Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino
Назва теми

Рівень вищої освіти *перший (бакалаврський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 2301105.23.37.08 ПЗ

Виконав здобувач III курсу, група КІ2с-23-1 _____ Костянтин ДУМАНСЬКИЙ
Підпис Ініціали, прізвище

Керівник _____ Ольга ПАВЛОВА
Науковий ступінь, учене звання Підпис Ініціали, прізвище

Нормоконтролер _____ Сергій ЛИСЕНКО
Науковий ступінь, учене звання Підпис Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС _____ Ольга ПАВЛОВА
«10» червня 2026 р. підпис Ініціали, прізвище
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Рівень вищої освіти перший (бакалаврський)

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
_____ Ольга ПАВЛОВА

" 12 " 02 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Думанському Костянтину Володимировичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino
Керівник проекту (роботи) Павлова Ольга Олександрівна, д.т.н., проф.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 12.02.2026 р. №
2. Термін подання здобувачем роботи на кафедру 01.06.2026 р.
3. Вихідні дані до роботи Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino та постановка задачі щодо її удосконалення
Проєктування системи обробки інформації у кіберфізичній системі контролю доступу до приміщення
Програмно-апаратна реалізація кіберфізичної системи контролю доступу до приміщення з використанням RFID-технологій та Arduino
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Апаратне забезпечення проєкту
Архітектура ПЗ для кіберфізичної системи
Розроблений фізичний прототип кіберфізичної системи

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання пр

7. Дата видачі завдання «_12_»_____02_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Пр
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2026	вик
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2026	вик
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2026	вик
4	Робота над розділом 2 – вибір компонентів для проєктування кіберфізичної системи контролю доступу до приміщення	01.04.2026	вик
5	Робота над розділом 3 – проєктування кіберфізичної системи контролю доступу до приміщення	29.04.2026	вик
6	Оформлення пояснювальної записки згідно вимог	25.05.2026	вик
7	Попередній захист ВКР	26.05.2026	вик
8	Захист ВКР на засіданні ЕК	Червень 2026 року	

Здобувач_____ Костянтин ДУМАНСЬКИЙ
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи_____ Ольга ПАВЛОВА
Підпис Ім'я, ПРІЗВИЩЕ

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 2301105.23.37.08	Пояснювальна записка	55		
			Графічні матеріали			
2		КвРКІ 2301105.23.37.08	Апаратне забезпечення проєкту	1		
3		КвРКІ 2301105.23.37.08	Архітектура ПЗ для кіберфізичної системи	1		
4		КвРКІ 2301105.23.37.08	Розроблений фізичний прототип кіберфізичної системи	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 190186.19.01.08 ВП		
Розробив		Думанський			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Павлова				У	1	1
Н. контр.		Лисенко				ХНУ, КІ2с-23-1		
Затв.		Павлова						

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino».

Автор роботи: Костянтин ДУМАНСЬКИЙ.

Керівник роботи: Ольга ПАВЛОВА.

Пояснювальна записка: 55 с., 15 рис., 10 табл., 3 дод., 40 джерел.

Графічна частина: 3 креслення.

АРХІТЕКТУРА, БАЗА ДАНИХ, RFID, ARDUINO, КІБЕРФІЗИЧНА СИСТЕМА, КОНТРОЛЬ ДОСТУПУ.

Кваліфікаційна робота бакалавра присвячена розробці та дослідженню кіберфізичної системи контролю доступу до приміщення з використанням RFID-технологій та мікроконтролерної платформи Arduino. Актуальність теми зумовлена зростанням потреб у забезпеченні безпеки об'єктів, контролю доступу персоналу, а також автоматизації процесів ідентифікації та обліку відвідувачів у різних сферах діяльності. Використання RFID-технологій дає змогу забезпечити швидку, безконтактну та надійну ідентифікацію користувачів, зменшити ризики несанкціонованого доступу та підвищити рівень захищеності приміщень.

Метою роботи є проєктування, реалізація та тестування апаратно-програмного комплексу контролю доступу, що забезпечує зчитування RFID-міток, оброблення даних, керування виконавчими механізмами (замками, сигналізацією) та ведення бази даних користувачів. Для досягнення поставленої мети було проведено аналіз сучасних підходів до побудови систем контролю доступу, обрано апаратну платформу Arduino та RFID-модулі, розроблено структурну та функціональну схеми системи, створено програмне забезпечення мікроконтролера, а також реалізовано адміністрування доступу і моніторинг подій.

_____

Підпис здобувача

30.05.2026

Дата

ЗМІСТ

1 КІБЕРФІЗИЧНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ З ВИКОРИСТАННЯМ RFID-ТЕХНОЛОГІЙ ТА ПОСТАНОВКА ЗАДАЧІ ЩОДО ЇЇ УДОСКОНАЛЕННЯ

1.1 Аналіз структурних і функціональних особливостей кіберфізичної системи контролю доступу на базі RFID і Arduino

Кіберфізична система (КС) — це інформаційно-технологічна концепція, яка передбачає інтеграцію обчислювальних і фізичних компонентів у єдине середовище, що забезпечує взаємодію між ними в режимі реального часу. У таких системах обчислювальні ресурси тісно пов'язані з фізичними об'єктами, гарантуючи збір, оброблення та передачу даних, а також керування виконавчими механізмами.

У кіберфізичних системах контролю доступу обчислювальна складова інтегрується з апаратними компонентами, такими як RFID-зчитувачі, мікроконтролери, електронні замки та інші пристрої, що фізично обмежують доступ до приміщень. Така система функціонує як єдиний комплекс, де всі елементи взаємодіють між собою для виконання завдань ідентифікації користувачів, перевірки прав доступу та керування виконавчими пристроями.

Термін «кіберфізичні системи» набув широкого використання в контексті концепції Індустрії 4.0, яка передбачає автоматизацію процесів, інтеграцію інформаційних технологій і фізичних систем, а також впровадження інтелектуальних рішень у різних сферах діяльності. Одним із перспективних напрямів застосування КС є системи безпеки та контролю доступу.

Сучасні системи контролю доступу класифікуються залежно від способів ідентифікації користувачів, серед яких можна виділити картки доступу, біометричні методи, PIN-коди та RFID-технології. Найбільшого поширення набули RFID-системи завдяки їх високій швидкодії, надійності, безконтактності та зручності використання.

RFID-система контролю доступу включає такі основні компоненти: RFID-мітки (карти або брелоки), RFID-зчитувач, мікроконтролер (зокрема платформа Arduino), база даних користувачів і виконавчі пристрої (електромагнітні замки, реле тощо). При піднесенні RFID-мітки до зчитувача відбувається її ідентифікація, після чого мікроконтролер обробляє отриману інформацію та приймає рішення щодо надання або заборони доступу.

Під час розроблення систем контролю доступу важливо враховувати стабільність зчитування RFID-міток, оперативність перевірки отриманого UID, захист збережених ідентифікаторів та можливість збільшення кількості користувачів. Платформа Arduino є зручною для реалізації такого прототипу, тому що підтримує підключення RFID-зчитувача, виконавчих механізмів і додаткових сенсорів, та дає можливість змінювати логіку роботи системи без ускладнення апаратної частини. Це робить Arduino придатною основою для побудови програмно-апаратної системи контролю доступу.

Найпростіший набір компонентів є таким:

1) мікроконтролер (платформа Arduino);
2) RFID-зчитувач;
3) RFID-мітки (карти або брелоки);
4) модуль зв'язку або інтерфейс передавання даних;
5) блок живлення;
6) пам'ять (для збереження ідентифікаторів користувачів);
7) виконавчий пристрій (електромагнітний замок, реле);
8) приймач/передавач сигналу (за необхідності для віддаленого керування).

Збір інформації для мікроконтролера та користувача здійснюється за допомогою RFID-зчитувача та додаткових сенсорів (наприклад, датчиків відкриття дверей, руху тощо). Використовуються різні методи ідентифікації та передачі даних, зокрема радіочастотні (RFID), дротові та бездротові технології.

Зазвичай система контролю доступу з використанням RFID складається з таких основних елементів:

1. RFID-мітка (картка або брелок користувача).
2. RFID-зчитувач.
3. Мікроконтролер Arduino.
4. Виконавчий механізм (електромагнітний замок або сервопривід).
5. Джерело живлення.
6. Корпус або конструктивна основа системи.

При аналізі структурних особливостей кіберфізичної системи контролю доступу бажано розглядати її не як набір окремих пристроїв, а як багаторівневу систему. На нижньому рівні розташовані фізичні компоненти: RFID-мітка, зчитувач, датчик відстані, сервопривід, світлодіодна та звукова індикація. На середньому рівні знаходиться мікроконтролер Arduino, який виконує функції збору даних, їх попередньої обробки та формування керуючих сигналів. На верхньому рівні розміщується інформаційна логіка системи, що включає базу ідентифікаторів, правила надання доступу, алгоритми переходу між станами та журналювання подій.

У системах контролю доступу на ряду з фактом успішного зчитування RFID-мітки важливим є і правильна інтерпретація отриманого ідентифікатора. Один і той самий апаратний сигнал може мати різне значення залежно від поточного стану системи. Наприклад, у стані очікування піднесення master-картки може переводити систему у режим реєстрації, тоді як у стані реєстрації піднесення нової картки призводить до її додавання у пам'ять. Саме тому для опису логіки роботи будемо використовувати модель скінченного автомата станів.

До основних станів розроблюваної системи можна віднести стан очікування, стан відкритого доступу та стан реєстрації. У стані очікування система не виконує активних дій щодо зміни положення механізму, а лише періодично перевіряє наявність картки біля RFID-зчитувача. У стані відкритого

доступу сервопривід переводиться у положення, яке дозволяє відкрити двері, а система контролює фізичний стан дверного полотна за допомогою ультразвукового датчика. У стані реєстрації система очікує нову RFID-мітку та після перевірки умов додає її ідентифікатор до EEPROM-сховища.

Важливою функціональною особливістю є наявність master-картки. Вона виконує службову роль і використовується для керування процедурою додавання нових користувачів. Цей метод спрощує адміністрування системи без необхідності використання додаткового комп'ютера або зовнішнього інтерфейсу. Разом з тим він потребує підвищеної уваги до захисту master-картки, оскільки її втрата або несанкціоноване використання може призвести до неконтрольованого додавання нових ідентифікаторів.

Для стабільності роботи системи разом з логічним станом замка також необхідно розглядати фактичний стан дверей. Наприклад, система може видати команду на закриття механізму, але двері фізично залишаться відчиненими. У такому випадку відсутність датчика стану не дозволить виявити невідповідність. Використання ультразвукового датчика відстані дає змогу контролювати положення дверей незалежно від логічного стану сервоприводу та створює умови для виявлення помилкових або несанкціонованих ситуацій.

Система контролю доступу повинна відповідати ряду вимог (табл. 1.1). До функціональних вимог належать зчитування RFID-міток, перевірка ідентифікаторів, відкриття механізму, реєстрація нових міток, індикація станів і контроль положення дверей. До нефункціональних вимог належать швидкодія, стабільність роботи, простота використання, збереження даних після вимкнення живлення, можливість обслуговування та розширення. Виконання цих вимог дозволить системі бути безпечно використаною в реальних умовах.

Таблиця 1.1 – Вимоги до кіберфізичної системи контрлю доступу

Група вимог	Зміст вимоги	Призначення
Ідентифікація	Зчитування UID RFID-мітки	Визначення користувача

Кінець таблиці 1.1

Авторизація	Перевірка UID у пам'яті системи	Надання або заборона доступу
Керування	Формування PWM-сигналу для сервоприводу	Фізичне відкриття або блокування
Контроль стану	Вимір відстані до дверей	Визначення фактичного положення дверей
Індикація	Використання LED та buzzer	Повідомлення користувача про результат
Збереження даних	Використання EEPROM	Збереження карток після вимкнення живлення
Адміністрування	Наявність master-картки	Додавання нових користувачів
Масштабування	Модульна структура	Можливість додавання нових компонентів

Основними функціями системи контролю доступу слід вважати: ідентифікацію користувачів; керування доступом до приміщень; реєстрацію подій доступу; підвищення рівня безпеки; моніторинг і адміністрування системи (табл. 1.2).

Таблиця 1.2 – Функції та завдання системи контролю доступу

1.	Ідентифікація користувачів	– зчитування RFID-міток; – визначення унікального ідентифікатора користувача; – перевірка даних у базі користувачів; – виключення несанкціонованого доступу

Кінець таблиці 1.2

2.	Керування доступом	– надання або заборона доступу до приміщення; – керування електромагнітним замком; – реалізація різних рівнів доступу для користувачів
3.	Адміністрування системи	– додавання та видалення користувачів; – оновлення бази даних RFID-міток; – налаштування параметрів доступу
4.	Підвищення безпеки	– запобігання несанкціонованому проникненню; – інтеграція з сигналізацією; – автоматичне блокування доступу у разі загрози
5.	Інтеграція з іншими системами	– взаємодія з системами відеоспостереження; – передавання даних у центральну базу або хмару; – розширення функціоналу системи
6.	Повідомлення та сповіщення	– інформування користувачів про стан доступу; – передавання повідомлень адміністратору; – сигналізація про спроби несанкціонованого доступу
7.	Автоматизація доступу	– реалізація сценаріїв доступу (наприклад, за розкладом); – обмеження доступу за часом або ролями; – автоматичне відкриття/закриття доступу.
8.	Масштабування системи	– розширення кількості користувачів; – підключення додаткових пристроїв; – адаптація до різних типів об'єктів.

1.1.1 Класифікація сучасних систем контролю доступу

Системи контролю доступу є важливим елементом комплексних систем безпеки та використовуються для обмеження доступу осіб до визначених приміщень, територій або інформаційних ресурсів. Основним призначенням таких систем є ідентифікація користувача, перевірка його прав доступу та прийняття рішення щодо надання або заборони доступу до об'єкта.

Залежно від принципу функціонування системи контролю доступу можуть бути автономними та мережевими. Автономні системи функціонують незалежно від зовнішніх інформаційних ресурсів і приймають рішення безпосередньо на локальному контролері. Такі системи характеризуються простотою реалізації, низькою вартістю та високою надійністю. Водночас вони мають обмежені можливості адміністрування та централізованого контролю.

Мережеві системи контролю доступу передбачають підключення контролерів до центрального сервера або бази даних. Це робить можливим централізовано керувати правами користувачів, вести журнали подій, здійснювати моніторинг стану обладнання та інтегрувати систему з іншими підсистемами безпеки. Серед обмежень мережевих рішень можна виділити складність реалізації та підвищені вимоги до мережевої інфраструктури.

За способом ідентифікації користувачів системи контролю доступу можна поділити на декілька основних груп:

- системи на основі механічних ключів;
- системи на основі PIN-кодів;
- системи на основі RFID-технологій;
- біометричні системи;
- комбіновані системи.

Системи з використанням механічних ключів є найпростішими та найдешевшими рішеннями. Проте вони не дозволяють вести облік відвідувань,

оперативно змінювати права доступу або контролювати використання ключів різними користувачами.

Системи на основі PIN-кодів використовують введення секретної числової комбінації через клавіатуру. Їхньою перевагою є відсутність необхідності носити фізичний ідентифікатор. Недоліком є можливість підглядання або передачі коду іншим особам.

Біометричні системи використовують фізичні характеристики людини для ідентифікації користувача. Найчастіше застосовуються відбитки пальців, розпізнавання обличчя, райдужної оболонки ока або голосу. Такі системи гарантують високий рівень захисту, але мають значно вищу вартість, і їх складніше реалізувати.

Окрему групу складають RFID-системи контролю доступу, які використовують радіочастотну ідентифікацію користувачів. Вони швидше зчитують інформацію, є дуже зручними для використання та легко інтегруються з цифровими системами керування.

Для порівняння різних способів ідентифікації наведено таблицю 1.3.

Таблиця 1.3 – Порівняльна характеристика способів ідентифікації користувачів

Спосіб ідентифікації	Вартість	Рівень безпеки	Простота використання
Механічний ключ	Низька	Низький	Висока
PIN-код	Низька	Середній	Середня
RFID	Середня	Середній-високий	Висока
Біометрія	Висока	Високий	Висока

В результаті цей розділ показує, що RFID-технології є оптимальним рішенням, враховуючи вартість реалізації, швидкодію, надійність та зручність

використання. Саме тому сьогодні вони широко застосовуються у системах контролю доступу різного призначення.

1.1.2 Аналіз RFID-технологій та стандартів ідентифікації

RFID (Radio Frequency Identification) — це технологія автоматичної ідентифікації об'єктів за допомогою радіохвиль. Основною перевагою RFID є можливість безконтактного зчитування інформації без необхідності прямої видимості між зчитувачем і міткою.

Типова RFID-система складається з трьох основних компонентів: RFID-мітки, RFID-зчитувача та пристрою обробки інформації. RFID-мітка містить унікальний ідентифікатор, який передається зчитувачу за допомогою електромагнітного поля. Отримана інформація передається до мікроконтролера або комп'ютерної системи для подальшої обробки.

Залежно від способу живлення RFID-мітки поділяються на пасивні, активні та напівактивні.

Пасивні RFID-мітки не мають власного джерела живлення та отримують енергію від електромагнітного поля зчитувача. Такі мітки характеризуються невеликою вартістю, компактними розмірами та тривалим терміном експлуатації.

Активні RFID-мітки містять власне джерело живлення, що дає змогу збільшити дальність зчитування та обсяг збережених даних. Недоліками активних міток є вища вартість та необхідність періодичної заміни елементів живлення.

Напівактивні RFID-мітки поєднують характеристики пасивних та активних рішень. Вони мають власне живлення для роботи внутрішньої електроніки, але використовують енергію зчитувача для передачі даних.

За робочою частотою RFID-системи поділяються на декілька категорій:

– LF (Low Frequency) – 125–134 кГц;

- HF (High Frequency) – 13,56 МГц;
- UHF (Ultra High Frequency) – 860–960 МГц;
- Microwave RFID – понад 2,4 ГГц.

У даній роботі використовується RFID-модуль RC522, який працює на частоті 13,56 МГц та належить до категорії HF-систем. Цей модуль може надійно зчитувати дані на відстані до декількох сантиметрів та широко застосовується у системах контролю доступу, електронних перепустках і транспортних картках.

Важливим в RFID-технологій є стандартизація процесів ідентифікації. Найбільш поширеними міжнародними стандартами є серія ISO/IEC 18000 та стандарт ISO/IEC 14443, що використовується для безконтактних смарт-карт і RFID-пристроїв малого радіуса дії.

Стандартизація необхідна для сумісності обладнання різних виробників, та уніфікує процедури обміну даними між RFID-мітками та зчитувачами. Це особливо важливо при побудові масштабованих систем контролю доступу та інтеграції обладнання в єдину інформаційну інфраструктуру.

Однією з переваг RFID-технологій є висока швидкість зчитування. У більшості випадків процес ідентифікації займає менше однієї секунди. Також RFID-системи можуть працювати без фізичного контакту між міткою та зчитувачем, що покращує зручність використання порівняно з магнітними картками або механічними ключами.

Водночас RFID-технології мають певні обмеження. До них належать можливість дублювання простих RFID-міток, вплив електромагнітних завад та залежність дальності зчитування від умов експлуатації. Для підвищення рівня захисту сучасні RFID-системи використовують криптографічні алгоритми, взаємну автентифікацію пристроїв та захищені канали обміну даними.

Для навчального прототипу, який розробляється у даній роботі, використання RFID-модуля RC522 є оптимальним рішенням завдяки його доступності, простоті підключення до Arduino та наявності великої кількості готових програмних бібліотек.

В результаті аналізу визначено, що RFID-технології є ефективними для автоматичної ідентифікації користувачів, та що вони широко використовуються у подібних програмно-апаратних комплексах. Їх застосування дає можливість реалізувати швидку, надійну та зручну систему авторизації користувачів із можливістю подальшого розширення функціональних можливостей.

1.2 Аналіз програмно-апаратного забезпечення обробки інформації в кіберфізичній системі контролю доступу з використанням RFID та Arduino

Кількість наукових досліджень, присвячених універсальним архітектурам програмного забезпечення для систем контролю доступу, є обмеженою, оскільки більшість робіт зосереджені на вирішенні окремих прикладних задач, таких як ідентифікація користувачів або керування виконавчими пристроями. Водночас існує значна кількість практичних інструкцій і рекомендацій щодо розробки подібних систем, які, хоча й не мають повноцінного наукового обґрунтування, можуть бути корисними при реалізації конкретних рішень.

У контексті побудови кіберфізичної системи контролю доступу частина таких підходів може бути використана, експериментально перевірена та інтегрована в загальну архітектуру системи після підтвердження їх ефективності. Проте більшість із них орієнтована на вузькі задачі (зчитування RFID-міток, керування замками, ведення журналів подій), що не дозволяє використовувати їх як універсальний метод побудови програмного забезпечення.

Програмно-апаратне забезпечення системи контролю доступу на базі Arduino та RFID складається з декількох взаємопов'язаних рівнів: апаратного (мікроконтролер, RFID-зчитувач, виконавчі механізми), програмного (прошивка мікроконтролера) та прикладного (інтерфейс користувача і база даних). Обробка інформації включає етапи зчитування ідентифікатора RFID-мітки, перевірку його у базі даних, прийняття рішення щодо доступу та передачу керуючого сигналу на виконавчий пристрій.

Для вибору засобів ідентифікації порівняємо декілька найбільш поширених підходів: механічний ключ, PIN-код, RFID-ідентифікацію та біометричні методи. Механічний ключ є найпростішим рішенням, однак не має журналювання подій і не дає змоги швидко змінити права доступу без фізичної заміни замка або ключів. PIN-код простіший для адміністрування, але може бути переданий іншій особі або підглянутий. Біометричні методи мають високий рівень персоналізації, однак є складнішими та дорожчими у реалізації, а також потребують додаткового врахування питань конфіденційності.

RFID-ідентифікація знаходиться посередині між простотою та функціональністю. Вона не потребує фізичного контакту, дає змогу швидко виконати перевірку користувача та легко реалізується у мікроконтролерних системах. Для навчального або експериментального прототипу RFID є доцільним вибором, оскільки поєднує доступність компонентів, оперативність та простоту програмної реалізації, а також тому що це є темою цієї роботи.

Таблиця 1.4 – Порівняння методів ідентифікації користувачів

Метод	Переваги	Недоліки	Доцільність для прототипу
Механічний ключ	Простота, автономність	Відсутність журналу подій, складне адміністрування	Низька
PIN-код	Не потрібен фізичний носій	Можливість передачі коду іншій особі	Середня
RFID	Швидкість, безконтактність, простота інтеграції	Потреба у захисті карток і master-картки	Висока

Кінець таблиці 1.4

Біометрія	Персоналізована ідентифікація	Вища вартість і складність	Середня або низька для навчального прототипу

З погляду програмної архітектури система контролю доступу повинна дозволяти послідовне виконання декількох операцій: очікування події, отримання даних, перевірка коректності, прийняття рішення, виконання дії та повернення у початковий стан. Ці операції є зручними для реалізації на Arduino, бо основна функція loop виконується безперервно, а отже система може постійно реагувати на нові події.

Додатково слід врахувати обробку помилкових ситуацій. До них можна віднести піднесення невідомої картки, повторне сканування вже зареєстрованої картки, спробу реєстрації при заповненому сховищі, відсутність відповіді від RFID-зчитувача, некоректне значення датчика відстані або механічне невідповідне положення дверей. Для кожної з таких ситуацій система повинна мати передбачувану реакцію: відмову в доступі, звукове попередження, світлову індикацію, повернення в стан очікування або службове повідомлення у Serial Monitor.

У контексті безпеки важливо враховувати, що проста RFID-система не повинна розглядатися, як повноцінна промислова система захисту високого рівня. Вона є навчальним і функціональним прототипом, який демонструє принципи кіберфізичної взаємодії, автоматизації доступу та обробки ідентифікаторів. Для реального впровадження у критичних об'єктах необхідно додатково передбачити криптографічний захист, захищений обмін даними, контроль спроб підбору, резервне живлення, антивандальний корпус і централізоване адміністрування.

Особлива увага при розробці таких систем приділяється надійності зчитування даних, швидкодії оброблення інформації, захищеності бази даних користувачів, а також безперервності роботи системи. Важливими є також можливості масштабування та інтеграції з іншими інформаційними системами безпеки.

1.3 Висновки до першого розділу

У першому розділі було розглянуто, з яких частин складається кіберфізична система контролю доступу, і яку роль виконує кожен її елемент. Основну увагу приділено взаємодії між RFID-міткою, зчитувачем, мікроконтролером, пам'яттю для збереження ідентифікаторів та виконавчим механізмом, який відповідає за фізичне відкриття або блокування доступу до приміщення.

Також було розглянуто основні типи систем контролю доступу та способи ідентифікації користувачів. Порівняння механічних ключів, PIN-кодів, RFID-міток і біометричних методів показало, що для навчального прототипу RFID є найбільш зручним варіантом. Такий спосіб ідентифікації не потребує фізичного контакту зі зчитувачем, не вимагає введення пароля та може бути реалізований на мікроконтролері Arduino без складної апаратної частини.

Окремо проаналізовано принцип роботи RFID-технологій, типи RFID-міток і стандарти, які використовуються для безконтактної ідентифікації. У межах цієї роботи важливим є те, що RFID-зчитувач дає змогу отримати UID картки, а мікроконтролер може порівняти цей ідентифікатор із даними, збереженими в пам'яті системи. Саме на цій логіці будується подальший алгоритм перевірки користувача та прийняття рішення про надання або заборону доступу.

Платформа Arduino була обрана як основа для прототипу через просте підключення периферійних модулів і наявність готових бібліотек для роботи з

RFID-зчитувачем, EEPROM-пам'яттю, сервоприводом та іншими компонентами. Її можливостей достатньо для реалізації базових функцій системи: зчитування UID, перевірки картки, збереження ідентифікаторів, керування виконавчим механізмом та виведення службових повідомлень.

У результаті аналізу було визначено функціональні вимоги до розроблюваної системи, зокрема зчитування RFID-міток, перевірку прав доступу, роботу з master-карткою, збереження даних після вимкнення живлення, індикацію станів і контроль фізичного положення дверей. Отримані результати стали основою для подальшого проєктування апаратної частини, інформаційної моделі та алгоритмів роботи системи контролю доступу.

2 ПРОЄКТУВАННЯ СИСТЕМИ ОБРОБКИ ІНФОРМАЦІЇ У КІБЕРФІЗИЧНІЙ СИСТЕМІ КОНТРОЛЮ ДОСТУПУ З ВИКОРИСТАННЯМ RFID ТА ARDUINO

2.1 Визначення апаратних і програмних підсистем програмно-технічного засобу

Аналіз, проведений у попередньому розділі, дає змогу визначити основні апаратні та програмні підсистеми програмно-технічного засобу кіберфізичної системи контролю доступу (рис. 2.1). До складу системи входять такі підсистеми:

– програмне забезпечення мікроконтролерної платформи Arduino;

– апаратні підсистеми: ідентифікації на основі RFID-технологій, виміру відстані, механічного контролю дверей.

– програмно-інформаційна підсистема керування та адміністрування доступу.

Програмне забезпечення мікроконтролера Arduino відповідає за зчитування ідентифікаторів RFID-міток і відстані до дверей, попередню обробку даних, логічну перевірку прав доступу та формування керуючих сигналів для виконавчих пристроїв. Воно реалізується у вигляді прошивки, що функціонує в реальному часі та взаємодіє з апаратними компонентами системи.

Апаратна підсистема RFID-ідентифікації включає RFID-зчитувач, RFID-мітки користувачів та інтерфейси обміну даними з мікроконтролером. Основним її завданням є безконтактна ідентифікація користувачів та передавання унікального коду мітки до обчислювального модуля системи.

Апаратна підсистема виміру відстані включає ультразвуковий датчик відстані та інтерфейси обміну даними з мікроконтролером. Її завданням є визначення відстані до дверей та передача цієї відстані до системи. На основі цих даних визначається, чи відкриті двері фізично, чи ні.

Апаратна підсистема механічного контролю дверей включає сервопривод та інтерфейси для запису даних з мікроконтролера. Ця система відповідальна безпосередньо за контроль доступу до приміщення.

Програмно-інформаційна підсистема керування зберігає дані користувачів, веде облік подій, адмініструє систему та візуалізує інформацію. Вона може бути реалізована у вигляді локальної або віддаленої бази даних із відповідним інтерфейсом користувача.

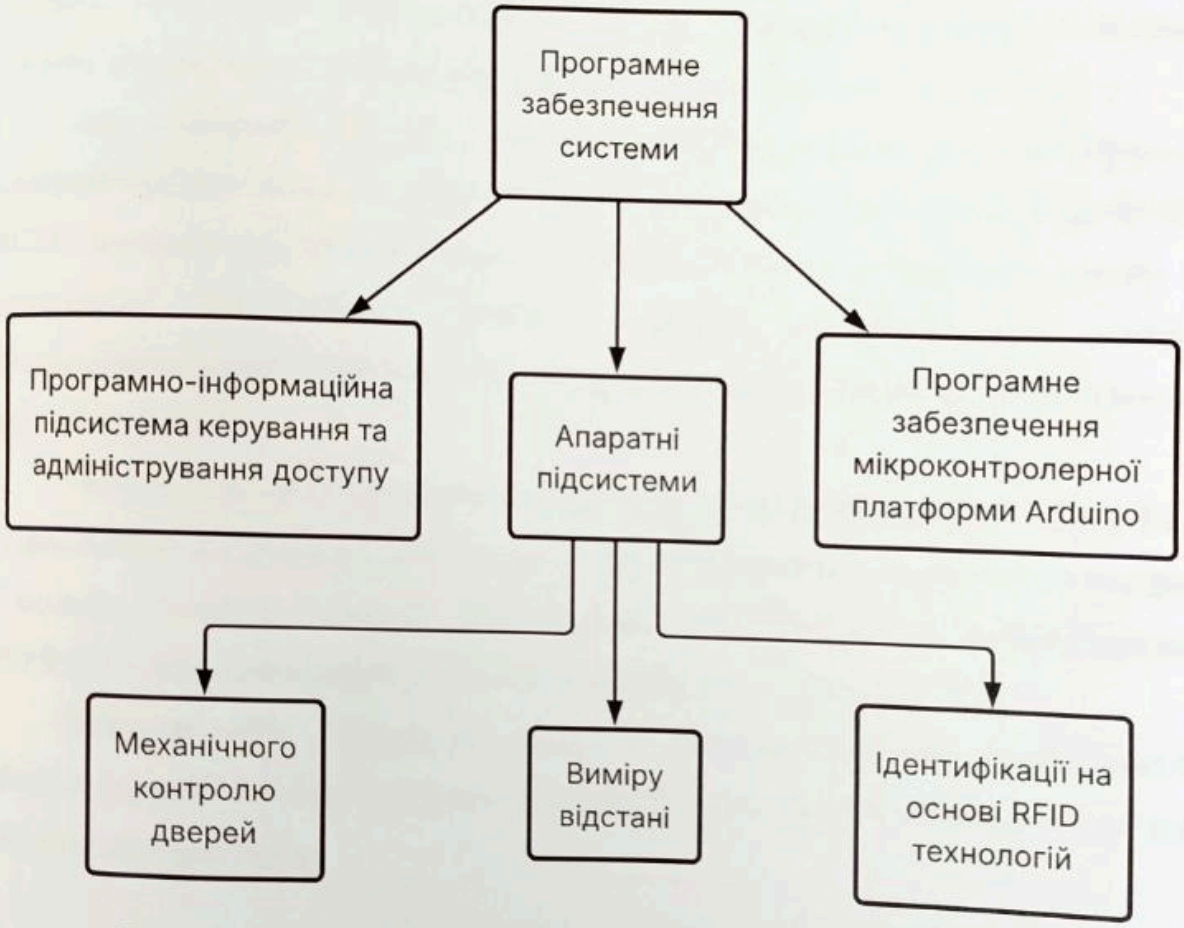


Рисунок 2.1 – Структура програмного забезпечення системи

Запропонована структура системи є модульною, тому робить можливим розглядати кожну підсистему незалежно під час розробки, тестування та подальшої модернізації. Підсистема RFID-ідентифікації відповідає за отримання первинних даних про користувача. Підсистема обробки інформації на базі

Arduino виконує логічне порівняння UID з даними EEPROM. Підсистема механічного контролю відповідає за фізичну дію над дверним механізмом. Підсистема індикації повідомляє користувача про поточний стан, а підсистема контролю дверей перевіряє, чи відповідає фізичний стан дверей прийнятому рішенню.

Важливою перевагою такого підходу є можливість окремого тестування компонентів. Наприклад, RFID-зчитувач може бути перевірений незалежно від сервоприводу, а сервопривід може бути протестований без роботи EEPROM-сховища. Це спрощує пошук помилок під час складання прототипу, оскільки створює умови для локалізації несправність на рівні конкретного модуля.

Для стабільної роботи системи необхідно правильно організувати призначення пінів Arduino (табл. 2.1). При розподілі пінів враховується, що RFID RC522 використовує SPI-інтерфейс, сервопривід потребує цифрового виходу з можливістю формування керуючого імпульсу, ультразвуковий датчик використовує окремі лінії Trigger та Echo, а RGB-світлодіод потребує декількох керуючих виходів.

Під час проєктування необхідно враховувати обмеження Arduino UNO R3, зокрема обсяг оперативної пам'яті, обсяг EEPROM та кількість доступних входів і виходів. Оскільки система зберігає лише UID RFID-міток, використання EEPROM є достатнім для невеликої кількості користувачів (рис. 2.2).

Водночас при збільшенні кількості користувачів або необхідності зберігати розширені дані необхідно буде перейти до зовнішнього модуля пам'яті або окремої бази даних.

Таблиця 2.1 – Розподіл пінів Arduino для апаратних модулів системи

Компонент	Призначення	Піни Arduino	Тип сигналу
RFID RC522	Зчитування UID	SCK, SS, MISO, MOSI, D8	Цифровий обмін
HC-SR04	Вимірювання відстані	D3 (Trig), D4 (Echo)	Цифровий імпульсний
Servo MG995	Керування механізмом	D2	Керуючий імпульс
Buzzer	Звукова індикація	D7	Цифровий
RGB LED	Світлова індикація	D9, D6, D5	PWM / керування каналами
EEPROM	Зберігання UID	Вбудована пам'ять	Програмний доступ

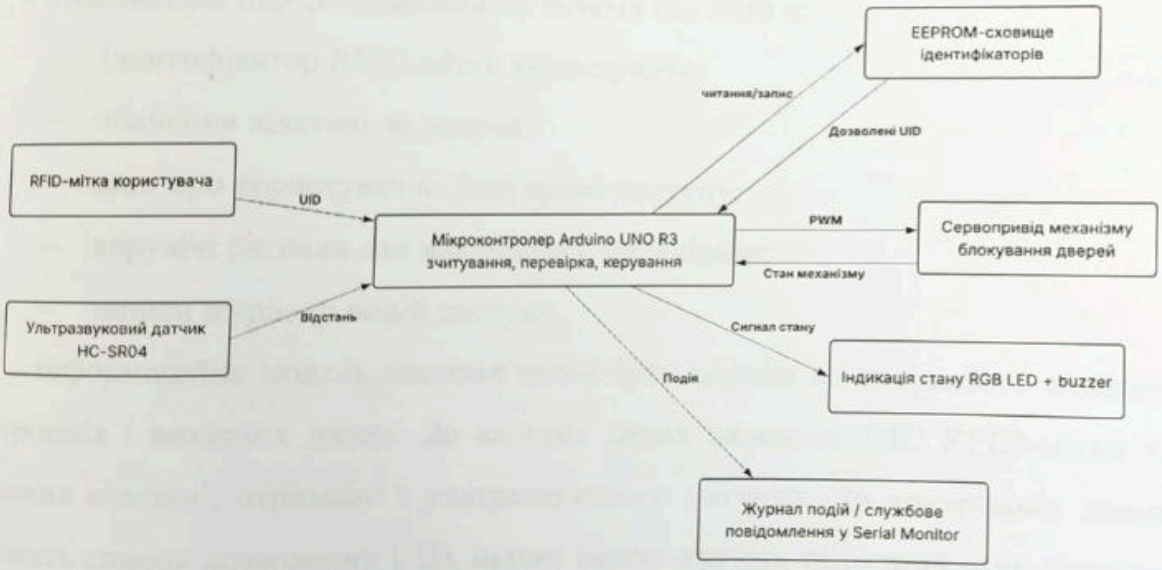


Рисунок 2.2 – Інформаційні потоки кіберфізичної системи контролю доступу

Для керування логікою роботи системи використовується відкрите програмне середовище Arduino IDE, тому що це є стандартним середовищем для

розробки ПЗ для платформ Arduino, яке дає можливість компілювати і одразу завантажувати код на підключений через USB контролер.

2.2 Проєктування інформаційної моделі та алгоритмів обробки даних у кіберфізичній системі контролю доступу

Проєктування інформаційної моделі кіберфізичної системи контролю доступу до приміщення передбачає визначення структури інформаційних потоків між програмними та апаратними підсистемами, а також розроблення алгоритмів обробки даних у реальному часі. Відповідно до обраної архітектури, система складається з програмного забезпечення мікроконтролерної платформи Arduino, апаратних підсистем ідентифікації, виміру відстані та механічного контролю дверей, а також програмно-інформаційної підсистеми керування та адміністрування доступу.

Основними інформаційними об'єктами системи є:

- ідентифікатор RFID-мітки користувача;
- значення відстані до дверей;
- дані про користувачів і їхні права доступу;
- керуючі сигнали для виконавчих механізмів;
- записи журналу подій доступу.

Інформаційна модель системи може бути подана як сукупність вхідних, внутрішніх і вихідних даних. До вхідних даних належать UID RFID-мітки та значення відстані, отримане з ультразвукового датчика. До внутрішніх даних належать список дозволених UID, індекс master-картки, поточний стан системи та службові таймери. До вихідних даних належать сигнали для сервоприводу, LED, buzzer та повідомлення для моніторингу.

Обробка UID виконується за принципом послідовного порівняння отриманого ідентифікатора з елементами, збереженими в EEPROM. Оскільки

кожен UID має фіксовану довжину, адреса конкретного запису може бути визначена за формулою:

$$address = DATA\_START\_ADDR + index * UID\_SIZE, \quad (2.1)$$

де *address* – ціле число, а саме номер байта з початку пам'яті;

DATA_START_ADDR – початкова адреса області зберігання UID;

index – порядковий номер запису;

UID_SIZE – кількість байтів, які займає один ідентифікатор.

Цей алгоритм є простим у реалізації та не потребує складних структур даних. Його недоліком є лінійний характер пошуку, але для невеликої кількості карток це не створює суттєвого навантаження на мікроконтролер. При максимальній кількості 50 записів система виконує обмежену кількість операцій порівняння, що є прийнятним для навчального прототипу (рис. 2.3).

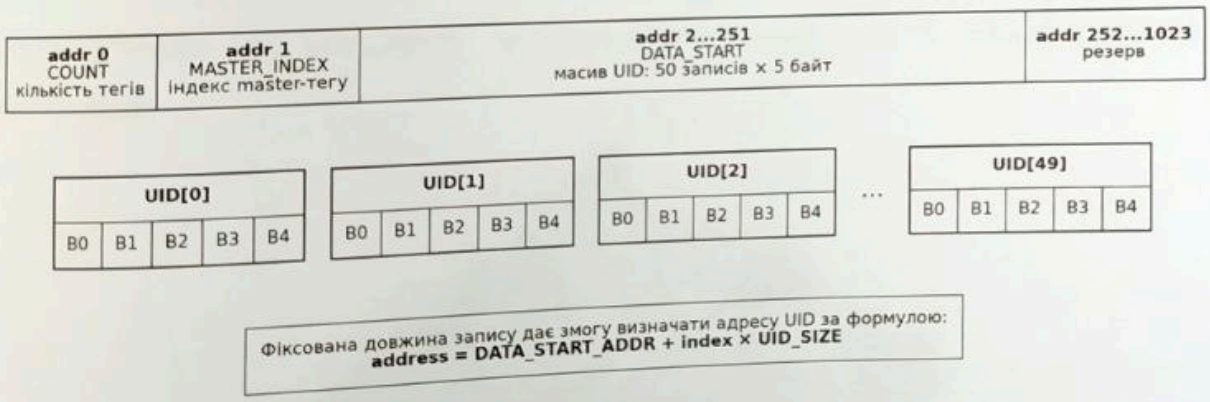


Рисунок 2.3 – Структура зберігання RFID-міток у EEPROM Arduino UNO R3

Для визначення стану дверей використовується значення відстані, отримане з ультразвукового датчика. Якщо середнє або поточне значення відстані менше встановленого порогу, двері вважаються зачиненими. Якщо значення перевищує поріг, система інтерпретує це як відчинений стан. Для підвищення точності можна використовувати декілька послідовних вимірювань і відкидати явно помилкові значення.

Алгоритм прийняття рішення можна описати таким чином. Спочатку система визначає поточний стан. Якщо система перебуває у стані очікування, вона перевіряє наявність RFID-мітки. Якщо мітка відсутня, цикл завершується без зміни стану. Якщо мітка присутня, UID порівнюється із записами EEPROM. У разі збігу зі звичайною карткою система відкриває механізм. У разі збігу з master-карткою система переходить у режим реєстрації. У разі відсутності збігу система відмовляє у доступі та подає відповідний сигнал.

2.3 Проєктування апаратної реалізації кіберфізичної системи контролю доступу

Апаратна реалізація кіберфізичної системи контролю доступу базується на мікроконтролерній платформі Arduino UNO R3 (рис. 2.4), яка виконує функції центрального керуючого та обчислювального елемента, а також сховища даних. Вибір даної платформи обумовлений її відкритою архітектурою, простотою програмування та широкими можливостями інтеграції з периферійними пристроями.

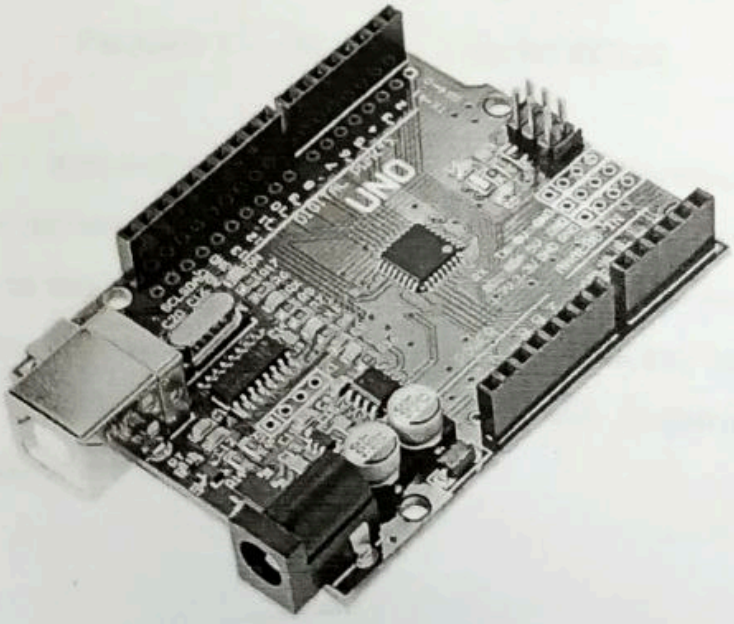


Рисунок 2.4 – Мікроконтролерна платформа Arduino UNO R3

Апаратна підсистема ідентифікації на основі RFID-технологій включає RFID-зчитувач, RFID-мітки користувачів та інтерфейси обміну даними з мікроконтролером (рис. 2.5). Основним завданням даної підсистеми є безконтактна ідентифікація користувачів шляхом зчитування унікального коду RFID-мітки та передавання його до Arduino для подальшої обробки.

Рисунок 2.5 – RFID-зчитувач MFRC522

Апаратна підсистема виміру відстані реалізується на основі ультразвукового датчика відстані, який підключається до мікроконтролера через цифрові входи та виходи (рис. 2.6). Її призначенням є визначення відстані до дверей з метою контролю їх фізичного стану. Отримані дані дозволяють визначити, чи перебувають двері у відкритому або закритому положенні, незалежно від логічного стану замка.

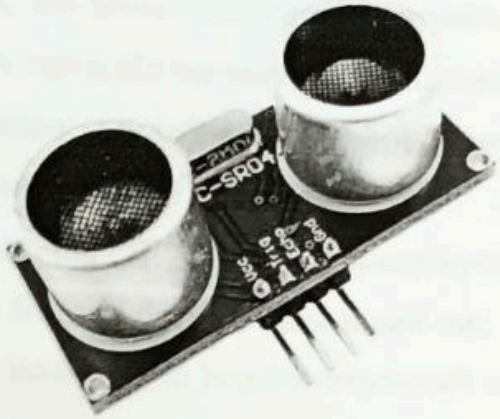


Рисунок 2.6 – Ультразвуковий датчик відстані HC-SR04

Апаратна підсистема механічного контролю дверей включає сервопривод та відповідні інтерфейси керування з боку мікроконтролера (рис. 2.7). Дана підсистема безпосередньо відповідає за фізичне відкриття або блокування дверей відповідно до прийнятого рішення щодо доступу.

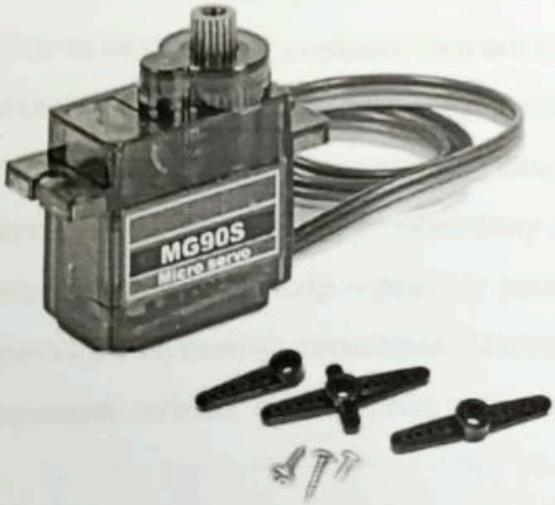


Рисунок 2.7 – Сервопривід MG90S

Під час апаратного проєктування важливо також врахувати електричні характеристики всіх компонентів. RFID-модуль RC522 зазвичай працює з напругою живлення 3,3 В, тоді як Arduino UNO R3 має логічні рівні 5 В. Тому при підключенні модуля необхідно дотримуватися рекомендованої схеми та

уникати подачі напруги, що може пошкодити зчитувач. Сервопривід MG995 може споживати значний струм під час запуску або під навантаженням, тому для стабільної роботи бажано передбачити окреме джерело живлення для сервоприводу із загальною землею з Arduino.

Ультразвуковий датчик HC-SR04 використовується для визначення фізичного стану дверей. Він має бути розташований так, щоб сигнал стабільно відбивався від дверного полотна або іншої контрольної поверхні. Якщо датчик встановлено під неправильним кутом, частина імпульсів може не повертатися до приймача, що призведе до некоректних значень. Тому під час складання прототипу необхідно експериментально підібрати положення датчика та порогове значення відстані.

Сервопривід у системі виконує роль виконавчого механізму. У реальних системах замість сервоприводу можуть використовуватися електромагнітні або електромеханічні замки, однак для навчального прототипу сервопривід є зручним рішенням. Він дозволяє наочно продемонструвати зміну стану системи, легко керується з Arduino та не потребує складної силової схеми.

Звукова та світлова індикація не є обов'язковою для базового функціонування, але значно підвищує зручність використання системи. Наприклад, зелений сигнал може відповідати дозволеному доступу, червоний – відмові, жовтий або інший службовий колір – режиму реєстрації. Buzzer може дублювати ці стани короткими звуковими сигналами. Завдяки цьому користувач отримує миттєвий зворотний зв'язок без потреби підключати комп'ютер до Serial Monitor.

2.3.1 Обґрунтування вибору апаратних компонентів

Одним із важливих етапів проєктування кіберфізичної системи контролю доступу є вибір апаратних компонентів, які дають можливість ідентифікувати користувачів, обробляти інформацію, контролювати фізичний стан дверей та

керувати виконавчими механізмами. Правильний вибір обладнання безпосередньо впливає на надійність, вартість, масштабованість та ефективність функціонування всієї системи.

У якості центрального обчислювального вузла обрано мікроконтролерну платформу Arduino UNO R3. Дана платформа є однією з найбільш поширених серед навчальних і прототипних рішень завдяки відкритій архітектурі, великій кількості доступної документації та широкій підтримці з боку спільноти розробників. Arduino UNO R3 побудована на базі мікроконтролера ATmega328P, який має достатню продуктивність для виконання задач обробки RFID-ідентифікаторів, роботи з датчиками та керування виконавчими механізмами.

До переваг Arduino UNO R3 можна віднести простоту програмування, підтримку великої кількості бібліотек, наявність цифрових та аналогових входів і виходів, а також вбудовану EEPROM-пам'ять, яка використовується для зберігання RFID-ідентифікаторів користувачів. Використання даної платформи створює умови для реалізації функціонального прототипу без необхідності застосування складних апаратних рішень.

Для реалізації підсистеми ідентифікації було обрано RFID-модуль MFRC522. Даний модуль є одним із найпоширеніших рішень для побудови систем контролю доступу на базі Arduino. Він працює на частоті 13,56 МГц та підтримує безконтактні RFID-картки стандарту MIFARE. Основними перевагами модуля є низька вартість, простота підключення через інтерфейс SPI та наявність готових програмних бібліотек для Arduino IDE.

Вибір саме MFRC522 обумовлений тим, що для системи контролю доступу не потрібна велика дальність зчитування. Навпаки, невелика відстань спрацьовування зміцнює безпеку та зменшує ймовірність випадкового зчитування сторонніх RFID-міток. Практична дальність роботи модуля становить від 2 до 5 см, що є достатнім для поставленої задачі.

Для визначення фізичного стану дверей використовується ультразвуковий датчик HC-SR04. Основною причиною вибору цього датчика є його доступність,

висока точність вимірювання на невеликих відстанях та простота інтеграції з Arduino. На відміну від кінцевих вимикачів або магнітних герконів, ультразвуковий датчик не потребує безпосереднього контакту з рухомими елементами дверей, що спрощує монтаж і зменшує механічне зношування компонентів.

Принцип роботи HC-SR04 полягає у випромінюванні ультразвукового імпульсу та вимірюванні часу його повернення після відбиття від поверхні. Отримані значення дозволяють визначити відстань до дверного полотна та зробити висновок щодо його положення. Це дає можливість контролювати фактичний стан дверей навіть у випадках, коли логічний стан виконавчого механізму не відповідає реальному положенню дверей.

Для реалізації механічного блокування доступу обрано сервопривід TowerPro MG90S. Даний сервопривід характеризується достатнім крутним моментом, високою надійністю та можливістю точного позиціонування. На відміну від звичайних електродвигунів, сервопривід може задавати конкретний кут повороту, що суттєво спрощує реалізацію механізму відкриття та закриття.

Використання сервоприводу також дає змогу відмовитися від складних схем керування двигунами та додаткових силових модулів. Керування здійснюється безпосередньо з Arduino за допомогою широтно-імпульсної модуляції, що спрощує апаратну реалізацію системи.

Для індикації стану системи використовується RGB-світлодіод. На відміну від окремих світлодіодів різних кольорів, RGB-компонент дозволяє реалізувати декілька режимів відображення за допомогою одного елемента. Наприклад, зелений колір може відповідати успішній авторизації, червоний – відмові у доступі, а синій – режиму реєстрації нових користувачів.

Додатково в системі використовується звуковий індикатор (buzzer), який акустично підтверджує виконання певних дій. Звукові сигнали дозволяють користувачу отримувати інформацію про стан системи навіть без візуального контакту зі світлодіодом.

Для зберігання RFID-ідентифікаторів користувачів використовується вбудована EEPROM-пам'ять мікроконтролера. Основною перевагою такого підходу є відсутність необхідності застосування зовнішніх модулів пам'яті або баз даних. EEPROM є енергонезалежною пам'яттю, тому інформація зберігається навіть після повного відключення живлення системи.

Перелік компонентів та причин їх вибору відображений в таблиці 2.2.

Таблиця 2.2 – Обґрунтування вибору основних апаратних компонентів

Компонент	Призначення	Причина вибору
Arduino UNO R3	Центральний контролер	Простота програмування, наявність EEPROM, велика кількість бібліотек
MFRC522	RFID-зчитування	Низька вартість, підтримка MIFARE, SPI-інтерфейс
HC-SR04	Контроль стану дверей	Безконтактне вимірювання відстані, висока точність
TowerPro MG90S	Механізм блокування	Високий крутний момент, точне позиціонування
RGB LED	Візуальна індикація	Відображення кількох станів одним компонентом
Buzzer	Звукова індикація	Простота реалізації та інформування користувача

Тому, обраний набір апаратних компонентів має забезпечити реалізацію всіх необхідних функцій кіберфізичної системи контролю доступу при відносно невисокій вартості та достатньому рівні надійності. Використання широко поширених модулів спрощує процес розробки, тестування та подальшої модернізації системи, а також створює умови для використання її як основи для створення більш складних рішень у сфері автоматизації та безпеки.

2.4 Висновки до другого розділу

В другому розділі визначено апаратні та програмні підсистеми програмно-технічного засобу кіберфізичної системи контролю доступу на основі RFID-технологій та платформи Arduino. Розглянуто способи взаємодії між підсистемами, а також описано функціональне призначення основних програмних модулів, апаратних компонентів і інформаційних ресурсів системи.

Отримані результати є основою для подальшої реалізації, тестування та оптимізації системи контролю доступу з метою підвищення її надійності, безпеки та ефективності функціонування.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

3.1 Опис реалізації модулів апаратного та програмного забезпечення програмно-технічного засобу

Програмно-апаратна реалізація кіберфізичної системи контролю доступу базується на взаємодії мікроконтролерної платформи Arduino UNO R3 з апаратними підсистемами ідентифікації, виміру відстані та механічного контролю дверей, а також із програмно-інформаційною підсистемою керування.

Програмне забезпечення мікроконтролера реалізоване у вигляді прошивки, що функціонує в режимі реального часу. Воно виконує:

- ініціалізацію всіх апаратних модулів;
- зчитування ідентифікаторів RFID-міток користувачів;
- отримання даних з ультразвукового датчика відстані;
- логічну перевірку прав доступу;
- формування керуючих сигналів для сервоприводу;
- передавання інформації до програмно-інформаційної підсистеми.

В якості апаратної частини бази даних виступатиме вбудована пам'ять мікроконтролера Arduino. В конкретній версії Arduino UNO R3 наявна EEPROM (Electrically Erasable Programmable Read-Only Memory) – енергонезалежна пам'ять обсягом 1024 байт (1 КБ), яка здатна зберігати невелику кількість даних, таку як RFID мітки. Це чудовий варіант для поточної задачі.

Модуль RFID-ідентифікації реалізовано на основі стандартного RFID-RC522 зчитувача, підключеного до Arduino через інтерфейс SPI. При піднесенні RFID-мітки відбувається зчитування її унікального ідентифікатора, який передається до центрального модуля для перевірки.

Модуль виміру відстані реалізовано з використанням ультразвукового датчика. Він дає можливість визначити фактичний стан дверей (відчинені або

зачинені) шляхом аналізу відстані до поверхні дверного полотна. Це дає змогу виявляти несанкціоновані дії, наприклад, примусове відкриття дверей.

Модуль механічного контролю дверей побудований на основі сервоприводу, який керується мікроконтролером через цифровий вихід. Залежно від результатів перевірки доступу сервопривід переводить механізм у стан відкриття або блокування.

Після реалізації програмно-апаратна структура забезпечує надійне, оперативне та автоматизоване керування доступом до приміщення.

3.2 Опис процесу створення баз даних

Так як база даних імплементована в EEPROM сховищі, її будуть репрезентувати окремі байти даних, в яких зберігається ID міток з RFID зчитувача. Надалі дизайн БД залежить лише від імплементації інтерфейсу взаємодії з цим сховищем.

Для досягнення цього створюється окремий клас RFIDStorage, що використовуватиме бібліотеку EEPROM.h, яка дає прямий доступ до EEPROM.

Кожна комірка – 1 байт. Деякі комірки пам'яті будуть використовуватись для зберігання мета-даних, таких як кількість запам'ятованих тегів в системі, і також положення адреси мастер-тегу, який дозволить при скануванні "зареєструвати" новий ID в систему. Пропишемо константи для класу RFIDStorage: UID_SIZE = 5, MAX_TAGS = 50, COUNT_ADDR = 0, MASTER_INDEX_ADDR = 1, DATA_START_ADDR = 2.

Якщо зрозуміліше, то в комірці 0 зберігається кількість збережених тегів, в комірці 1 – індекс майстер-тегу, а з комірки 2 починається безпосередньо сховище тегів максимальною місткістю 50 тегів, де кожен тег представляється рядком довжиною 5 символів.

Клас RFIDStorage виступає в ролі програмного інтерфейсу до EEPROM-сховища. Він приховує низькорівневі операції читання та запису окремих байтів

і надає більш зрозумілі функції для основної логіки програми (табл. 3.1). До таких функцій можуть належати: отримання кількості збережених карток, перевірка наявності UID, додавання нового UID, визначення master-картки, очищення сховища та отримання адреси запису за індексом.

Основною перевагою використання окремого класу є відокремлення логіки зберігання даних від логіки керування станами системи. У такому випадку основна програма не працює безпосередньо з адресами EEPROM, а звертається до методів класу. Це зменшує ризик помилок, спрощує читання коду та полегшує подальше розширення системи. Наприклад, у майбутньому EEPROM можна замінити на зовнішній модуль пам'яті, не змінюючи основну логіку роботи з RFID-картками.

Таблиця 3.1 – Основні операції класу RFIDStorage

Операція	Призначення	Очікуваний результат
getCount()	Отримати кількість збережених UID	Повертає число записів
isEmpty()	Перевірити, чи є база порожньою	true або false
contains(uid)	Перевірити наявність UID	true, якщо UID знайдено, інакше false
add(uid)	Додати новий UID	Запис у EEPROM
isMaster(uid)	Перевірити на master-картку	true для мастер картки
getAddress(index)	Обчислити адресу запису	Адреса першого байта UID

При записі даних у EEPROM необхідно враховувати обмеження кількості циклів перезапису. Хоча у межах навчального прототипу це обмеження не є критичним, програма не повинна виконувати зайві операції запису. Наприклад, якщо картка вже є у сховищі, її не потрібно записувати повторно. Якщо сховище

заповнене, система повинна відмовитися від додавання нового UID та повідомити про це користувача за допомогою індикації.

Окремо слід розглянути перший запуск системи. Якщо EEPROM порожня, перша зчитана картка може бути зареєстрована як master-картка. Після цього вона використовується для переходу у режим додавання нових користувацьких карток. Це полегшує перше налаштування системи і її гнучкість, тому що не потрібно попередньо програмувати конкретний UID у коді мікроконтроллера.

3.3 Опис взаємодії програмної та апаратної частин системи

Взаємодія програмної та апаратної частин системи контролю доступу організована через мікроконтролер Arduino, який виконує роль основного керуючого вузла. Він приймає сигнали від RFID-зчитувача та датчика відстані, обробляє отримані значення і передає команди на виконавчі пристрої.

Після піднесення RFID-мітки система зчитує її UID, паралельно контролює відстань до дверей і на основі цих даних визначає подальшу дію. Програмна частина перевіряє, чи збережений отриманий ідентифікатор у пам'яті системи, після чого приймає рішення про надання або заборону доступу. Якщо доступ дозволено, Arduino формує керуючий сигнал для сервоприводу, а інформація про подію може бути виведена у Serial Monitor або збережена в журналі подій.

Такий принцип роботи дає змогу узгодити зчитування даних, перевірку прав доступу та фізичне керування дверним механізмом. Завдяки цьому система реагує на дії користувача послідовно й передбачувано, а всі основні модулі працюють як єдиний програмно-апаратний комплекс.

3.4 Опис розробки апаратної частини системи

Розробка апаратної частини системи здійснювалася з урахуванням вимог до функціональності, надійності та можливості розширення системи. Початкова схема з'єднання компонентів була сформована з використанням онлайн-ресурсу https://www.circuito.io/, за допомоги якого можна автоматизувати процес

проєктування електричних схем для мікроконтролерних систем. На основі згенерованої схеми виконано доопрацювання та адаптацію апаратної частини відповідно до поставлених задач. Загальна структурна схема апаратної частини системи наведена на рис. 3.1.

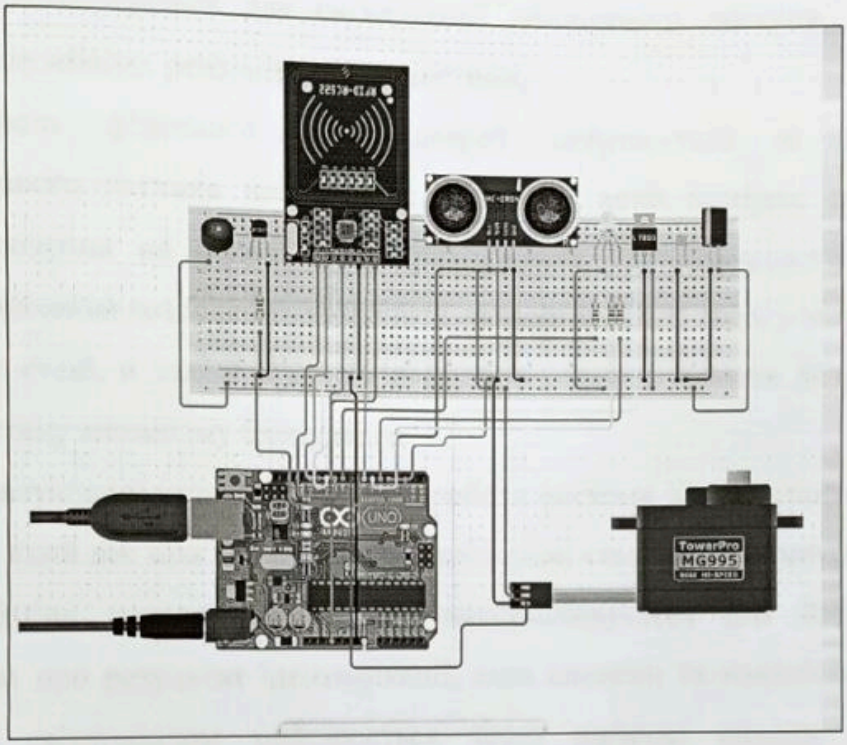


Рисунок 3.1 – Початкова схема апаратної частини системи

Центральним елементом апаратної частини є мікроконтролер Arduino Uno R3, який виконує функції збору та обробки даних з датчиків, керування виконавчими пристроями та взаємодії з програмно-інформаційною підсистемою. Вибір даної платформи обумовлений її доступністю, стабільністю роботи, достатньою кількістю входів і виходів, а також широкою підтримкою бібліотек для підключення периферійних модулів.

Для реалізації підсистеми ідентифікації використано RFID-модуль RC522, який працює на частоті 13,56 МГц та підключається до Arduino за допомогою інтерфейсу SPI. Модуль зчитує унікальні ідентифікатори RFID-міток

користувачів і передає їх у цифровому вигляді до мікроконтролера для подальшої перевірки прав доступу.

Звукова індикація станів системи реалізована за допомогою buzzer (пищалки). Для керування buzzer використано транзистор, який зменшує навантаження на вихід мікроконтролера та стабілізує звуковий сигнал. Звукова індикація застосовується для сигналізації дозволеного доступу, відмови у доступі та службових режимів роботи системи.

Контроль фізичного стану дверей здійснюється за допомогою ультразвукового датчика наближення HC-SR04, який вимірює відстань до дверного полотна на основі часу проходження ультразвукового імпульсу. Отримані значення дозволяють визначити, чи перебувають двері у закритому або відкритому стані, а також виявити несанкціоноване відкриття незалежно від логічного стану механізму блокування.

Для візуальної індикації режимів роботи системи використано RGB LED світлодіод, який дає можливість відображати різні стани за допомогою кольорів світіння. Зміна кольору світлодіода використовується для інформування користувача про результат ідентифікації, стан системи та наявність помилок. Керування світлодіодом здійснюється через цифрові виходи Arduino з використанням струмообмежувальних резисторів.

Механічний контроль доступу до приміщення реалізовано за допомогою сервоприводу TowerPro MG90S, який виконує фізичне відкриття або блокування дверей. Сервопривід керується мікроконтролером за допомогою широтно-імпульсної модуляції (PWM), що забезпечує точне позиціонування та надійну роботу механізму замикання. Обраний сервопривід має достатній крутний момент для використання у системах контролю доступу.

Усі апаратні компоненти з'єднані відповідно до розробленої схеми та функціонують, як єдина кіберфізична система (рис. 3.2). Запропонована апаратна реалізація є модульною, яку легко модифікувати, замінювати окремі компоненти

або інтегрувати додаткові датчики та виконавчі пристрої без суттєвих змін у загальній архітектурі.

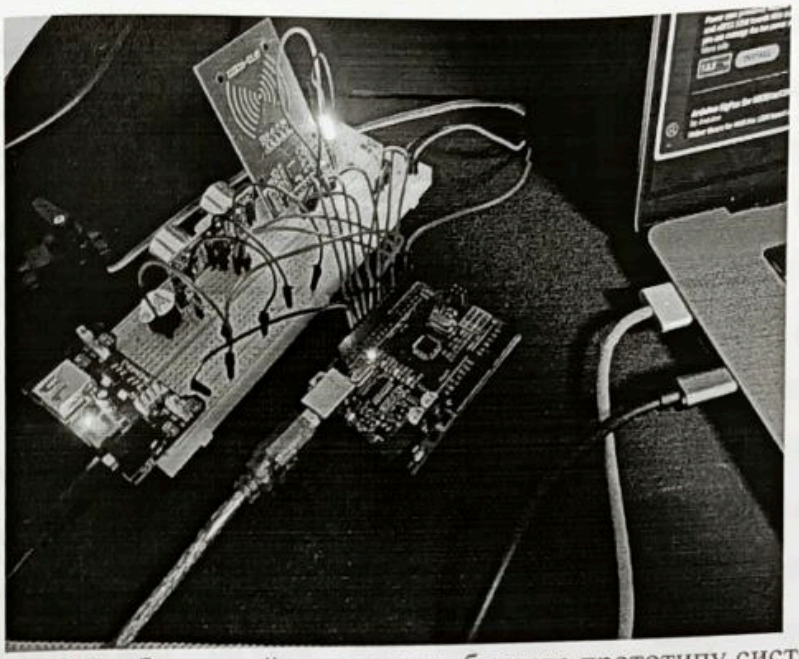


Рисунок 3.2 – Загальний вигляд розробленого прототипу системи

3.5 Опис розробки програмної частини системи

Щоб забезпечити основну функціональність системи через взаємодію з картками доступу система розробляється за принципом лінійного керування та state-driven development, де відбувається постійне опитування RFID-модуля, після чого при відсутності сканованих тегів виконання ітерації припиняється.

Також при розробці використовуються сторонні бібліотеки для взаємодії з модулями системи, а саме:

- NewPing – для взаємодії з ультразвуковим датчиком відстані;
- RGBLed – для взаємодії з різнокольоровим світлодіоїдом, для індикації стану системи;
- MFRC522 – стандартна бібліотека для взаємодії з RFID антенами по стандарту RC522;
- Servo.h – вбудована в Arduino бібліотека для взаємодії з сервоприводами.

Для початку потрібно ініціалізувати усі необхідні для функціонування системи об'єкти, які дозволяють взаємодіяти з апаратною частиною системи. Для цього розподілимо номери пінів до відповідних апаратних модулів.

Пін для модуля пищалки - 6. Датчик відстані займатиме піни 12 та 13. Сигнал для сервоприводу йтиме через пін 5. RFID сканер комунікуватиме через піни 7 та 8. Для RGB-світлодіоду потрібний аналоговий сигнал, для чого підійдуть аналогові піни A0, A1 та A2 для відповідних каналів R, G, B.

Далі потрібно визначити деякі постійні значення, які допоможуть керувати поведінкою системи. Вони включають максимальну дистанцію для виміру відстані в 2 см., яка визначена в характеристиках самого модуля; різні кольори, які складаються з трьох базових RGB кольорів; початкова та активна позиція сервоприводу в градусах; максимальний час перебування в одному зі станів системи. Вони допоможуть контролювати логіку в основній програмі.

Далі оголосимо об'єкти для взаємодії з модулями системи, використовуючи оголошені константи, і також оголосимо головний state програми, який керуватиме поведінкою. Станів буде три – Очікування, Відкрито, Реєстрація; і також таймер, який рахуватиме, скільки часу проведено в одному стані.

Для правильного функціонування системи на базі Arduino потрібно оголосити дві функції – setup та loop.

Функція setup викликається кожен раз, коли на мікроконтролер подається живлення, і використовується для початкової ініціалізації системи та її модулів. В нашому випадку використаємо цю функцію для задання початкових значень змінним, та визначення початкового стану системи в залежності від заповненості сховища RFID тегів.

Функція loop викликається в нескінченному циклі, поки в мікроконтроллера є живлення, та зазвичай використовується для імплементації логіки кіберфізичних систем. Тут ця функція виступатиме як роутер для

подальшої логіки, та в залежності від стану системи викликатиме відповідні функції (Очікування, Відкрито, Реєстрація).

При стані "Відкрито" система взнаватиме, чи відкриті двері фізично, та через деякий проміжок часу знову взнаватиме те ж саме. Якщо вони виявляються закритими – значить двері дійсно закриті, і можна змінити стан системи на Waiting (рис. 3.3).

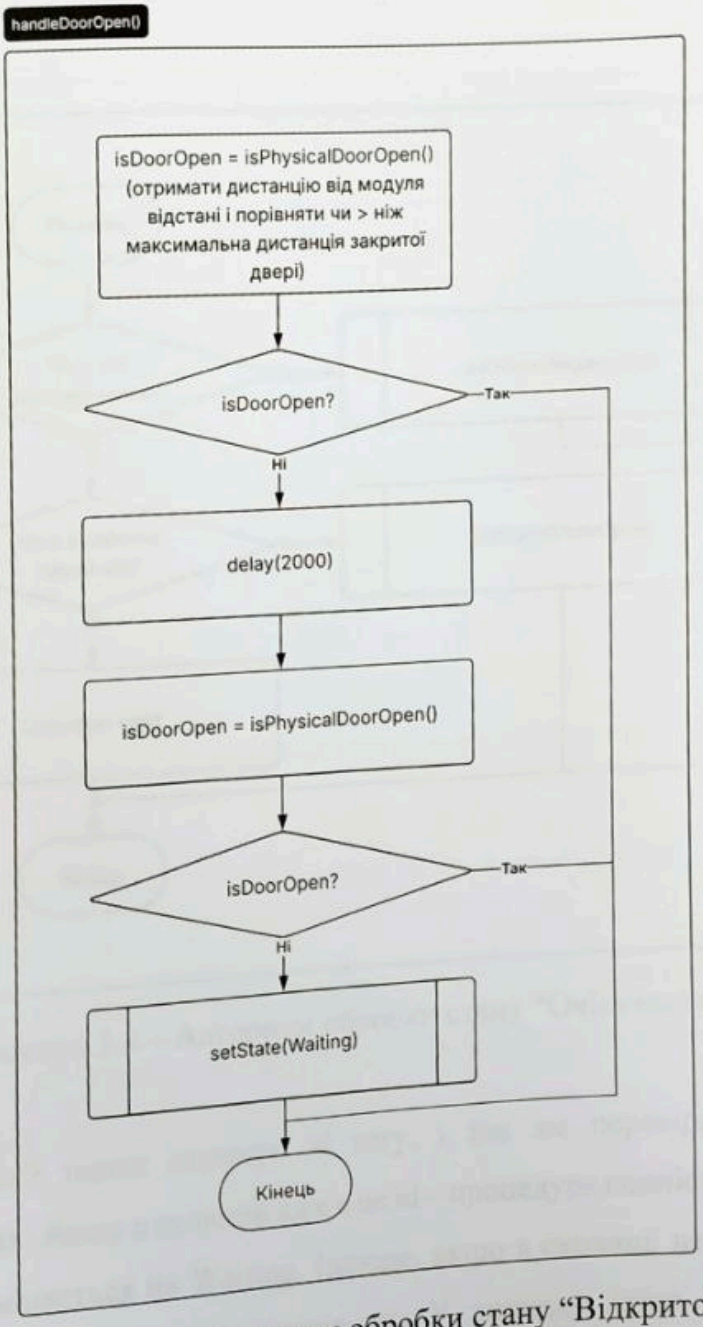


Рисунок 3.3 – Алгоритм обробки стану "Відкрито"

Обробники станів “Очікування” та “Реєстрація” викликаються тільки тоді, коли до RFID зчитувача підноситься картка, тому її наявність перевіряється, тільки якщо стан системи не є “Відкрито”.

“Очікування” отримує id тегу, та вирішує що робити з ним в залежності від стану сховища. Якщо тег є мастер-тегом, то стан системи стає “Реєстрація”. Інакше, якщо карта присутня в сховищі, двері відчиняються, і стан системи стає “Відкрито” (рис. 3.4).

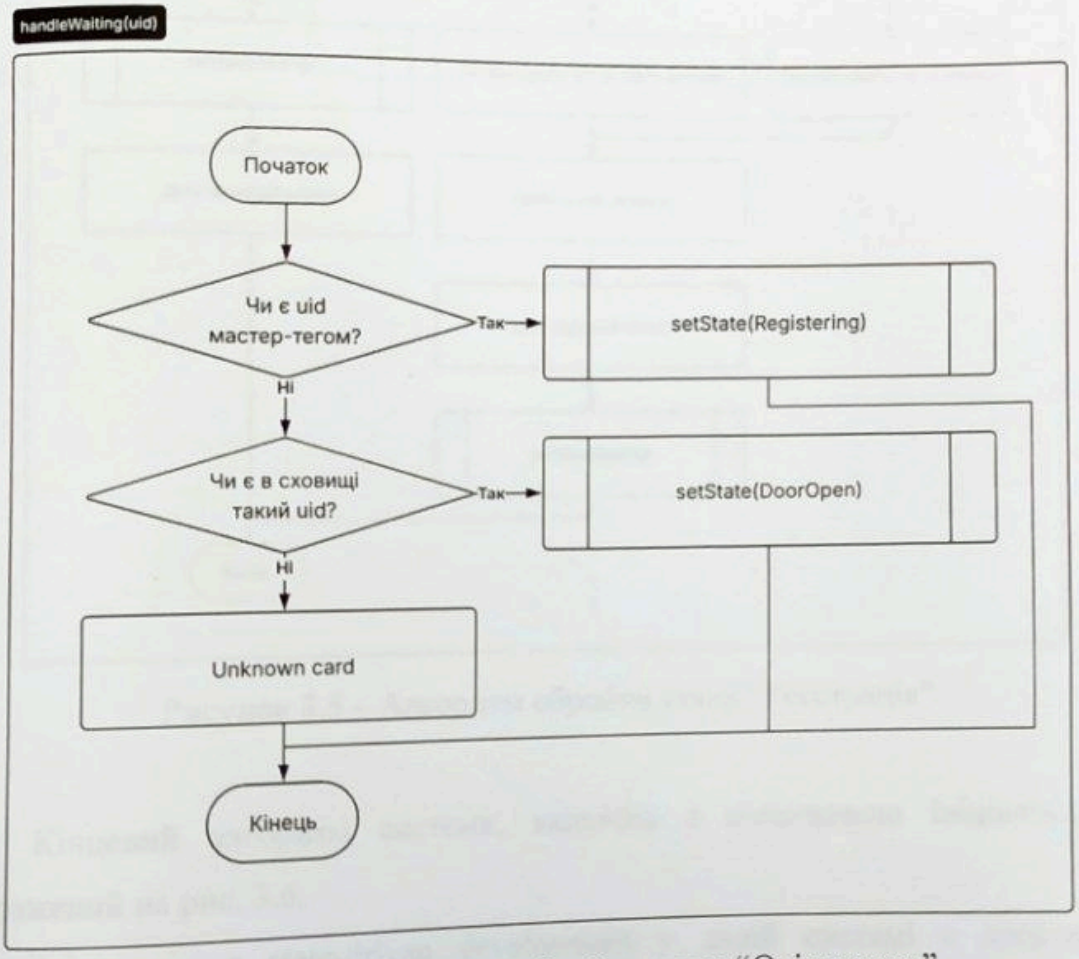


Рисунок 3.4 – Алгоритм обробки стану “Очікування”

“Реєстрація” також отримує id тегу, і так же перевіряє сховище по декільком умовах. Якщо в сховищі вже є це id – процедура повністю зупиняється, і стан системи міняється на Waiting. Інакше, якщо в сховищі нема мастер-тегу, цей id реєструється як новий мастер-тег. У випадку якщо мастер-тег вже

присутній, цей тег додається до сховища, і може використовуватись для доступу до приміщення (рис. 3.5).

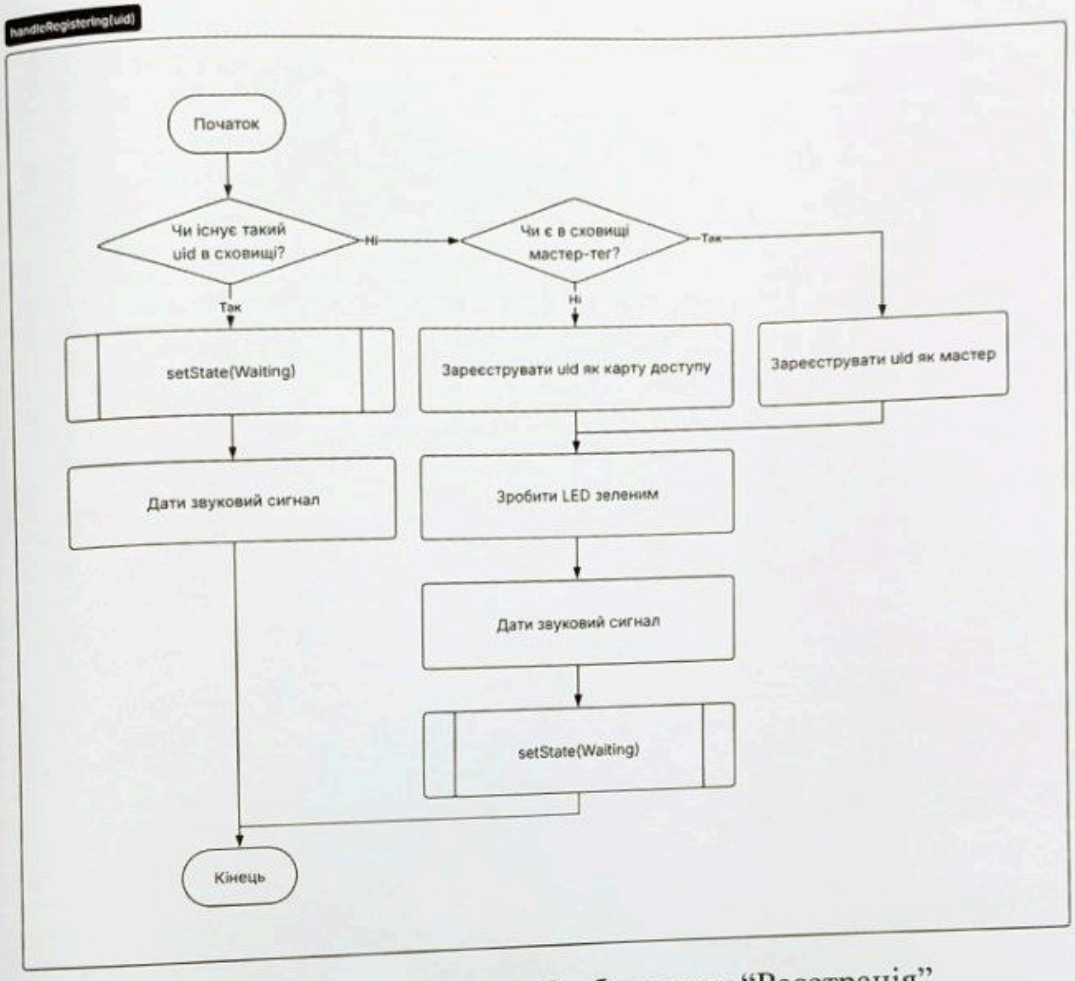


Рисунок 3.5 – Алгоритм обробки стану “Реєстрація”

Кінцевий алгоритм системи, включно з початковою ініціалізацією, зображений на рис. 3.6.

Застосування state-driven development у даній системі є доцільним, оскільки поведінка пристрою залежить від поточного стану. Це дозволяє уникнути складної структури вкладених умов і зробити логіку програми більш зрозумілою.

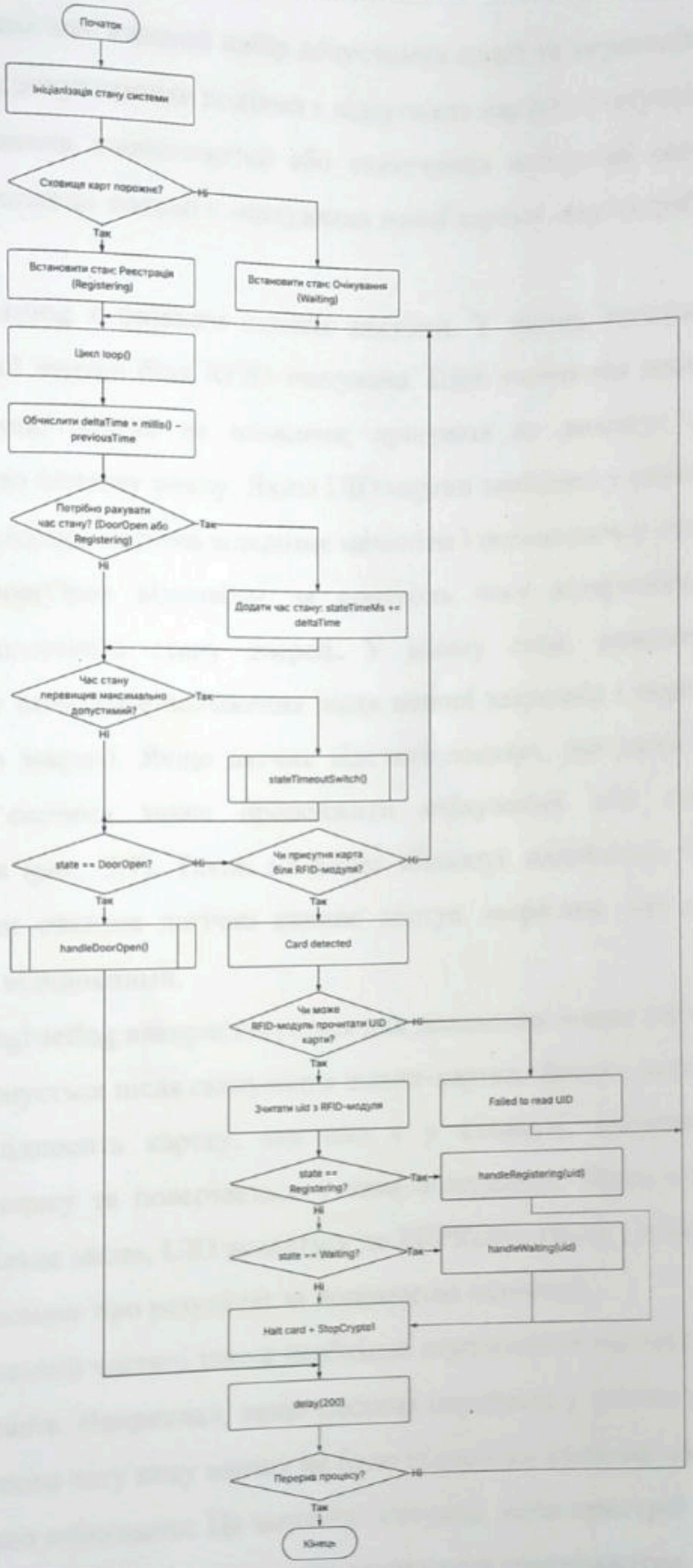


Рисунок 3.6 – Алгоритм роботи кіберфізичної системи

Кожен стан має власний набір допустимих подій та переходів. Наприклад, у стані Waiting допустимими подіями є відсутність картки, зчитування звичайної картки, зчитування master-картки або зчитування невідомої картки. У стані Registering основною подією є зчитування нової картки, яку потрібно додати до EEPROM.

Стан Waiting є базовим станом системи. У ньому програма перевіряє наявність нової картки біля RFID-зчитувача. Щоб зменшити навантаження на контролер, якщо картка не виявлена, програма не виконує зайвих дій і повертається до початку циклу. Якщо UID картки знайдено у сховищі та картка не є master-карткою, система відкриває механізм і переходить у стан DoorOpen.

Стан DoorOpen відповідає за контроль часу відкритого доступу та перевірку фактичного стану дверей. У цьому стані важливо повернути сервопривід у початкове положення після певної затримки і переконатися, що двері фізично закриті. Якщо датчик відстані показує, що двері залишаються відкритими, система може продовжити очікування або подати сигнал попередження (рис. 3.7). Такий механізм збільшує надійність, бо уникається ситуація, коли система логічно вважає доступ закритим, але двері фізично залишаються відчиненими.

Стан Registering використовується для додавання нових карток. Перехід у цей стан виконується після сканування master-картки. Якщо у режимі реєстрації користувач підносить картку, яка вже є у сховищі, система не виконує повторного запису та повертається у стан очікування. Якщо картки немає у сховищі і є вільне місце, UID додається до EEPROM. Після успішної реєстрації система повідомляє про результат за допомогою індикації.

У програмній частині також необхідно передбачити часові обмеження для службових станів. Наприклад, якщо система перейшла у режим реєстрації, але протягом певного часу нову картку не було піднесено, система має автоматично перейти в стано очікування. Це запобігає ситуації, коли пристрій залишається у службовому режимі після випадкового сканування master-картки.

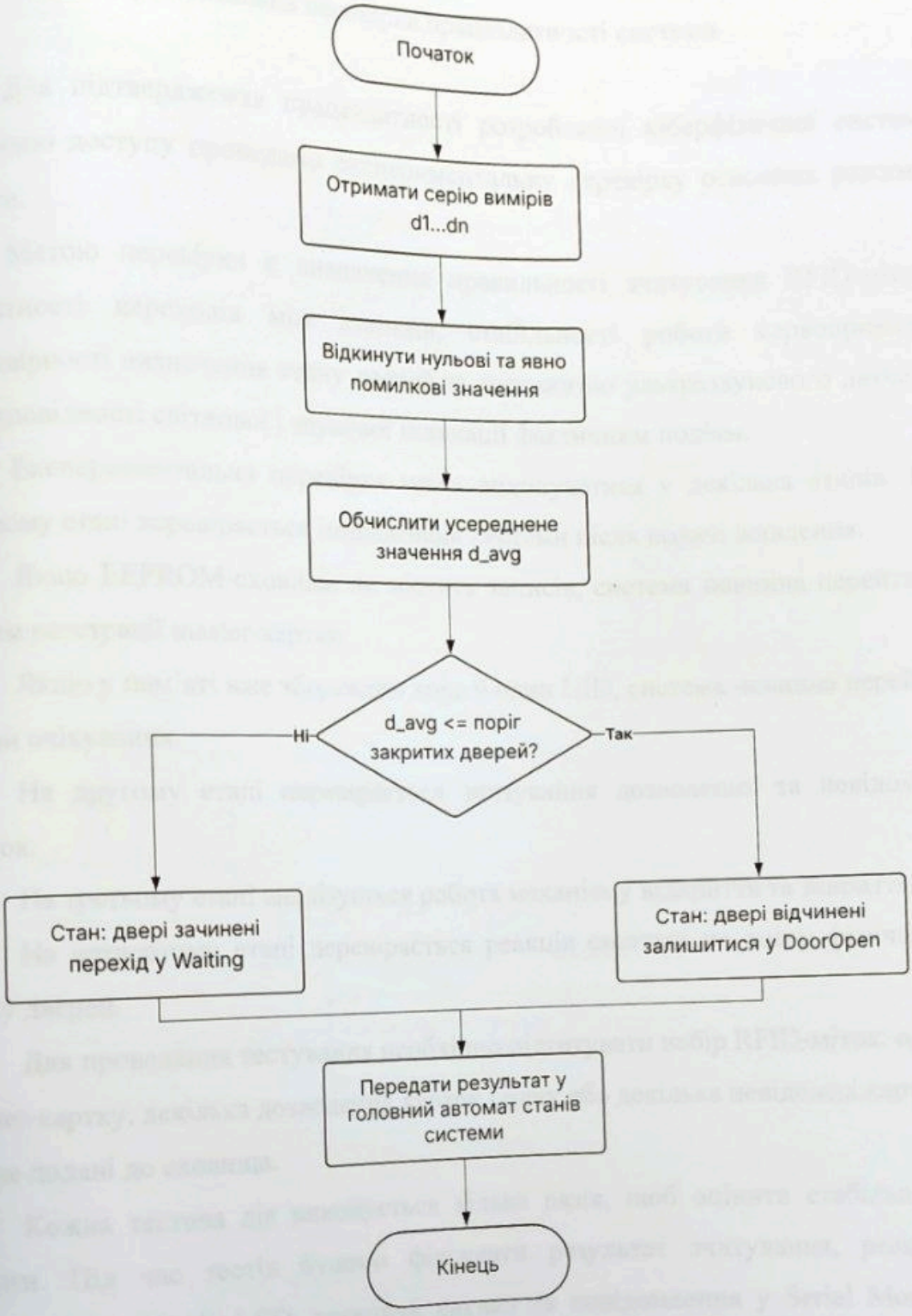


Рисунок 3.7 – Обробка даних ультразвукового датчика для визначення стану дверей

3.6. Експериментальна перевірка працездатності системи

Для підтвердження працездатності розробленої кіберфізичної системи контролю доступу проведемо експериментальну перевірку основних режимів роботи.

Метою перевірки є визначення правильності зчитування RFID-міток, коректності переходів між станами, стабільності роботи сервоприводу, достовірності визначення стану дверей за допомогою ультразвукового датчика та відповідності світлової і звукової індикації фактичним подіям.

Експериментальна перевірка може виконуватися у декілька етапів. На першому етапі перевіряється ініціалізація системи після подачі живлення.

Якщо EEPROM-сховище не містить записів, система повинна перейти у режим реєстрації master-картки.

Якщо у пам'яті вже збережено хоча б один UID, система повинна перейти у стан очікування.

На другому етапі перевіряється зчитування дозволених та невідомих карток.

На третьому етапі аналізується робота механізму відкриття та закриття.

На четвертому етапі перевіряється реакція системи на зміну фізичного стану дверей.

Для проведення тестування необхідно підготувати набір RFID-міток: одну master-картку, декілька дозволених карток і одну або декілька невідомих карток, які не додані до сховища.

Кожна тестова дія виконується кілька разів, щоб оцінити стабільність роботи. Під час тестів будемо фіксувати результат зчитування, реакцію сервоприводу, колір LED, звуковий сигнал та повідомлення у Serial Monitor (рис. 3.8).

Сценарії тестування наведено в таблиці 3.2.

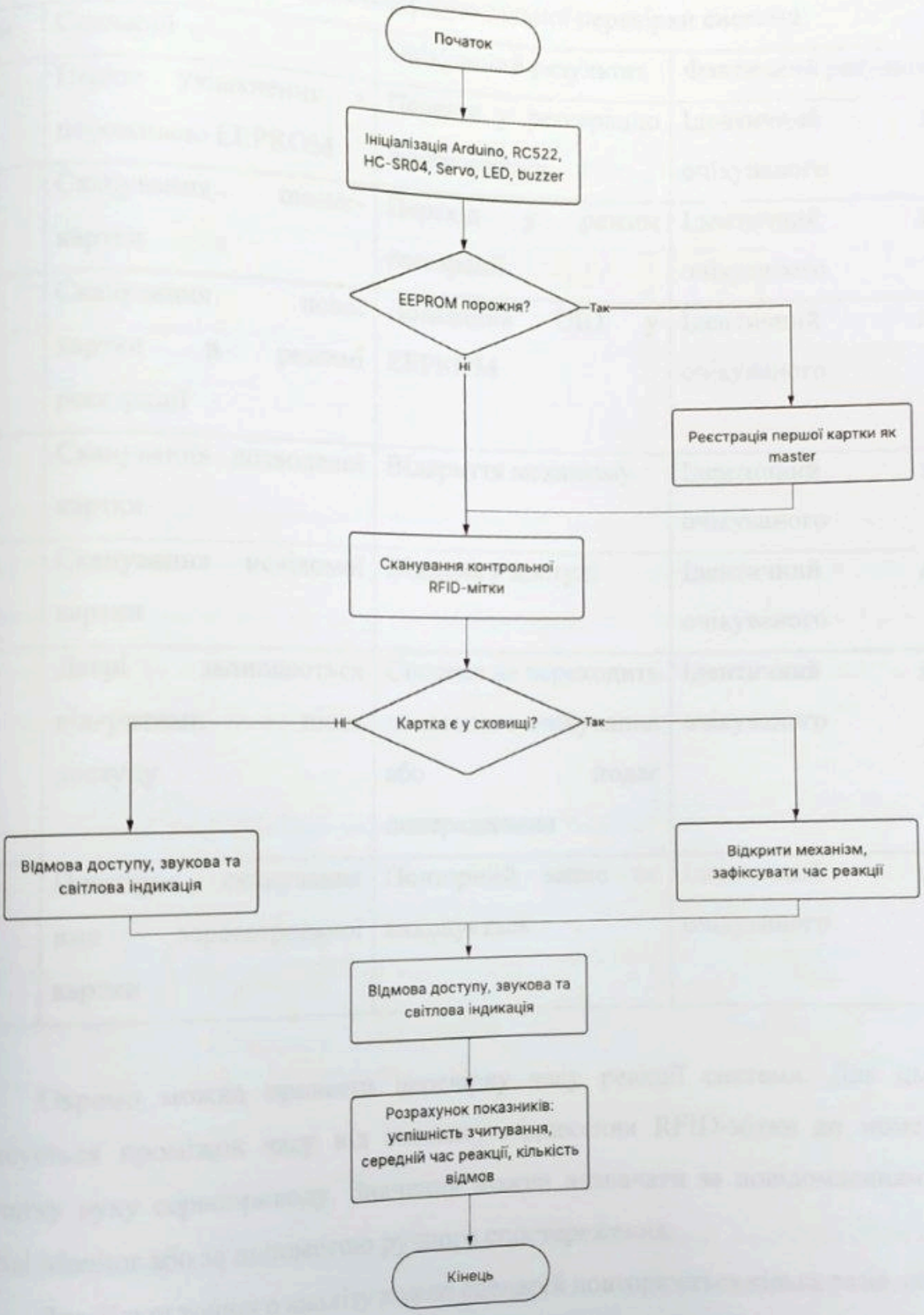


Рисунок 3.8 – Алгоритм експериментальної перевірки роботи прототипу

Таблиця 3.2 – Сценарії експериментальної перевірки системи

№	Сценарій	Очікуваний результат	Фактичний результат
1	Перше увімкнення з порожньою EEPROM	Перехід у реєстрацію master-картки	Ідентичний до очікуваного
2	Сканування master-картки	Перехід у режим реєстрації	Ідентичний до очікуваного
3	Сканування нової картки в режимі реєстрації	Додавання UID у EEPROM	Ідентичний до очікуваного
4	Сканування дозволеної картки	Відкриття механізму	Ідентичний до очікуваного
5	Сканування невідомої картки	Відмова у доступі	Ідентичний до очікуваного
6	Двері залишаються відкритими після доступу	Система не переходить до повного очікування або подає попередження	Ідентичний до очікуваного
7	Повторне сканування вже зареєстрованої картки	Повторний запис не виконується	Ідентичний до очікуваного

Окремо можна провести перевірку часу реакції системи. Для цього фіксується проміжок часу від моменту піднесення RFID-мітки до моменту початку руху сервоприводу. Значення можна визначати за повідомленнями у Serial Monitor або за допомогою ручного спостереження.

Для більш точного аналізу кожен сценарій повторюється кілька разів, після чого обчислюється середнє значення.

Таблиця 3.3 – Шаблон фіксації часу реакції системи

№ спроби	Тип картки	Результат доступу	Час реакції, мс	Примітка
1	Дозволена	Дозволено	2.9	
2	Дозволена	Дозволено	3	
3	Невідома	Заборонено	3.3	
4	Master	Реєстрація	2.6	
5	Дозволена	Дозволено	3.1	

Для перевірки ультразвукового датчика необхідно визначити порогову відстань, яка відповідає закритому положенню дверей. Після цього проводиться серія вимірювань у двох станах: двері зачинені та двері відчинені. Якщо отримані значення суттєво відрізняються, система може надійно використовувати датчик для визначення стану. Якщо значення нестабільні, необхідно змінити положення датчика або використовувати усереднення кількох вимірювань.

Таблиця 3.4 – Шаблон перевірки датчика відстані

№ вимірювання	Стан дверей	Відстань, см	Висновок системи
1	Зачинені	2.3	Зачинені
2	Зачинені	2.4	Зачинені
3	Відчинені	0	Зачинені
4	Відчинені	60	Відчинені
5	Зачинені	2.3	Зачинені

Як видно, в більшості випадків результат виявлявся вірним. В випадку вимірювання номер 3, сенсор був направлений всередину кімнати, через що відстань між імпульсами була занадто великою. Щоб модуль працював коректно, потрібно обмежити максимальну дальність імпульсів, тому сенсор доведеться

встановлювати таким чином, щоб він знаходився всередині дверної коробки, направлений паралельно до механізму контролю дверей.

За результатами експериментальної перевірки можна зробити висновок щодо працездатності системи, стабільності алгоритму та доцільності обраної апаратної платформи. Якщо всі тестові сценарії виконуються відповідно до очікуваних результатів, система може вважатися працездатною у межах навчального прототипу. Якщо під час тестування виявлено помилки, їх необхідно проаналізувати та усунути шляхом зміни програмної логіки, налаштування порогових значень або коригування підключення апаратних компонентів.

3.7. Висновки до третього розділу

У межах третього розділу було описано програмно-апаратну реалізацію прототипу кіберфізичної системи контролю доступу на базі Arduino, RFID-зчитувача, EEPROM-пам'яті, сервоприводу, ультразвукового датчика, світлової та звукової індикації. Реалізована система забезпечує зчитування UID RFID-мітки, перевірку ідентифікатора у пам'яті, роботу з master-карткою, перехід між основними станами системи та керування механізмом доступу.

Описано програмну логіку системи, яка базується на використанні станів Waiting, DoorOpen та Registering. Це дозволило формалізувати поведінку системи, спростити обробку подій та гарантувати передбачувану реакцію на різні типи RFID-карток. Окремо розглянуто роль master-картки, яка використовується для переходу у службовий режим реєстрації нових користувачів.

Запропоновано методику експериментальної перевірки працездатності прототипу. Вона передбачає перевірку першого запуску, реєстрації карток, відкриття доступу, відмови для невідомої картки, контролю стану дверей і фіксації часу реакції системи. Така методика дозволяє оцінити як і факт

працездатності окремих модулів, так і коректність взаємодії всієї кіберфізичної системи.

Разом з тим окремі функції, характерні для повноцінних промислових систем контролю доступу, у межах даного прототипу не реалізовано. Зокрема, не було додано веб-інтерфейс адміністратора для перегляду користувачів і керування правами доступу. Це пов'язано з тим, що основною метою роботи була перевірка взаємодії апаратних модулів і базової логіки ідентифікації, а не створення окремого програмного комплексу для адміністрування.

Також у системі не реалізовано зовнішню базу даних і повноцінний журнал подій доступу. На даному етапі ідентифікатори карток зберігаються у EEPROM Arduino, чого достатньо для навчального прототипу з невеликою кількістю користувачів, проте EEPROM має обмеження за обсягом пам'яті та не дає змоги зручно зберігати розширену інформацію про користувачів, час входу, спроби несанкціонованого доступу або історію змін.

Не було реалізовано й мережевий обмін даними, наприклад через Wi-Fi або Ethernet-модуль. Причиною цього є використання Arduino UNO R3 як основної платформи, яка має обмежені ресурси пам'яті та не містить вбудованого мережевого інтерфейсу. Додавання мережевого модуля ускладнило б апаратну схему та програмну логіку, тому ця можливість розглядається як напрям подальшого вдосконалення.

Крім того, у прототипі не передбачено криптографічний захист RFID-міток і захищений обмін даними. Система орієнтована на демонстрацію принципу роботи RFID-ідентифікації та керування доступом, тому питання захисту від клонування карток, підбору ідентифікаторів або несанкціонованого втручання потребують окремого дослідження.

Отже, реалізований прототип підтверджує працездатність основної логіки кіберфізичної системи контролю доступу, однак має низку обмежень, пов'язаних із навчальним характером розробки, вибором апаратної платформи та обсягом поставлених задач. Подальший розвиток системи варто спрямувати на додавання

зовнішньої бази даних, журналу подій, веб-інтерфейсу адміністратора, мережевого модуля, резервного живлення та засобів підвищення інформаційної безпеки.

Отримані результати підтверджують можливість побудови функціонального прототипу системи контролю доступу на базі доступних апаратних компонентів. Розроблена система може бути використана як основа для подальшого розширення.

ВИСНОВКИ

У кваліфікаційній роботі виконано дослідження, проєктування та реалізацію кіберфізичної системи контролю доступу до приміщення з використанням RFID-технологій та мікроконтролерної платформи Arduino. Розроблена система поєднує апаратні засоби ідентифікації, обробку інформації, контроль фізичного стану дверей та керування виконавчим механізмом. Це дає змогу розглядати її як програмно-апаратний комплекс, у якому зчитування фізичних параметрів пов'язане з програмною логікою прийняття рішень.

У першому розділі проведено дослідження предметної області, визначено особливості кіберфізичних систем та розглянуто їх застосування у сфері контролю доступу. Проаналізовано основні способи ідентифікації користувачів, серед яких механічні ключі, PIN-коди, RFID-технології та біометричні методи. Обґрунтовано вибір RFID-технологій у поєднанні з Arduino для створення навчального та функціонального прототипу системи контролю доступу.

У другому розділі виконано проєктування системи обробки інформації. Визначено основні апаратні та програмні підсистеми, описано інформаційні потоки між ними, розглянуто структуру EEPROM-сховища та алгоритми обробки RFID-ідентифікаторів. Запропонована архітектура має модульний характер, тому окремі компоненти системи можна тестувати та вдосконалювати незалежно один від одного.

У третьому розділі описано програмно-апаратну реалізацію системи. Центральним елементом прототипу є Arduino UNO R3, який взаємодіє з RFID-зчитувачем RC522, ультразвуковим датчиком відстані, сервоприводом, RGB-світлодіодом та звуковим індикатором. Програмна частина реалізує логіку роботи системи на основі станів, тому поведінка прототипу є послідовною і зрозумілою під час очікування картки, реєстрації нового ідентифікатора або відкриття доступу.

Практичним результатом роботи є створення прототипу, який може зчитувати RFID-мітки, перевіряти права доступу, керувати механізмом відкриття, індикувати стан системи та контролювати фактичне положення дверей. Використання EEPROM дозволяє зберігати ідентифікатори карток навіть після вимкнення живлення, що є важливою умовою автономної роботи пристрою.

Розроблена система має кілька переваг: нескладну апаратну реалізацію, невисоку вартість компонентів, поділ на окремі функціональні модулі та наочний принцип роботи. Разом з тим прототип має обмеження, пов'язані з невеликим обсягом EEPROM, відсутністю криптографічного захисту RFID-міток, обмеженою кількістю користувачів та відсутністю централізованого журналу подій. Ці обмеження не знижують значення розробленого прототипу, але показують, які функції потрібно додати для його подальшого вдосконалення.

У подальшому систему можна розширити шляхом підключення Wi-Fi або Ethernet-модуля, створення веб-інтерфейсу адміністратора, використання зовнішньої бази даних, реалізації журналу подій, додавання резервного живлення, встановлення електромагнітного замка та впровадження додаткових механізмів захисту. Також перспективним є використання мобільного застосунку або хмарного сервісу для адміністрування користувачів і моніторингу стану системи.

У результаті мету кваліфікаційної роботи було досягнуто, а поставлені задачі виконано. Розроблений прототип показує, що RFID-технології, платформа Arduino та програмна логіка обробки даних можуть бути використані для автоматизації доступу до приміщення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Lee E. A. Cyber-Physical Systems: Design Challenges. 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing. Orlando, 2008. 7 p.

2. Rajkumar R., Lee I., Sha L., Stankovic J. Cyber-Physical Systems: The Next Computing Revolution. Design Automation Conference. Anaheim, 2010. 6 p.

3. Want R. An Introduction to RFID Technology. IEEE Pervasive Computing, 2006. Vol. 5, № 1. 33 p.

4. Finkenzeller K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. 3rd ed. Hoboken : John Wiley & Sons, 2010. 480 p.

5. Monk S. Programming Arduino: Getting Started with Sketches. 2nd ed. New York : McGraw-Hill Education, 2016. 176 p.

6. Margolis M. Arduino Cookbook. 3rd ed. Sebastopol : O'Reilly Media, 2020. 658 p.

7. Banzi M., Shiloh M. Getting Started with Arduino. Sebastopol : Maker Media, 2014. 130 p.

8. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. Boston : Pearson Education, 2017. 432 p.

9. ISO/IEC 18000-3:2010. Information technology. Radio frequency identification for item management. Part 3: Parameters for air interface communications at 13,56 MHz. [Чинний від 2010-11]. Вид. офіц. Geneva : ISO, 2010. 163 p.

10. Arduino Official Documentation : офіц. вебсайт. URL: https://www.arduino.cc/reference/en/ (дата звернення: 22.05.2026).

11. Конструктор Arduino. URL: https://www.circuito.io/app (дата.звернення: 7.04.2026).

12. Форум Arduino. URL: https://forum.arduino.cc/ (дата звернення: 20.04.2026).

13. Arduino + MFRC522 RFID READER. URL: https://www.instructables.com/Arduino-MFRC522-RFID-READER/ (дата звернення: 25.04.2026).

14. Arduino UNO R3 Datasheet / User manual. URL: https://docs.arduino.cc/resources/datasheets/A000066-datasheet.pdf (дата звернення: 25.04.2026).

15. MFRC522 RFID Reader Datasheet. URL: https://www.alldatasheet.com/datasheet-pdf/view/227839/NXP/MFRC522.html (дата звернення: 25.04.2026).

16. HC-SR04 Ultrasonic Sensor Datasheet. URL: https://www.alldatasheet.com/datasheet-pdf/view/1132204/ETC2/HCSR04.html (дата звернення: 25.04.2026).

17. MG90S Metal Gear Servo Datasheet. URL: https://www.alldatasheet.com/datasheet-pdf/view/1132104/ETC2/MG90S.html (дата звернення: 25.04.2026).

18. NewPing Library for Arduino. URL: https://bitbucket.org/teckel12/arduino-new-ping/wiki/Home (дата звернення: 02.05.2026).

19. Servo Library for Arduino. URL: https://github.com/arduino-libraries/Servo (дата звернення: 02.05.2026).

20. MFRC522 Library for Arduino. URL: https://github.com/miguelbalboa/rfid (дата звернення: 02.05.2026).

21. ДСТУ ISO/IEC 14443-1:2008 Картки ідентифікаційні. Картки на інтегрованих мікросхемах безконтактні. Картки близької взаємодії. Частина 1. Фізичні характеристики (ISO/IEC 14443-1:2000, IDT). [Чинний від 2010-01-01]. Вид. офіц. Київ : Держспоживстандарт України, 2013. 5 с.

22. ISO/IEC 14443-1:2018. Cards and security devices for personal identification. Contactless proximity objects. Part 1: Physical characteristics. [Чинний від 2018-04-01]. Вид. офіц. Geneva : ISO, 2018. 11 p.

23. ISO/IEC 14443-2:2020. Cards and security devices for personal identification. Contactless proximity objects. Part 2: Radio frequency power and signal interface. [Чинний від 2020-07-01]. Вид. офіц. Geneva : ISO, 2020. 47 p.

24. ISO/IEC 14443-3:2018. Cards and security devices for personal identification. Contactless proximity objects. Part 3: Initialization and anticollision. [Чинний від 2018-07-01]. Вид. офіц. Geneva : ISO, 2018. 56 p.

25. ISO/IEC 14443-4:2018. Cards and security devices for personal identification. Contactless proximity objects. Part 4: Transmission protocol. [Чинний від 2018-06-01]. Вид. офіц. Geneva : ISO, 2018. 55 p.

26. ATmega328P. 8-bit AVR Microcontroller with 32K Bytes In-System Programmable Flash : datasheet. Microchip Technology Inc., 2015. 294 p.

27. MIFARE Classic EV1 1K. Mainstream contactless smart card IC for fast and easy solution development : product data sheet. NXP Semiconductors, 2018. 36 p.

28. Alur R. Principles of Cyber-Physical Systems. Cambridge : The MIT Press, 2015. 464 p.

29. Juels A. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications. 2006. Vol. 24, № 2. 19 p.

30. De Koning Gans G., Hoepman J.-H., Garcia F. D. A Practical Attack on the MIFARE Classic. Smart Card Research and Advanced Applications : CARDIS 2008. Lecture Notes in Computer Science. Berlin : Springer, 2008. Vol. 5189. 15 p.

31. Gunes V., Peter S., Givargis T., Vahid F. A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. KSII Transactions on Internet and Information Systems. 2014. Vol. 8, № 12. 159 p.

32. Baheti R., Gill H. Cyber-Physical Systems. The Impact of Control Technology. Piscataway : IEEE Control Systems Society, 2011. 6 p.

33. Wolf W. Computers as Components: Principles of Embedded Computing System Design. 3rd ed. Burlington : Morgan Kaufmann, 2012. 786 p.

34. Barrett S. F., Pack D. J. Arduino Microcontroller Processing for Everyone!. 3rd ed. San Rafael : Morgan & Claypool Publishers, 2022. 493 p.

35. Blum J. Exploring Arduino: Tools and Techniques for Engineering Wizardry. Indianapolis : Wiley Publishing, 2019. 512 p.

36. Simson G., Beth R. RFID: Applications, Security and Privacy. Boston : Addison-Wesley, 2006. 555 p.

37. NXP Semiconductors. MF1S503x MIFARE Classic 1K : Data Sheet. Eindhoven : NXP Semiconductors, 2021. 46 p.

38. Arduino EEPROM Library : офіц. вебсайт. URL: https://docs.arduino.cc/learn/built-in-libraries/eeprom/ (дата звернення: 22.05.2026).

39. Arduino SPI Library : офіц. вебсайт. URL: https://docs.arduino.cc/learn/built-in-libraries/spi/ (дата звернення: 22.05.2026).

40. NFC Forum Technical Specifications : офіц. вебсайт. URL: https://nfc-forum.org/build/specifications (дата звернення: 22.05.2026).

41. Dobkin D. M. The RF in RFID: UHF RFID in Practice. 2nd ed. Amsterdam : Newnes, 2012. 529 p.

42. Lahiri S. RFID Sourcebook. Upper Saddle River : IBM Press, 2005. 276 p.

43. Miles S. B., Sarma S. E., Williams J. R. RFID Technology and Applications. Cambridge : Cambridge University Press, 2008. 218 p.

44. Paret D. RFID at Ultra and Super High Frequencies: Theory and Application. Chichester : John Wiley & Sons, 2009. 527 p.

45. Noergaard T. Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers. 2nd ed. Amsterdam : Newnes, 2012. 672 p.

46. Marwedel P. Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems. 3rd ed. Cham : Springer, 2018. 447 p.

47. Platzer A. Logical Foundations of Cyber-Physical Systems. Cham : Springer, 2018. 423 p.

48. Ferraiolo H., Mehta K., Ghadiali N., Mohler J., Johnson V., Brady S. Guidelines for the Use of PIV Credentials in Facility Access. NIST Special Publication 800-116, Revision 1. Gaithersburg : National Institute of Standards and Technology, 2018. 71 p.

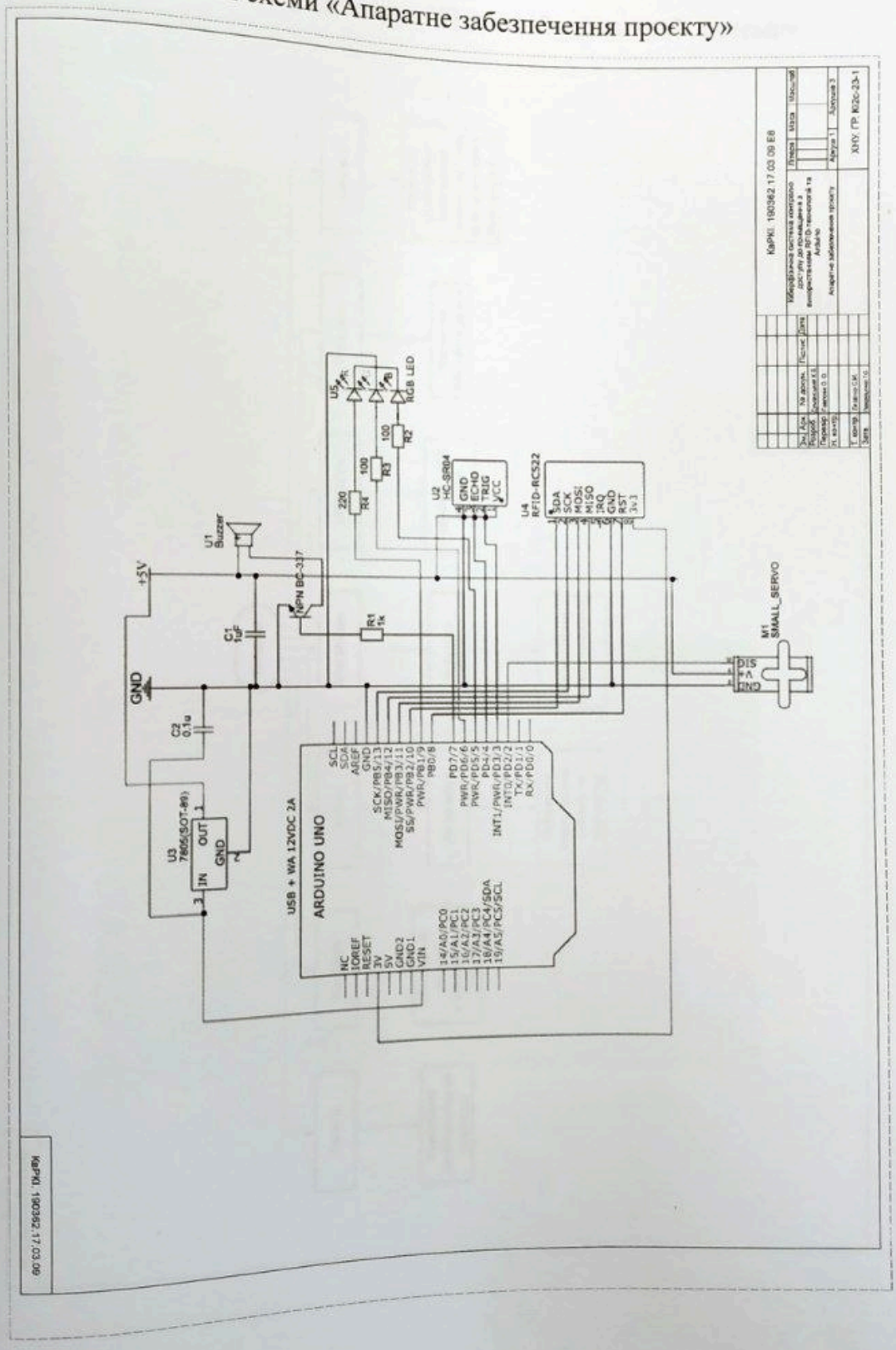
49. Zuehlke D. SmartFactory — Towards a Factory-of-Things. Annual Reviews in Control. 2010. Vol. 34, No. 1. 138 p.

50. Jazdi N. Cyber Physical Systems in the Context of Industry 4.0. IEEE International Conference on Automation, Quality and Testing, Robotics. Cluj-Napoca, 2014. 4 p.

ДОДАТОК А

(обов'язковий)

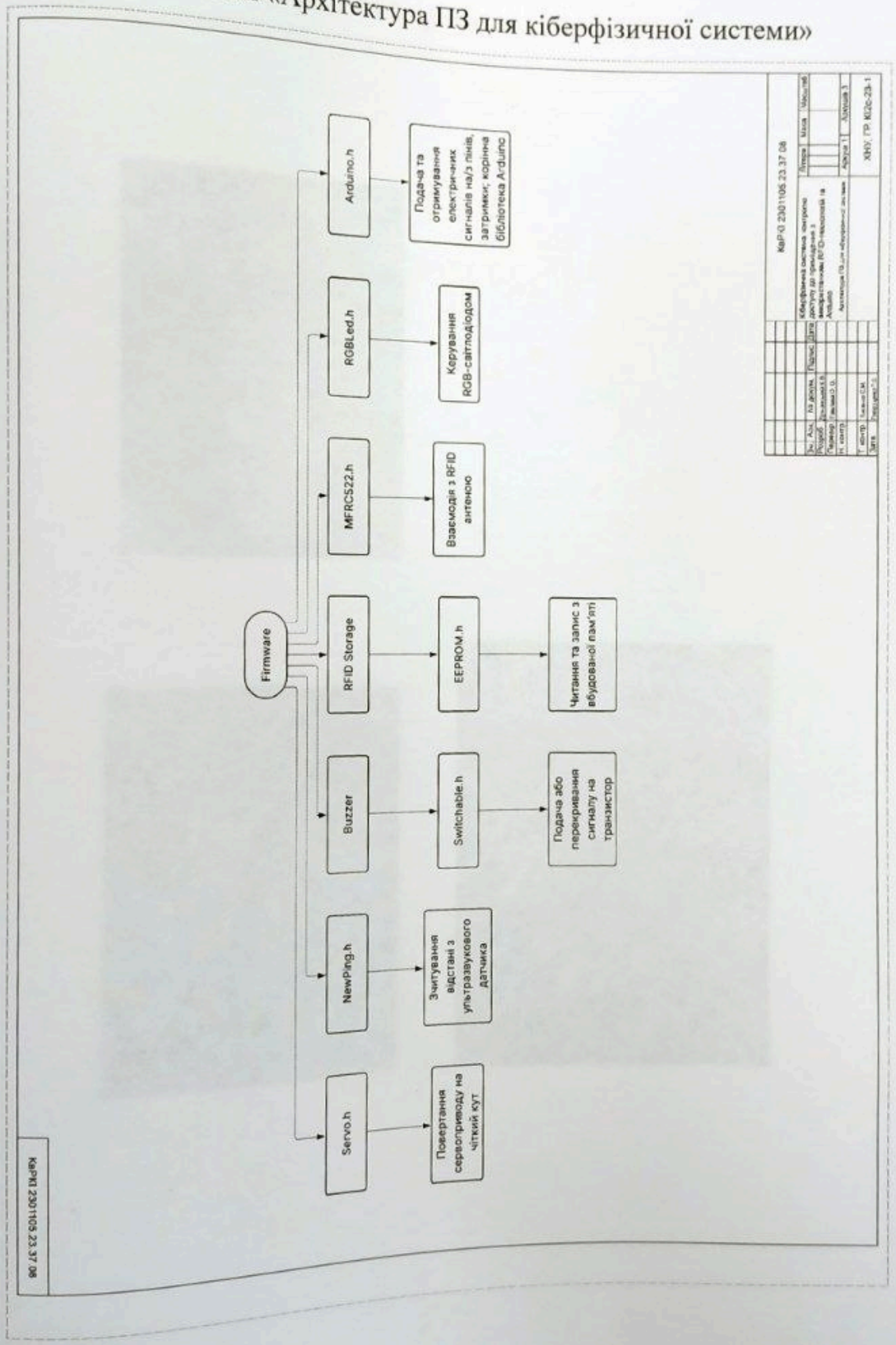
Копія схеми «Апаратне забезпечення проєкту»



ДОДАТОК Б

(обов'язковий)

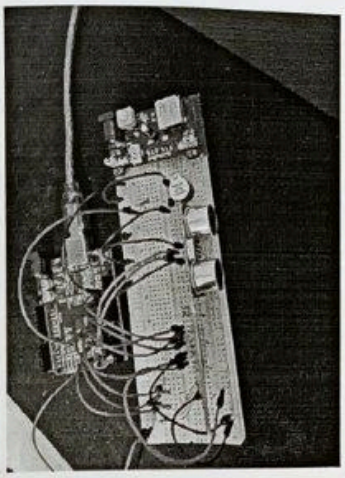
Копія схеми «Архітектура ПЗ для кіберфізичної системи»

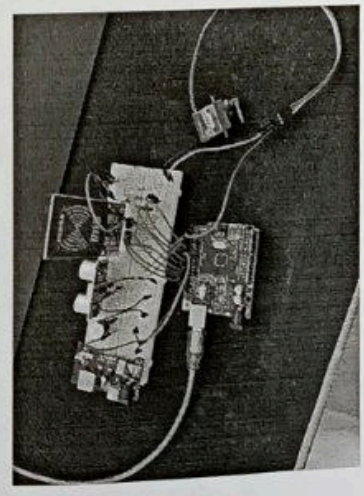


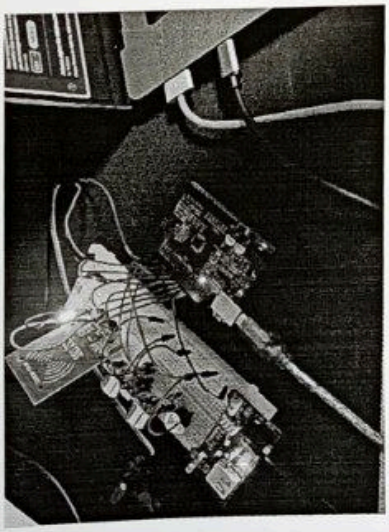
ДОДАТОК В

(обов'язковий)

Розроблений фізичний прототип кіберфізичної системи







Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Костянтин ДУМАНСЬКИЙ

Співавтор:

Назва: Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino

Експерт: Ольга ПАВЛОВА

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:4.05%

Коефіцієнт подібності 2:0.95%

Мікропробіли: 4

Заміна букв: 19

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2026-06-17 21:21:22.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-06-18 Доцент Андрій Нічепорук

Дата експерт

Wed Jun 17 22:09:42 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

	Документ		Сумарний збіг по Базі Даних	
ID: 275787 Назва: БКР Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino Додано в БД: 2026-06-17 Автора: Костянтин ДУМАНСЬКИЙ Керівники: Ольга ПАВЛОВА Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	72235	582	1733 (2%)	23 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Думанський Костянтин Володимирович

Тема: Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___55___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проектування та імплементація кіберфізичної системи контролю доступу до приміщення з використанням RFID-технологій та Arduino

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено дослідження предметної області (проаналізовано поняття кіберфізичних систем, сучасні підходи до побудови систем контролю доступу, особливості використання RFID-технологій, методи ідентифікації користувачів, а також програмно-апаратні засоби обробки інформації в системах контролю доступу) та виконано постановку задачі дослідження. В другому розділі кваліфікаційної роботи проведено проєктування кіберфізичної системи контролю доступу до приміщення з використанням RFID-технологій та Arduino, а саме: визначено апаратні та програмні підсистеми програмно-технічного засобу; розроблено структуру системи обробки інформації; визначено інформаційні потоки між апаратними і програмними компонентами; спроєктовано інформаційну модель системи; розроблено алгоритми обробки даних; обґрунтовано вибір мікроконтролерної платформи Arduino UNO R3, RFID-зчитувача MFRC522, ультразвукового датчика відстані, сервоприводу та засобів світлової і звукової індикації; розроблено апаратну структуру системи. В третьому розділі кваліфікаційної

роботи виконано програмно-апаратну реалізацію кіберфізичної системи контролю доступу до приміщення, а саме: реалізовано взаємодію мікроконтролера Arduino з RFID-зчитувачем, ультразвуковим датчиком та сервоприводом; описано процес створення бази даних RFID-міток у EEPROM-пам'яті; розроблено алгоритми роботи системи у режимах очікування, відкриття доступу та реєстрації нових карток; реалізовано програмну частину системи в середовищі Arduino IDE; виконано опис взаємодії програмної та апаратної частин системи.

4. Позитивні сторони роботи: висока практична цінність роботи, актуальність теми та реалізація працездатного програмно-апаратного прототипу системи контролю доступу.

5. Негативні сторони роботи: недостатня увага експериментальному дослідженню швидкодії та надійності роботи системи в різних умовах експлуатації.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному технічному рівні.

8. Інші зауваження: —

9. Оцінка дипломної роботи: добре (75 С)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Мазурець Олександр Вікторович, доцент кафедри комп'ютерних наук

"18" 06 2026 р. (підпис)

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Костянтин ДУМАНСЬКИЙ
ПІБ здобувача вищої освіти

ФІТ, 3 курсу, групи КІ2с-23-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1 травня 2026 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Кіберфізична система контролю доступу до приміщення з використанням RFID-технологій та Arduino
Автор Костянтин ДУМАНСЬКИЙ
Освітня програма Інформаційні системи та технології
Рівень вищої освіти перший (бакалаврський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: д.філ.н. Ольга ПАВЛОВА

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 5% і адресується до 37 першоджерела; та системою Anti-Plagiarism складає 6%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

15.12.2025

Завідувач кафедри _____ Підпис Ольга ПАВЛОВА Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Підпис Андрій НІЧЕПОРУК Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Підпис Ольга ПАВЛОВА Ім'я, ПРІЗВИЩЕ