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 кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

СИСТЕМА ДОСТУПУ НА ОСНОВІ ARDUINO

ACCESS SYSTEM BASED ON ARDUINO

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІз-41
Хвіц Дмитро Вікторович

(підпис)

Керівник:
к.т.н., доцент
Поліщук Микола Миколайович

(підпис)

Кваліфікаційну роботу
допущено до захисту
« _____ » червня 2023 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2023 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Хвіцу Дмитру Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Система доступу на основі Arduino*
Керівник роботи *к.т.н., доцент Поліщук Микола Миколайович*
затверджені наказом закладу вищої освіти від «28» грудня 2022 року № 982/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 01.06.2023р.
3. Вихідні дані до роботи
Види реалізації осцилографа (електронні ресурси); опис архітектури системи та технічні вимоги до осцилографа з використанням наукових видань
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Аналіз предметної області
Огляд технологій та комплектуючих систем доступу на базі Arduino
Практична реалізація системи доступу на основі Arduino
Схемотехнічна розробка осцилографа
Візуалізація результатів на екрані
5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Розділ 1	*Поліщук М.М.*		
Розділ 2	*Поліщук М.М.*		
Розділ 3	*Поліщук М.М.*		
Висновки	*Поліщук М.М.*		
Нормоконтроль	*Поліщук М.М.*		

7. Дата видачі завдання 01.11.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Вивчення літератури*	До 29.01.2023 р.	Виконано
2.	*Огляд існуючих рішень*	До 20.02.2023 р.	Виконано
3.	*Вибір апаратного забезпечення*	До 29.03.2023 р.	Виконано
4.	*Розробка*	До 10.04.2023 р.	Виконано
5.	*Програмування мікроконтролера*	До 05.05.2023 р.	Виконано
6.	*Оформлення матеріалів роботи*	До 25.05.2023 р.	Виконано
7.	*Нормоконтроль*	До 01.06.2023 р.	Виконано
8.	*Інструментальна перевірка на академічний плагіат*	До 03.06.2023 р.	Виконано
9.	*Представлення кваліфікаційної роботи бакалавра до захисту*	До 17.06.2023 р.	Виконано

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

Керівник кваліфікаційної роботи _____ Поліщук М.М.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Хвіц Д.В. Система доступу на основі Arduino. Рукопис

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2023.

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

У роботі розроблено систему доступу на основі мікроконтролера Arduino Uno та представлено теоретичний матеріал про системи доступу на основі інтелектуальних систем і мікроконтролерів, переваги та недоліки інтелектуальних систем та різні види їх виконання. Описано принципи роботи безпровідних технологій NFC RFID та різницю між ними. Представлено характеристики всіх комплектуючих, які використовуються для розробки системи доступу і також особливості підключення кожного з цих елементів до мікроконтролера Arduino Uno.

Інтерактуальні системи, Arduino, Сервопривід, RFID, Мікроконтролер, Технології, Комплектуючі, Система, Зчитувач

ANNOTATION

Khvits D.V. Access system based on Arduino. Manuscript

Bachelor's qualifying thesis of the OP "Computer Engineering" specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2023.

The bachelor's qualification work consists of an introduction, three sections, conclusions, a list of used sources, and appendices.

The work develops an access system based on the Arduino Uno microcontroller and presents theoretical material about access systems based on intelligent systems and microcontrollers, advantages and disadvantages of intelligent systems and various types of their implementation. The principles of wireless NFC RFID technologies and their differences are described. The characteristics of all components used for the development of the access system are presented, as well as the features of connecting each of these elements to the Arduino Uno microcontroller.

Interactive systems, Arduino, Servo drive, RFID, Microcontroller, Technologies, Components, System, Reader

ЗМІСТ

ВСТУП 7
РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ 8
1.1 Опис систем доступу за допомогою інтелектуальних систем 8
1.1.1 Поняття інтелектуальнлї системи 8
1.1.2 Приклади інтелектуальних систем 10
1.1.3 Огляд систем доступу 14
1.2 Системи доступу на базі мікроконтролерів 20
1.3 Переваги та недоліки інтелектуальної системи 22
1.4 Різні виконання інтелектуальних систем 23
РОЗДІЛ 2 ОГЛЯД ТЕХНОЛОГІЙ ТА КОМПЛЕКТУЮЧИХ СИСТЕМИ ДОСТУПУ НА БАЗІ ARDUINO 26
2.1 Безпровідні технології NFC RFID 26
2.1.1 Що таке NFC RFID? 26
2.1.2 Різниця між NFC та RFID 28
2.2 Комплектуючі системи системи доступу на базі Arduino 30
2.2.1 Вибір мікроконтролера для розробки системи 30
2.2.2 Кнопка 32
2.2.3 RGB світлодіод 32
2.2.4 Сервопривід 33
2.2.5 Зумер 34
2.2.6 Зчитувач RFID RC522 35
2.2.7 LCD дисплей 37
РОЗДІЛ 3 39
ПІДКЛЮЧЕННЯ ЕЛЕМЕНТІВ ДО МІКРОКОНТРОЛЕРА 39
3.1 Підключення кнопки до мікроконтролера 39
3.2 Підключення RGB світлодіода 40
3.3 Підключення сервопривода до мікроконтролера 42
3.4 Підключення зумера до мікроконтролера 43
3.5 Підключення зчитувача RFID RC522 до мікроконтролера 44

3.6 Підключення LCD дисплея до мікроконтролера 46
3.7 Створення коду в Arduino IDE та складання проєкту 49
ВИСНОВКИ 53
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 54
ДОДАТКИ 57

ВСТУП

Актуальність. Сучасні інноваційні технології стають все частіше частиною нашого повсякденного життя. Під час застосування, ми можемо підвищити свій комфорт та зекономити час на виконання різних завдань. Тому використання так званих інтелектуальних системи, на сьогоднішній день є досить актуальним. Застосування систем доступу до дверей за допомогою інтелектуальних систем може бути для прикладу в домашнії сейфах, комірках для зберігання речей, або навіть в сучасних «розумних будинках».

Мета кваліфікаційної роботи – створення системи доступу до дверей за допомогою мікроконтролера Arduino та технології RFID.

Для вирішення поставленої мети можна виділити ряд завдань:

- огляд існуючих інтелектуальних систем;
- визначення переваг та недоліків інтелектуальних систем;
- вибір типу та елементної бази для створення таких систем;
- реалізація проєкту.

Об'єкт кваліфікаційної роботи – технології RFID в системі доступу до дверей на основі мікроконтролера Arduino.

Предмет кваліфікаційної роботи – система доступу до дверей за допомогою мікроконтролера Arduino Uno.

Пояснювальна записка випускної кваліфікаційної роботи містить теоретичний матеріал про системи доступу на основі інтелектуальних систем, системи доступу на базі мікроконтролерів, переваги та недоліки інтелектуальних систем та різні види їх виконання. Також описані принципи роботи безпровідних технологій NFC RFID та різницю між ними. Описано всі комплектуючі, які використовуються для розробки системи доступу, а також особливості підключення кожного з цих елементів до мікроконтролера Arduino Uno.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Опис систем доступу за допомогою інтелектуальних систем

1.1.1. Поняття інтелектуальнлї системи

Інтелектуальна система – це вдосконалена комп’ютерна система, яка може збирати, аналізувати та реагувати на дані, які вона збирає з навколишнього середовища. Вона може працювати та спілкуватися з іншими системами, такими як користувачі чи інші комп’ютерні системи. Також може вчитися на досвіді та адаптуватися відповідно до поточного стану. Інтелектуальна система також може підтримувати віддалений моніторинг і керування.

Єдиного визначення інтелектуальної системи в дійсності немає. У різних джерелах цей термін трактується по-різному [1, 2]. Наприклад, робот-пилосос часто називають інтелектуальною системою. Проте можна стверджувати, що його обмежена здатність до навчання, наприклад нездатність уникнути тієї самої перешкоди, виключає його з цієї категорії. З іншого боку, також можна вважати, що безпілотний автомобіль є інтелектуальною системою або правильною спробою створення інтелектуальної системи.

Немає єдиного стандарту, який би визначав інтелектуальну систему. Часто це визначається ступенем інтелекту, а не переліком характеристик. Мартін Моліна, професор кафедри штучного інтелекту Технічного університету Мадрида, запропонував наступний опис інтелектуальної системи у своїй статті [3]:

Інтелектуальна система:

– працює в середовищі з іншими агентами;

– володіє когнітивними здібностями, такими як сприйняття, контроль дій, міркування або використання мови;

– дотримується принципів поведінки, заснованих на раціональності та соціальних нормах;

– має здатність адаптуватися через навчання.

Автор додав, що його визначення не слід сприймати як «жорстку характеристику, щоб визначити, чи є система розумною чи ні» [3]. Натомість визначення окреслило звичайні характеристики, які можуть бути присутніми в інтелектуальній системі. Наприклад, система може вважатися розумною, якщо вона має сприйняття і може контролювати дії, навіть якщо вона не володіє міркуваннями або здатністю до навчання. Також, що «концепція інтелектуальної системи з'явилася в інформаційних технологіях як тип системи, отриманої в результаті успішного застосування штучного інтелекту». Фактично штучний інтелект зазвичай називають центральною характеристикою будь-якої інтелектуальної системи. Моліна також сказав, що «одним із найважливіших аспектів у побудові інтелектуальної системи є вибір методів штучного інтелекту , які надають системі когнітивні здібності, необхідні для функціонування як цілісної системи» [3].

Людство досягло значного прогресу завдяки розробці дедалі потужніших і досконаліших інструментів. В епоху промислової революції було створено велику кількість інструментів у вигляді машин, які автоматизували завдання, що вимагали фізичних зусиль. У цифрову епоху створюються комп'ютерні інструменти для автоматизації завдань, які потребують розумових зусиль. Можливості цих інструментів поступово розширювалися для виконання завдань, які потребують дедалі більшого інтелекту. Ця еволюція породила тип інструменту, який ми називаємо інтелектуальною системою.

Інтелектуальні системи допомагають нам виконувати спеціалізовані завдання в професійних сферах, таких як медична діагностика (наприклад, розпізнавання пухлин на рентгенівських знімках) або управління аеропортом (наприклад, створення нового призначення виходів на аеропорт за наявності інциденту). Вони також можуть виконувати для нас стомлюючі завдання (наприклад, автономне водіння автомобіля чи прибирання будинку) або небезпечні завдання, такі як дослідження невідомих територій (наприклад, підводне дослідження).

Розробка такого типу систем зараз є інженерною дисципліною інформаційних технологій, що вимагає ефективних методів і засобів. Точна

характеристика інтелектуальної системи є нетривіальною, оскільки вона базується на концепціях, пов’язаних із когнітивними функціями, сферою, яка не повністю зрозуміла, термінологія та рівень абстракції якої можуть відрізнятися залежно від галузі дослідження (нейронаука, інформатика, робототехніка, філософія, когнітивна психологія тощо). Деякі з використовуваних термінів можуть навіть змінитися з пропозицією нових обчислювальних моделей інтелекту та новими науковими відкриттями, пов’язаними з нашим розумінням розуму.

Однак інтелектуальна система — це не те саме, що ШІ, хоча ці терміни іноді використовуються як синоніми. За допомогою штучного інтелекту комп’ютери та інші машини намагаються імітувати людський інтелект , але його наявність автоматично не означає інтелектуальну систему. Наприклад, комп’ютер, на якому працює програма на основі штучного інтелекту, не означає, що сам комп’ютер є інтелектуальною системою, хоча він може робити внесок у таку систему як один із її агентів [4].

1.1.2 Приклади інтелектуальних систем

Інтелектуальні системи всюдисущі та пропонують безмежні можливості. Вони можуть принести користь багатьом галузям і вплинути як на наше особисте, так і на професійне життя. Приклади використання інтелектуальних систем у різних галузях промисловості та щоденного життя людини:

1) Транспорт: системи керування дорожнім рухом, аналіз транспортного потоку та моніторинг заторів, координація парку доставки, автономні автомобілі, системи громадського транспорту, запобігання аваріям (рис.1.1).

Рисунок 1.1 – Приклад використання інтелектуальних систем в транспорті

2) Аерокосмічна: елементи управління в кабіні авіакомпанії (рис. 1.2), дрони, моніторинг космічного корабля, планування місії, розширене керівництво та навігація, управління повітряним рухом.

Рисунок 1.2 – Інтелектуальна система в кабіні пілота літака АН-178

3) Ідентифікація людини: візуальне спостереження, біометричний моніторинг (наприклад, розпізнавання обличчя або відбитків пальців, як на рис. 1.3), розпізнавання символів або мови.

Рисунок 1.3 – Приклад біометричної функції доступу

4) Кліматологія: прогнозування, системи попереднього попередження (наприклад, торнадо або цунамі), польові дослідження та моніторинг, супутникові зображення та аналіз.

5) Виробництво: передова робототехніка та автоматизація, автономні системи, діагностика та ремонт, управління запасами, візуальний огляд, зварювання (рис. 1.4).

Рисунок 1.4 – Застосування інтелектуальних систем у зварюванні

6) Освіта: репетиторство, визначення моделей навчання студентів, системи запитань і відповідей, планування та розклад курсів, інтерактивна онлайн-навчання.

7) Роздрібна торгівля: рекомендації щодо покупок в Інтернеті , термінали для торгових точок (POS), цифрові вивіски, планування та доставка товару (рис. 1.5);

Рисунок 1.5 – Мікромаркет від компанії Modern Expo

8) Домашня автоматизація (рис. 1.6): розумна техніка, управління кліматом і освітленням, розваги.

Рисунок 1.6 – Управління всією побутовою технікою зі смартфона

9. Громадське здоров'я: медична допомога, медична діагностика, телемоніторинг, управління кризовими ситуаціями у сфері охорони здоров’я (наприклад, пандемія COVID-19), виявлення моделей насильства, біомедична інженерія (рис. 1.7).

Рисунок 1.7 – Застосування штучного інтелекту в медицині

Вбудований інтелект є невід’ємним компонентом Інтернету речей (IoT). Пристрої IoT мають можливість автоматично передавати дані через мережу без участі людини. Використовуючи AI та 5G , IoT може створювати інтелектуальні системи з потенціалом впливати на наше життя на всіх рівнях [1, 5].

1.1.3 Огляд систем доступу

Рішення контролю доступу, особливо бездротові, знаходяться на піку розвитку. Організації по всьому світу використовують новітні технології для захисту свого фізичного простору. Таким чином, за прогнозами, ринок зросте до 14,9 мільярдів доларів у 2028 році.

Якщо ви хочете залишатися попереду в безпеці, ця публікація стане вашим головним путівником щодо найактуальніших функцій системи контролю доступу у 2023 році.

Методи автентифікації користувачів. Впровадження функцій двофакторної автентифікації є останньою тенденцією в автоматизованих системах контролю доступу (а також у носимих пристроях IoT). Тим не менш, у 2023 році вкрай важливо мати декілька методів автентифікації користувачів. Вони забезпечать передовий рівень безпеки, більшу гнучкість і зручність для користувачів. Ось кілька сучасних варіантів автентифікації, з яких ви можете вибрати:

- QR-коди;
- bluetooth;
- зчитувачі UHF RFID;
- вбудована технологія HomeLink (в сучасних автомобілях);
- номерні знаки транспортних засобів;
- теги NFC;
- банківські картки;
- віддалений доступ через мобільні програми або веб-інтерфейси;
- Apple Pay/Google Pay на смартфоні чи годиннику;
- телефонні дзвінки;
- пульти дистанційного керування;

– біометричні функції доступу: відбиток пальця (рисунок 1.3), райдужка, долоня, розпізнавання обличчя.

Інтеграція з іншими сервісами та додатками: Google Assistant, Siri, Alexa та IFTTT.

Можна зауважити, що фізичні ідентифікатори, такі як брелоки та картки, застарівають. Приємно мати їх як резервні, але найкращі методи автентифікації користувача включають бездротові технології.

Чим більше можливостей автентифікації, тим ефективніша система контролю доступу. Таким чином, він задовольнить потреби будь-якого користувача та забезпечить безпеку найвищого рівня.

Хмарне керування. Найновіші можливості системи контролю доступу повинні включати хмарне керування. Це дозволяє віддалено контролювати фізичні простори через веб-браузер або мобільний додаток.

Серед основних переваг хмарних систем доступу :

– просте керування доступом з будь-якої точки світу;

– шифрування даних, сповіщення в реальному часі, системні звіти та автоматичні оновлення програмного забезпечення для високого рівня безпеки;

– підвищена масштабованість без дорогого оновлення апаратного забезпечення;

Заглядаючи в майбутнє, хмарні системи контролю доступу широко використовуватимуть технології AI та IoT, а також прогнозну аналітику.

Мобільний контроль доступу. Рішення для мобільного доступу дозволяють користувачам отримувати доступ до фізичного простору за допомогою мобільного пристрою замість звичайного брелока чи картки доступу. Такі системи використовують технології Інтернету, Bluetooth або NFC для перевірки особи користувачів, щоб згодом відкривати двері, ворота чи інші бар’єри.

Переваги впровадження мобільного доступу як однієї з сучасних функцій системи контролю доступу:

– зручність, користувачам більше не потрібно носити традиційні картки доступу або ключі, які можна легко втратити або забути;

– покращена безпека, ідентичність користувачів перевіряється за допомогою біометричних датчиків, таких як відбиток пальця або розпізнавання обличчя;

– гнучкість, користувачі можуть надавати або скасовувати доступ віддалено.

Не всі мобільні пристрої можуть бути сумісні з вашою системою контролю доступу. Але це можна виправити, встановивши універсальний контролер.

Універсальний контролер. Система контролю доступу повинна керувати багатьма об'єктами, такими як:

- замки;
- ворота;
- бар'єри;
- турнікети;
- ліфти;
- болларди.

Він також повинен обслуговувати ще більше пристроїв ідентифікації:

- зчитувачі тегів RFID та NFC;
- зчитувачі номерних знаків або камери;
- біометричні зчитувачі;
- зчитувачі QR-кодів;
- та багато іншого.

Таким чином, універсальний контролер є однією з найважливіших характеристик систем контролю доступу. Він повинен успішно працювати з різними пристроями та вирішувати проблеми сумісності та доступу. Універсальний контролер також корисний у багатьох сценаріях підключення та конфігурації програмного забезпечення.

Отже, для хорошої роботи такий контролер повинен відповідати таким специфікаціям:

– універсальна підтримка читачів;

– універсальна підтримка управління пристроями;

– універсальна підтримка кнопок виходу, систем безпеки, протипожежних систем, кнопок охорони та ін;

– різні методи хмарного підключення, включаючи Wi-Fi, Ethernet, GSM, Modbus;

– методи керування резервним копіюванням, такі як локальна панель адміністратора, Bluetooth тощо;

– зовнішні датчики відкриття, проходу та ін.

Не кожен розроблений контролери відповідають всім характеристикам, зазначеним вище. Мікроконтролер для системи контролю та управління доступом «Пропускатор».

Штучний інтелект в контролі доступу. Доступ на основі штучного інтелекту є однією з найефективніших функцій системи контролю доступу нового покоління. Він використовує розширені алгоритми для виявлення потенційних загроз безпеці та аномалій. Доступ на основі штучного інтелекту допомагає аналізувати дані з різних джерел, як-от біометричних датчиків, систем відеоспостереження або журналів доступу.

Штучний інтелект в безпечних системах контролю доступу включає:

1) Підвищена точність (алгоритми ШІ швидко аналізують величезні обсяги даних);

2) Посилена безпека (системи на основі штучного інтелекту розпізнають обличчя, голоси та моделі поведінки, що ускладнює доступ неавторизованим особам);

3) Покращений досвід користувача (системи контролю доступу на базі ШІ можуть увімкнути персоналізоване розпізнавання голосу або функції безконтактного доступу).

Індивідуальні рішення на основі штучного інтелекту можуть бути занадто дорогими для реалізації. Але організації можуть отримати доступ до функцій штучного інтелекту через навігаційні пристрої Siri, Alexa та GPS.

Системні інтеграції. Системна інтеграція поєднує різні технології, API та системи у програмному забезпеченні для керування доступом. Вони можуть включати рішення домашньої автоматизації Інтернету речей , виявлення вторгнень

або пожежну сигналізацію для створення більш комплексного та ефективного рішення безпеки.

Характеризуючи API, чим відкритіша платформа, тим краще. Прикладний програмний інтерфейс повинен приймати дані і наповнювати ними систему швидко і без зусиль.

Іншою важливою інтеграцією для ACS є системи управління взаємовідносинами з клієнтами (CRM). Вони часто необхідні для отримання даних користувача для створення рахунків клієнта або розрахунку зарплати співробітникам.

Переваги різноманітних системних інтеграцій включають:

1) кращу безпеку (різні системи оброблятимуть ваші фізичні активи);

2) покращену ефективність (системна інтеграція зменшує потребу в ручному втручанні);

3) розширений аналіз даних (ви збираєте інформацію з кількох джерел).

Перш ніж інтегрувати різні системи у ваше рішення контролю доступу, врахуйте потенційні обмеження, такі як складність і вимоги до обслуговування.

Функції керування відвідувачами. Система управління відвідувачами – це інструмент, який керує потоком людей, які входять і виходять з будівлі чи приміщення. Він відстежує та перевіряє особу відвідувачів і контролює їхні переміщення на сайті.

Як сучасні функціональні можливості системи контролю доступу, управління відвідувачами може надати: покращена безпека (спрощена реєстрація відвідувачів і реєстрації, система забезпечує доступ до приміщення лише авторизованих відвідувачів); кращий аналіз даних (система надає дані про людей, які відвідують ваші приміщення).

Цю функцію може бути непросто налаштувати. Але з відповідними експертами ви зможете використовувати його на повну силу.

Настроювані функції контролю доступу. Настроювані функції контролю доступу адаптують ACS до конкретних вимог об’єкта. Вони дозволяють контролеру змінювати рівні доступу, дозволи та формувати групи користувачів, щоб люди могли отримати доступ до потрібних областей у потрібний час.

Хорошим прикладом цього є гостьовий доступ. Мешканці будинку можуть надати дозвіл своїм гостям за допомогою тимчасових QR-кодів, мобільних додатків тощо.

Переваги настроюваних функцій контролю доступу включають:

– більший контроль, організації можуть налаштувати дозволи доступу;

– покращену гнучкість, користувачі можуть вибрати необхідні функції контролю доступу;

– покращену зручність, організації адаптують ACS до своїх конкретних потреб.

Тим не менш, можливість налаштування іноді супроводжується складністю. Користувачі можуть зіткнутися з високими витратами на налаштування та тривалим обслуговуванням системи . Отже, враховуйте ці обмеження, перш ніж застосовувати спеціальні функції.

Однією з інших обов’язкових функцій систем контролю доступу є доступ до кількох сайтів . Це допомагає керувати доступом до кількох областей з однієї платформи.

Основні переваги багатосайтових рішень контролю доступу включають:

– централізоване управління, організації контролюють свої активи з одного місця;

– економію часу та скорочення адміністративних витрат, користувачі можуть оптимізувати процеси контролю доступу на кількох сайтах.

ACS дозволяє контролювати різні місця за допомогою мобільного додатку: керування доступом до кількох сайтів через мобільний додаток та керування доступом до кількох сайтів через мобільний додаток користувача.

Відеодомофон та відеоспостереження. Охорона будівлі зазвичай використовує відеодомофон, щоб перевірити особу людини, перш ніж впустити її в охоронювану зону. Але відеоспостереження дозволяє підійти до безпеки більш комплексно.

Відеоспостереження стане у нагоді користувачам, які відкривають двері своїм гостям, а також адміністраторам СКУД, які стежать за ситуацією на об'єкті.

Інші функції включають автоматичне збереження кадрів або зображень для вирішення конфліктних ситуацій або порушень.

Переваги, які ви можете очікувати від цих функцій: покращена безпека (система відеоспостереження забезпечує цілодобовий моніторинг) та підвищена відповідальність (можна використовувати відеоматеріали, щоб перевірити, хто і коли входив і виходив із зони)

Це найважливіші характеристики систем контролю доступу. Проте ви можете включити деякі додаткові, щоб ще більше покращити рішення безпеки. Наприклад, розгляньте підтримку приватного сервера або перевірте, чи ACS пропонує максимальну автономію для користувача.

Численні функції системи контролю доступу наступного покоління допоможуть забезпечити розширений захист фізичних сайтів. До них належать хмарне керування, контроль мобільного доступу, інтеграція AI, настроювані функції та інші, які ми щойно розглянули [6].

1.2 Системи доступу на базі мікроконтролерів

Існує багато різних систем доступу на базі мікроконтролерів, які використовуються в різних пристроях, таких як електронні замки, системи безпеки та інші. Ось декілька прикладів:

Системи зчитування біометричних даних: ці системи використовують сканери відбитків пальців, сканери сітківки ока або системи розпізнавання обличчя для ідентифікації користувачів. Мікроконтролери використовуються для зберігання та обробки біометричних даних та керування доступом.

RFID-системи: ці системи використовують радіочастотні мітки для ідентифікації предметів або людей. Мікроконтролери використовуються для зчитування та обробки даних, що містяться на мітках, та для керування доступом до об'єктів.

PIN-кодові системи: ці системи використовуються для захисту від несанкціонованого доступу за допомогою введення користувачем PIN-коду.

Мікроконтролери використовуються для зберігання та обробки кодів, перевірки їх на відповідність та керування доступом.

Bluetooth-системи: ці системи використовують Bluetooth-технологію для передачі даних між пристроями та керування доступом. Мікроконтролери використовуються для обробки даних, що передаються через Bluetooth, та керування доступом на основі цих даних.

ZigBee-системи: ці системи використовують ZigBee-технологію для передачі даних між пристроями та керування доступом. Мікроконтролери використовуються для обробки даних, що передаються через ZigBee, та керування доступом на основі цих даних.

Ці системи можуть бути різних типів та використовувати різні методи ідентифікації та автентифікації користувачів. Наприклад, системи зчитування біометричних даних та RFID-системи використовують методи ідентифікації, які базуються на унікальних фізичних характеристиках особи або предмета. PIN-кодові системи використовують методи ідентифікації на основі знання спеціального коду, який може бути відомим лише користувачеві. Bluetooth-системи та ZigBee-системи використовують методи ідентифікації на основі ідентифікаторів пристроїв та спеціальних ключів доступу.

Із перевагами систем доступу на базі мікроконтролерів можна відзначити їх високу надійність, швидкість обробки даних та можливість програмування для різноманітних варіантів використання. Водночас, серед недоліків можна виділити відносну складність налаштування та програмування таких систем, а також вартість обладнання.

Загалом, системи доступу на базі мікроконтролерів забезпечують високий рівень безпеки та надійності, тому вони широко використовуються в різних областях, де важливо захистити важливі об'єкти та інформацію від несанкціонованого доступу [7].

1.3 Переваги та недоліки інтелектуальної системи

Інтелектуальна система – це програмний продукт, здатний до виконання завдань, які зазвичай вимагають людського інтелекту. Основна перевага інтелектуальної системи полягає у здатності до автоматизації рутинних та складних процесів, що дозволяє економити час та зусилля людей. Окрім того, інтелектуальні системи можуть збирати та аналізувати великі обсяги даних, що дозволяє зробити точні прогнози та приймати обґрунтовані рішення.

Серед інших переваг інтелектуальних систем можна відзначити:

– ефективність: інтелектуальні системи можуть виконувати задачі значно швидше, ніж люди;

– точність: інтелектуальні системи можуть здійснювати аналіз даних та приймати рішення з високою точністю;

– надійність: інтелектуальні системи можуть працювати безперебійно та без помилок протягом тривалого часу.

Однак, на жаль, інтелектуальні системи також мають деякі недоліки, які потрібно враховувати:

– необхідність навчання: інтелектуальні системи потребують певного часу та зусиль, щоб навчитися виконувати нові задачі;

– обмеженість: інтелектуальні системи можуть бути обмежені в тому, що вони можуть виконувати, залежно від їхнього типу та складності;

– незрозумілість: іноді рішення, прийняті інтелектуальною системою, можуть бути незрозумілими для людей, що може створити проблеми в деяких випадках;

– ризик зловживання: інтелектуальні системи можуть використовуватися для зловживання та порушення приват ності, що може призвести до небезпеки для людей та суспільства в цілому;

– вартість: розробка та використання інтелектуальних систем може бути досить дорогим, що може створити фінансові проблеми для деяких організацій;

– технічні проблеми: інтелектуальні системи можуть бути вразливі до технічних проблем, таких як збої апаратного забезпечення або помилки програмного забезпечення.

Загалом, інтелектуальні системи мають безліч переваг, але також потребують обережного використання та врахування їхніх недоліків, щоб максимально ефективно використовувати їхні можливості та уникнути можливих проблем [5].

1.4 Різні виконання інтелектуальних систем

Інтелектуальні системи можуть бути реалізовані багатьма різними способами, залежно від їх призначення та використовуваних технологій. Ось кілька прикладів різних типів інтелектуальних систем:

1) Експертні системи: це комп’ютерні програми, які імітують здатність людини-експерта в певній галузі приймати рішення. Вони призначені для вирішення складних проблем шляхом обґрунтування сукупності знань, представлених переважно у вигляді правил «якщо-тоді», і можуть використовуватися в таких сферах, як медицина, фінанси та інженерія.

2) Нейронні мережі: це комп’ютерні системи, які намагаються імітувати структуру та функції людського мозку. Вони складаються із взаємопов’язаних вузлів, які з часом можуть вивчати нові дані та адаптуватися до них, і їх можна використовувати для таких завдань, як розпізнавання зображень і мови.

3) Системи нечіткої логіки: це системи, які використовують нечіткі набори та нечіткі міркування для роботи з невизначеністю та неточністю. Вони часто використовуються в системах управління, де точні рішення не завжди можливі або необхідні.

4) Генетичні алгоритми: це алгоритми, які використовують принципи природного відбору та генетики для пошуку найкращого вирішення проблеми. Їх можна використовувати в задачах оптимізації, таких як пошук найкращої конфігурації компонентів машини.

5) Робототехніка: інтелектуальні системи також можуть бути реалізовані у фізичних роботах, яких можна запрограмувати сприймати навколишнє середовище

та розумно реагувати на нього. Роботизовані системи можна використовувати в таких сферах, як виробництво, медицина та дослідження космосу.

6) Обробка природної мови (NLP): це галузь дослідження, яка стосується взаємодії між комп'ютерами та людьми за допомогою природної мови. Техніки обробки природної мови можна використовувати для створення чат-ботів і віртуальних помічників, перекладу мов, узагальнення текстів і аналізу настроїв.

7) Машинне навчання: це підмножина штучного інтелекту, яка дозволяє системам автоматично покращувати ефективність виконання завдання, навчаючись на даних. Алгоритми машинного навчання можна використовувати для визначення шаблонів і зв'язків у даних, а також для прогнозування чи прийняття рішень на основі цих даних.

8) Інтелектуальний аналіз даних: це процес виявлення закономірностей у великих наборах даних за допомогою алгоритмів машинного навчання, статистичного аналізу та систем баз даних. Методи інтелектуального аналізу даних можна використовувати для отримання корисної інформації з великих обсягів даних, наприклад поведінки клієнтів, тенденцій у продуктах і виявлення шахрайства.

9) Комп'ютерний зір: це галузь дослідження, яка дає можливість комп'ютерам інтерпретувати та розуміти візуальну інформацію з навколишнього світу. Технології комп'ютерного зору можна використовувати для створення систем розпізнавання зображень і відео, відстеження об'єктів, вимірювання відстаней, ідентифікації та класифікації об'єктів.

10) Інтелектуальні агенти: це програмне забезпечення, яке діє від імені користувача або іншої програми, зі здатністю сприймати їхнє оточення, міркувати про нього та вживати заходів для досягнення цілей. Інтелектуальні агенти можна використовувати в таких сферах, як електронна комерція, ігри та робототехніка.

Це лише кілька прикладів різних типів інтелектуальних систем, які можна реалізувати. Вибір реалізації залежить від конкретних потреб і вимог програми, а також від наявних технологій і ресурсів.

Таким чином, інтелектуальні системи можуть бути реалізовані різними способами залежно від конкретних потреб і вимог програми. Деякі з

найпоширеніших типів інтелектуальних систем включають експертні системи, нейронні мережі, системи нечіткої логіки, генетичні алгоритми, робототехніку, обробка природної мови, машинне навчання, інтелектуальний аналіз даних, комп’ютерне зір та інтелектуальні агенти. Кожен тип інтелектуальної системи має свої переваги та обмеження, а вибір впровадження залежить від таких факторів, як доступ до даних, ресурсів та бажаних результатів [8].

РОЗДІЛ 2
ОГЛЯД ТЕХНОЛОГІЙ ТА КОМПЛЕКТУЮЧИХ СИСТЕМИ ДОСТУПУ НА БАЗІ ARDUINO

2.1 Безпровідні технології NFC RFID

2.1.1. Що таке NFC RFID?

NFC (Near Field Communication) і RFID (Radio Frequency Identification) — це технології бездротового зв’язку, які використовують радіохвилі для бездротової передачі даних між пристроями.

NFC – це форма безконтактного зв’язку, яка працює на частоті 13,56 МГц і може передавати дані на короткій відстані близько 10 сантиметрів. NFC використовується в основному для мобільних платіжних систем, контролю доступу та інших програм, які вимагають безпечного та надійного бездротового зв’язку малої дальності між пристроями.

RFID, з іншого боку, є більш універсальною технологією бездротового зв’язку, яка може працювати на діапазоні частот, від низьких частот (LF) до надвисоких частот (UHF). RFID використовується для широкого спектру застосувань, таких як управління запасами, відстеження активів і управління ланцюгом поставок. RFID-мітки можуть бути пасивними, що живляться від енергії зчитувача, або активними з власним джерелом живлення.

Хоча і NFC, і RFID використовують радіохвилі для бездротової передачі даних, вони відрізняються за діапазоном зв’язку, швидкістю передачі даних і сумісністю пристроїв. NFC призначений для зв’язку між мобільними пристроями на близькій відстані, тоді як RFID використовується для зв’язку на великій відстані в спеціалізованих пристроях промислового та комерційного застосування [9].

2.1.2 Принцип роботи NFC RFID

NFC RFID або радіочастотна ідентифікація ближнього поля (NFC) – це технологія, яка дозволяє двом пристроям обмінюватися бездротовим зв’язком, коли вони розташовані близько один до одного. Принцип роботи NFC RFID складається з двох основних компонентів: пристрою читання/запису NFC і мітки NFC.

Мітка NFC – це невеликий пасивний пристрій, який містить крихітний мікрочіп і маленьку рамкову антену. Коли пристрій зчитування/запису NFC наближається до мітки NFC, він викликає електричний струм у рамковій антені мітки, яка, у свою чергу, живить мікрочіп у мітці. Після живлення мікрочіп може спілкуватися з пристроєм читання/запису, модулюючи електричне поле навколо антени мітки.

NFC RFID працює на частоті 13,56 МГц і може передавати дані на швидкості до 424 Кбіт/с. Це робить його придатним для програм, які вимагають бездротового зв’язку малого радіусу дії, наприклад мобільних платежів, контролю доступу та передачі даних між мобільними пристроями.

Принцип роботи NFC RFID базується на тих самих фундаментальних принципах, що й інші технології RFID, такі як пасивна та активна RFID. Однак NFC RFID має додаткову перевагу в тому, що він сумісний з більшістю мобільних пристроїв, що робить його популярним вибором для широкого спектру програм.

Окрім основного принципу роботи NFC RFID, є кілька інших факторів, які впливають на його функціональність і продуктивність.

Одним з важливих аспектів NFC RFID є відстань зв’язку між зчитувачем/записувачем і тегом. NFC RFID має відносно короткий діапазон зв’язку – близько 10 сантиметрів, який призначений для запобігання небажаному або випадковому зв’язку між пристроями. Цей короткий радіус дії також забезпечує більш точний зв’язок і покращує безпеку таких програм, як безконтактні платежі.

Ще одним ключовим фактором принципу роботи NFC RFID є швидкість передачі даних. NFC RFID може передавати дані зі швидкістю до 424 Кбіт/с, що значно повільніше, ніж інші протоколи бездротового зв’язку, такі як Wi-Fi або Bluetooth. Однак цієї нижчої швидкості достатньо для більшості програм NFC, які зазвичай включають невеликі обсяги даних, наприклад облікові дані автентифікації або невеликі передачі даних між пристроями.

Нарешті, NFC RFID покладається на різні протоколи та стандарти для забезпечення сумісності між пристроями. Ці стандарти визначають різні аспекти зв’язку NFC, такі як формати обміну даними, режими зв’язку та протоколи безпеки.

Найпоширеніші стандарти для NFC RFID включають ISO/IEC 14443 та ISO/IEC 18092.

Загалом, принцип роботи NFC RFID — це простий, але ефективний спосіб увімкнути бездротовий зв’язок між пристроями малого радіусу дії. Його низьке енергоспоживання, сумісність з мобільними пристроями та високий рівень безпеки роблять його популярним вибором для широкого спектру додатків, від безконтактних платежів і контролю доступу до передачі даних і мобільної реклами [10].

2.1.2 Різниця між NFC та RFID

NFC (Near Field Communication) і RFID (Radio Frequency Identification) – це технології бездротового зв’язку, які використовують радіохвилі для передачі даних. Хоча вони мають певну схожість у принципах роботи та сферах застосування, між двома технологіями є кілька ключових відмінностей.

Основна відмінність між NFC і RFID полягає в їх дальності зв'язку. NFC працює на набагато меншій відстані, ніж RFID, зазвичай у межах 10 сантиметрів, тоді як RFID може працювати в діапазоні кількох метрів. Цей короткий діапазон NFC є навмисним, оскільки він розроблений для зв’язку між пристроями на близькій відстані, тоді як RFID зазвичай використовується для додатків, які вимагають зв’язку на більшій відстані, наприклад для відстеження інвентарю або моніторингу руху транспортних засобів.

Ще одна відмінність між NFC і RFID полягає в типах пристроїв, які підтримують кожну технологію. NFC розроблено для роботи зі смартфонами та іншими мобільними пристроями, тоді як RFID зазвичай використовується в спеціалізованих пристроях, таких як сканери штрих-кодів або системи управління запасами. Це означає, що NFC є більш доступним для споживачів і його легше інтегрувати в існуючі мобільні пристрої, тоді як RFID більше підходить для конкретних промислових або комерційних застосувань.

Нарешті, NFC і RFID відрізняються за швидкістю передачі даних. NFC має максимальну швидкість передачі даних 424 Кбіт/с, тоді як RFID зазвичай працює на набагато нижчих швидкостях передачі даних, зазвичай менше 10 Кбіт/с. Хоча ця нижча швидкість передачі даних може обмежувати типи даних, які можна передати

через RFID, зазвичай її достатньо для типів програм, для яких вона використовується. NFC і RFID мають певну схожість щодо використання радіохвиль для бездротової передачі даних, вони відрізняються за діапазоном зв’язку, сумісністю пристроїв і швидкістю передачі даних. NFC призначений для зв’язку між мобільними пристроями на близькій відстані, тоді як RFID використовується для зв’язку на великій відстані в спеціалізованих пристроях промислового та комерційного застосування.

Ще одна відмінність між NFC і RFID полягає в тому, як вони забезпечують захист даних. Обидві технології використовують шифрування та інші функції безпеки для запобігання несанкціонованому доступу та забезпечення конфіденційності даних. Однак NFC має більш просунутий протокол безпеки, ніж RFID, що робить його більш придатним для конфіденційних програм, таких як безконтактні платежі.

Однією з ключових функцій безпеки NFC є процес взаємної автентифікації, який відбувається між пристроєм NFC і тегом. Цей процес включає в себе як пристрій, так і тег, які перевіряють особу один одного та гарантують, що вони авторизовані спілкуватися один з одним. Після завершення процесу автентифікації пристрої можуть безпечно обмінюватися даними без ризику перехоплення чи підробки.

З іншого боку, RFID не має такого рівня безпеки і більш вразливий до таких атак, як підслуховування та перехоплення даних. Частково це пов’язано з більшим діапазоном зв’язку RFID, що робить його більш сприйнятливим до перешкод і несанкціонованого доступу.

Ще одна ключова відмінність між NFC і RFID – типи тегів, які вони використовують. Теги NFC зазвичай менші та компактніші, ніж мітки RFID, що полегшує їх інтеграцію в мобільні пристрої та іншу невелику електроніку. Теги NFC також можна перезаписувати, що дозволяє багаторазово використовувати та застосовувати.

Мітки RFID, з іншого боку, бувають різних розмірів і типів залежно від їхнього призначення. Деякі RFID-мітки є пасивними, тобто вони покладаються на енергію зчитувача для живлення, тоді як інші активні та мають власне джерело

живлення. Теги RFID також можуть бути лише для читання, тобто їх можна запрограмувати лише один раз, або для читання та запису, що дозволяє багаторазове читання та запис.

Загалом, хоча NFC і RFID мають певну схожість щодо використання радіохвиль для бездротової передачі даних, вони відрізняються за діапазоном зв'язку, функціями безпеки та типами тегів. NFC розроблений для зв'язку на близькій відстані між мобільними пристроями з розширеними протоколами безпеки, тоді як RFID більше підходить для зв'язку на більшій відстані в спеціалізованих пристроях із ширшим діапазоном типів тегів і програм [11].

2.2 Комплектуючі системи системи доступу на базі Arduino

2.2.1 Вибір мікроконтролера для розробки системи

Arduino – популярна платформа для розробки електронних пристроїв і проектів. Мікроконтролери Arduino – це невеликі програмовані пристрої, які можна використовувати для керування та взаємодії з різними електронними компонентами, такими як датчики, двигуни та освітлення. Вони засновані на мікроконтролері Atmel AVR і використовують спрощену версію мови програмування C++.

Плати Arduino доступні в різних форм-факторах і з різними можливостями, що дозволяє користувачам вибрати плату, яка найкраще відповідає потребам їх проекту. Деякі з найпоширеніших плат Arduino включають Arduino Uno (рис. 2.1), Arduino Mega (рис. 2.2) та Arduino Nano (рис. 2.3).

Рисунок 2.1 – Arduino Uno

Рисунок 2.2 – Arduino Mega

Рисунок 2.3 – Arduino Nano

Однією з ключових особливостей Arduino є простота використання. Середовище розробки програмного забезпечення має відкритий вихідний код і його можна безкоштовно завантажити, а також містить зручний інтерфейс для написання та завантаження коду в мікроконтролер. Мова програмування Arduino заснована на C++, але зі спрощеним синтаксисом і набором бібліотек, які полегшують роботу з електронними компонентами.

Ще однією важливою особливістю Arduino є його модульність. Плати Arduino можна підключати до широкого спектру датчиків і приводів, що дозволяє користувачам створювати власні електронні пристрої та інтерактивні проекти. Крім того, існує велика спільнота користувачів і розробників Arduino, які діляться ідеями, кодом і проектами, що полегшує навчання та початок роботи з Arduino.

Загалом, мікроконтролери Arduino – це універсальна та проста у використанні платформа для розробки електронних пристроїв та інтерактивних проектів. Вони підходять як для початківців, так і для експертів і можуть використовуватися в широкому діапазоні програм, включаючи роботизацію, домашню автоматизацію та проекти Інтернету речей (IoT) [12-14].

2.2.2 Кнопка

Кнопка є одним з базових елементів управління мікроконтролером (рис. 2.4). Вона забезпечує можливість взаємодії користувача з мікроконтролером шляхом введення сигналу.

Рисунок 2.4 – Кнопка

Фізично, кнопка складається з контактів, які з'єднані механічною пружиною. Коли кнопку натискають, контакти з'єднуються, створюючи електричне замикання. При відпусканні кнопки контакти роз'єднуються, і замикання переривається.

Загалом, кнопка є важливим базовим елементом управління мікроконтролером, яка надає можливість користувачу взаємодіяти з пристроєм. Вона використовується в різних проектах і залежно від потреб може мати різні режими роботи та функції [15].

2.2.3 RGB світлодіод

RGB LED розшифровується як Red, Green, Blue Light-Emitting Diode. Це тип світлодіодів, які можуть випромінювати світло трьох основних кольорів: червоного, зеленого та синього. На відміну від традиційного світлодіода, який випромінює один колір, світлодіод RGB містить три окремі світлодіодні мікросхеми, кожна з яких здатна відтворювати один із основних кольорів.

Три кольори, червоний, зелений і синій, можна комбінувати з різною інтенсивністю для створення широкого діапазону кольорів. Регулюючи інтенсивність кожного окремого світлодіодного чіпа, можна створювати мільйони кольорів, включаючи різні відтінки, відтінки та навіть біле світло.

Світлодіоди RGB широко використовуються в різних додатках, таких як системи освітлення, панелі дисплеїв, вивіски, візуальні ефекти та декоративне освітлення. Вони пропонують гнучкість і контроль над відтворенням кольорів, дозволяючи створювати динамічні та настроювані рішення освітлення. Світлодіоди RGB часто використовуються в поєднанні з мікроконтролерами або спеціалізованими контролерами для створення різних світлових ефектів, колірних візерунків і анімації.

Щоб керувати світлодіодом RGB, кожен колірний канал (червоний, зелений і синій) підключається до окремого вихідного контакту мікроконтролера або спеціального контролера світлодіодів RGB. Маніпулюючи напругою або струмом на кожному контакті, можна регулювати інтенсивність відповідного кольору, що призводить до отримання потрібного кольору.

Загалом світлодіоди RGB забезпечують універсальний і яскравий варіант освітлення, що дозволяє використовувати творчі та візуально привабливі додатки [16].

2.2.4 Сервопривід

В електроніці сервопривід або серводвигун – це пристрій, який забезпечує точне керування положенням, швидкістю та прискоренням механічної системи. Він зазвичай використовується в різних програмах, таких як робототехніка, автоматизація та системи дистанційного керування (рисунок 2.5).

Рисунок 2.5 – Сервопривід

Серводвигун складається з кількох компонентів, у тому числі двигуна постійного струму, механізму зворотного зв’язку (наприклад, потенціометра або кодера) і схеми керування. Схема керування отримує вхідні сигнали, як правило, у формі імпульсів, які визначають потрібне положення або рух. На основі цих вхідних сигналів схема керування регулює вихідну потужність двигуна для досягнення бажаного положення або руху.

Механізм зворотного зв’язку в серводвигуні постійно передає інформацію про поточне положення двигуна в схему керування. Цей зворотний зв'язок дозволяє ланцюгу керування порівнювати бажане положення з фактичним положенням і вносити необхідні налаштування для мінімізації будь-яких помилок. Постійно контролюючи та регулюючи потужність двигуна, серводвигун може досягти точного контролю над його рухом.

Серводвигуни відомі своєю здатністю підтримувати певне положення та протистояти зовнішнім силам, які можуть спробувати зрушити їх із цього положення. Вони широко використовуються в програмах, які вимагають точних і контрольованих рухів, таких як роботизовані руки, транспортні засоби з дистанційним керуванням (дистанційне керування), промислова автоматизація, карданні камери та 3D-принтери [17].

2.2.5 Зумер

Зумер – це пристрій, який видає звуковий або тональний сигнал (рис. 2.6). Він зазвичай використовується для надання звукових сповіщень, сповіщень або попереджень у різних електронних системах і пристроях.

Рисунок 2.6 – Зумер

Типовий зумер містить електромеханічний перетворювач, який відповідає за перетворення електричної енергії в звукову. Цей перетворювач зазвичай складається з невеликої магнітної котушки, охопленої діафрагмою або п’єзоелектричним елементом. Коли електричний струм протікає через котушку, він створює магнітне поле, яке взаємодіє з діафрагмою або п’єзоелектричним матеріалом, що призводить до вібрації та створення звукових хвиль.

Компоненти зумера можуть відрізнятися за дизайном і конструкцією. Деякі зумери є самостійними пристроями з вбудованою ланцюгом осцилятора, який створює безперервний тон при подачі живлення. Вони відомі як самокеровані або автоколивальні зумери. Іншим потрібен зовнішній генератор або джерело сигналу для генерації бажаного тону або звукової моделі.

Зумери широко використовуються в різних програмах, включаючи будильники, таймери, дверні дзвінки, ігрові консолі та електронні іграшки, щоб надавати користувачам звукову індикацію або зворотний зв’язок [18].

2.2.6 Зчитувач RFID RC522

Зчитувач RC522 RFID (радіочастотна ідентифікація) є популярним модулем, який використовується для зчитування та взаємодії з картами RFID або мітками в електронних системах (рис. 2.7). Він зазвичай використовується в різних програмах, включаючи системи контролю доступу, системи відвідування, управління запасами та системи автентифікації.

Рисунок 2.7 – Зчитувач RC522 RFID

Модуль RC522 заснований на інтегральній схемі MFRC522, яка включає зчитувач RFID, блок обробки цифрового сигналу та різноманітні інтерфейси керування та зв’язку. Модуль зв'язується з мікроконтролером або хост-системою за допомогою простого протоколу SPI (Serial Peripheral Interface).

Основні характеристики та можливості зчитувача RFID RC522:

– сумісність з RFID: модуль RC522 підтримує стандарт ISO/IEC 14443A, який є одним із широко використовуваних стандартів для безконтактних карток і тегів. Він може зчитувати RFID-карти або мітки, що працюють на частоті 13,56 МГц.

– читання та запис: модуль дозволяє як зчитувати унікальний ідентифікатор (UID) RFID-карт або тегів, так і записувати дані на певні типи записуваних карток або тегів, наприклад карти MIFARE Classic.

– антена: модуль RC522 має вбудовану антену, що усуває потребу у зовнішній антені. Він забезпечує помірний діапазон зчитування, як правило, до кількох сантиметрів, залежно від конструкції антени та RFID-картки чи мітки, що використовується.

– інтерфейс зв'язку: модуль зв'язується з головною системою або мікроконтролером за допомогою протоколу SPI, який забезпечує простий і ефективний спосіб обміну даними.

– підтримка бібліотеки: доступні різні бібліотеки програмного забезпечення та приклади для популярних платформ мікроконтролерів, таких як Arduino, для полегшення інтеграції модуля RC522 у проекти. Ці бібліотеки абстрагують деталі зв’язку низького рівня та забезпечують високорівневі функції для взаємодії зі зчитувачем RFID.

Використовуючи модуль зчитування RFID RC522, можна реалізувати такі функції, як виявлення карток, автентифікація та зберігання даних відповідно до конкретних вимог вашого проекту. Гнучкість і простота використання модуля зробили його популярним вибором серед любителів, студентів і професіоналів, які працюють з технологією RFID [19].

2.2.7 LCD дисплей

LCD (рідкокристалічний дисплей) – це тип плоскопанельного дисплея, який зазвичай використовується в електронних пристроях, таких як телевізори, комп'ютерні монітори, смартфони та цифрові годинники (рис. 2.8).

Рисунок 2.8 – LCD дисплей

РК-монітори мають ряд переваг, які сприяли їх широкому впровадженню:

– рідкокристалічні дисплеї тонкі та легкі порівняно зі старими технологіями відображення, такими як електронно-променеві трубки (CRT). Завдяки цьому вони добре підходять для портативних пристроїв і створюють елегантний і тонкий дизайн у різних сферах застосування;

– вони вимагають значно менше енергії для роботи, що робить їх ідеальними для пристроїв, що живляться від батарейок, технологія РК-дисплея забезпечує точне керування окремими пікселями, дозволяючи використовувати такі функції енергозбереження, як затемнення або вимкнення невикористаних частин екрана.

– РК-дисплеї пропонують високу роздільну здатність і чітку якість зображення, вони складаються з масиву крихітних пікселів, які можуть індивідуально змінювати свої характеристики пропускання світла, це дозволяє точно відтворювати текст, зображення та відео з яскравими кольорами та чудовою чіткістю.

– РК-дисплеї зазвичай забезпечують широкі кути огляду, гарантуючи, що відображуваний вміст залишається видимим з різних точок зору, це робить РК-

дисплеї придатними для застосувань, де кільком глядачам потрібен одночасний доступ до дисплея, наприклад, для презентацій або перегляду телебачення.

– рідкокристалічні дисплеї випромінюють менше мерехтіння порівняно зі старими технологіями відображення, зменшуючи навантаження на очі під час тривалого перегляду. Вони також містять такі функції, як покриття проти відблисків, щоб мінімізувати відблиски та покращити видимість за різних умов освітлення.

– LCD-технологію можна масштабувати до різних розмірів і пропорцій, що робить її адаптованою для різних застосувань, від невеликих дисплеїв на портативних пристроях до великих екранів для телевізорів або громадських вивісок, РК-дисплеї пропонують гнучкість у задоволенні різноманітних вимог до відображення.

– РК-дисплеї зазвичай мають довший термін служби, ніж ЕЛТ-дисплеї, вони менш чутливі до таких проблем, як вигоряння, що може вплинути на довговічність інших технологій відображення.

Хоча рідкокристалічні дисплеї мають численні переваги, варто зазначити, що нові технології, такі як дисплеї OLED (органічні світловипромінювальні діоди), пропонують додаткові переваги, як-от глибші рівні чорного, ширшу кольорову гаму та потенційну гнучкість. Проте рідкокристалічні дисплеї продовжують широко використовуватися завдяки своїй надійності, економічній ефективності та розвиненому виробничому процесу. Тому в проекті було вибрано використовувати саме такий тип дисплею [20].

РОЗДІЛ 3
ПІДКЛЮЧЕННЯ ЕЛЕМЕНТІВ ДО МІКРОКОНТРОЛЕРА

3.1 Підключення кнопки до мікроконтролера

Для підключення кнопки до мікроконтролера необхідно підключити контакти кнопки до вхідних/виходних пінів мікроконтролера. Це може бути зроблено шляхом підключення одного контакту до землі (GND), а іншого контакту до вхідного піна мікроконтролера. Також можна використовувати підтяжку резистора (пулл-ап або пулл-даун), щоб забезпечити стійкий стан піна, коли кнопка не натиснута.

Програмно, для взаємодії з кнопкою потрібно використовувати підтримувані мовою програмування функції для читання стану піна, до якого підключена кнопка. Це може бути функція, яка повертає значення 0 або 1 в залежності від стану піна (натиснута або не натиснута кнопка). Залежно від значення, яке повертається, можна виконувати певні дії або взаємодіяти з іншими частинами програми.

Кнопки широко використовуються в багатьох проектах, які вимагають взаємодії з користувачем, включаючи прості системи керування, вимикачі, ігрові пристрої та багато інших. Вони є надійним і простим способом отримання введення від користувача та виклику певних дій у програмі або контролю над певними функціями. Наприклад, кнопки можуть використовуватись для перемикання режимів роботи, введення параметрів, запуску або зупинки процесів, і багатьох інших функцій.

Однак, при роботі з кнопками слід враховувати кілька важливих моментів. Перш за все, кнопка може мати шуми або дрібні коливання при натисканні, що може призвести до спонтанного спрацювання. Це можна уникнути застосуванням дебаунсінгу - техніки, що виключає шуми під час читання стану кнопки.

Крім того, кнопка може працювати в режимі нормально відкритого (Normally Open, NO) або нормально закритого (Normally Closed, NC). В залежності від режиму роботи, програмне зчитування стану піна може змінитися.

Також, можна використовувати розрізнювальні кнопки, які підтримують кілька рівнів натискання, наприклад, одиночне натискання, подвійне натискання

або тривале натискання. Це дозволяє розширити можливості взаємодії з користувачем і додати більше функцій до програми [21].

Кнопка може бути підключена до любого цифорового піну, в нашому випадку використовуємо Arduino NANO тому з’єднуємо D0-D13, A0-A5 та запитуватись як цифрове значення (аналогові піни не використовуємо). Підключення кнопки обов'язково передбачає підтягування піна до протилежного від кнопки значення, так як напруга на цифровому піні має бути точно визначена. Кнопка підключаєтьс до GND, а пін підтягується допомогою pinMode (pin, INPUT_PULLUP). Приклад підключення кнопоки на макетній платі представлено на рисунку 3.1.

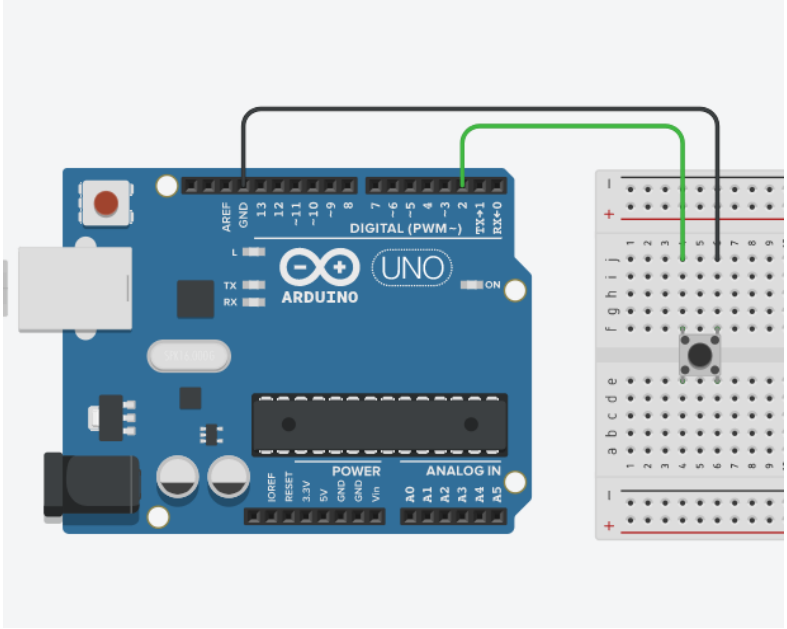

Рисунок 3.1 – Приклад підключення кнопоки на макетній платі

3.2 Підключення RGB світлодіода

RGB світлодіод підключається до джерела живлення 5V або за допомогою резисторів, щоб досить швидко не вийшов з ладу. Зазвичай резистори вже впаяні до плати де розміщується, сам світлодіод має загальний катод. Достатньо підключити GND до піну “-“, а піни RGB – до будь-яких цифрових пін мікроконтролера.

При підключенні до звичайних цифрових пін ми отримаємо лише 8 кольорів – чорний (всі вимкнені), білий (всі включені) та 6 поєднань між трьома кольорами.

При підключенні до ШИМ пніїв у нас з'явиться можливість контролювати яскравість кожного каналу кольору, що при стандартних налаштуваннях дає 256 градацій яскравості та 256*256*256 = 16.7 мільйонів відтінків для RGB світлодіода.

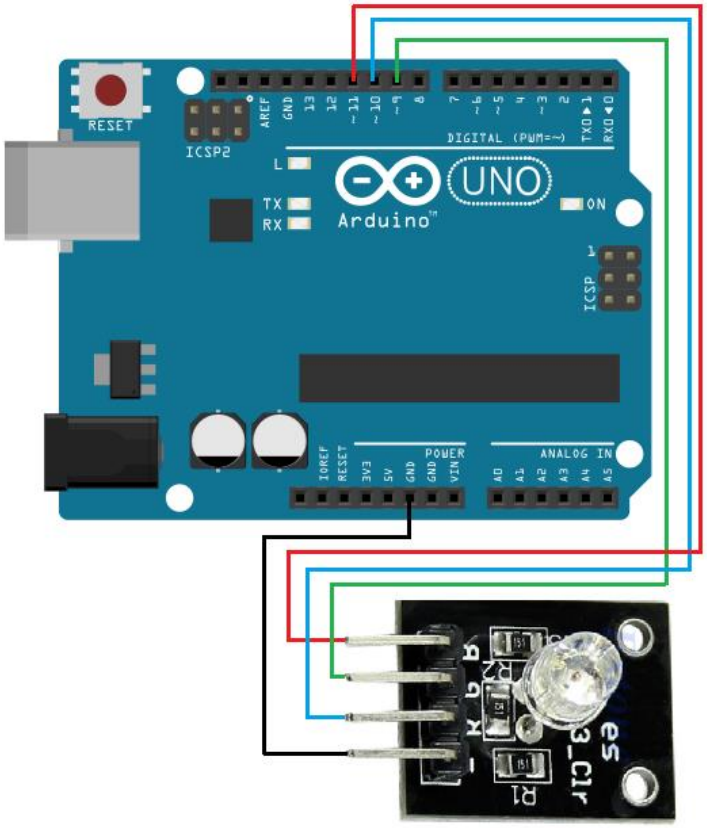

Рисунок 3.2 – Приклад підключення RGB світлодіода на макетній платі

Для програмування RGB світлодіода насправді бібліотеки непотрібні, оскільки світлодіодом можна керувати за допомогою базових функцій виведення. Але для зручності роботи з різними кольоровими моделями зручніше використовувати вже готові алгоритми (рисунок 3.3) [22].

```
#define R_PIN 6
#define G_PIN 5
#define B_PIN 3

setup()

pinMode(R_PIN, OUTPUT);
pinMode(G_PIN, OUTPUT);
pinMode(B_PIN, OUTPUT);

#define R_PIN 6
#define G_PIN 5
#define B_PIN 3
void setup() {
  pinMode(R_PIN, OUTPUT);
  pinMode(G_PIN, OUTPUT);
  pinMode(B_PIN, OUTPUT);
}
void loop() {
  digitalWrite(R_PIN, 1);
  delay(500);
  digitalWrite(R_PIN, 0);
  digitalWrite(G_PIN, 1);
  delay(500);
  digitalWrite(G_PIN, 0);
 digitalWrite(B_PIN, 1);

  delay(500);
  digitalWrite(B_PIN, 0);
}
```

Рисунок 3.3 – Лістинг програми підключення RGB світлодіода

3.3 Підключення сервопривода до мікроконтролера

Сервопривід – це тип двигуна, який зазвичай використовується в електроніці та робототехніці для точного керування положенням, швидкістю або прискоренням механізму. Сервоприводи зазвичай складаються з невеликого двигуна постійного струму, набору передач і системи зворотного зв’язку.

Система зворотного зв'язку зазвичай складається з потенціометра, який є змінним резистором, який вимірює положення валу двигуна, і схеми керування, яка порівнює фактичне положення з бажаним положенням і регулює швидкість і напрямок двигуна, щоб виправити будь-яку помилку.

Коли сервопривід отримує керуючий сигнал, зазвичай у формі сигналу широтно-імпульсної модуляції (ШІМ), схема керування обчислює необхідне положення двигуна на основі тривалості сигналу та регулює двигун для досягнення цього положення. Це дозволяє сервоприводам рухатися з високою точністю, що

робить їх корисними в різноманітних додатках, включаючи робототехніку, моделі літаків і промислову автоматизацію [23]. Приклад підключення сервоприводу до мікроконтролера Arduino зображено на рисунку 3.4.

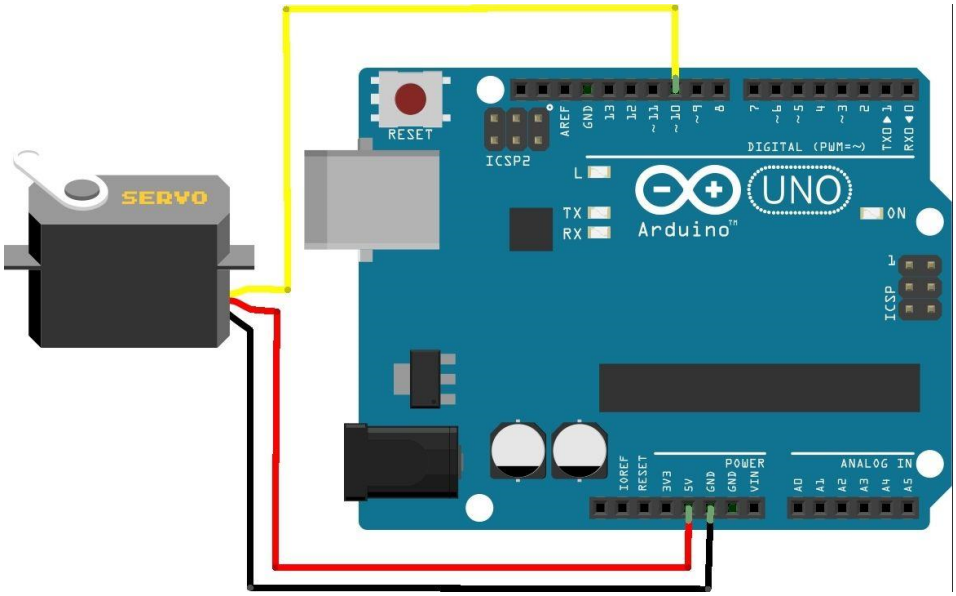

Рисунок 3.4 – Приклад підключення сервоприводу на макетній платі

Для керування сервоприводом можна використовувати стандартну бібліотеку Servo (рисунок 3.5).

```
#include <Servo.h>
Servo myservo;
uint8_t attach(int pin);           // підключити із вказанням піна
uint8_t attach(int pin, int min, int max); // " підключити із вказанням піна  та мінімальні і
максимальні значення
void detach();                     // відключити
void write(int value);             // повернути на кут в градусах
void writeMicroseconds(int value); // повернути на довжину імпульсу
```

```
#include <Servo.h>
```

Рисунок 3.5 – Лістинг програми підключення

3.4 Підключення зумера до мікроконтролера

Зумер зазвичай складається з електромеханічного перетворювача, який перетворює електричну енергію на звукову. Перетворювач зазвичай являє собою

невелику магнітну котушку, оточену діафрагмою або п’єзоелектричним елементом. Коли електричний струм проходить через котушку, він створює магнітне поле, яке взаємодіє з діафрагмою або п’єзоелектричним матеріалом, змушуючи його вібрувати та виробляти звукові хвилі [24]. Приклад підключення зумера до мікроконтролера Arduino (рисунок 3.6).

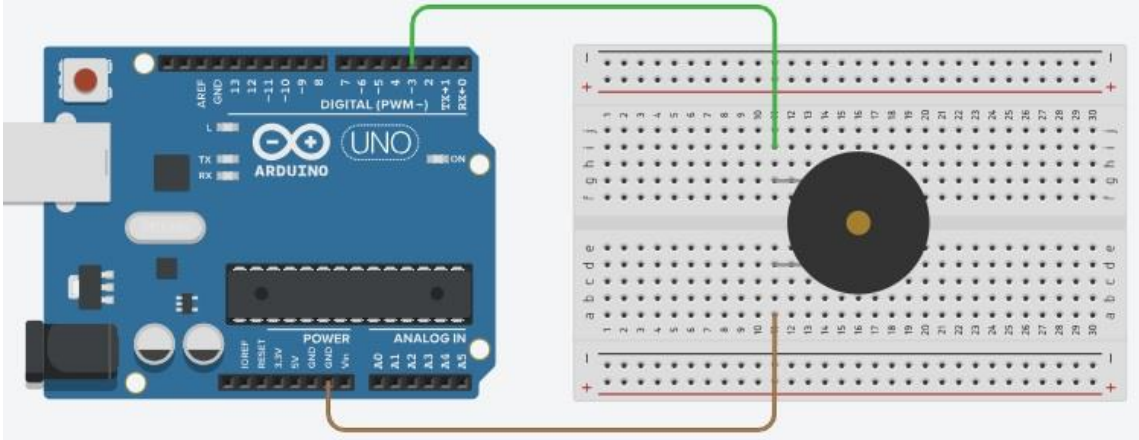

Рисунок 3.6 – Приклад підключення зумера на макетній платі

Якщо зумер пасивний, тоді можна генерувати звук потрібної частоти, тобто тон. Цей код змусить зумер видавати звуковий сигнал із частотою 1 кГц. І не потрібно робити пін вихідним, він вбудований у функцію tone() (риунок 3.7)

```
void setup() {
  tone(3, 1000);
}
```

Рисунок 3.7 – Лістинг програми підключення зумера

3.5 Підключення зчитувача RFID RC522 до мікроконтролера

Технологія RFID дозволяє обмінюватися даними зі спеціальними мітками по радіоканалу на невеликій відстані. Спочатку RFID використовували для створення електронних перепусток, а з часом багато NFC, як і більшість людей оплачує покупкиНіякого джерела живлення їм не потрібно і саме це дозволяє помістити мітку в пластикову картку, браслет або навіть наклейку. Тобто, буквально будь-що

RFID має кілька стандартів частот на яких ведеться радіозв'язок Дуже популярний модуль RC-552, а точніше його міні-версія, який і використано.

Використовуючи модуль зчитування RFID RC522, можна реалізувати такі функції, як виявлення карток, автентифікація та зберігання даних відповідно до конкретних вимог проекту. Гнучкість і простота використання модуля зробили його популярним вибором серед любителів, студентів і професіоналів, які працюють з технологією RFID [19]. Приклад підключення модуля RC522 до Arduino представлено на рисунку 3.8.

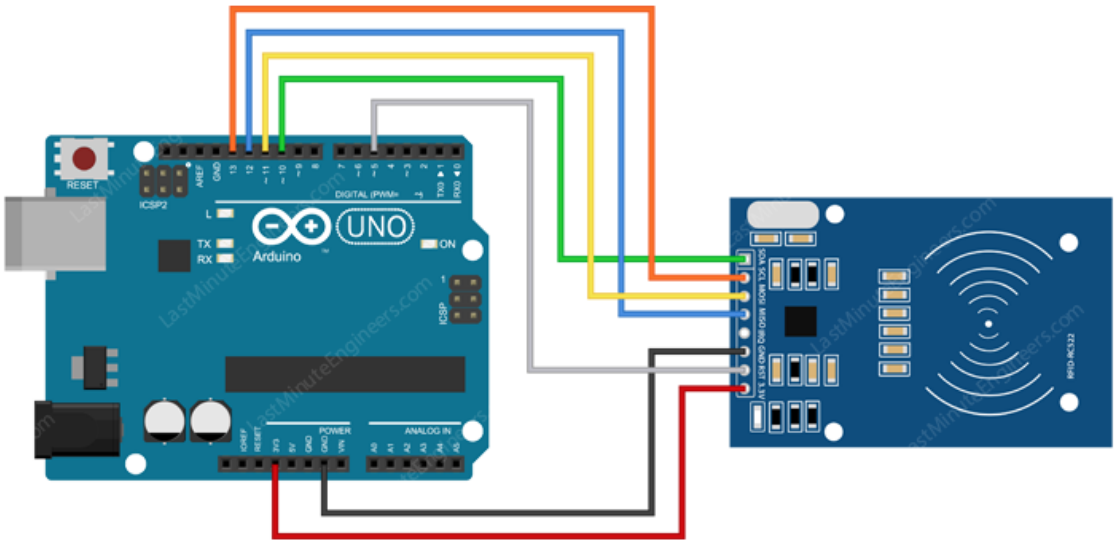

Рисунок 3.8 – Приклад підключення модуля RC522 до Arduino Uno

Бібліотека досить складна у використанні, особливо для читання та запису інформації, що зберігається на тегу. Але всі теги мають свій унікальний ID - ідентифікаційний номер (4-10 байт), для більшості тегів він жорстко закодований і не може бути змінений, який можна використовувати для ідентифікації. Простий приклад читання ідентифікатора тегу як 4-байтового числа зображено на рисунку 3.9.

```
#include <MFRC522.h>
MFRC522 rfid(10, 9); // SDA, RST
void setup() {
  Serial.begin(9600);
  SPI.begin();      // запуск шини
  rfid.PCD_Init();  // ініціалізація модуля
}
void loop() {
  // якщо підесена мітка
  if (rfid.PICC_IsNewCardPresent() && rfid.PICC_ReadCardSerial()) {
    // запишем мітку
    uint32_t ID;
    for (byte i = 0; i < 4; i++) {
      ID <<= 8;
      ID |= rfid.uid.uidByte[i];
    }
    // виведемо
    Serial.println(ID, HEX);
    delay(500);
  }
}
```

Рисунок 3.9 – Лістинг програми підключення модуля RC522

3.6 Підключення LCD дисплея до мікроконтролера

LCD дисплей, або РК-монітор мають ряд переваг, які сприяли їх широкому впровадженню:

1) Тонкі та легкі: рідкокристалічні дисплеї тонкі та легкі порівняно зі старими технологіями відображення, такими як електронно-променеві трубки (CRT). Завдяки цьому вони добре підходять для портативних пристроїв і створюють елегантний і тонкий дизайн у різних сферах застосування.

2) Низьке енергоспоживання: рідкокристалічні дисплеї відомі своєю енергоефективністю. Вони вимагають значно менше енергії для роботи порівняно з ЕПТ, що робить їх ідеальними для пристроїв, що живляться від батарейок. Технологія РК-дисплея забезпечує точне керування окремими пікселями, дозволяючи використовувати такі функції енергозбереження, як затемнення або вимкнення невикористаних частин екрана.

3) Висока роздільна здатність і якість зображення: РК-дисплеї пропонують високу роздільну здатність і чітку якість зображення. Вони складаються з масиву крихітних пікселів, які можуть індивідуально змінювати свої характеристики пропускання світла. Це дозволяє точно відтворювати текст, зображення та відео з яскравими кольорами та чудовою чіткістю.

4) Широкі кути огляду: РК-дисплеї зазвичай забезпечують широкі кути огляду, гарантуючи, що відображуваний вміст залишається видимим з різних точок зору. Це робить РК-дисплеї придатними для застосувань, де кільком глядачам потрібен одночасний доступ до дисплея, наприклад, для презентацій або перегляду телебачення.

5) Зменшене навантаження на очі: рідкокристалічні дисплеї випромінюють менше мерехтіння порівняно зі старими технологіями відображення, зменшуючи навантаження на очі під час тривалого перегляду. Вони також містять такі функції, як покриття проти відблисків, щоб мінімізувати відблиски та покращити видимість за різних умов освітлення.

6) Універсальність: LCD-технологію можна масштабувати до різних розмірів і пропорцій, що робить її адаптованою для різних застосувань. Від невеликих дисплеїв на портативних пристроях до великих екранів для телевізорів або громадських вивісок, РК-дисплеї пропонують гнучкість у задоволенні різноманітних вимог до відображення.

7) Довговічність: РК-дисплеї зазвичай мають довший термін служби, ніж ЕЛТ-дисплеї. Вони менш чутливі до таких проблем, як вигоряння, що може вплинути на довговічність інших технологій відображення.

Хоча рідкокристалічні дисплеї мають численні переваги, варто зазначити, що нові технології, такі як дисплеї OLED (органічні світловипромінювальні діоди), пропонують додаткові переваги, як-от глибші рівні чорного, ширшу кольорову гаму та потенційну гнучкість. Проте рідкокристалічні дисплеї продовжують широко використовуватися завдяки своїй надійності, економічній ефективності та розвиненому виробничому процесу [25]. Тому в проекті було вибрано використовувати саме їх, схему підключення до Arduino Uno представлено на рисунку 3.10.

Підключення пінів LCD дисплею з модулем I2C доволі не важке і стандартне для багатьох видів дисплеїв (таблиця 3.1), код підключенн представлено на рисунку 3.11.

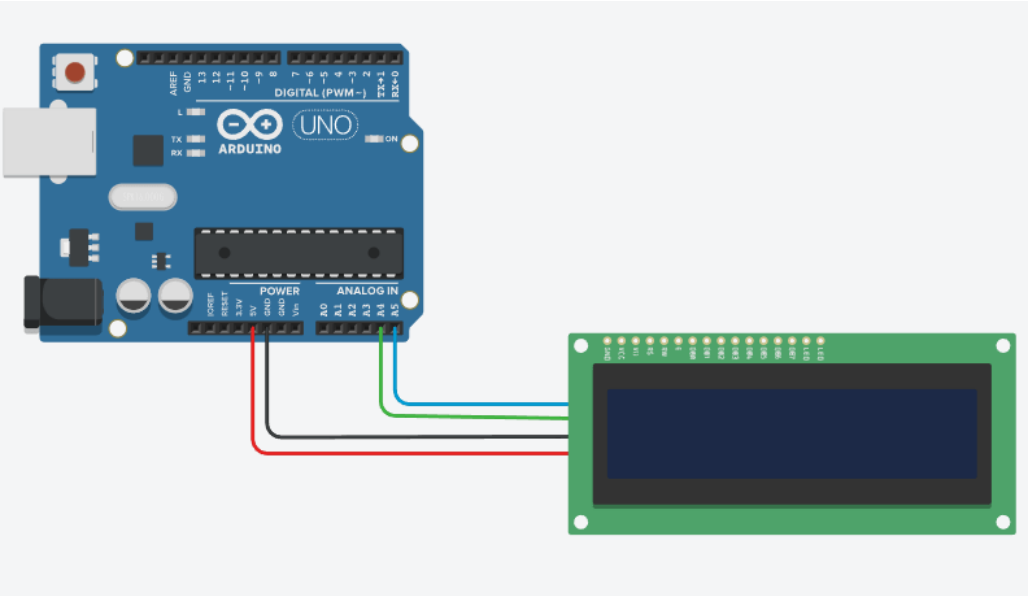

Рисунок 3.10 – Схема підключення LCD дисплея до мікроконтролера

Таблиця 3.1 – Підключення LCD дисплею до мікроконтролера Arduino

LCD	**Arduino**
GND	GND
VCC	5V
SDA	A4
SCL	A5

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

LiquidCrystal_I2C lcd(0x27,20,4);
void setup()
{
  lcd.begin();
  lcd.backlight();
}
void loop()
{
  lcd.setCursor(1, 0);
  lcd.print("RoboStore.com.ua 1");
  lcd.setCursor(1, 1);
  lcd.print("RoboStore.com.ua 2");
  lcd.setCursor(1, 2);
  lcd.print("RoboStore.com.ua 3");
  lcd.setCursor(1, 3);
  lcd.print("RoboStore.com.ua 4");
  delay(2000);
}
```

Рисунок 3.11 – Лістинг програми підключення дисплея

3.7 Створення коду в Arduino IDE та складання проєкту

Спочатку відкриваємо програму програму Arduino IDE (рисунок 3.12).

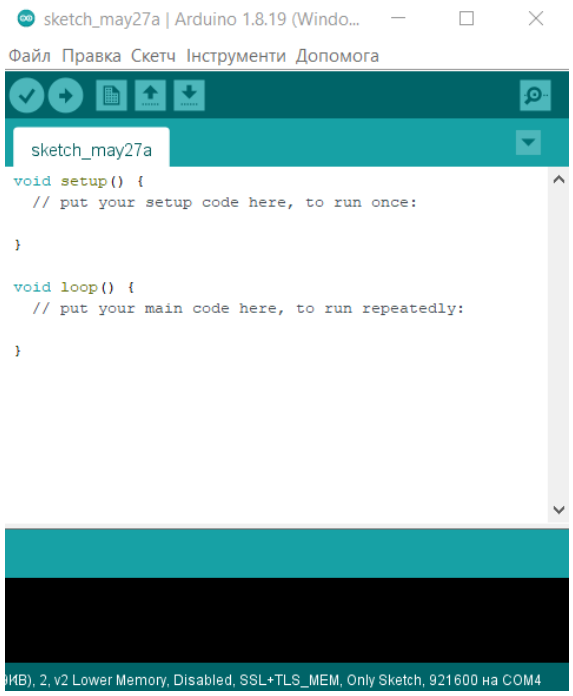

Рисунок 3.12 – Вікно відкриття програми

Далі потрібно додати на плату Arduino Uno через Інструменти \ Менеджер плат та вибрати Arduino AVR Boards (рисунок 3.13).

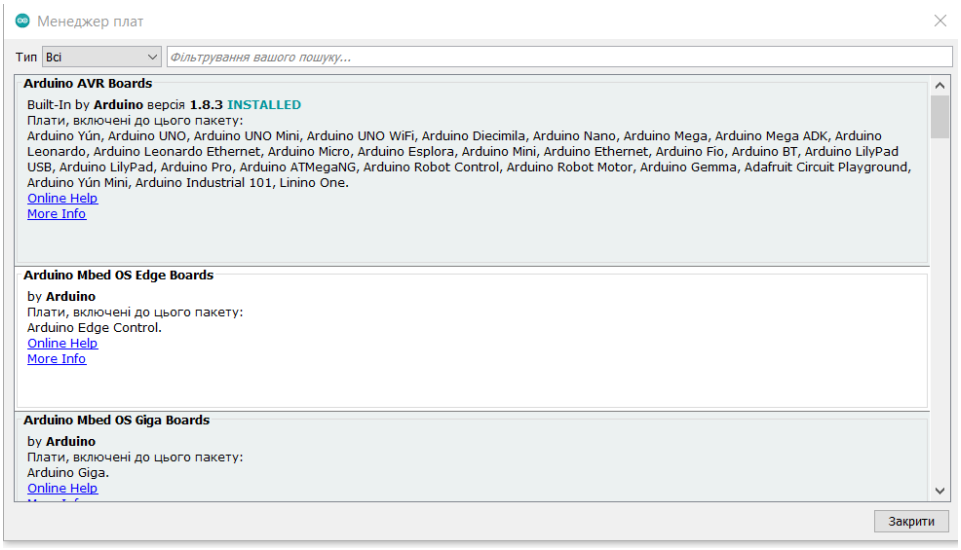

Рисунок 3.13 – Вікно Менеджер плат

Наступний крок – це вибір підключеної до персонального комп’ютера плати Arduino Uno, щоб не отримати помилку під час того, коли будемо завантажувати код. Це виконується через кнопки меню Інструменти\Плати\ Arduino AVR Boards\ Arduino Uno (рисунок 3.14).

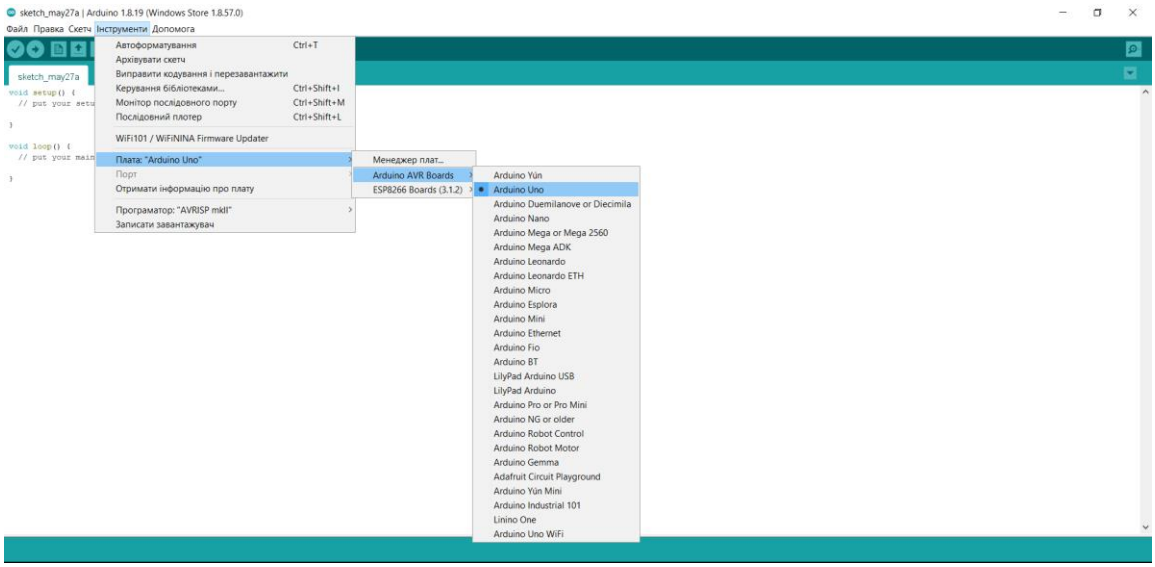

Рисунок 3.14 – Вибір плати Arduino Uno для програмування

Після вибору плати вибирається правильний COM-порт, його можна побачити після того, як встановлено драйвер. В нашому випадку це COM-порт 4 (рисунок 3.15).

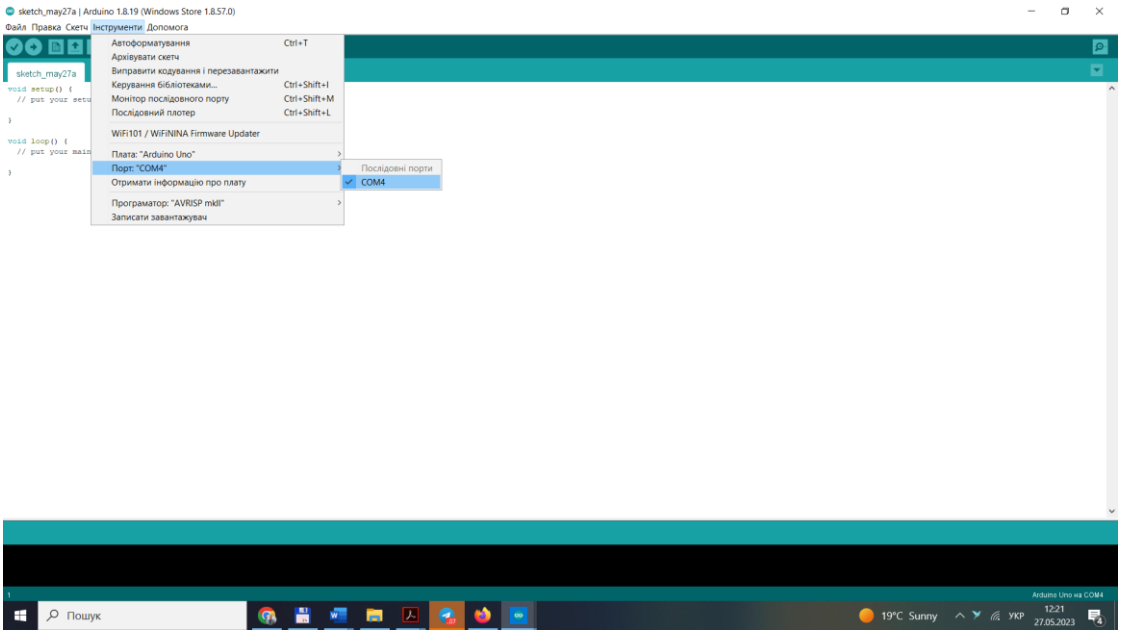

Рисунок 3.15 – Вибір COM-порта

Наступний крок – створювати програму: відкриваємо файл, щоб вибрати приклад, вибираємо Button з прикладу 02 Digital (рисунок 3.16).

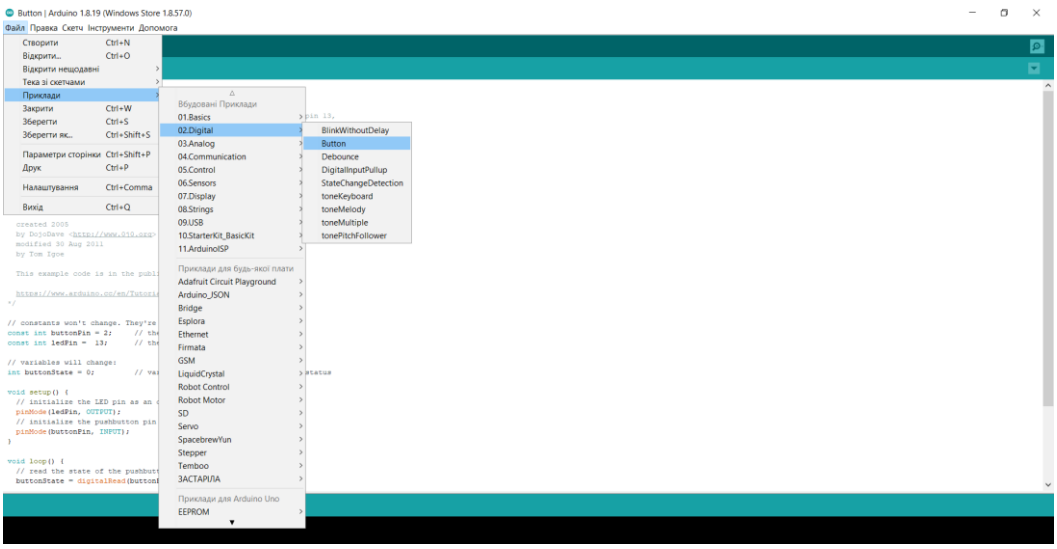

Рисунок 3.16 – Створення програми

Після встановлення плати на COM-порт, встановлюємо бібліотеки для модуля RC522 (рисунок 3.17).

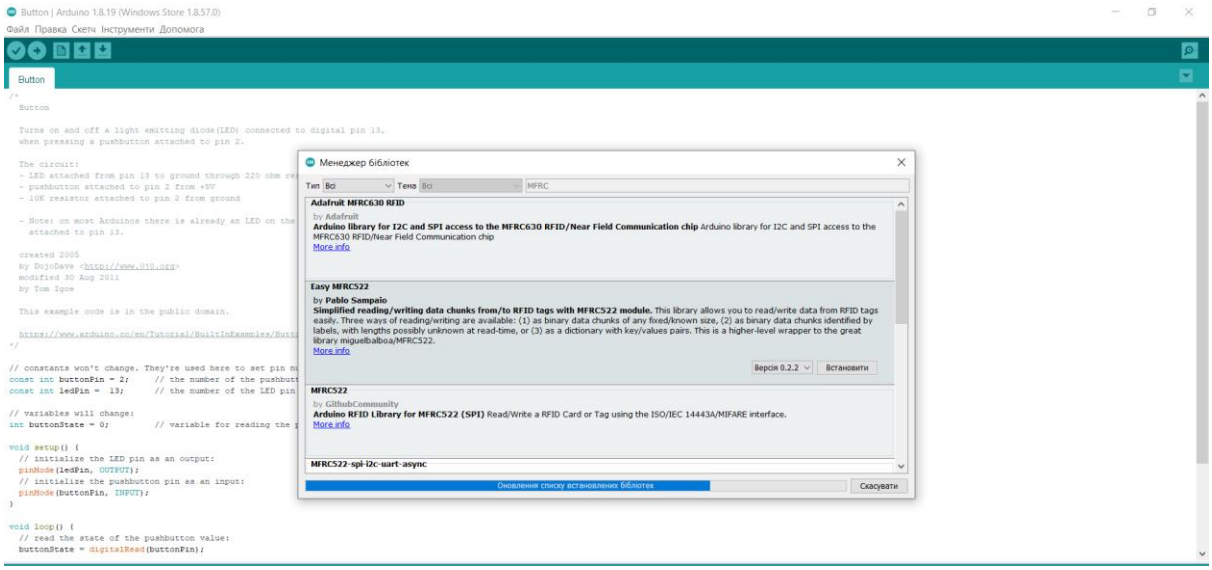

Рисунок 3.17 – Встановлення бібліотеки MFRC522

Наступний крок – найважчий: підключення всіх елементів до мікроконтролера та написання коду в Arduino IDE. Фото складеного проєкту та код програми предтавлено в додатках.

Перед заливтям коду на мікроконтролер потрібно зробити перевірку програми помилок натиснувши на «галочку» в лівому верхньому куті, щоб розпочати компіляцію програми (рисунок 3.18).

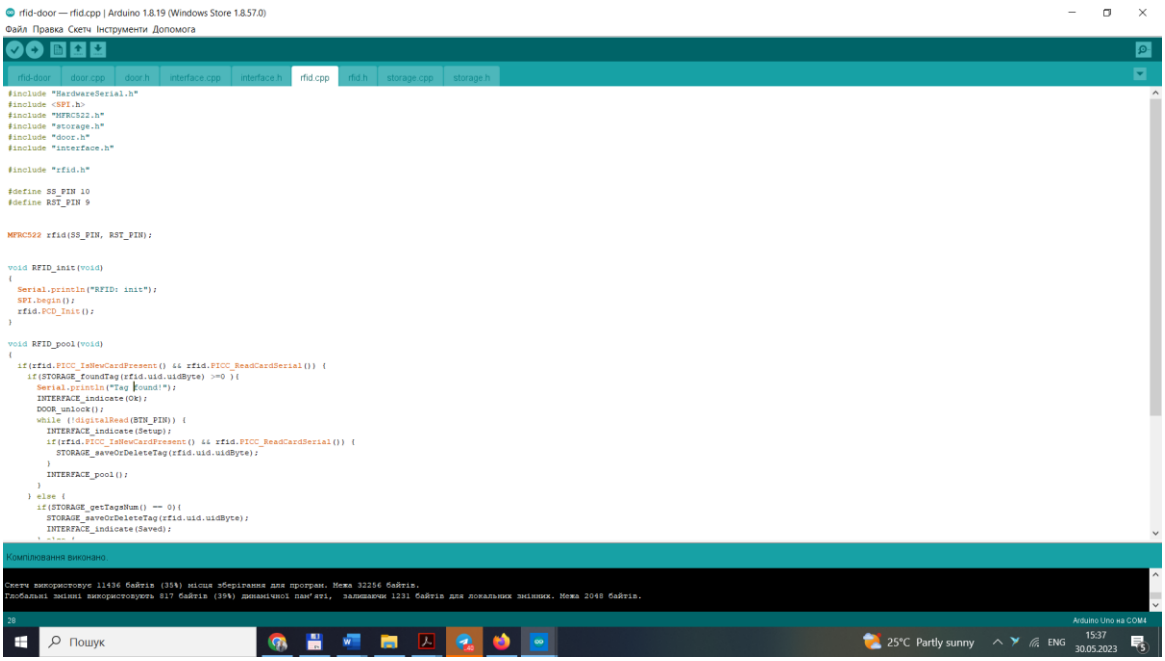

Рисунок 3.18 – Перевірка помилок

Далі можна завантажити програму на мікроконтролер та перевірити функціонування кожного з елементів та настроїти сервопривод, щоб не пошкодити конструкцію макету дверей. Код програми представлено в додатках А-В, фото розробленої системи доступу на базі мікроконтролера Arduino представлено в додатку Д.

ВИСНОВКИ

В кваліфікаційній роботі було створено системи доступу до дверей за допомогою мікроконтролера Arduino та технології RFID. У першому розділі було оглянуто існуючі інтелектуальні системи та визначено їх переваги та недоліки. У другому розділі описано тип та елементну базу, яку було вибрано для створення системи доступу. У третьому розділі було представлено опис підключення кожного елементу до мікроконтролера Arduino Uno та написано коу його прошивки.

Використання RFID-карти або брелка для відкривання дверей є зручним і швидким способом доступу. Замість фізичного ключа, користувач може просто піднести картку або брелок до зчитувача, що значно спрощує процес входу. RFID-системи можуть бути більш безпечними порівняно з традиційними фізичними ключами. RFID-карти можуть мати вбудовані механізми шифрування та захисту, що робить їх важкими для підробки або копіювання. Використання RFID дозволяє легко керувати правами доступу. Адміністратор може програмувати картки або брелки з відповідними дозволами, що дозволяє забезпечити доступ лише авторизованим особам. RFID-системи можуть вести журнал доступу, що дозволяє відстежувати, хто, коли і де здійснював доступ. Це може бути корисною функцією для безпеки, аудиту або відслідковування присутності. RFID-системи можуть бути легко інтегровані з іншими системами безпеки або управління, такими як системи відеоспостереження або системи контролю доступу. Це дозволяє створювати комплексні рішення для забезпечення безпеки та керування простором.

Враховуючи переваги використання RFID для відкривання дверей, вважаємо, що це може бути ефективним та зручним рішенням, особливо в комерційних або офісних приміщеннях, де потрібно керувати доступом до певних зон або приміщень. Однак, варто враховувати такі фактори, як ціна системи, потенційні ризики забезпечення безпеки, а також можливість втрати або крадіжки RFID-карти або брелка, і вживати необхідні заходи для їх управління та захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is an intelligent system? URL: https://www.techtarget.com/whatis/definition/intelligent-system (дата звернення 22.12.2022).

2. Інтелектуальна інформаційна_система. URL: https://uk.wikipedia.org/wiki/Інтелектуальна_інформаційна_система (Дата звернення 20.12.2022).

3. Martin Molina. What is an intelligent system? URL: https://www.researchgate.net/publication/344334868_What_is_an_intelligent_system? (дата звернення 29.12.2022).

4. Робототехнічна система автоматичного пошуку джерела світла. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Kitonv_2017_26_41 (дата звернення 29.12.2022).

5. Прикладні системи штучного інтелекту URL: https://posibniki.com.ua/catalog-prikladni-sistemi-shtuchnogo-intelektu (дата звернення 09.01.2023).

6. Системи контролю та управління доступом. Огляд. URL: https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review (дата звернення 15.01.2023).

7. А.О. Новацький. Мікропроцесорні та мікроконтролерні системи: Частина 2. Проектування мікропроцесорних систем: Лабораторний практикум: навч. посіб. для студ. Освітньої програми «Інтегровані інформаційні системи» спеціальності 126 «Інформаційні системи та технології» /; КПІ ім. Ігоря Сікорського. Електронні текстові дані (1 файл: 22,38 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2021. 268 с.

8. Інтелектуальні системи і технології. URL: https://www.nam.kiev.ua/files/publications/nester-kovt-fal-2-ostanna.pdf (дата звернення 18.01.2023).

9. Мітки RFID NFC – як їх використовувати? URL: https://www.0372.ua/news/3500218/mitki-rfid-nfc-ak-ih-vikoristovuvati (дата звернення 02.02.2023).

10. Що таке чип NFC і для чого він потрібен? URL: https://kt.tntu.edu.ua/shho-take-chyp-nfc-i-dlya-chogo-vin-potriben/ (дата звернення 10.02.2023).

11. У чому полягає різниця між RFID і NFC? URL: http://ua.rfidcardcube.com/news/what-is-the-difference-between-rfid-and-nfc-1142303 (дата звернення 22.02.2023).

12. Arduino: можливості «розумного будинку», датчик температури і вологості, складання проекту і створення системи керування житлом своїми руками. URL: https://investif.in.ua/423-what-is-an-arduino-smart-home (дата звернення 25.12.2022).

13. What is Arduino? URL: https://www.arduino.cc/en/Guide/Introduction (Дата звернення 05.12.2022).

14. Introduction to Microcontrollers. URL: https://www.arrow.com/en/research-and-events/articles/engineering-basics-what-is-a-microcontroller (дата звернення 29.03.2023).

15. Кнопка тактова. URL: https://electronica.in.ua/p1534467994-knopka-taktovaya-tact.html (Дата звернення 10.04.2023).

16. Модуль RGB світлодіода KY-016 для Arduino. URL: https://arduino.ua/prod2966-modyl-rgb-svetodioda-ky-016-dlya-arduino (дата звернення 12.04.2023).

17. Sg90 9g сервопривід. URL: https://myproject.com.ua/sg90-9g-servoprivid-ua.html?gclid=CjwKCAjwg-GjBhBnEiwAMUvNW9k6Ya25SGMcqz19Jtuj1rUUCnLpIxs6F5DAeUSVQPK1e_iHIvlG7BoC88IQAvD_BwE (дата звернення 15.04.2023).

18. Зумер активний, buzzer, 5В 2300Гц, Arduino. URL: https://zerus.shop/ua/p1461034169-zummer-aktivnyj-buzzer.html?source=merchant_center&gclid=CjwKCAjwg-GjBhBnEiwAMUvNW9dr2bl7b_OispsDDDxPiwdr KtsChzkPD12sCMst_8Z7ftUhNP2I4xoCqM4QAvD_BwE (дата звернення 19.04.2023).

19. RFID модуль RC522 з карткою доступу для Arduino. URL: https://arduino.ua/prod649-rfid-modyl-rc522-s-kartochkoi-dostypa-dlya-arduino (дата звернення 20.04.2023).

20. Символьний LCD. URL: https://uamper.com/index.php?route=product/product&path=180&product_id=1257&gclid=CjwKCAjwg-GjBhBnEiwAMUvNW1ZSdVsQRxemBkkiKpjmAeWD0sI4zbHR6NaM21jpAwPnXvtGMZAZoBoC1owQAvD_BwE (дата звернення 20.04.2023).

21. Підключення тактових кнопок до Arduino. URL: https://qazf.com.ua/buttons-arduino/ (дата звернення 11.04.2023).

22. Як підключити RGB світлодіод до Arduino. URL: https://poradumo.com.ua/154489-iak-pidkluchiti-rgb-svitlodiod-do-arduino/ (дата звернення 22.04.2023).

23. Підключення і керування сервоприводом з Arduino. URL: https://buyfast.in.ua/ua/a360358-podklyuchenie-upravlenie-servoprivodom.html (дата звернення 15.04.2023).

24. В.С. Баран, Г.Г. Власюк, Ю.О. Оникієнко, О.І. Смоленська. Основи мікропроцесорної техніки: лабораторний практикум: навч. посіб. для студ. спеціальності 171 «Електроніка» / КПІ ім. Ігоря Сікорського. Електронні текстові данні (1 файл: 3,42 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2019. 140 с.

25. Підключення LCD1602 дисплея по I2C до Arduino. URL: https://qazf.com.ua/arduino-i2c-lcd2004-lcd1602/ (дата звернення 30.04.2023).

ДОДАТКИ

Додаток А
Файл програми door.cpp

```
#include <Arduino.h>
#include <Servo.h>
#include "storage.h"
#include "door.h"

#define LOCK_TIMEOUT 2000
#define DOOR_LOCK     0
#define DOOR_UNLOCK    160
#define SERVO_PIN     A0

Servo doorServo;
static bool doorLocked = false;
static uint32_t lockTimeout;

void DOOR_lock(void)
{
  if(doorLocked) {
    return;
  }
  for(int i = doorServo.read(); i > DOOR_LOCK; i-=10) {
    doorServo.write(i);
    delay(15);
  }
  Serial.println("DOOR: lock");
  doorLocked = true;
}

void DOOR_unlock(void)
{
  if(!doorLocked) {
    return;
  }
  for(int i = doorServo.read(); i < DOOR_UNLOCK; i+=10) {
    doorServo.write(i);
    delay(15);
  }
  Serial.println("DOOR: unlock");
  lockTimeout = millis();
  doorLocked = false;
}

void DOOR_init(void)
{
  doorServo.attach(SERVO_PIN);
}

void DOOR_pool(void)
{
  if(STORAGE_getTagsNum() == 0){
    DOOR_unlock();
  } else if(!doorLocked && (millis() - lockTimeout) >= LOCK_TIMEOUT) {
    DOOR_lock();
  }
}
bool DOOR_getState(void)
{
  return doorLocked;
}
```

Додаток Б
Файл програми interface.cpp

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Arduino.h>

#include "door.h"
#include "storage.h"

#include "interface.h"

#define DISPLAY_TIMEOUT 2000
#define BUZZER_PIN      7


LiquidCrystal_I2C lcd(0x27,16,2);

static uint32_t displayTimeout = 1;

void INTERFACE_indicate(IndicateSignal_t signal)
{
  switch (signal) {
    case Error:
      lcd.clear();
      lcd.setCursor(4, 0);
      lcd.print("Rejected!");
      for (uint8_t i = 0; i < 2; i++) {
        tone(BUZZER_PIN, 100);
        delay(300);
        noTone(BUZZER_PIN);
        delay(100);
      }
      break;
    case Ok:
      lcd.clear();
      lcd.setCursor(4, 0);
      lcd.print("Welcome!");
      tone(BUZZER_PIN, 890);
      delay(330);
      noTone(BUZZER_PIN);
      break;
    case Saved:
      lcd.clear();
      lcd.setCursor(3, 1);
      lcd.print("Tag saved");
      for (uint8_t i = 0; i < 2; i++) {
        tone(BUZZER_PIN, 890);
        delay(330);
        noTone(BUZZER_PIN);
        delay(100);
      }
      break;
    case Deleted:
      lcd.clear();
      lcd.setCursor(2, 1);
      lcd.print("Tag deleted");
      for (uint8_t i = 0; i < 3; i++) {
        tone(BUZZER_PIN, 890);
        delay(330);
        noTone(BUZZER_PIN);
        delay(100);
      }
```

```
      break;
    case Setup:
      lcd.clear();
      lcd.setCursor(5, 0);
      lcd.print("Setup");
      break;

  }
  displayTimeout = millis();
}

void INTERFACE_pool(void)
{
  if (DOOR_getState() && !digitalRead(BTN_PIN)) {
    DOOR_unlock();
    INTERFACE_indicate(Ok);
  }
  if ((millis() - displayTimeout) >= DISPLAY_TIMEOUT && displayTimeout != 0) {
    lcd.clear();
    lcd.setCursor(1,1);
    if(STORAGE_getTagsNum() > 0) {
      lcd.print("Waiting tag...");
    } else {
      lcd.setCursor(1, 0);
      lcd.print("Attach new tag");
    }
    displayTimeout = 0;
  }
}

void INTERFACE_init(void)
{
  pinMode(BTN_PIN, INPUT_PULLUP);
  pinMode(BUZZER_PIN, OUTPUT);
  lcd.init();
  lcd.backlight();
  lcd.print(":)");
  tone(BUZZER_PIN, 658*2);
  delay(170);
  noTone(BUZZER_PIN);
  tone(BUZZER_PIN, 740*2);
  delay(170);
  noTone(BUZZER_PIN);
  tone(BUZZER_PIN, 784*2);
  delay(170);
  noTone(BUZZER_PIN);
  lcd.clear();
  uint32_t start = millis();
  while (!digitalRead(BTN_PIN)) {
    if (millis() - start >= 3000) {
      STORAGE_clear();
      break;
    }
  }
  if(STORAGE_getTagsNum() == 0) {
    INTERFACE_indicate(Deleted);
    lcd.setCursor(1, 0);
    lcd.print("Attach new tag");
  }
}
```

Додаток В
Файл програми rfid.ccp

```
#include "HardwareSerial.h"
#include <SPI.h>
#include "MFRC522.h"
#include "storage.h"
#include "door.h"
#include "interface.h"

#include "rfid.h"

#define SS_PIN 10
#define RST_PIN 9


MFRC522 rfid(SS_PIN, RST_PIN);


void RFID_init(void)
{
  Serial.println("RFID: init");
  SPI.begin();
  rfid.PCD_Init();
}

void RFID_pool(void)
{
  if(rfid.PICC_IsNewCardPresent() && rfid.PICC_ReadCardSerial()) {
    if(STORAGE_foundTag(rfid.uid.uidByte) >=0 ){
      Serial.println("Tag found!");
      INTERFACE_indicate(Ok);
      DOOR_unlock();
      while (!digitalRead(BTN_PIN)) {
        INTERFACE_indicate(Setup);
        if(rfid.PICC_IsNewCardPresent() && rfid.PICC_ReadCardSerial()) {
          STORAGE_saveOrDeleteTag(rfid.uid.uidByte);
        }
        INTERFACE_pool();
      }
    } else {
      if(STORAGE_getTagsNum() == 0){
        STORAGE_saveOrDeleteTag(rfid.uid.uidByte);
        INTERFACE_indicate(Saved);
      } else {
        Serial.println("Unknown tag!");
        INTERFACE_indicate(Error);
      }
    }
  }
  static uint32_t rfidRebootTimer = millis();
  if (millis() - rfidRebootTimer > 500) {
    rfidRebootTimer = millis();
    digitalWrite(RST_PIN, HIGH);
    delay(10);
    digitalWrite(RST_PIN, LOW);
    rfid.PCD_Init();
  }
}
```

Додаток Д

Фото розробленої системи доступу на базі мікроконтролера Arduino