Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
(повна назва)

Кафедра Мікроелектроніки, електронних приладів та пристроїв
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

СИСТЕМА БЛОКУВАННЯ ПРИМІЩЕННЯ НА БАЗІ МІКРОКОНТРОЛЕРА.

(тема)

Виконав:
студент 4 курсу, групи ЕЕПС-21-1
Тріма Д.С.
(прізвище, ініціали)

Спеціальність 171 Електроніка
(код і повна назва спеціальності)

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

Освітня програма «Електронні пристрої та системи»
(повна назва освітньої програми)

Керівник ст. викл. каф. МЕЕПП Васильєв Ю.С.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Бондаренко І.М.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії

Кафедра Мікроелектроніки, електронних приладів та пристроїв

Рівень вищої освіти перший (бакалаврський)

Спеціальність 171 «Електроніка»
(код і повна назва)

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

Освітня програма «Електронні пристрої та системи»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Тріма Дмитро Станіславович
(прізвище, ім'я, по батькові)

1. Тема роботи Система блокування приміщення на базі мікроконтролера.

затверджена наказом університету від «26» 05 2025 р. №415 Ст
2. Термін подання студентом роботи до екзаменаційної комісії _____ _____ 2025 р.
3. Вихідні дані до роботи Технічний продукт – електронний замок, призначений для обмеження доступу до приміщення стороннім особам
3.1 Загальні відомості та використання систем контролю доступу
3.2 Проектування апаратної частини системи
3.3 Пакет комп'ютерного моделювання Autodesk Circuits та Fritzing
3.4 Оформлення пояснювальної записки за ДСТУ 8302:2015

4. Перелік питань, що потрібно опрацювати в роботі
4.1 Електронні замки
4.2 Системи контролю доступу блокування приміщення
4.3 Проектування апаратної частини системи
4.4 Коефіцієнт посилення та спрямованої дії
4.5 Інструмент Autodesk

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Демонстраційний матеріал представлений у вигляді презентації PowerPoint (*.ppt) – 12 с. формату А4

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1.	Інформаційно-тематичний пошук та огляд літературних джерел про системи блокування приміщення на базі мікроконтролера	01.05.25 – 02.05.25	Виконано
2.	Проектування апаратної частини системи	02.05.25 – 07.05.25	Виконано
3.	Виконання чисельних розрахунків	07.05.25 – 12.05.25	Виконано
4.	Аналіз розрахунків та параметрів моделювання	12.05.25 – 16.05.25	Виконано
5.	Оформлення пояснювальної записки	16.05.25 – 17.05.25	Виконано
6.	Оформлення графічних та демонстраційних матеріалів	17.05.25 – 18.05.25	Виконано
7.	Проходження нормоконтролю і отримання рецензії	18.05.25 – 22.05.25	
8.	Проходження перевірки на плагіат	24.05.25 – 25.05.25	
9.	Підготовка та захист кваліфікаційної роботи	26.05.25 – 12.06.25	

Дата видачі завдання 01 05 2025 р.

Студент _____
(підпис)

Керівник роботи _____ ст. вик. МЕЕПП Васильєв Ю.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 33 с. , 19 рис., 0 табл., 3 додатка, 8 джерел.

ІНСТРУМЕНТ МОДЕЛЮВАННЯ AUTODESK CIRCUITS, СИСТЕМИ КОНТРОЛЮ ДОСТУПУ, ЕЛЕКТРОННИЙ ЗАМОК, КОЕФІЦІЄНТ ПОСИЛЕННЯ, КОЕФІЦІЄНТ СПРЯМОВАНОЇ, МІКРОКОНТРОЛЕР

Об’єкт дослідження – конструкція пристрою мікроконтролера змодельована з допомогою програми Autodesk Circuits.

Мета роботи – використати інструмент Autodesk Circuits, для моделювання пристрою мікроконтролера.

Методи дослідження – аналітичний та експериментальний за допомогою інструменту Autodesk Circuits та Fritzing.

У роботі були розглянуті питання щодо систем контролю доступу з використанням електронних замків, з допомогою комп’ютерного пакета для моделювання решіток – Autodesk (Circuits). Проведено роботу з проектуванням пристрою мікроконтролера.

ABSTRACT

Explanatory note of attestation work: 33 pp., 19 Fig., 0 Tables, 3 addition, 8 sources.

AUTODESK CIRCUITS MODELING TOOL, ACCESS CONTROL SYSTEMS, ELECTRONIC LOCK, GAIN FACTORY, DIRECTION FACTORY, MICROCONTROLLER

The object of research – the microcontroller device design is modeled using Autodesk Circuits.

The purpose of the work – use the Autodesk Circuits tool to model a microcontroller device.

Research methods – analytical and experimental using Autodesk Circuits and Fritzing tools.

The work considered issues related to access control systems using electronic locks, using a computer package for modeling lattices – Autodesk (Circuits). Work was carried out on the design of a microcontroller device.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

ДБЖ – джерело безперебійного живлення;

RFID – радіочастотна ідентифікація;

SDA та SCL – порти.

ВСТУП

У сучасному світі безпека об'єктів, приміщень і персоналу є одним із пріоритетних завдань як у промисловості, так і в побуті. Із розвитком цифрових технологій традиційні механічні системи захисту поступово витісняються більш зручними та ефективними електронними аналогами. Особливої актуальності набули системи контролю доступу, що базуються на мікроконтролерах та електронних замках.

Тому виникає потреба в розробці універсальної, недорогої та надійної системи блокування приміщення, яка поєднує функціонал електронного замка з можливістю адаптації під різні сценарії користування. Основна ідея даної дипломної роботи полягає у створенні багатофункціонального пристрою контролю доступу на основі мікроконтролера, який дозволяє здійснювати блокування або розблокування дверей за допомогою RFID-ідентифікації або введення кодової комбінації.

Електронний замок – це спеціальний пристрій, призначений для обмеження доступу до приміщення стороннім особам. У поєднанні з різними системами ідентифікації, такими як кодові клавіатури, RFID-мітки, біометричні сенсори та інші, електронні замки забезпечують високий рівень безпеки й автоматизації контролю доступу. Однак більшість комерційних рішень є дорогими або надмірно складними для побутового використання.

Метою атестаційної роботи є розробка, виготовлення та влагодження діючої моделі системи контролю доступу, яка поєднує електронний замок і програмовані засоби доступу. Застосування мікроконтролерного керування дозволяє реалізувати гнучке налаштування пристрою, ведення обліку доступів, аварійне блокування, а також збереження налаштувань у енергонезалежній пам'яті. Результатом є функціональна система, яка може бути використана для блокування приміщень у побуті, на підприємствах або в навчальних закладах, слугуючи прикладом ефективного використання недорогих апаратних засобів для забезпечення безпеки.

1 ЗАГАЛЬНІ ВІДОМОСТІ ТА ВИКОРИСТАННЯ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

1.1 Аналіз вихідних даних та існуючих технічних рішень систем контролю доступу

Існує чимало варіантів замків, для відкриття чи закриття яких не потрібен звичайний ключ у традиційному його розумінні. Замість цього можуть використовуватись альтернативні засоби, зокрема магнітні ключі у вигляді картки чи брелка або введення цифрового коду на спеціальній панелі, встановленій на дверях.

Кодові замки зазвичай класифікують за кількома ознаками: способом монтажу, типом керування запірним механізмом і можливістю змінювати кодову комбінацію.

За способом встановлення такі замки поділяються на навісні та врізні. Навісні моделі зазвичай застосовують у допоміжних приміщеннях – складах, гаражах чи сараях. Натомість для житлових об’єктів перевагу надають врізним замкам (рис. 1.1), оскільки їх механізми сховані всередині дверного полотна, що ускладнює спроби злому. Навісні замки, своєю чергою, можуть виступати як додатковий рівень захисту.

Рисунок 1.1 – Приклад врізного дверного замка

Залежно від способу керування запірним механізмом, замки поділяються на два основні типи: механічні (рис. 1.2) та електронні. Хоча електронні системи з кожним роком набирають все більшої популярності, механічні замки все ще залишаються широко використовуваними, особливо через звичність та доступність для споживачів.

Повністю витіснити їх із вжитку поки що складно, адже у багатьох сферах "механіка" продовжує залишатися стандартом. Втім, механічні моделі мають низку суттєвих недоліків. По-перше, через часте використання вони швидше зношуються, що зменшує термін їх експлуатації. По-друге, порівняно з більш сучасними аналогами, такі замки легше зламати – досвідченим зловмисникам не становить великої складності підібрати потрібну комбінацію [1].

Рисунок 1.2 – Приклад механічного кодового замку

Механічні кодові замки зазвичай бувають двох типів: з кнопковим механізмом або з поворотною ручкою. На практиці кнопкові варіанти виявляються найменш надійними. Через постійне натискання їх поверхня поступово стирається, кнопки починають залипати, і це значно полегшує завдання стороннім особам – підібрати правильну комбінацію стає доволі просто. На цьому тлі поворотні механізми виглядають більш захищеними.

Навіть при тривалому використанні складно визначити, скільки саме обертів і в якому напрямку потрібно здійснити, адже сліди зношування не дають очевидної підказки.

Окремої уваги заслуговують електронні кодові замки, які мають серйозну перевагу над механічними аналогами. Їхній блок керування може бути встановлений окремо від самого запірного механізму, наприклад, у прихованому місці. Це реалізує концепцію так званого «невидимого замка»: зловмиснику стає складно зрозуміти, з чим саме він має справу. Крім того, сучасні електронні замки керуються мікропроцесором, що дозволяє реалізувати мільйони унікальних комбінацій, істотно підвищуючи рівень безпеки.

Усі електронні кодові замки умовно можна поділити на три основні групи, кожна з яких має свої переваги та недоліки:

– кодові замки з кнопковим введенням та електронним керуванням. Цей тип замків є одним із найпоширеніших завдяки простоті конструкції та доступності. Проте, незважаючи на широку популярність, вони вважаються найменш захищеними серед електронних систем. Основна причина – зношення кнопок при частому використанні: з часом вони можуть западати або втрачати чіткість натискання, що створює ризик підбору коду сторонніми особами. Такі замки зазвичай встановлюють у місцях, де не зберігаються цінні речі, наприклад, у під'їздах, на складах або в підсобках малих підприємств і магазинів;

– замки з магнітним носієм коду. Ці пристрої забезпечують високий рівень безпеки, оскільки для їх відкриття потрібен спеціальний ідентифікатор – наприклад, магнітна картка, брелок або пульт, який передає код за допомогою радіосигналу чи інфрачервоного променя. Основною вразливістю таких систем є те, що для несанкціонованого доступу зловмиснику потрібно отримати сам носій, а переданий сигнал у деяких випадках може бути перехоплений і розкритий;

– комбіновані кодові замки (рис. 1.3). Найсучаснішим та найнадійнішим рішенням вважаються комбіновані замки, які для відкриття вимагають проходження кількох етапів автентифікації. Наприклад, потрібно спочатку ввести правильний код, а потім прикласти відповідну картку. Такий підхід значно ускладнює процес злому, адже недостатньо лише одного елементу – потрібно виконати весь ланцюжок дій. Крім того, подібні системи часто мають додаткову перевагу – вони не реагують на сторонні ключі або носії, які не були попередньо запрограмовані.

Рисунок 1.3 – Електронний замок із сенсорною панеллю вводу (Samsung)

Конструкція електронного замка передбачає наявність чотирьох основних компонентів, кожен із яких виконує свою функцію:

– запірний механізм. Цей елемент відповідає за фізичне блокування або відкривання дверей. Щоб змінити його стан (відкрити чи закрити), на нього подається короткочасний електричний імпульс. Якщо введений користувачем код збігається з запрограмованим, система дає команду на відкриття;

– пристрій введення коду (або зчитувач). Це панель або інше пристосування, через яке користувач вводить код або прикладає

ідентифікаційний ключ. Сам пристрій не містить керуючої логіки – він лише передає інформацію до керуючого блоку;

– блок для керування. Центральний елемент системи, який приймає рішення щодо подачі імпульсу на запірний механізм. У разі збігу даних, отриманих від зчитувача, із дозволеними, подається команда на розблокування. У більшості випадків замок зачиняється автоматично, подібно до звичайних механічних замків, що захлопуються;

– джерело безперебійного живлення (ДБЖ). Наявність акумуляторного джерела живлення в електронних замках має велике значення. У разі перебоїв з електропостачанням замок блокується, що унеможливлює вхід у приміщення. ДБЖ дозволяє системі працювати автономно протягом певного часу, зберігаючи її функціональність навіть під час аварійного відключення струму.

Для створення системи контролю доступу на базі мікроконтролера було обрано два основні способи ідентифікації користувача: введення цифрового коду за допомогою кнопкової клавіатури та використання технології радіочастотної ідентифікації (RFID). Обидва методи передбачають інтеграцію з модулями, спеціально адаптованими для взаємодії з мікроконтролерними платформами. Далі розглянемо детальніше принцип дії RFID-систем.

Технологія RFID (радіочастотна ідентифікація) є однією з найпростіших та водночас ефективних форм бездротової передачі даних. Попри свою відносну доступність, раніше вона не отримувала широкого поширення в промисловості через відсутність єдиних стандартів у виробництві. Проте сьогодні RFID-системи вважаються більш надійними та зручними у порівнянні з багатьма іншими методами ідентифікації. Суть цієї технології полягає у присвоєнні кожному об’єкту або користувачу унікального ідентифікаційного коду, що міститься в RFID-мітці. Така мітка кріпиться або вбудовується у предмет, що підлягає ідентифікації – це може бути особиста картка, брелок, елемент одягу чи навіть інструмент. Зчитувач, у свою чергу,

розпізнає цей код при наближенні мітки та передає його до системи для подальшої обробки.

Радіочастотна ідентифікація (RFID) – це не просто окремий пристрій, а цілісна система, яка складається з кількох ключових компонентів. Стандартна конфігурація RFID-рішення включає в себе: мітку (транспондер), яка містить унікальний ідентифікаційний код; зчитувач (трансивер або запитувач), що приймає сигнал від мітки; та програмне забезпечення, яке виконує обробку, аналіз і зберігання інформації у базі даних, підключеній до комп'ютерної мережі. Саме програмна частина відповідає за адміністрування користувачів, моніторинг подій, ведення журналів доступу та управління роботою всієї системи. У контексті цифрового контролю доступу RFID-зчитувач відіграє центральну роль: він відповідає за перевірку автентичності користувача та приймає рішення про відкриття дверей у разі успішного розпізнавання. Окрім цього, зчитувач також може зберігати або оновлювати інформацію про кожного користувача.

Одним із ключових моментів у роботі таких систем є саме аутентифікація – вона має бути здійснена до моменту надання доступу до захищеного приміщення. RFID-технологія забезпечує це швидко, надійно й зручно. Користувач лише прикладає свою мітку до зчитувача, після чого система миттєво порівнює отримані дані з інформацією у базі. Якщо збіг підтверджено – двері автоматично відчиняються. Таким чином, радіочастотна ідентифікація дозволяє ефективно управляти процесами входу та виходу, забезпечуючи високий рівень безпеки.

RFID-мітки класифікують залежно від джерела живлення, яке вони використовують. За цим критерієм їх поділяють на активні та пасивні. Активні мітки мають вбудоване джерело енергії (зазвичай батарею), що дозволяє їм самостійно передавати дані на запит зчитувача. Проте через високу вартість такі мітки застосовуються обмежено та, як правило, лише в специфічних сферах. Натомість пасивні RFID-мітки працюють без внутрішнього джерела живлення – вони активуються завдяки енергії, яку отримують від зчитувача.

Це робить їх значно дешевшими у виробництві, а також компактнішими за розмірами, що пояснює їх широке застосування в різних системах автоматичної ідентифікації. Передача даних від пасивної мітки відбувається в той момент, коли вона потрапляє в зону дії електромагнітного поля, створеного зчитувачем. Принцип її роботи базується на законі електромагнітної індукції Фарадея. Коли через котушку зчитувача протікає електричний струм, навколо неї утворюється магнітне поле. Це поле індукує електричний струм у котушці транспондера (мітки), після чого мітка змінює свою навантажувальну характеристику, впливаючи на струм у зчитувачі.

Таким чином, мітка фактично генерує модульований сигнал, який зчитувач вловлює через явище взаємної індукції між обома котушками. Після прийому сигнал декодується та надсилається до комп’ютера для подальшої обробки. Водночас додаткове використання компактної антени дозволяє зменшити габарити пристрою, зберігаючи його ефективність.

Існує кілька підходів до класифікації RFID-міток. Один із найбільш поширених поділяє їх на мітки з вбудованим чіпом (рис. 1.4) та безчіпові, або безмікросхемні мітки (рис. 1.5 [2].

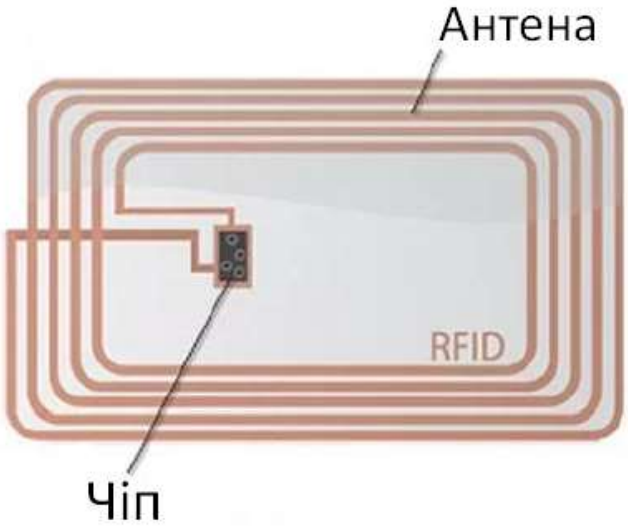

Рисунок 1.4 – RFID-мітка з вбудованою мікросхемою

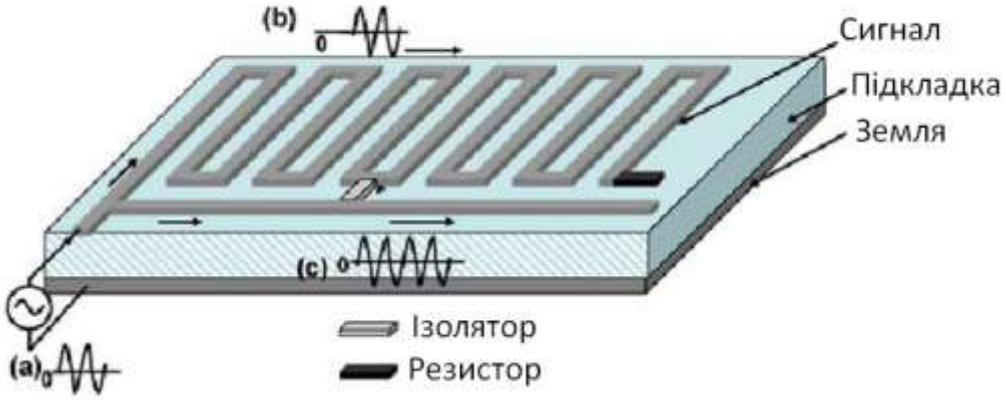

Рисунок 1.5 – RFID-мітка без вбудованого чипа

RFID-мітки класифікують за кількома параметрами, серед яких однією з найпоширеніших є наявність мікросхеми. Розрізняють мітки з вбудованим чипом та безчипові (безмікросхемні) варіанти. Ще одна важлива класифікація поділяє мітки за типом живлення: на пасивні, напівактивні та активні. Пасивні мітки не містять власного джерела енергії чи активного передавача – вони отримують живлення безпосередньо від зчитувача. Напівактивні мітки вже мають елемент живлення (наприклад, батарею), однак не передають сигнал самостійно, а лише у відповідь на запит. Активні мітки, своєю чергою, поєднують наявність джерела живлення та власного передавача, що дає їм змогу самостійно надсилати дані. Існує також поділ за типом пам’яті: мітки, які дозволяють лише зчитування, та ті, що підтримують як зчитування, так і запис інформації. Перші отримують свій ідентифікаційний код ще на етапі виробництва, а їх пам’ять є або незмінною, або однократно програмованою з можливістю багаторазового зчитування. У мітках другого типу інформацію можна змінювати або дописувати у процесі експлуатації, що дозволяє використовувати їх не лише для збереження серійного номера, а й для запису додаткових відомостей. Окрім того, класифікація міток здійснюється за діапазоном робочих частот: мітки низькочастотного діапазону працюють у межах від 125 кГц до 134 кГц, високочастотні – на частоті 13,56 МГц, а мітки

надвисокочастотного діапазону функціонують у межах від 860 МГц до 960 МГц [3].

2 ПРОЕКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1 Проектування електричної схеми та підбір відповідних компонентів

В якості головного елемента, що відповідає за керування всіма процесами в пристрої, було обрано мікроконтролер серії Arduino UNO R3 (рис. 2.1).

Рисунок 2.1 – Зовнішній вигляд передньої панелі Arduino Uno R3

Arduino Uno R3 – це плата, побудована на базі мікроконтролера ATmega328. Вона включає в себе 14 цифрових входів/виходів, позначених номерами від 0 до 13, при цьому 6 з них можуть працювати як ШІМ-виходи (на платі позначені символом “~”). Окрім цього, пристрій оснащено шістьма аналоговими входами (A0–A5), кварцовим генератором з частотою 16 МГц, роз’ємами для підключення USB та зовнішнього живлення, роз'ємом ICSP для прошивки мікроконтролера, а також кнопкою скидання налаштувань (reset).

Для запуску плати необхідно підключити живлення, яке може подаватися через адаптер змінного/постійного струму, батарею або USB-кабель, з'єднаний із комп'ютером. Контакт AREF використовується для задання опорної напруги аналоговим входам. Крім того, плата має контакт IOREF, який дозволяє модулям розширення автоматично адаптуватися до напруги живлення Arduino. Завдяки цьому забезпечується сумісність як із 5-вольтовими платами на базі AVR, так і з платами Arduino Due, що працюють на 3,3 В.

Плата Arduino Uno R3 функціонує при робочій напрузі 5 В. Для її стабільної роботи виробник рекомендує подавати напругу в межах від 7 до 12 В, однак допустимий діапазон живлення коливається від 6 до 20 В.

Конструктивно пристрій оснащений 14 цифровими портами, які можуть використовуватись як для введення, так і для виведення сигналів, а також шістьма аналоговими входами. Максимальне значення струму, яке може протікати через один цифровий пін, становить 40 мА. Крім того, на платі передбачено вихід з напругою 3,3 В, здатний видавати струм до 50 мА. Для зберігання даних використовується вбудована флеш-пам'ять обсягом 32 КБ, з яких 0,5 КБ зарезервовано під завантажувач. Також є енергонезалежна пам'ять EEPROM на 1 КБ, що дозволяє зберігати налаштування або змінні між перезавантаженнями пристрою. Частота тактового генератора, встановленого на платі, дорівнює 16 МГц.

Для організації безконтактної ідентифікації було обрано RFID-модуль моделі RC522. Він живиться від напруги 3,3 В та споживає струм не більше 30 мА. Модуль працює в радіочастотному діапазоні від 13,55 МГц до 13,57 МГц, а зчитування міток можливе на відстані до 25 мм. Фізичні розміри пристрою складають 40 на 60 мм. Щодо температурного режиму, модуль здатен працювати у доволі широкому діапазоні – від −20 °C до +80 °C, що дозволяє використовувати його в різних умовах.

RFID-модуль підтримує роботу з картами кількох класів: S50, S70, Ultralight, Pro та DESFire. До них належать такі типи міток, як Mifare S50,

Mifare S70, Mifare Ultralight, а також Mifare Pro та Mifare DESfire. Обмін даними відбувається на швидкостях 106, 212, 424 або 848 кбіт/с. Система безпеки реалізована відповідно до стандартів Mifare Classic™, однак важливо зазначити, що торгова марка «Mifare» належить компанії NXP Semiconductors. Виробництво чипів під цією назвою можливе лише за наявності офіційної ліцензії від правовласника. Мітки Mifare Classic функціонують у високочастотному діапазоні — на частоті 13,56 МГц. Ця частота також є стандартною для більшості пристроїв, що підтримують технологію NFC (Near Field Communication). У конструкції таких RFID-міток не передбачено наявності повноцінного мікропроцесора чи захищеного елемента, здатного здійснювати автентифікацію на рівні апаратного забезпечення. Технологію MiFare було вперше представлено компанією NXP Semiconductors ще у 1995 році, і з того часу по всьому світу реалізовано понад мільярд таких міток. Їх активно застосовують у системах безконтактного доступу, а також у ролі електронних платіжних засобів. Особливу увагу мітки Mifare Classic привернули з боку наукової спільноти, яка здійснила чимало досліджень, присвячених їхній інформаційній безпеці [4].

На рисунку 2.2 зображено зовнішню схему пристрою, призначеного для зчитування RFID-міток.

Рисунок 2.2 – Зовнішній вигляд передньої панелі Arduino Uno R3

Контактна схема RFID-модуля RC522 включає в себе кілька основних ліній, кожна з яких виконує окрему функцію. Пін VCC відповідає за живлення пристрою напругою 3,3 В. Контакт RST служить для скидання налаштувань модуля – це вхідна лінія, що використовується для перезапуску. Провід GND є загальним, або, як його ще називають, "землею". Лінія MISO (Master Input Slave Output) передає дані від RFID-модуля до мікроконтролера і виконує функцію виходу в інтерфейсі SPI. У той час як MOSI (Master Output Slave Input), навпаки, приймає інформацію від головного пристрою (мікроконтролера) – це вхідна SPI-лінія. Контакт SCK (Serial Clock) забезпечує подачу синхросигналу, необхідного для узгодженої роботи модуля. Пін SDA (Slave Select) відповідає за вибір периферійного пристрою в системі SPI, і також є вхідною лінією. Останній елемент – IRQ, вихідна лінія переривань, яка використовується для повідомлення про зміну стану або події, що потребують реакції з боку контролера.

Під час роботи з платформою Arduino для взаємодії з RFID-зчитувачем RC522 доцільно використовувати спеціалізовані сторонні бібліотеки, які значно спрощують процес програмування. Для реалізації зчитування та запису даних на RFID-карту необхідно мати доступ до її унікального ідентифікаційного номера – саме він є ключовим елементом у системах радіочастотної ідентифікації. Щоб отримати цей ідентифікатор, варто скористатися прикладом із бібліотеки RFID під назвою «CardInfo», який доступний безпосередньо в середовищі розробки Arduino IDE. Для цього потрібно попередньо підключити модуль RC522 до плати Arduino, після чого завантажити та запустити вказаний приклад. Коли робоча мітка потрапить у зону дії зчитувача, у вікні монітора порту з’явиться інформація про карту. Як саме виглядає цей вивід, показано на рисунку 2.3.

```
Card found
Cardnumber:
Dec: 60, 121, 172, 213, 60
Hex: 3C, 79, AC, D5, 3C
```

Рисунок 2.3 – Унікальні ідентифікатори RFID-міток

У процесі виконання програми на екран виводиться послідовність чисел: 60, 121, 172, 213, 60. Для подальшої обробки ці дані потрібно змінити певним чином. Спочатку числа розташовуються у зворотному порядку, при цьому перше значення (яке спочатку було останнім) відкидається, оскільки воно є контрольною сумою. Решту чисел слід перевести у шістнадцяткову систему числення, а потім об’єднати в єдиний рядок без пробілів між елементами. У результаті утворюється довге шістнадцяти значне число, яке необхідно конвертувати у десятковий формат. Саме це число і буде слугувати унікальним ідентифікаційним кодом RFID-картки. Надалі його можна використовувати в прикладних задачах – наприклад, створювати програми для систем контролю доступу до приміщень. Щоб реалізувати можливість введення кодів вручну, зручно застосовувати спеціальну матричну клавіатуру, розраховану на взаємодію з мікроконтролером. Вона містить 16 кнопок, розміщених у вигляді сітки з 4 рядків і 4 стовпців. Схематичне зображення внутрішньої будови такої клавіатури наведено на рисунку 2.4 [5].

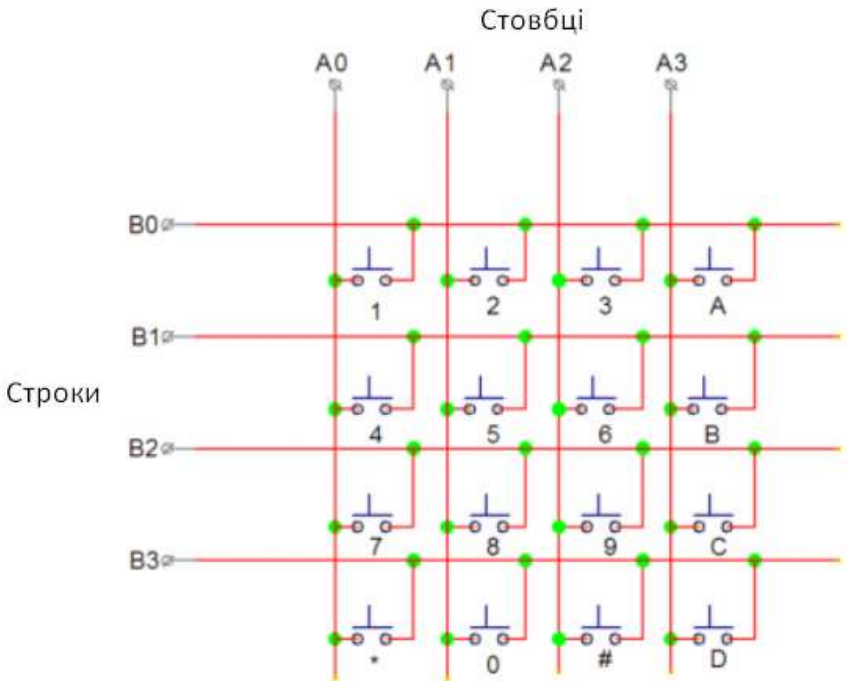

Рисунок 2.4 – Електрична схема клавіатури з матричним розташуванням кнопок 4×4

2.2 Моделювання конструкції пристрою в середовищі Autodesk Circuits

Щоб наочно продемонструвати конструкцію пристрою для системи контролю доступу, було обрано зручний онлайн-інструмент, який дозволяє візуалізувати роботу з платформою Arduino на всіх етапах. Мова йде про програму Autodesk Circuits, що доступна на сайті circuits.io. Цей сервіс є безкоштовним і не потребує встановлення на комп’ютер, оскільки працює безпосередньо у веббраузері. За його допомогою можна створювати електронні схеми та макети, що зручно відображають логіку з'єднань і взаємодію компонентів системи. У межах цього проєкту за допомогою Autodesk Circuits було змодельовано підключення окремих модулів до мікроконтролера Arduino Uno R3. Схеми з’єднань, що відображають ці модулі, подані на рисунках 2.5 – 2.7.

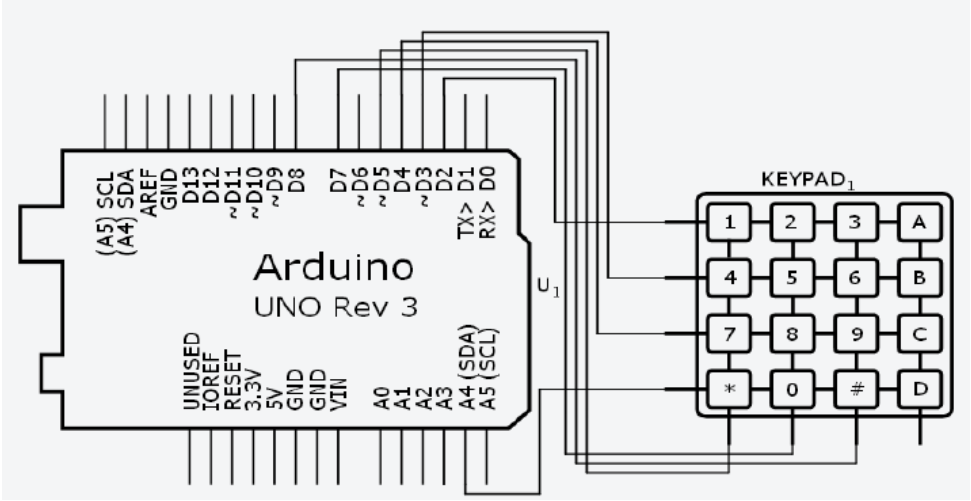

Рисунок 2.5 – Схематичне зображення підключення матричної клавіатури

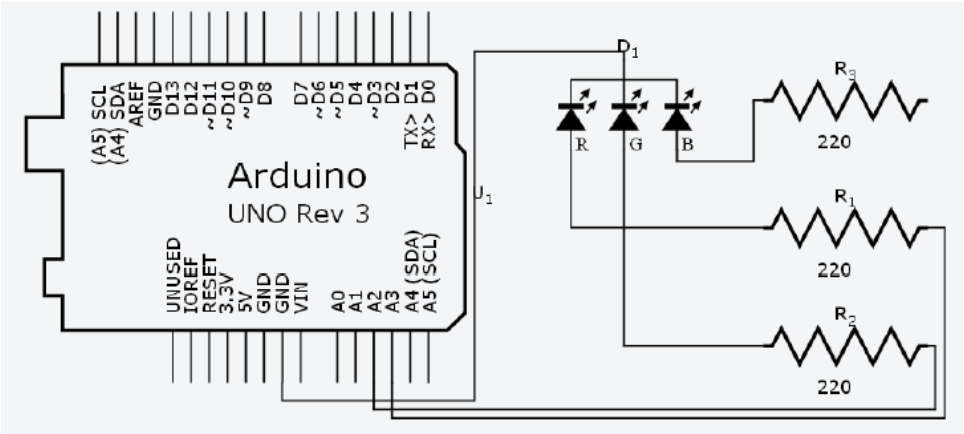

Рисунок 2.6 – Схематичне зображення з'єднання RGB-світлодіода

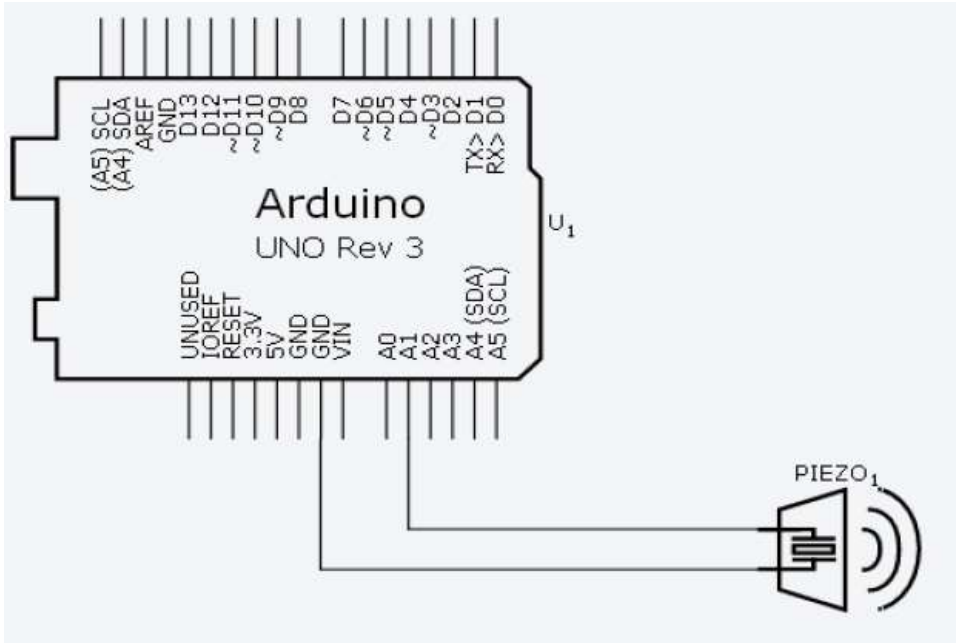

Рисунок 2.7 – Схематичне зображення кнопки скидання EEPROM

Хоча зазначена вище програма має багато переваг, вона суттєво обмежена у кількості доступних елементів для моделювання. Через це подальша розробка системи проводилась у середовищі Fritzing – спеціалізованому інструменті для створення схем на базі Arduino. Схеми підключень, створені в цій програмі, наведені на рисунках 2.8 – 2.10.

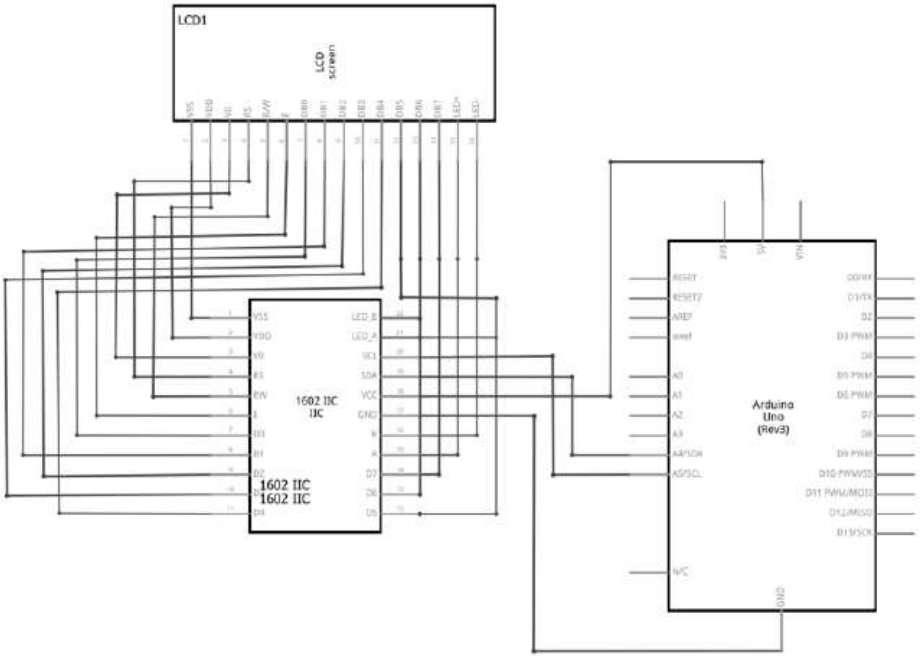

Рисунок 2.8 – Схематичне зображення підключення дисплея LCD1602 через інтерфейс I2C

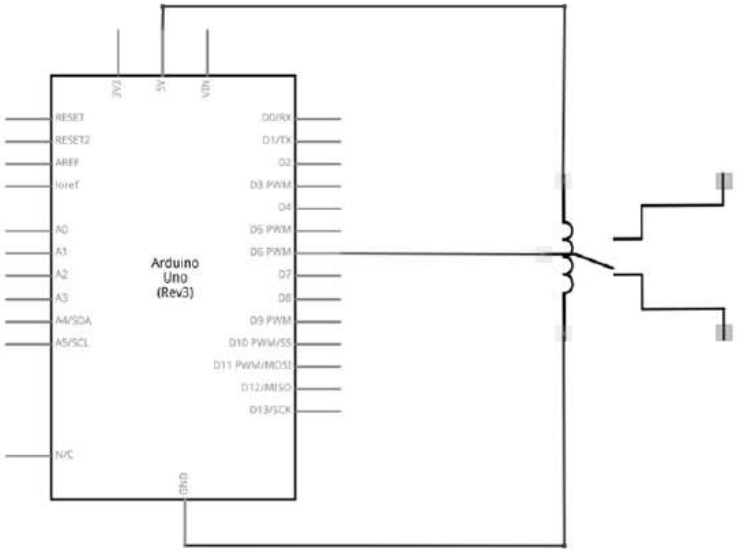

Рисунок 2.9 – Схематичне зображення одноканального реле

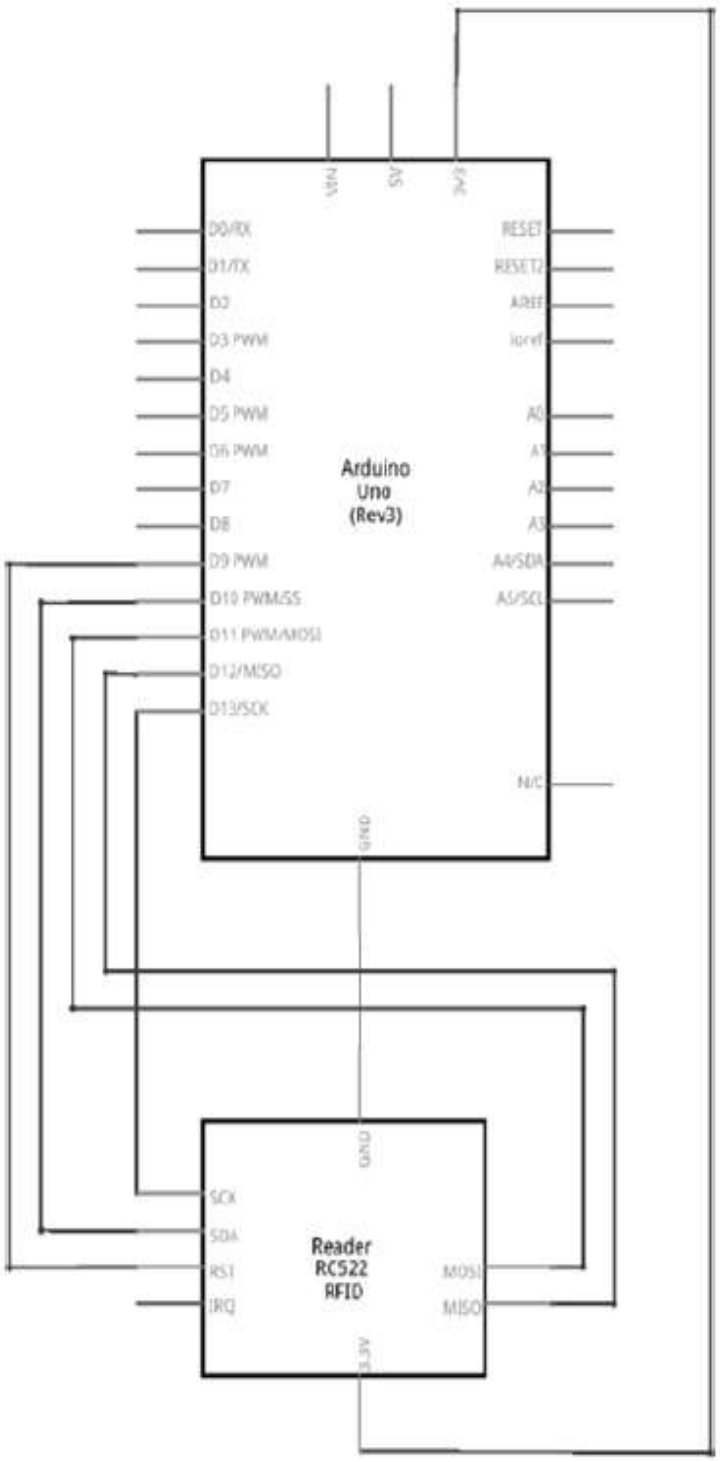

Рисунок 2.9 – Схематичне зображення підключення RFID-зчитувача RC522

В результаті всі модулі були об’єднані в одну схему, яка наведена на рисунку 2.10 [6].

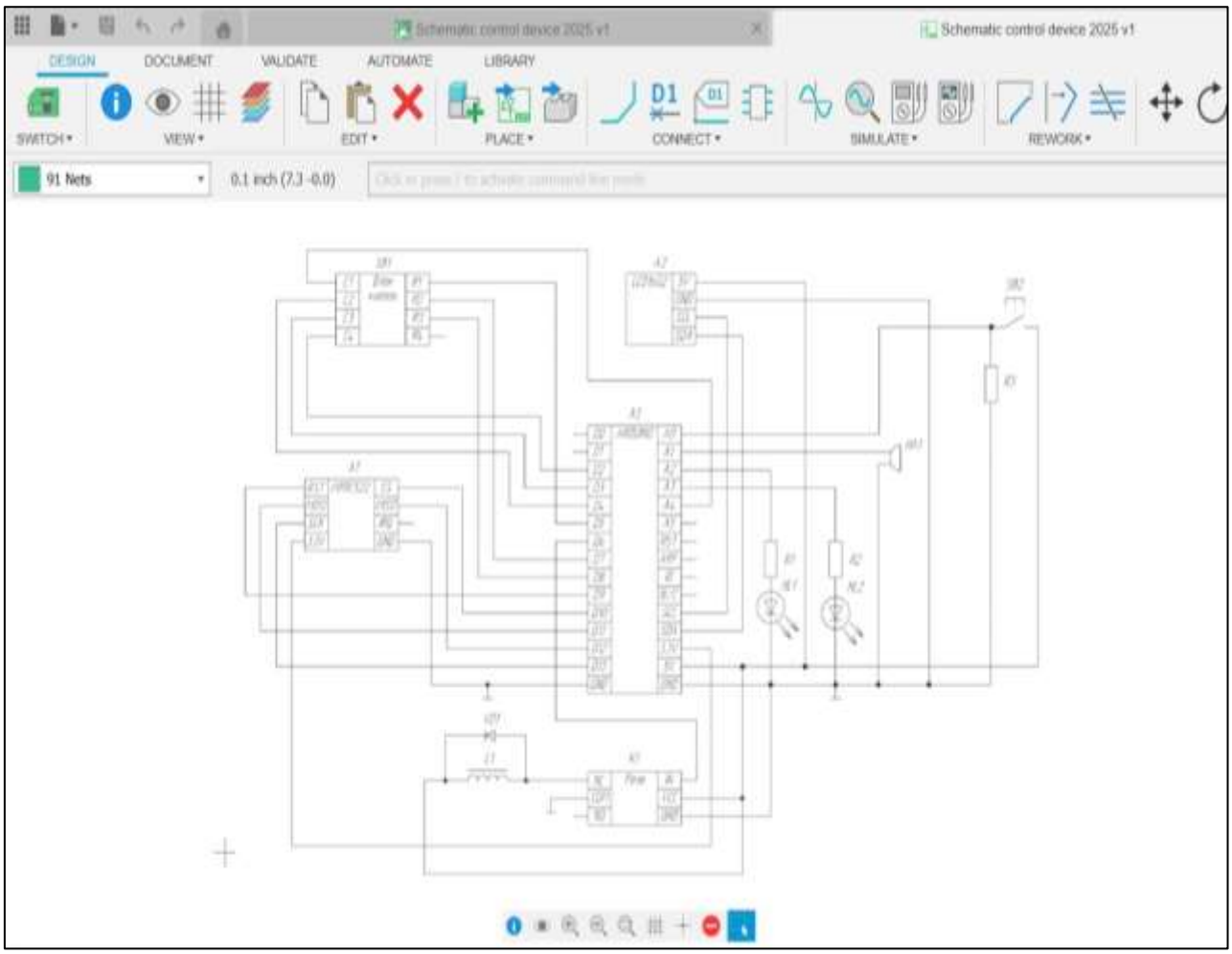

Рисунок 2.10 – Загальна схема з’єднання всіх компонентів пристрою контролю доступу з мікроконтролером

2.3 Реалізація програмної частини для керування пристроєм

Перш ніж перейти безпосередньо до написання програмного коду, необхідно визначити базовий алгоритм функціонування пристрою. Це дозволить краще зрозуміти логіку роботи системи в різних ситуаціях та забезпечити правильне виконання всіх етапів. Візуальне представлення алгоритму наведено на рисунку 2.11.

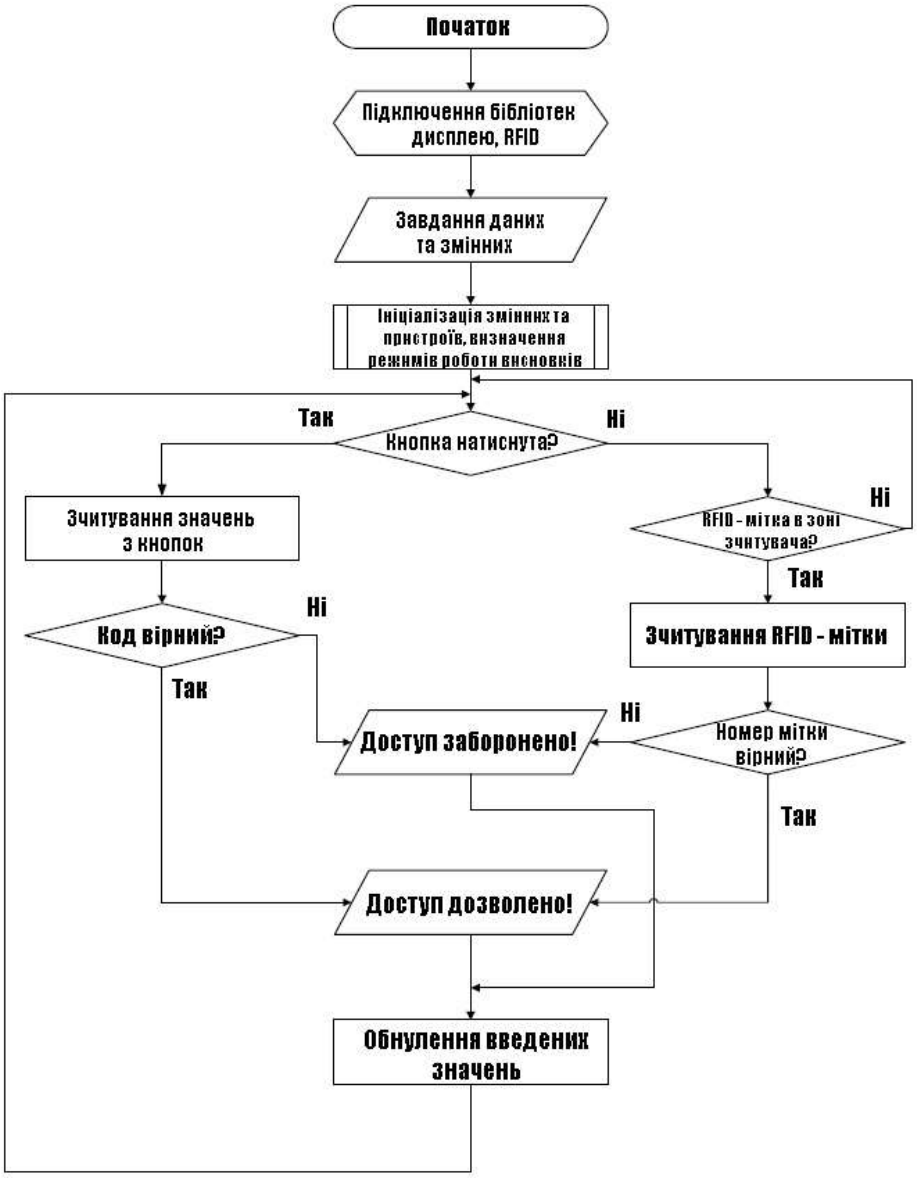

Рисунок 2.11 – Алгоритм, основна логіка функціонування системи контролю доступу

Для створення програмного забезпечення було використано середовище розробки Arduino IDE, спеціально розроблене для роботи з мікроконтролерами цієї серії. Після тривалого процесу тестування, внесення змін та виправлення помилок, вдалося розробити робочий варіант програми, яка забезпечує базову функціональність електронного замка на базі контролера Arduino Uno R3. Готовий програмний код, що реалізує принцип роботи системи контролю доступу до приміщення, наведений у додатку В [7].

3 ФІЗИЧНЕ ВТІЛЕННЯ РОЗРОБЛЕНОЇ СИСТЕМИ

3.1 Побудова апаратної частини проекту

Для зручного підключення різноманітних модулів до мікроконтролера Arduino використовується спеціальна макетна плата. Вона дозволяє легко розміщувати елементи схеми, а також з'єднувати їх між собою та з мікроконтролером за допомогою дротів. У результаті була зібрана схема, яку можна побачити на рисунку 3.1. Всі компоненти підключені відповідно до принципових схем, попередньо створених у програмах для моделювання – Autodesk Circuits та Fritzing.

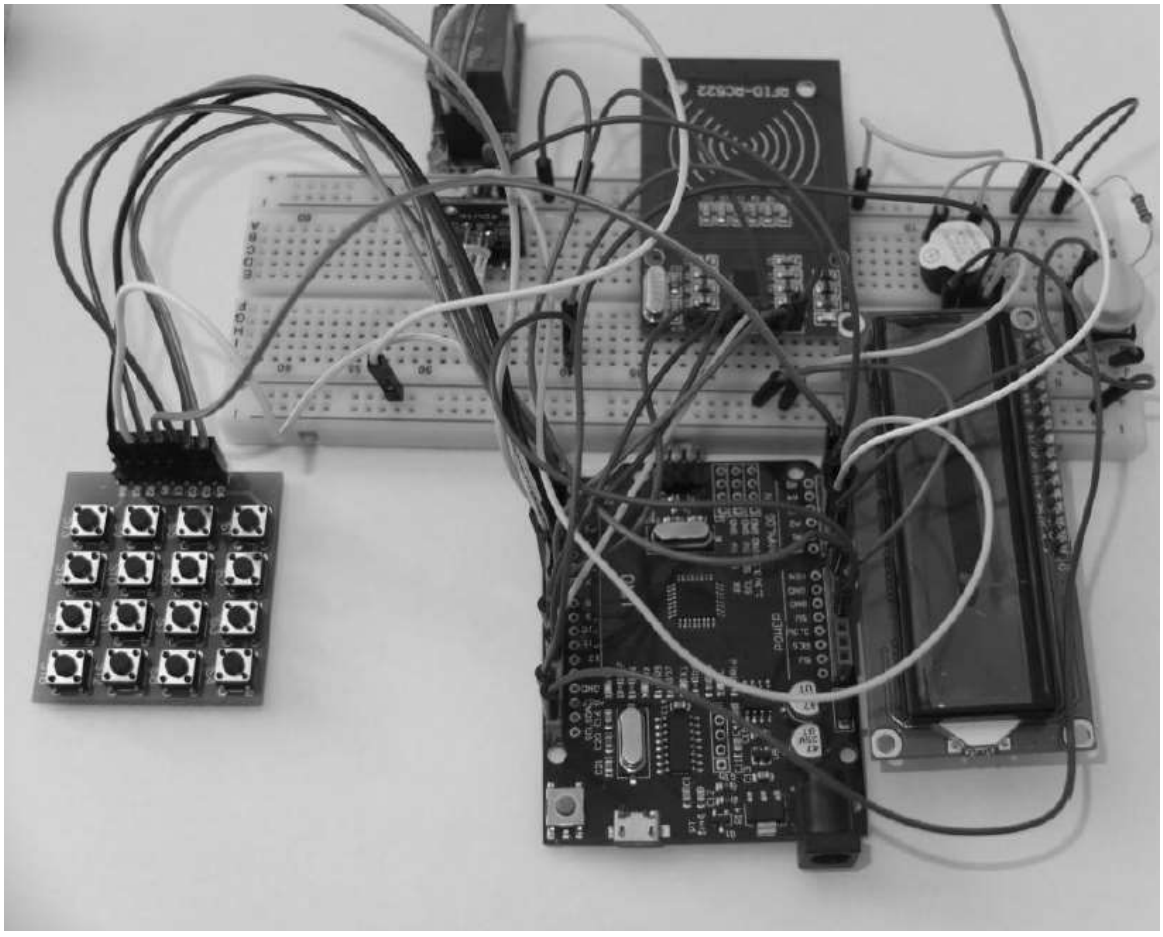

Рисунок 3.1 – Алгоритм, основна логіка функціонування системи контролю доступу

Детальніше зупинимося на підключенні RFID-зчитувача RC522, схема якого показана на рисунку 3.2, а також розглянемо підключення світлодіода, зображеного на рисунку 3.3.

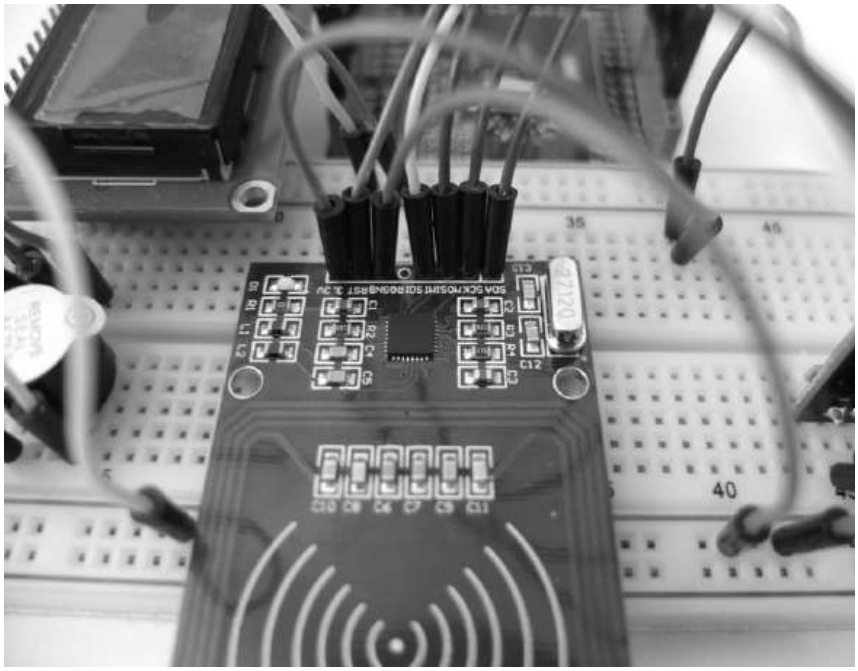

Рисунок 3.2 – Підключення RC522 до мікроконтролера

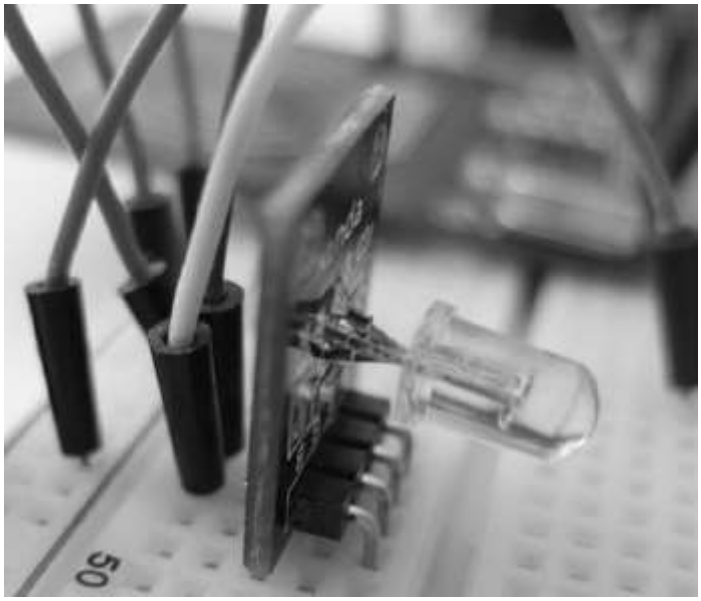

Рисунок 3.3 – Підключення RGB-світлодіода до мікроконтролера

3.2 Перевірка та налагодження програмного забезпечення пристрою

У процесі створення та практичної реалізації моделі електронної системи контролю доступу виникли не лише певні труднощі, а й з’явилися нові ідеї щодо вдосконалення програмного забезпечення. Зокрема, було прийнято рішення замінити бібліотеку Rfid.h на більш функціональну MFRC522, яка забезпечує розширені можливості взаємодії з RFID-модулем.

Також для полегшення роботи з п’єзодинаміком до програмного коду було додано окрему функцію squeaker(), що спростило налаштування звукових сигналів. Окрім того, увагу було звернено на особливості мікроконтролера Arduino UNO R3, зокрема на додаткові порти SDA та SCL, які забезпечують можливість обміну даними за протоколом I2C. Це дозволило підключити LCD-дисплей 1602, який використовується для виведення інформації в реальному часі. Водночас було вирішено змінити формат символів на дисплеї – початково весь текст відображався латинською абеткою, що обмежувало зручність використання. Цю проблему вдалося вирішити шляхом підключення сторонньої бібліотеки LCD_1602_UA.h, яка підтримує виведення кириличних символів. Однак найбільш значущим етапом модернізації стало впровадження роботи з енергонезалежною пам’яттю EEPROM, вбудованою в мікроконтролер. Завдяки цьому з’явилася можливість зберігати у пам’яті не лише RFID-ідентифікатори, а й кодову комбінацію, введену через матричну клавіатуру. Таким чином, дані більше не потребували жорсткого задання у програмному коді, а зчитувалися безпосередньо з EEPROM і передавалися у послідовний порт комп’ютера під час роботи пристрою. Додатково до системи було інтегровано окрему кнопку для очищення пам’яті мікроконтролера. Її функція полягала в обнуленні всіх записів у EEPROM, за винятком тих, що містять пароль, з метою збереження доступу навіть після скидання [8].

ВИСНОВКИ

У межах цієї атестаційної роботи було розроблено, запрограмовано, зібрано, протестовано та налагоджено працездатний макет пристрою для контролю доступу до приміщення, керованого мікроконтролером.

Створена система відтворює базові функції моніторингу стану різних датчиків і периферійних компонентів, що входять до складу електронної частини пристрою. Макет електронного замка дозволяє реалізувати основні сценарії обмеження доступу до приміщення, використовуючи два способи авторизації: введення цифрового коду через матричну клавіатуру або прикладання RFID-мітки, яка виступає в ролі ключ-картки.

Для симуляції стану замкнених або відчинених дверей використано релейний модуль, до якого підключено електромагніт. У випадку втрати майстер-ключа в системі передбачена можливість скидання пам’яті мікроконтролера, що дозволяє задати новий головний ключ та здійснити перепризначення доступу для нових RFID-карт.

Налагоджувальні дані надходять на комп’ютер лише у разі прямого підключення мікроконтролера через USB-інтерфейс. Водночас, у штатному режимі пристрій може функціонувати автономно за допомогою зовнішнього блока живлення, хоча при цьому доступ до діагностичної інформації буде обмежений.

Основною метою даної роботи було створення макету системи контролю доступу на базі мікроконтролера. Отриманий результат дозволяє ефективно відтворити функціонал, подібний до вже існуючих систем безпеки, але без використання складних апаратних рішень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Цирульник С. М., Азаров О. Д., Крупельницький Л. В., Трояновська Т. І. Програмування мікроконтролерів AVR: навчальний посібник. – Вінниця: ВНТУ, 2018. – 111 с.

2. Павловський О. М. Мікроконтролери та мікропроцесорна техніка: лабораторний практикум. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 104 с.

3. Засорнов О. С., Засорнова І. О. Програмування мікроконтролерних та робототехнічних систем: навчальний посібник. – Київ: Кондор, 2023. – 280 с.

4. Якименко Ю. І. Схемотехніка електронних систем. Книга 3: Мікропроцесори та мікроконтролери. – Київ: Наукова думка, 2010. – 328 с.

5. Немцов О. В. Радіочастотна ідентифікація (RFID). – Суми: Сумський державний університет, 2022. – 65 с.

6. Кравченко І. В. Основи мікропроцесорної техніки: навчальний посібник. – Харків: ХНУРЕ, 2015. – 200 с.

7. Гончарук В. І. Мікроконтролери та їх застосування: навчальний посібник. – Львів: Видавництво Львівської політехніки, 2017. – 180 с.

8. Перре Етьєн Radio Frequency Identification and Sensors: From RFID to Chipless RFID. – Chichester: John Wiley & Sons Ltd, 2014. – 254 с.