Printed Organic Diodes / F. A. Viola et al. *Advanced Materials*. 2020. Vol. 32, no. 33. P. 2002329. URL: https://doi.org/10.1002/adma.202002329 (date of access: 04.05.2025).

21. Smart Home Prototype with HC-05 Bluetooth and RFID Modules, Based on Microcontroller / I. Fenriana et al. *bit-Tech*. 2022. Vol. 5, no. 2. P. 77-84. URL: https://doi.org/10.32877/bt.v5i2.564 (date of access: 08.05.2025).

# ДОДАТКИ

# Додаток А

## Код пристрою

```
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <SoftwareSerial.h>

#define SS_PIN 10
#define RST_PIN 9
#define BUZZER_PIN 8
#define SERVO_PIN 7
#define BT_RX 2
#define BT_TX 3

MFRC522 rfid(SS_PIN, RST_PIN);
Servo lockServo;
SoftwareSerial bluetooth(BT_RX, BT_TX);  // RX, TX

byte expectedUid[] = { 0x8D, 0x38, 0x35, 0x02 };
bool cardHandled = false;

void setup() {
  Serial.begin(9600);
  bluetooth.begin(9600);
  SPI.begin();
  rfid.PCD_Init();

  pinMode(BUZZER_PIN, OUTPUT);
  lockServo.attach(SERVO_PIN);
  lockServo.write(90);
  delay(1000);

  Serial.println("System ready");
  bluetooth.println("Bluetooth ready");
}

void unlockSequence() {
  Serial.println("Unlocking...");
  bluetooth.println("Unlocking...");

  tone(BUZZER_PIN, 2000, 300);
  delay(300);
  noTone(BUZZER_PIN);

  lockServo.write(0);
  delay(1000);

  lockServo.write(90);
  delay(3000);

  lockServo.write(180);
  delay(1000);
```

```
  lockServo.write(90);

  Serial.println("Door action complete");
  bluetooth.println("Door action complete");
}

void loop() {
  if (bluetooth.available()> 0) {
    int toSend = bluetooth.read();
    Serial.println(toSend);
    lockServo.write(toSend);
  }

  if (rfid.PICC_IsNewCardPresent() && rfid.PICC_ReadCardSerial()) {
    byte uid[4];
    for (int i = 0; i < 4; i++) {
      uid[i] = rfid.uid.uidByte[i];
    }

    if (memcmp(uid, expectedUid, 4) == 0 && !cardHandled) {
      Serial.println("Card authorized");
      bluetooth.println("Card authorized");
      unlockSequence();
      cardHandled = true;
    } else if (memcmp(uid, expectedUid, 4) != 0) {
      Serial.println("Card not authorized");
      bluetooth.println("Card not authorized");
      tone(BUZZER_PIN, 500, 400);
      delay(400);
      noTone(BUZZER_PIN);
    }

    rfid.PICC_HaltA();
    rfid.PCD_StopCrypto1();
  }

  if (!rfid.PICC_IsNewCardPresent()) {
    cardHandled = false;
  }
}
```