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

КВАЛІФІКАЦІЙНА РОБОТА

Програмно-технічний засіб контролю доступу до приміщення
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 022037.22.02.69 ПЗ

Виконав здобувач IV курсу, група КІ2-22-2 _____ Анастасія КОПИЦЯК
Підпис Ініціали, прізвище

Керівник доктор філософії _____ Навло РЕГІДА
Науковий ступінь, учене звання Підпис Ініціали, прізвище

Нормоконтролер канд. фіз.-мат. наук, доц. _____ Тетяна КИСІЛЬ
Науковий ступінь, учене звання Підпис Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС _____ Ольга ПАВЛОВА
«01» 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
" 10 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Копицяк Анастасії Андріївній
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Програмно-технічний засіб контролю доступу до примішення

Керівник проекту (роботи) Регіда Павло Геннадійович, д.ф.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 20.01.2026 р. № 7

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)

Теоретичні основи досліджуваної проблеми.

Структурні частини програмно-технічного засобу контролю доступу до приміщення.

Програмно-апаратна реалізація програмно-технічного засобу контролю доступу до приміщення.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Алгоритм роботи

Схема взаємодії користувача з системою

Схема підключення компонентів

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання «_10_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2026	виконано
3	Робота над розділом 1 – теоретичні основи досліджуваної проблеми	01.03.2026	виконано
4	Робота над розділом 2 – структурні частини програмно-технічного засобу контролю доступу до приміщення	01.04.2026	виконано
5	Робота над розділом 3 – Програмно-апаратна реалізація програмно-технічного засобу контролю доступу до приміщення	29.04.2026	виконано
6	Оформлення пояснювальної записки згідно вимог	25.05.2026	виконано
7	Попередній захист ВКР	26.05.2026	виконано
8	Захист ВКР на засіданні ЕК	Червень 2026 року	

Здобувач _____ Анастасія КОПИЦЯК
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Павло РЕГІДА
Підпис Ім'я, ПРІЗВИЩЕ

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 022037.22.02.69 ПЗ	Пояснювальна записка	79		
			Графічні матеріали			
2		КвРКІ.022037.22.02.69 Е8	Алгоритм роботи	1		
3		КвРКІ.022037.22.02.69 Е8	Схема взаємодії користувача з системою	1		
4		КвРКІ.022037.22.02.69 Е8	Схема підключення компонениів	1		

КвРКІ 022037.22.02.69 ВП

Зм	Арк	№ докум	Підпис	Дата
Розробив		Копицяк		
Перевір.		Регіда		
Н. контр.		Кисіль		
Затв.		Павлова		9.06

Відомість проекту

Літера	Аркуш	Аркушів
У	1	79

ХНУ, КІ2-22-2

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Програмно-технічний засіб контролю доступу до приміщення».

Автор роботи: Анастасія КОПИЦЯК.

Керівник роботи: Павло РЕГІДА.

Пояснювальна записка: 79 с., 30 рис., 10 табл., 4 дод., 50 джерел.

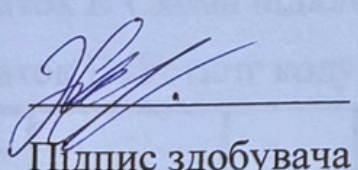
Графічна частина: 3 креслення.

ARDUINO UNO, RFID, PIN-КОД, АВТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, МІКРОКОНТРОЛЕР, СЕРВОПРИВІД.

Кваліфікаційна робота присвячена розробленню програмно-технічного засобу контролю доступу до приміщення на базі мікроконтролерної платформи Arduino Uno. У роботі розглянуто принципи побудови систем контролю доступу, проаналізовано промислові та автономні рішення, обґрунтовано вибір апаратних компонентів і розроблено структуру пристрою.

Розроблений засіб реалізує двофакторну автентифікацію користувача за RFID-карткою та PIN-кодом. До складу системи входять RFID-зчитувач RC522, матрична клавіатура 4x4, LCD-дисплей 16x2 з I2C-інтерфейсом, сервопривід та світлодіоди для індикації стану. Програмна логіка забезпечує перевірку RFID-ідентифікатора, введення PIN-коду, надання або заборону доступу та тимчасове блокування після трьох невдалих спроб.

Моделювання та тестування пристрою виконано у середовищі Wokwi. Результати підтвердили працездатність розробленої системи, коректну роботу двофакторної автентифікації, виконавчого механізму, LCD-дисплея та світлової індикації.



Підпис здобувача

30.05.2026

Дата

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасних умовах питання безпеки приміщень є важливим для офісів, навчальних лабораторій, службових і складських приміщень. Для обмеження доступу сторонніх осіб використовують системи контролю доступу, які автоматизують перевірку користувача та керування виконавчим механізмом.

Звичайні механічні ключі не завжди є зручними та надійними, оскільки їх можна загубити, передати іншій особі або скопіювати. Тому доцільним є використання електронних засобів доступу, зокрема RFID-карток і PIN-кодів. Однак застосування лише одного способу перевірки має недоліки: картку можна втратити, а код – підглянути або розголосити. Саме тому в роботі використано комбіновану автентифікацію, яка передбачає послідовну перевірку RFID-картки та PIN-коду.

Метою кваліфікаційної роботи є розроблення програмно-технічного засобу контролю доступу до приміщення з використанням RFID-картки та PIN-коду. У роботі розглянуто принципи роботи систем контролю доступу, проаналізовано існуючі рішення, обґрунтовано вибір компонентів, розроблено структуру пристрою, алгоритм його роботи та виконано моделювання системи.

Об’єктом дослідження є процес контролю доступу до приміщення. Предметом дослідження є програмно-технічний засіб контролю доступу з використанням RFID-картки та PIN-коду.

Практичне значення роботи полягає у створенні моделі автономної системи контролю доступу, яка забезпечує перевірку користувача, керування виконавчим механізмом, відображення стану системи та блокування після невдалих спроб доступу.

1 ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖУВАНОЇ ПРОБЛЕМИ

1.1 Системи контролю доступу: актуальність, принцип функціонування та класифікація

У сучасних умовах підвищення вимог до безпеки об’єктів різного призначення системи контролю доступу (СКД) є необхідним елементом технічного захисту. Вони забезпечують обмеження несанкціонованого проникнення, захист матеріальних цінностей, інформації та персоналу [1]. Традиційні засоби організації пропускного режиму, що базуються на механічних ключах або візуальному контролі, не відповідають сучасним вимогам надійності та керованості.

Автоматизовані СКД реалізують процедури ідентифікації користувачів, перевірки їхніх повноважень та керування виконавчими механізмами блокування [1, 2]. Крім обмеження доступу, такі системи дозволяють фіксувати події, централізовано керувати правами користувачів та інтегруватися з іншими підсистемами безпеки.

Рисунок 1.1 – Приклад сучасної електронної системи контролю доступу до приміщення

На рисунку 1.1 наведено приклад сучасної електронної системи контролю доступу, інтегрованої безпосередньо у дверну конструкцію.

Сучасні рішення поєднують декілька способів ідентифікації, зокрема введення PIN-коду, використання електронних ключів або безконтактних ідентифікаторів [2, 3]. З метою підвищення рівня безпеки все частіше застосовується багатофакторна автентифікація, що передбачає підтвердження двох незалежних ознак доступу [4].

Розвиток мікроконтролерної техніки дозволяє створювати доступні автономні системи контролю доступу без використання складної серверної інфраструктури [5, 6]. Це особливо актуально для невеликих об’єктів та навчальних проєктів, де важливо забезпечити оптимальне співвідношення функціональності, складності реалізації та вартості.

Таким чином, розробка автономного програмно-технічного засобу контролю доступу з комбінованою ідентифікацією є актуальною та відповідає сучасним тенденціям розвитку систем безпеки.

Система контролю доступу (СКД) – це сукупність апаратних і програмних засобів, призначених для регламентування доступу користувачів до визначених приміщень або зон шляхом ідентифікації особи, перевірки її повноважень та керування виконавчими механізмами [1]. Основною метою функціонування такої системи є обмеження несанкціонованого доступу та забезпечення контрольованого середовища перебування в межах об’єкта.

Функціонування СКД базується на послідовному виконанні декількох етапів [1, 2]. Спочатку здійснюється зчитування ідентифікаційної ознаки користувача за допомогою пристрою введення (клавіатури, RFID-зчитувача або іншого засобу). Отримані дані передаються до контролера, який виконує їх обробку та порівняння з попередньо збереженими значеннями. У разі підтвердження прав доступу формується керуючий сигнал на виконавчий механізм, що забезпечує відкриття дверей або розблокування проходу. У

випадку невідповідності система блокує доступ та формує відповідний сигнал індикації.

Система складається з блоку введення (RFID-зчитувач та клавіатура для введення PIN-коду), блоку контролю та управління на базі мікроконтролера Arduino, блоку виконавчих пристроїв та блоку індикації. Мікроконтролер виконує перевірку ідентифікаційних даних, реалізує алгоритм доступу та формує сигнали керування виконавчим механізмом і пристроями індикації. Зберігання дозволених ідентифікаторів і параметрів роботи здійснюється у внутрішній пам’яті контролера.

Структурно будь-яка система контролю доступу включає такі основні компоненти: пристрій ідентифікації, контролер, виконавчий механізм та модуль індикації. У промислових рішеннях контролер може бути окремим спеціалізованим пристроєм або частиною мережевої інфраструктури, тоді як в автономних системах його функції виконує програмований мікроконтролер.

Залежно від архітектури системи контролю доступу поділяються на автономні та мережеві. Автономні системи зберігають інформацію у пам’яті контролера та не потребують підключення до серверної інфраструктури, що робить їх доцільними для невеликих об’єктів. Мережеві рішення забезпечують централізоване адміністрування та ведення журналів подій, проте характеризуються більшою складністю реалізації.

У сучасних системах все частіше застосовується багатофакторна автентифікація, зокрема поєднання RFID-карти та PIN-коду, що підвищує рівень захищеності та зменшує ризик несанкціонованого доступу.

Отже, система контролю доступу є програмно-технічним рішенням, яке поєднує апаратні компоненти та алгоритмічну логіку для забезпечення регламентованого доступу до приміщень.

Сучасні системи контролю доступу відрізняються за способом ідентифікації користувача, архітектурою побудови, способом передавання даних та рівнем функціональної складності.

За способом ідентифікації розрізняють кодові, радіочастотні (RFID), біометричні та комбіновані системи. Кодонабірні системи базуються на введенні секретного PIN-коду та відзначаються простотою реалізації, однак мають обмежений рівень захищеності. Радіочастотні системи використовують електронні мітки з унікальним ідентифікатором, що забезпечує зручність і швидкість доступу, проте існує ризик втрати або копіювання картки [3, 7]. Біометричні системи застосовують фізіологічні характеристики людини (відбиток пальця, обличчя) та забезпечують високий рівень достовірності, але потребують складнішої апаратної реалізації.

Найбільш ефективними є комбіновані системи, що реалізують багатофакторну автентифікацію, наприклад поєднання RFID-карти та PIN-коду [4, 8]. Такий підхід дозволяє суттєво підвищити рівень безпеки за рахунок підтвердження декількох незалежних факторів.

За архітектурою побудови системи поділяються на автономні та мережеві. Автономні системи функціонують без центрального сервера та зберігають дані у пам’яті локального контролера. Вони доцільні для невеликих об’єктів і характеризуються простотою реалізації. Мережеві системи забезпечують централізоване адміністрування, ведення журналів подій та інтеграцію з іншими підсистемами безпеки, проте потребують складнішої інфраструктури.

За способом передавання даних виділяють провідні, бездротові та гібридні рішення. Провідні системи відзначаються надійністю, бездротові — простотою монтажу, а гібридні поєднують обидва підходи.

За рівнем функціональної складності системи можуть бути базовими (лише керування виконавчим механізмом), середнього рівня (облік користувачів та реєстрація подій) та комплексними (інтеграція з іншими системами безпеки).

Таким чином, вибір конкретного типу системи залежить від умов експлуатації та вимог до рівня захисту. Для невеликих об’єктів доцільним є використання автономних рішень із комбінованою ідентифікацією, що забезпечують достатній рівень безпеки при помірній складності реалізації.

1.2 Аналіз промислових систем контролю доступу

Сучасний ринок систем контролю доступу представлений різноманітними промисловими рішеннями, що відрізняються архітектурою, функціональністю та вартістю впровадження. Найбільш поширеними є системи компаній BOLID, PERCo, Hikvision та ZKTeco, які широко застосовуються на підприємствах, у бізнес-центрах та державних установах.

Система контролю доступу на базі комплексу «Оріон» компанії BOLID є прикладом масштабованого мережевого рішення з централізованим керуванням. Архітектура передбачає використання контролерів доступу, зчитувачів ідентифікаторів та серверного програмного забезпечення. Система підтримує керування електрозамками, турнікетами та інтеграцію з відеоспостереженням, охоронною і пожежною сигналізацією [9].

Перевагами такого рішення є висока функціональність та можливість побудови комплексної системи безпеки. Водночас впровадження потребує значних фінансових витрат, серверної інфраструктури та кваліфікованого технічного супроводу.

У складі таких систем контролер виконує роль центрального елемента, який приймає дані від зчитувачів, перевіряє права користувача та формує керуючий сигнал для виконавчого механізму. Саме через контролер здійснюється зв’язок між засобами ідентифікації, програмним забезпеченням і пристроями блокування доступу. У мережевих рішеннях контролер також забезпечує обмін даними із сервером, передавання інформації про події доступу та виконання команд адміністрування.

Для системи BOLID С2000-2 характерним є використання спеціалізованого контролера, призначеного для роботи у складі комплексної системи безпеки. Такий пристрій може обслуговувати точки проходу, взаємодіяти зі зчитувачами ідентифікаторів та керувати виконавчими пристроями [10]. Це дозволяє будувати більш складні системи контролю

доступу, однак водночас підтверджує, що подібне рішення орієнтоване переважно на об’єкти з розгалуженою інфраструктурою.

Зовнішній вигляд типового контролера BOLID C2000-2 наведено на рисунку 1.3.

Рисунок 1.3 – Контролер системи контролю доступу BOLID C2000-2

Як видно з рисунка 1.3, контролер BOLID C2000-2 є спеціалізованим пристроєм для керування точками доступу. Його застосування доцільне у складі повноцінної промислової системи, однак для автономного контролю доступу до одного приміщення таке рішення є надлишковим.

Системи контролю доступу PERCo широко застосовуються для організації пропускного режиму на підприємствах різного масштабу, у бізнес-центрах та адміністративних установах. Рішення компанії орієнтовані на інтеграцію з

турнікетами, електронними проходними та підсистемами обліку робочого часу, що дозволяє реалізувати комплексний підхід до контролю переміщення персоналу та відвідувачів. Архітектура систем PERCo передбачає використання мережевих контролерів, централізованого програмного забезпечення та бази даних користувачів, у якій зберігається інформація про права доступу та події проходу [11].

Система підтримує RFID-карти, електронні брелоки та PIN-код, що забезпечує гнучке налаштування прав доступу. Рішення PERCo відзначаються надійністю, можливістю масштабування та інтеграції з іншими системами безпеки.

Водночас їх впровадження потребує складного налаштування, мережевої інфраструктури та значних фінансових витрат.

Рисунок 1.4 – Турнікет із системою контролю доступу PERCo

На рисунку 1.4 показано приклад турнікета, який може використовуватися як виконавчий пристрій у системах PERCo. Такі рішення орієнтовані на контроль потоків людей у місцях із великою кількістю користувачів, тому для задачі контролю доступу до одного приміщення вони є функціонально надлишковими.

Компанія Hikvision, відома рішеннями у сфері відеоспостереження, також розробляє мережеві системи контролю доступу, що інтегруються в єдину інфраструктуру безпеки. Пристрої підтримують RFID-карти, PIN-коди та біометричну ідентифікацію, забезпечуючи централізоване адміністрування через IP-мережу [12].

Архітектура передбачає підключення терміналів до локальної мережі з передачею даних на сервер або в хмарний сервіс. Це дозволяє вести журнал подій, здійснювати віддалене налаштування прав доступу та інтеграцію з відеоспостереженням і сигналізацією.

Водночас такі системи потребують розвиненої мережевої інфраструктури та належного кіберзахисту, що ускладнює їх використання в автономних умовах.

Рисунок 1.5 – Термінал системи контролю доступу Hikvision.

На рисунку 1.5 наведено приклад термінала Hikvision, який поєднує кілька способів ідентифікації користувача. Такі пристрої забезпечують розширені можливості контролю доступу, однак їх використання передбачає наявність мережевої інфраструктури та відповідного адміністрування.

Системи контролю доступу компанії ZKTeco спеціалізуються на використанні біометричних технологій, зокрема ідентифікації за відбитком пальця та розпізнавання обличчя. Такі рішення забезпечують високий рівень достовірності автентифікації користувачів і часто застосовуються у поєднанні з функціями обліку робочого часу [13]. Архітектура системи передбачає використання спеціалізованих терміналів із вбудованими алгоритмами обробки біометричних даних, а також можливість інтеграції з централізованим програмним забезпеченням для адміністрування прав доступу та ведення журналу подій.

Основними перевагами біометричних систем є підвищений рівень безпеки та зручність для користувача, оскільки відсутня необхідність використання фізичних ідентифікаторів, які можуть бути втрачені або передані третім особам. Водночас такі рішення характеризуються більшою вартістю, складністю налаштування та підвищеними вимогами до продуктивності апаратної частини й захисту персональних даних.

Рисунок 1.6 – Біометричний термінал системи контролю доступу ZKTeco

На рисунку 1.6 подано біометричний термінал ZKTeco, який призначений для ідентифікації користувачів за біометричними ознаками. Такі системи забезпечують високий рівень достовірності перевірки, проте мають більшу вартість і складнішу апаратно-програмну реалізацію порівняно з автономними мікроконтролерними засобами.

Проведений аналіз свідчить, що промислові системи контролю доступу орієнтовані насамперед на побудову масштабованих мережевих комплексів із централізованим керуванням та інтеграцією з іншими підсистемами безпеки. Вони забезпечують розширений функціонал, включаючи ведення журналів подій, гнучке адміністрування прав доступу та можливість віддаленого моніторингу. Разом із тим їх впровадження супроводжується значними фінансовими витратами, потребує розвиненої інфраструктури та кваліфікованого технічного супроводу.

Для невеликих об’єктів або навчальних проєктів застосування повноцінних промислових систем є економічно недоцільним. У таких випадках більш раціональним є використання мікроконтролерних рішень, які дозволяють реалізувати основні функції контролю доступу з мінімальними витратами та без необхідності створення серверної інфраструктури.

Проведений аналіз промислових і мікроконтролерних систем контролю доступу дозволяє здійснити їх узагальнене порівняння за такими критеріями, як вартість реалізації, рівень безпеки, масштабованість, складність впровадження та потреба в додатковій інфраструктурі.

Промислові системи (BOLID, PERCo, Hikvision, ZKTeco) орієнтовані на побудову мережевих комплексів із централізованим керуванням. Вони забезпечують розширене адміністрування, інтеграцію з відеоспостереженням і сигналізацією, ведення журналів подій та масштабування на значну кількість точок доступу. Водночас їх впровадження потребує значних фінансових витрат, серверної інфраструктури та спеціалізованого обслуговування, що робить їх недоцільними для невеликих об’єктів.

Мікроконтролерні системи на базі Arduino відзначаються нижчою вартістю та простотою реалізації [14]. Вони забезпечують базові функції контролю доступу без складної інфраструктури та є достатніми для одного або кількох приміщень. Рівень безпеки залежить від способу ідентифікації, при цьому двофакторна автентифікація суттєво підвищує захищеність системи.

Платформа ESP32 має більші обчислювальні можливості та підтримує бездротовий зв'язок, що дозволяє створювати мережеві рішення з віддаленим адмініструванням [15]. Однак для автономної системи такі можливості є надлишковими та ускладнюють реалізацію.

Узагальнені результати порівняння наведено в таблиці 1.1.

Таблиця 1.1 – Порівняльна характеристика систем контролю доступу

Критерій	BOLID	PERCo	Hikvision	ZKTeco	Arduino	ESP32
Тип системи	Мережева	Мережева	Мережева	Біометрична/мережева	Автономна	Автономна/мережева
Метод ідентифікації	RFID, PIN	RFID, PIN	RFID, біометрія	Біометрія, RFID	RFID, PIN	\RFID, PIN, мережа
Рівень безпеки	Високий	Високий	Високий	Дуже високий	Середній / Високий (комб.)	Високий
Масштабованість	Висока	Висока	Висока	Середня	Низька	Середня
Необхідність серверу	Так	Так	Так	Так	Ні	Опційно
Складність монтажу	Висока	Висока	Висока	Висока	Низька	Середня
Вартість впровадження	Висока	Висока	Висока	Висока	Низька	Середня

Кінець таблиці 1.1

Доцільність для 1 приміщення	Низька	Низька	Низька	Низька	Висока	Середня
Гнучкість програмування	Обмежена	Обмежена	Обмежена	Обмежена	Висока	Висока

Як видно з таблиці 1.2, промислові системи забезпечують максимальну функціональність та масштабованість, однак характеризуються високою вартістю впровадження і складністю монтажу. Їх використання є виправданим для великих об’єктів із розгалуженою структурою та необхідністю централізованого адміністрування доступу. Для задачі контролю доступу до одного приміщення такі рішення є надлишковими.

Мікроконтролерні системи на базі Arduino забезпечують оптимальний баланс між функціональністю, рівнем безпеки та простотою реалізації. Використання комбінованої моделі ідентифікації RFID + PIN дозволяє підвищити рівень захисту до значень, достатніх для автономної системи малого масштабу. Платформа ESP32 є перспективною для створення мережевих або інтегрованих систем, проте її застосування доцільне лише за наявності вимог до віддаленого керування або інтеграції з іншими інформаційними середовищами.

З урахуванням поставленої мети розробки автономного програмно-технічного засобу контролю доступу до приміщення з комбінованою ідентифікацією користувачів найбільш обґрунтованим є використання платформи Arduino. Вона забезпечує необхідні апаратні ресурси для підключення RFID-зчитувача, клавіатури введення коду, індикаторів стану та виконавчого механізму, дозволяє реалізувати алгоритм двофакторної автентифікації й функцію блокування після кількох невдалих спроб доступу, а також характеризується простотою програмування та надійністю роботи.

Таким чином, проведений порівняльний аналіз підтверджує доцільність вибору автономної мікроконтролерної архітектури з використанням платформи Arduino та комбінованого методу ідентифікації RFID + PIN-код, що створює основу для подальшого проектування системи в наступному розділі роботи.

1.3 Приклади рішень контролю доступу

Поряд із промисловими системами контролю доступу, які застосовуються на великих підприємствах і багатофункціональних об’єктах, існують рішення, призначені для організації доступу до окремих приміщень, офісів, навчальних лабораторій, складських кімнат або службових зон. Такі пристрої є ближчими до теми даної роботи, оскільки орієнтовані на автономну роботу, перевірку користувача безпосередньо на місці встановлення та керування виконавчим механізмом без обов’язкового використання серверної інфраструктури.

Системи контролю доступу такого типу, як правило, поєднують кілька функціональних блоків: контролер, засіб ідентифікації користувача, пристрій введення коду, індикатори стану та виконавчий механізм. Саме така логіка побудови є характерною і для розроблюваного у даній роботі програмно-технічного засобу контролю доступу до приміщення.

Одним із прикладів таких рішень є обладнання SEVEN Systems. У межах цієї торгової марки пропонуються готові комплекти контролю доступу, а також окремі компоненти для побудови автономних систем: контролери, безконтактні зчитувачі, клавіатури, виконавчі пристрої та допоміжні елементи [16]. Такі комплекти можуть використовуватися в офісних, складських та службових приміщеннях і забезпечують керування доступом користувачів без складної централізованої інфраструктури. Для теми даної роботи такі рішення є важливими, оскільки демонструють практичний приклад автономної системи, у якій перевірка ідентифікаційних даних і формування керуючого сигналу відбуваються безпосередньо на місці встановлення.

Рисунок 1.7 – Приклад рішення контролю доступу SEVEN Systems

На рисунку 1.7 показано приклад комплекту SEVEN Systems, у якому поєднано елементи ідентифікації користувача та виконавчий механізм. Такий тип рішення демонструє практичну реалізацію автономного контролю доступу до окремого приміщення. Його перевагою є те, що основні елементи системи можуть працювати локально, без обов'язкового підключення до серверного програмного забезпечення.

Іншим прикладом є рішення ВАРТА, які застосовуються для організації автономного доступу до приміщень за допомогою безконтактних ідентифікаторів. Пристрої цього типу підтримують роботу з RFID-ідентифікаторами та передають отримані дані до контролера для подальшої перевірки [17]. Такі зчитувачі можуть використовуватися у складі простих систем доступу, де основним завданням є швидке розпізнавання користувача та передавання ідентифікаційного коду до блока керування.

На рисунку 1.8 наведено приклад зчитувача для системи контролю доступу ВАРТА.

Рисунок 1.8 – Приклад зчитувача системи контролю доступу ВАРТА

На рисунку 1.8 наведено приклад зчитувача ВАРТА, який використовується для безконтактної ідентифікації користувача. Основна роль такого пристрою полягає у зчитуванні RFID-ідентифікатора та передаванні отриманих даних до контролера системи.

Окрему групу рішень становить обладнання ATIS, до якої належать зчитувачі безконтактних карт, кодові клавіатури, автономні контролери та комбіновані пристрої, що поєднують кілька способів ідентифікації користувача [18]. Саме такі комбіновані рішення є особливо близькими до теми даної дипломної роботи, оскільки дозволяють реалізувати доступ за RFID-ідентифікатором, PIN-кодом або поєднанням цих методів [18, 19]. Наявність кількох способів автентифікації дає змогу підвищити рівень безпеки та наблизити реальні ринкові рішення до концепції розроблюваного програмно-технічного засобу. На рисунку 1.9 наведено приклад пристрою контролю доступу ATIS. Пристрій поєднує засіб введення коду та елементи індикації стану, що дозволяє використовувати його для організації доступу до окремого приміщення. Такий тип обладнання є близьким до теми даної роботи, оскільки передбачає локальну перевірку користувача та формування сигналу дозволу або заборони доступу.

Рисунок 1.9 – Приклад рішення контролю доступу ATIS

На рисунку 1.9 показано пристрій ATIS, який поєднує засіб введення коду та елементи індикації. Такі рішення є найбільш близькими до теми даної роботи, оскільки передбачають можливість використання декількох способів ідентифікації користувача.

Розглянуті приклади рішень контролю доступу мають спільну функціональну основу. У їхній структурі передбачено блок керування, засоби ідентифікації користувача, пристрої введення або зчитування даних, засоби індикації стану та виконавчий механізм. Такий принцип побудови відповідає загальній логіці систем контролю доступу, у яких спочатку здійснюється перевірка користувача, після чого формується сигнал дозволу або заборони доступу.

Рішення SEVEN Systems демонструє приклад комплексного підходу, коли в одному комплекті можуть поєднуватися пристрій введення коду, зчитувач і виконавчий механізм. Таке рішення є зручним для організації доступу до окремого приміщення, оскільки не потребує складної інфраструктури та орієнтоване на автономну роботу.

Рішення ВАРТА є прикладом використання безконтактної ідентифікації користувача. Основний акцент у такому випадку зроблено на RFID-ідентифікаторі, який дозволяє швидко виконати перевірку користувача без введення додаткових даних. Такий підхід є зручним, однак використання лише одного фактора ідентифікації має певні обмеження щодо рівня захищеності.

Обладнання ATIS є найбільш близьким до теми даної роботи, оскільки серед таких пристроїв поширені рішення, що поєднують декілька способів ідентифікації, зокрема RFID-картку та PIN-код. Саме комбінований спосіб перевірки користувача дозволяє підвищити рівень безпеки, оскільки для отримання доступу недостатньо лише мати фізичний ідентифікатор або лише знати код.

Для узагальнення характеристик розглянутих прикладів доцільно подати порівняльну таблицю.

Таблиця 1.2 – Порівняльна характеристика розглянутих рішень контролю доступу

Рішення	Тип рішення	Основні особливості
SEVEN Systems	Комплекти та окремі компоненти контролю доступу	Поєднання контролера, засобу ідентифікації та виконавчого механізму
ВАРТА	Контролери та зчитувачі ідентифікаторів	Робота з RFID-ідентифікаторами, передавання даних до контролера, керування виконавчим механізмом
ATIS	Зчитувачі, кодові клавіатури, контролери та комбіновані пристрої	Підтримка RFID, PIN-коду та поєднання кількох способів автентифікації

Як видно з таблиці 1.2, розглянуті рішення мають спільну мету — забезпечення контрольованого доступу до приміщення, однак відрізняються

способом ідентифікації користувача та рівнем функціональності. Найпростішими є рішення, що використовують лише RFID-ідентифікатор або лише кодове введення. Вони зручні в експлуатації, проте мають обмежений рівень захисту, оскільки фізичний ідентифікатор може бути втрачений або переданий іншій особі, а PIN-код – підглянутий чи розголошений.

Більш доцільним для підвищення рівня захищеності є застосування комбінованої автентифікації, за якої користувач повинен підтвердити право доступу двома способами. У межах даної роботи таким підходом є поєднання RFID-картки та PIN-коду. RFID-картка підтверджує наявність фізичного ідентифікатора, а PIN-код – знання персонального коду доступу. Це зменшує ризик несанкціонованого проходу у випадку втрати картки або розголошення коду.

Порівняння розглянутих рішень показує, що для задачі контролю доступу до одного приміщення недоцільно застосовувати складні мережеві комплекси з централізованим адмініструванням. Достатнім є автономний програмно-технічний засіб, який виконує перевірку користувача безпосередньо на місці встановлення, керує виконавчим механізмом і забезпечує індикацію стану системи.

Отже, аналіз розглянутих рішень підтверджує доцільність розроблення автономного програмно-технічного засобу контролю доступу до приміщення. Найбільш обґрунтованим для даної роботи є використання комбінованої автентифікації RFID + PIN-код, оскільки вона поєднує зручність безконтактної ідентифікації з додатковим рівнем перевірки користувача. Саме цей підхід покладено в основу подальшого розроблення структури та алгоритму роботи пристрою.

2 СТРУКТУРНІ ЧАСТИНИ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

2.1 Обґрунтування структури програмно-технічного засобу контролю доступу

На основі проведеного в першому розділі аналізу існуючих промислових, локальних та мікроконтролерних систем контролю доступу встановлено, що для невеликих об’єктів із обмеженою кількістю користувачів найбільш доцільним є застосування автономного програмно-технічного засобу з локальною обробкою даних [20]. Промислові мережеві рішення забезпечують високий рівень функціональності та масштабованості, однак їх використання пов’язане зі значними фінансовими витратами, необхідністю створення серверної інфраструктури та складністю адміністрування. У межах поставленої задачі, що передбачає організацію контролю доступу до одного приміщення, застосування таких систем є надлишковим.

Розроблюваний програмно-технічний засіб призначений для організації контрольованого доступу до приміщення з використанням комбінованої ідентифікації користувача. Основною особливістю системи є застосування двох факторів автентифікації: RFID-картки та PIN-коду [21]. Доступ надається лише у випадку, якщо користувач спочатку пред’явив дозволений RFID-ідентифікатор, а потім ввів правильний персональний код. Такий підхід дозволяє підвищити рівень захищеності системи, оскільки використання лише одного способу ідентифікації не забезпечує достатнього захисту.

Використання тільки PIN-коду пов’язане з ризиком його компрометації, зокрема через підглядання, передачу іншій особі або підбір. Використання лише RFID-картки також має певні недоліки, оскільки фізичний ідентифікатор може бути втрачений, переданий сторонній особі або скопійований. Поєднання RFID-картки та PIN-коду дозволяє зменшити ці ризики, оскільки для отримання доступу необхідно одночасно мати фізичний ідентифікатор і знати персональний код [21].

Структурно програмно-технічний засіб контролю доступу складається з таких основних блоків:

1) блоку керування;
2) блоку RFID-ідентифікації;
3) блоку введення PIN-коду;
4) блоку відображення інформації;
5) виконавчого механізму;
6) блоку світлової індикації.

Блок керування реалізовано на базі мікроконтролерної плати Arduino Uno [22]. Він виконує обробку даних, отриманих від RFID-зчитувача та клавіатури, порівнює їх із заданими значеннями та формує керуючі сигнали для виконавчого механізму, LCD-дисплея та засобів світлової індикації.

Блок RFID-ідентифікації забезпечує зчитування унікального ідентифікатора картки користувача. Він є першим етапом автентифікації, оскільки саме RFID-картка підтверджує наявність фізичного ідентифікатора доступу. Блок введення PIN-коду реалізує другий етап перевірки користувача та дозволяє підтвердити право доступу за допомогою персонального коду.

Блок відображення інформації призначений для виведення повідомлень про поточний стан системи. За допомогою LCD-дисплея користувач отримує підказки щодо необхідності піднесення RFID-картки, введення PIN-коду, а також повідомлення про дозвіл, заборону доступу або тимчасове блокування системи. Блок світлової індикації доповнює текстові повідомлення та дозволяє швидко визначити результат автентифікації: зелений світлодіод сигналізує про надання доступу, а червоний – про помилку або блокування.

У ролі виконавчого механізму в моделі використовується сервопривід. Він змінює своє положення після успішного проходження двох етапів автентифікації та імітує фізичне відкриття доступу до приміщення. У реальній апаратній реалізації замість сервоприводу може застосовуватися релейний модуль для керування електромагнітним або електромеханічним виконавчим пристроєм. У

межах моделювання сервопривід є доцільним, оскільки дозволяє наочно продемонструвати результат роботи алгоритму доступу без використання додаткового силового обладнання.

Узагальнена структурна схема програмно-технічного засобу контролю доступу до приміщення наведена на рисунку 2.1.

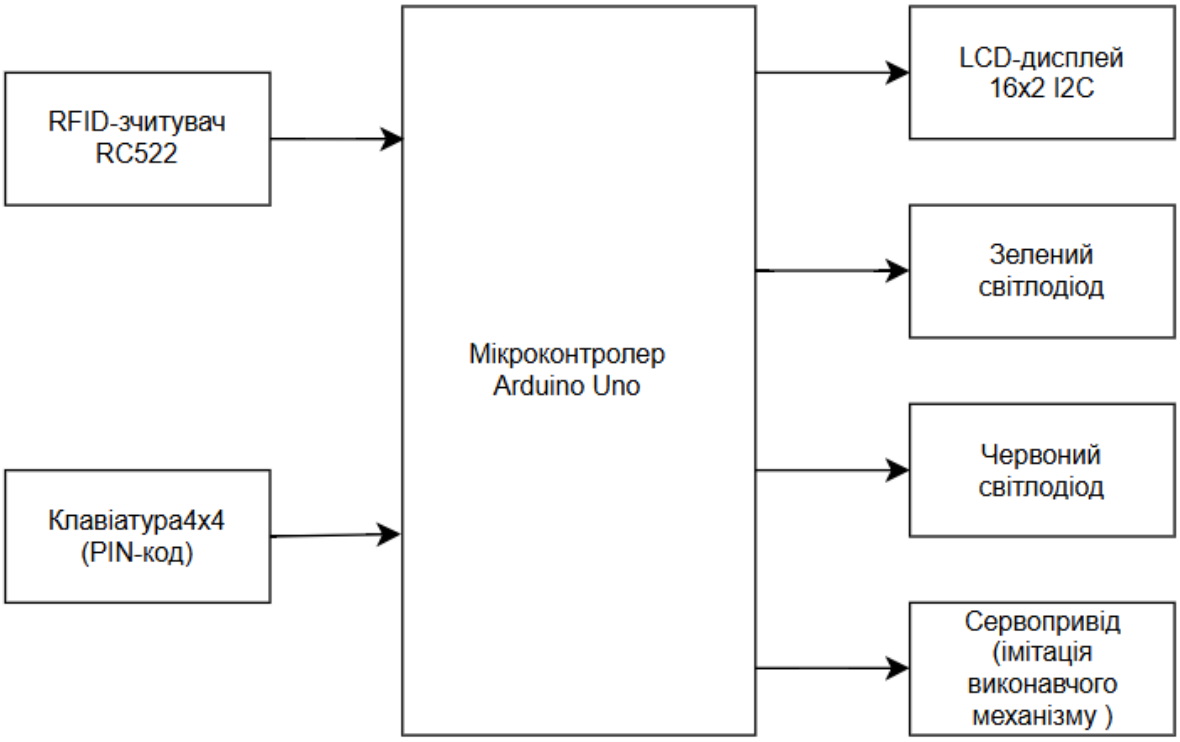


Рисунок 2.1 – Структурна схема програмно-технічного засобу контролю доступу до приміщення

Згідно зі структурною схемою, усі основні компоненти системи взаємодіють через мікроконтролер Arduino Uno. RFID-зчитувач передає до мікроконтролера UID-код картки, клавіатура – введений PIN-код, LCD-дисплей відображає поточний стан системи, а світлодіоди сигналізують про результат перевірки. У разі успішного проходження двофакторної автентифікації Arduino Uno формує керуючий сигнал на сервопривід, який переходить у положення відкриття доступу. Якщо RFID-картка або PIN-код не відповідають заданим

значенням, виконавчий механізм залишається у початковому стані, а система інформує користувача про відмову.

Таким чином, обрана структура програмно-технічного засобу забезпечує реалізацію автономного контролю доступу без використання серверної інфраструктури. Вона дозволяє виконувати перевірку RFID-картки, введення PIN-коду, керування виконавчим механізмом, відображення стану системи та блокування після багаторазових невдалих спроб доступу. Запропонована структура є достатньою для подальшої програмно-апаратної реалізації пристрою та моделювання його роботи у середовищі Wokwi.

2.2 Вибір мікроконтролерної платформи

У розроблюваному програмно-технічному засобі контролю доступу мікроконтролерна платформа виконує роль центрального блока керування. Вона забезпечує приймання даних від RFID-зчитувача та матричної клавіатури, обробку отриманої інформації, порівняння її із заданими у програмі значеннями та формування керуючих сигналів для виконавчого механізму, LCD-дисплея і світлодіодної індикації. Тому вибір мікроконтролерної платформи безпосередньо впливає на працездатність, простоту реалізації та надійність усього пристрою.

Для даної роботи важливо, щоб обрана платформа відповідала вимогам автономної системи контролю доступу до одного приміщення. Вона повинна мати достатню кількість входів і виходів для підключення всіх компонентів, підтримувати інтерфейси обміну даними з периферійними модулями, бути придатною для реалізації автономної мікроконтролерної системи та не потребувати складної мережевої інфраструктури. З огляду на ці вимоги доцільно розглянути дві поширені мікроконтролерні платформи: Arduino Uno та ESP32.

Платформа Arduino Uno є придатною для реалізації розроблюваного засобу контролю доступу, оскільки має достатню кількість виводів для

підключення RFID-зчитувача RC522, матричної клавіатури 4x4, LCD-дисплея, сервоприводу та світлодіодів [22]. Наявність інтерфейсів SPI та I2C дозволяє організувати взаємодію з основними модулями системи: RFID-зчитувач RC522 підключається через SPI-інтерфейс, а LCD-дисплей 16x2 з I2C-модулем використовує лінії SDA та SCL [23, 24]. Інші елементи пристрою, зокрема клавіатура, сервопривід і світлодіоди, підключаються до виводів загального призначення.

Зовнішній вигляд плати Arduino Uno наведено на рисунку 2.2.

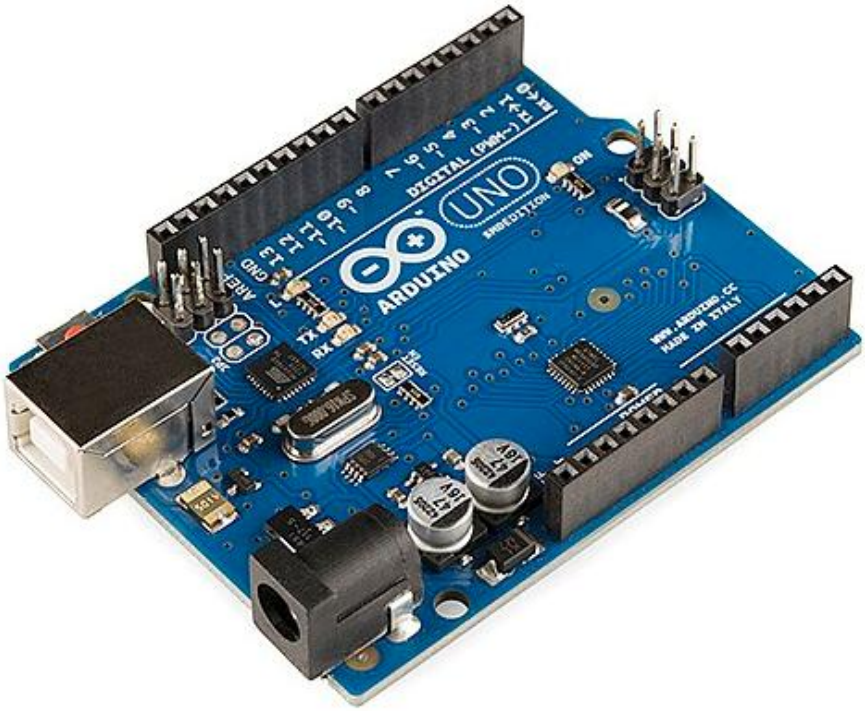


Рисунок 2.2 – Плата мікроконтролера Arduino Uno R3

Важливою перевагою Arduino Uno для даної роботи є простота програмування та наявність готових бібліотек для роботи з обраними компонентами [25]. Для реалізації системи можуть використовуватися бібліотеки для RFID-зчитувача, матричної клавіатури, LCD-дисплея та сервоприводу. Це спрощує створення програмної частини й дозволяє зосередитися не на низькорівневій взаємодії з модулями, а на реалізації алгоритму двофакторної автентифікації користувача.

Як альтернативу було розглянуто платформу ESP32. Вона має вищу продуктивність, більший обсяг пам’яті та підтримує бездротові інтерфейси Wi-Fi і Bluetooth [26]. Такі можливості є корисними для мережевих або розподілених систем контролю доступу, у яких потрібні віддалене адміністрування, передавання даних або інтеграція з хмарними сервісами.

Зовнішній вигляд плати ESP32 наведено на рисунку 2.3.

Рисунок 2.3 – Плата мікроконтролера ESP32 (модуль ESP-WROOM-32)

Однак у межах даної роботи розробляється автономний програмно-технічний засіб контролю доступу до одного приміщення. Така система не потребує віддаленого керування, передавання даних мережею або підключення до серверної інфраструктури. Використання ESP32 у цьому випадку ускладнило б програмну реалізацію та вимагало б додаткового врахування питань захисту бездротового з’єднання, хоча ці функції не є необхідними для поставленої задачі.

Порівняльну характеристику мікроконтролерних платформ Arduino Uno та ESP32 наведено в таблиці 2.1.

Таблиця 2.1 – Порівняння платформ Arduino та ESP32

Характеристика	Arduino Uno	ESP32
Архітектура	8-бітна	32-бітна
Мікроконтролер	Atmega328P	ESP32
Тактова частота	16 МГц	до 240 МГц
Flash-пам’ять	32 КБ	4 МБ і більше
Оперативна пам’ять	2 КБ	близько 520 КБ
Wi-Fi	Ні	Так
Bluetooth	Ні	Так
Кількість GPIO	14 цифрових, 6 аналогових	до 34 GPIO
Інтерфейси	UART, SPI, I2C	UART, SPI, I2C, Wi-Fi, Bluetooth
Енергоспоживання	Низьке	Середнє
Складність програмування	Низька	Середня
Доцільність для автономної СКД	Висока	Середня
Доцільність для мережевої СКД	Низька	Висока
Вартість	Низька	Середня

Як видно з таблиці 2.1, ESP32 має ширші технічні можливості, однак для автономного засобу контролю доступу вони є надлишковими. Основними вимогами до платформи у даній роботі є підтримка підключення обраних модулів, стабільна робота в автономному режимі, простота програмування та

підтримка необхідних інтерфейсів. За цими критеріями Arduino Uno є більш доцільним варіантом [22, 26].

Таким чином, для реалізації програмно-технічного засобу контролю доступу до приміщення обрано мікроконтролерну платформу Arduino Uno. Вона забезпечує достатні апаратні ресурси для підключення RFID-зчитувача, клавіатури, LCD-дисплея, сервоприводу та світлодіодів, підтримує необхідні інтерфейси SPI та I2C, а також дозволяє реалізувати алгоритм двофакторної автентифікації без надмірного ускладнення апаратної й програмної частини пристрою.

2.3 Апаратні компоненти програмно-технічного засобу контролю доступу

У розроблюваному програмно-технічному засобі контролю доступу RFID-зчитувач RC522 використовується як засіб первинної ідентифікації користувача. Його основне призначення полягає у зчитуванні унікального ідентифікаційного коду RFID-картки або брелока та передаванні цих даних до мікроконтролера Arduino Uno для подальшої перевірки.

У структурі пристрою RFID-зчитувач виконує роль першого фактора автентифікації. Це означає, що користувач спочатку повинен пред’явити фізичний ідентифікатор доступу. Після піднесення RFID-картки до зчитувача модуль RC522 зчитує її UID-код, який є унікальним ідентифікатором мітки. Далі Arduino Uno порівнює отримане значення з дозволеним UID, заданим у програмному коді. Якщо ідентифікатор збігається, система переходить до другого етапу автентифікації – введення PIN-коду. Якщо UID не відповідає дозволеному значенню, подальше введення PIN-коду не виконується, а доступ забороняється.

Такий принцип роботи дозволяє одразу відхиляти недозволені RFID-картки та не переходити до наступного етапу перевірки користувача. Це

підвищує логічну послідовність роботи системи та забезпечує попередній контроль доступу ще до введення персонального коду.

RFID-зчитувач RC522 є доцільним для використання у даній роботі, оскільки він підтримує безконтактне зчитування RFID-ідентифікаторів, має компактні розміри, невисоку вартість і сумісний із платформою Arduino Uno [27]. Для обміну даними з мікроконтролером модуль використовує SPI-інтерфейс, що забезпечує стабільне передавання UID-коду до центрального блока керування [27, 28]. Важливою умовою підключення RC522 є живлення від напруги 3,3 В, тому це враховано у схемі підключення компонентів пристрою.

Зовнішній вигляд RFID-зчитувача RC522 наведено на рисунку 2.4.

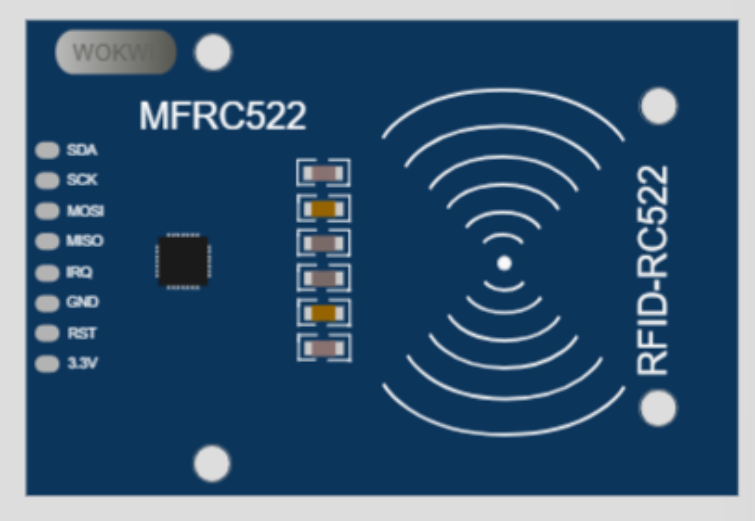


Рисунок 2.4 – RFID-зчитувач RC522

Основні характеристики RFID-зчитувача RC522 наведено в таблиці 2.2.

Таблиця 2.2 – Основні характеристики RFID-зчитувача RC522

Характеристика	Значення
Тип пристрою	RFID-зчитувач
Модель	RC522
Робоча частота	13,56 МГц

Кінець таблиці 2.2

Інтерфейс обміну даними	SPI
Напруга живлення	3,3 В
Тип ідентифікаторів	RFID-картки, RFID-брелоки
Основне призначення	Зчитування UID RFID-мітки

Застосування RFID-зчитувача як єдиного засобу ідентифікації не забезпечує достатнього рівня захисту, оскільки картка або брелок можуть бути втрачені, передані іншій особі або використані без відома власника. Саме тому в розроблюваному пристрої RFID-ідентифікація не завершує процес перевірки користувача, а лише відкриває доступ до другого етапу - введення PIN-коду. Такий підхід дозволяє реалізувати комбіновану модель автентифікації RFID + PIN-код.

Таким чином, RFID-зчитувач RC522 є важливою структурною частиною розроблюваного засобу контролю доступу. Він забезпечує зручне безконтактне зчитування ідентифікатора користувача, передає UID-код до Arduino Uno через SPI-інтерфейс і виконує функцію першого етапу автентифікації. У поєднанні з подальшим введенням PIN-коду це підвищує рівень захищеності доступу до приміщення.

У розроблюваному програмно-технічному засобі контролю доступу матрична клавіатура 4x4 використовується для реалізації другого етапу автентифікації користувача. Якщо RFID-зчитувач підтверджує наявність фізичного ідентифікатора, то введення PIN-коду дозволяє додатково перевірити, чи користувач знає персональний код доступу. Таким чином, клавіатура є важливою складовою комбінованої автентифікації RFID + PIN-код.

У межах даної системи клавіатура використовується тільки після успішного зчитування дозволеної RFID-картки. Після підтвердження UID-коду Arduino Uno переводить систему в режим очікування введення PIN-коду. Користувач вводить цифрову комбінацію за допомогою клавіш 09, а

підтвердження введення здійснюється клавішею #. Клавіша * може використовуватися для очищення введеної комбінації у випадку помилки під час набору.

Зовнішній вигляд матричної клавіатури 4x4 наведено на рисунку 2.5.

Рисунок 2.5 – Матрична клавіатура 4x4

Використання клавіатури 4x4 є доцільним для даної роботи, оскільки вона має достатню кількість клавіш для введення PIN-коду та службових команд, є простою у підключенні до Arduino Uno і підтримується стандартною бібліотекою Keypad [29]. Така бібліотека дозволяє програмно визначати натиснуту клавішу та формувати введену користувачем комбінацію без необхідності розробляти складний алгоритм опитування клавіатури вручну.

Матрична структура клавіатури дозволяє підключити 16 клавіш за допомогою 8 ліній - чотирьох рядків і чотирьох стовпців [30]. Це є важливим для розроблюваного пристрою, оскільки Arduino Uno має обмежену кількість виводів, які одночасно використовуються для RFID-зчитувача, LCD-дисплея, сервоприводу та світлодіодної індикації.

Основні характеристики матричної клавіатури наведено в таблиці 2.4.

Таблиця 2.4 – Основні характеристики матричної клавіатури 4x4

Характеристика	Значення
Тип пристрою	Матрична клавіатура
Кількість клавіш	16
Кількість рядків	4
Кількість стовпців	4
Клавіші введення	0-9
Службові клавіші	*, #, A, B, C, D
Кількість ліній підключення	8

Після введення PIN-коду Arduino Uno порівнює отриману комбінацію із заданим у програмі правильним значенням. Якщо код введено правильно, система формує сигнал надання доступу, вмикає зелений світлодіод і активує виконавчий механізм. Якщо PIN-код неправильний, доступ забороняється, вмикається червоний світлодіод, а кількість невдалих спроб збільшується. У разі досягнення встановленої кількості помилкових спроб система переходить у режим тимчасового блокування.

Таким чином, матрична клавіатура 4x4 у складі розроблюваного пристрою забезпечує введення персонального PIN-коду та реалізує другий фактор автентифікації користувача. Її використання у поєднанні з RFID-зчитувачем підвищує рівень захищеності системи, оскільки доступ до приміщення надається лише після успішної перевірки фізичного ідентифікатора та правильного персонального коду.

У розроблюваному програмно-технічному засобі контролю доступу LCD-дисплей 16x2 з I2C-інтерфейсом використовується як засіб відображення стану системи та інформування користувача про поточний етап роботи пристрою. Його наявність є важливою, оскільки система контролю доступу повинна не лише

виконувати перевірку користувача, а й повідомляти йому, які дії необхідно виконати.

У межах даної роботи LCD-дисплей забезпечує виведення коротких текстових повідомлень під час основних режимів роботи системи. На екрані можуть відображатися повідомлення про очікування RFID-картки, перехід до введення PIN-коду, результат автентифікації, відмову в доступі або тимчасове блокування після кількох невдалих спроб. Завдяки цьому користувач отримує зрозумілий зворотний зв’язок і може правильно взаємодіяти з пристроєм.

Формат дисплея 16x2, тобто два рядки по 16 символів, є достатнім для реалізації простого інтерфейсу користувача в автономній системі контролю доступу [31]. У даній роботі не передбачається складне меню або відображення великого обсягу інформації, тому можливостей такого дисплея достатньо для показу службових повідомлень і результатів перевірки.

Зовнішній вигляд LCD-дисплея 16x2 з I2C-інтерфейсом наведено на рисунку 2.6.

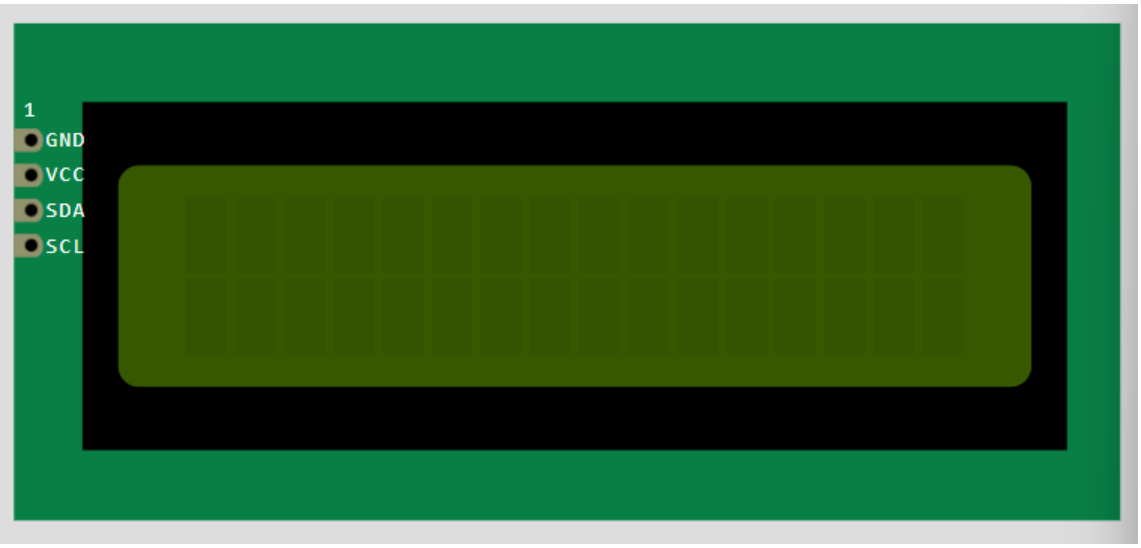


Рисунок 2.6 – LCD-дисплей 16x2 з I2C-інтерфейсом

Доцільність використання саме дисплея з I2C-інтерфейсом пояснюється обмеженою кількістю доступних виводів Arduino Uno. Звичайний LCD-дисплей без I2C-модуля потребував би більшої кількості цифрових ліній, що ускладнило

б підключення інших компонентів системи. Натомість I2C-інтерфейс використовує лише дві сигнальні лінії - SDA та SCL, що дозволяє раціонально розподілити виводи мікроконтролера між RFID-зчитувачем, клавіатурою, сервоприводом і світлодіодами [24, 31].

Основні характеристики LCD-дисплея наведено в таблиці 2.6.

Таблиця 2.6 – Основні характеристики LCD-дисплея 16x2 I2C

Характеристика	Значення
Тип пристрою	LCD-дисплей
Формат відображення	16 символів × 2 рядки
Інтерфейс обміну даними	I2C
Кількість сигнальних ліній	2
Лінії підключення	SDA, SCL
Напруга живлення	5 В

У програмній частині для роботи з дисплеєм використовується бібліотека LiquidCrystal_I2C [32]. Вона дозволяє ініціалізувати дисплей, очищувати екран, встановлювати позицію курсора та виводити текстові повідомлення. Це спрощує реалізацію інтерфейсу користувача та дозволяє швидко змінювати повідомлення залежно від поточного стану системи.

Таким чином, LCD-дисплей у складі розроблюваного пристрою виконує функцію інформаційного зворотного зв’язку. Він робить роботу системи більш зрозумілою для користувача, дозволяє відображати етапи автентифікації та повідомляти про результат перевірки без використання складнішого інтерфейсу керування.

Виконавчий механізм є елементом системи контролю доступу, який відображає результат прийнятого рішення: дозвіл або заборону проходу до приміщення. У розроблюваному програмно-технічному засобі він повинен спрацьовувати лише після успішного проходження двох етапів автентифікації: зчитування дозволеної RFID-картки та введення правильного PIN-коду. Якщо

хоча б один із цих етапів не пройдено, керуючий сигнал на відкриття доступу не формується.

У межах моделювання роботи пристрою в середовищі Wokwi як виконавчий механізм використано сервопривід [33]. Таке рішення є доцільним для навчального моделювання, оскільки сервопривід дозволяє наочно показати реакцію системи на результат автентифікації без використання додаткового силового обладнання. Зміна кута повороту сервоприводу умовно відповідає зміні стану доступу до приміщення.

Зовнішній вигляд сервоприводу наведено на рисунку 2.7.

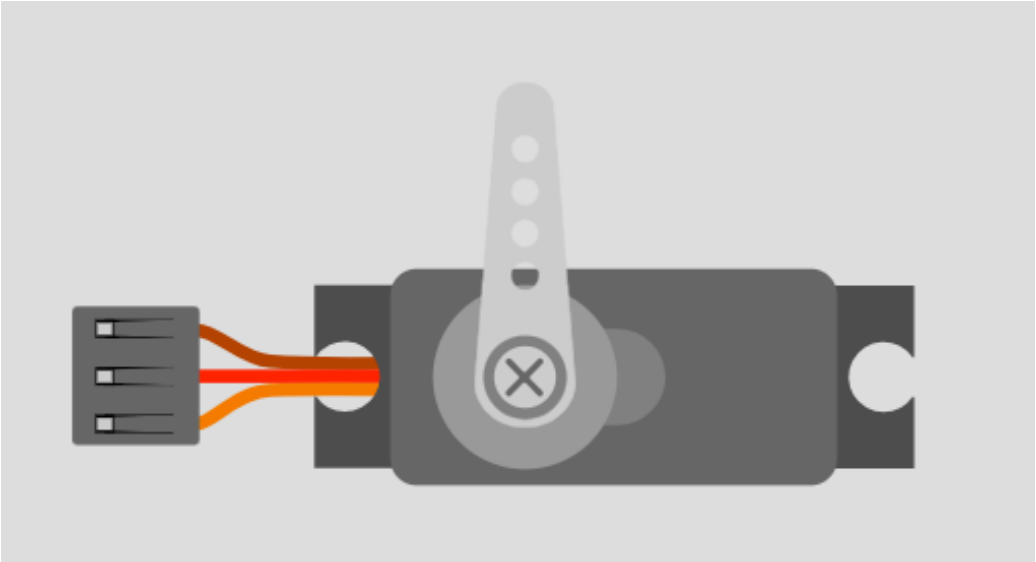


Рисунок 2.7 – Сервопривід як виконавчий механізм системи контролю доступу

Сервопривід керується сигналом широтно-імпульсної модуляції [34]. У програмній моделі початкове положення сервоприводу відповідає закритому стану доступу. Після успішної двофакторної автентифікації мікроконтролер Arduino Uno формує керуючий сигнал, унаслідок чого сервопривід повертається на заданий кут і імітує відкриття доступу до приміщення. Через встановлений проміжок часу сервопривід повертається у початкове положення.

У розробленій моделі прийнято такі положення сервоприводу: 0° - доступ закрито; 90° - доступ відкрито.

Такий принцип роботи дозволяє перевірити правильність алгоритму керування доступом. Якщо користувач підносить дозволену RFID-картку та вводить правильний PIN-код, сервопривід переходить у положення 90°. Якщо RFID-картка або PIN-код неправильні, сервопривід залишається у положенні 0°, а система інформує користувача про відмову.

Основні характеристики сервоприводу наведено в таблиці 2.8.

Таблиця 2.8 – Основні характеристики сервоприводу

Характеристика	Значення
Тип пристрою	Сервопривід
Керування	PWM-сигнал
Робоча напруга	5 В
Початкове положення	0°
Положення відкриття	90°
Керуючий вивід у моделі	A1

Слід зазначити, що в межах даної роботи сервопривід використовується не як реальний дверний виконавчий пристрій, а як наочний елемент для демонстрації реакції системи на результат автентифікації. У реальній апаратній реалізації замість сервоприводу може застосовуватися релейний модуль, який керує електромагнітним або електромеханічним виконавчим пристроєм. У такому випадку Arduino Uno формує керуючий сигнал на вхід реле, а реле виконує комутацію кола живлення виконавчого механізму.

Таким чином, сервопривід у розробленій моделі виконує функцію умовного виконавчого механізму. Його використання дозволяє безпечно та наочно перевірити, що відкриття доступу відбувається лише після успішної перевірки RFID-картки та PIN-коду, а в разі помилки система залишається у закритому стані.

У розроблюваному програмно-технічному засобі контролю доступу засоби світлової індикації використовуються для швидкого візуального відображення результатів роботи системи. Вони доповнюють повідомлення на LCD-дисплеї та дозволяють користувачу одразу визначити стан пристрою без необхідності детально зчитувати текстову інформацію з екрана.

У моделі використано два світлодіоди: зелений і червоний. Зелений світлодіод сигналізує про успішне проходження автентифікації та надання доступу до приміщення. Червоний світлодіод використовується для відображення помилки або небажаного стану системи: зчитування недозволеної RFID-картки, введення неправильного PIN-коду або тимчасового блокування після кількох невдалих спроб.

Зовнішній вигляд світлодіодів наведено на рисунку 2.8.

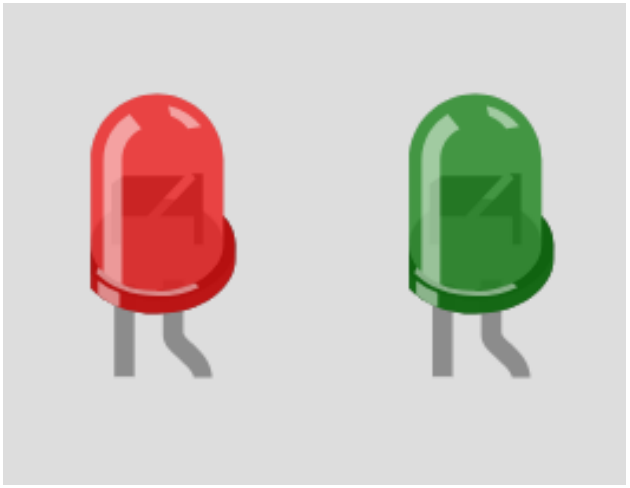


Рисунок 2.8 – Світлодіоди для індикації стану системи

Світлодіодна індикація є доцільною для даної роботи, оскільки вона проста в апаратній реалізації, не потребує складного програмного керування та забезпечує наочне підтвердження результату автентифікації. У моделі зелений світлодіод підключено до виводу A2 Arduino Uno, а червоний – до виводу A3 [35]. Аналогові входи A2 та A3 у цьому випадку використовуються як цифрові виходи, що дозволяє раціонально розподілити доступні виводи мікроконтролера між усіма компонентами пристрою .

Для коректної роботи світлодіоди підключаються через обмежувальні резистори. Це необхідно для обмеження струму та захисту елементів від пошкодження.

Основні стани світлової індикації наведено в таблиці 2.10.

Таблиця 2.10 – Стани світлової індикації системи

Стан системи	Зелений світлодіод	Червоний світлодіод
Очікування RFID-картки	Вимкнений	Вимкнений
RFID-картку прийнято, очікування PIN-коду	Вимкнений	Вимкнений
Доступ дозволено	Увімкнений	Вимкнений
Доступ заборонено	Вимкнений	Увімкнений
Тимчасове блокування системи	Вимкнений	Увімкнений

У процесі роботи системи світлодіоди керуються програмно відповідно до результату перевірки користувача [35]. Після успішного зчитування RFID-картки та введення правильного PIN-коду вмикається зелений світлодіод, що супроводжує відкриття доступу. Якщо користувач вводить неправильні дані або система переходить у режим блокування, вмикається червоний світлодіод. У стані очікування RFID-картки або введення PIN-коду обидва світлодіоди залишаються вимкненими, оскільки остаточний результат автентифікації ще не визначено.

Таким чином, засоби світлової індикації виконують функцію швидкого візуального зворотного зв’язку. Їх використання підвищує зручність роботи з пристроєм і дозволяє чітко розрізняти основні стани системи: очікування, дозвіл доступу, відмову та тимчасове блокування.

2.4 Алгоритм функціонування та програмна логіка пристрою

Робота програмно-технічного засобу контролю доступу ґрунтується на послідовному виконанні алгоритму двофакторної автентифікації користувача [36]. У розробленій системі доступ до приміщення надається лише після успішної перевірки двох незалежних факторів: RFID-ідентифікатора та PIN-коду [21]. Такий підхід дозволяє зменшити ризик несанкціонованого доступу у випадку втрати картки або розголошення коду.

Алгоритм роботи системи побудовано як послідовність станів. Після запуску виконується ініціалізація підключених модулів, встановлення виконавчого механізму у початкове положення та перехід системи в режим очікування RFID-картки. У цьому стані пристрій не виконує перевірку PIN-коду, доки не буде зчитано дозволений RFID-ідентифікатор.

Першим етапом автентифікації є перевірка RFID-картки. Після її піднесення до зчитувача програма отримує UID-код і порівнює його з дозволеним значенням, заданим у програмному коді. Якщо UID не відповідає дозволеному значенню, система формує відмову в доступі, повідомляє користувача про помилку та повертається до режиму очікування RFID-картки. У цьому випадку другий етап автентифікації не запускається.

Якщо UID-код є правильним, система переходить до другого стану - очікування введення PIN-коду. Користувач вводить код за допомогою матричної клавіатури, а підтвердження введення виконується клавішею #. Після підтвердження введений код порівнюється із заданим у програмі правильним PIN-кодом. До моменту підтвердження система лише накопичує введені символи та не приймає рішення про надання або заборону доступу.

У разі правильного введення PIN-коду система переходить у стан надання доступу. У цьому режимі вмикається зелений світлодіод, на LCD-дисплеї відображається повідомлення про успішну автентифікацію, а сервопривід змінює положення, імітуючи відкриття доступу до приміщення. Після

завершення встановленого часу відкриття виконавчий механізм повертається у початкове положення, індикація вимикається, а система знову переходить у режим очікування RFID-картки.

Якщо PIN-код введено неправильно, система переходить у стан відмови в доступі. У цьому випадку вмикається червоний світлодіод, на LCD-дисплеї відображається повідомлення про помилку, а лічильник невдалих спроб збільшується на одиницю. Якщо кількість неправильних спроб не перевищує встановленого обмеження, система повертається до початкового стану та очікує нову спробу автентифікації.

Для підвищення захищеності передбачено механізм тимчасового блокування. Якщо кількість неправильних спроб досягає трьох, система переходить у заблокований стан на 10 секунд. У цей період нові спроби автентифікації не обробляються, на LCD-дисплеї відображається повідомлення про блокування, а червоний світлодіод сигналізує про помилковий стан. Після завершення часу блокування лічильник невдалих спроб скидається, і система повертається до режиму очікування RFID-картки.

Узагальнений алгоритм роботи системи наведено на рисунку 3.2.

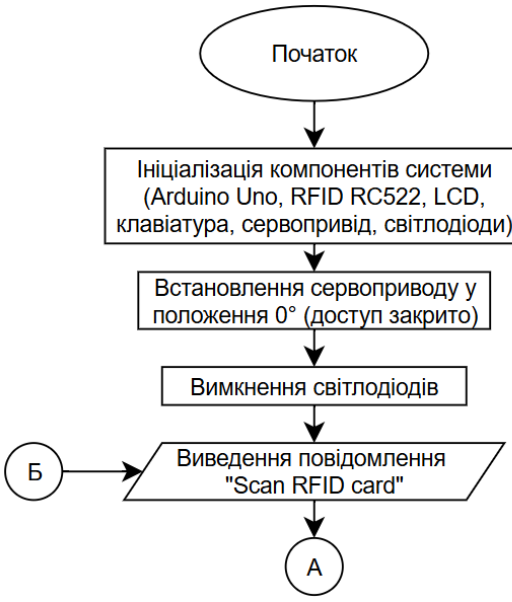
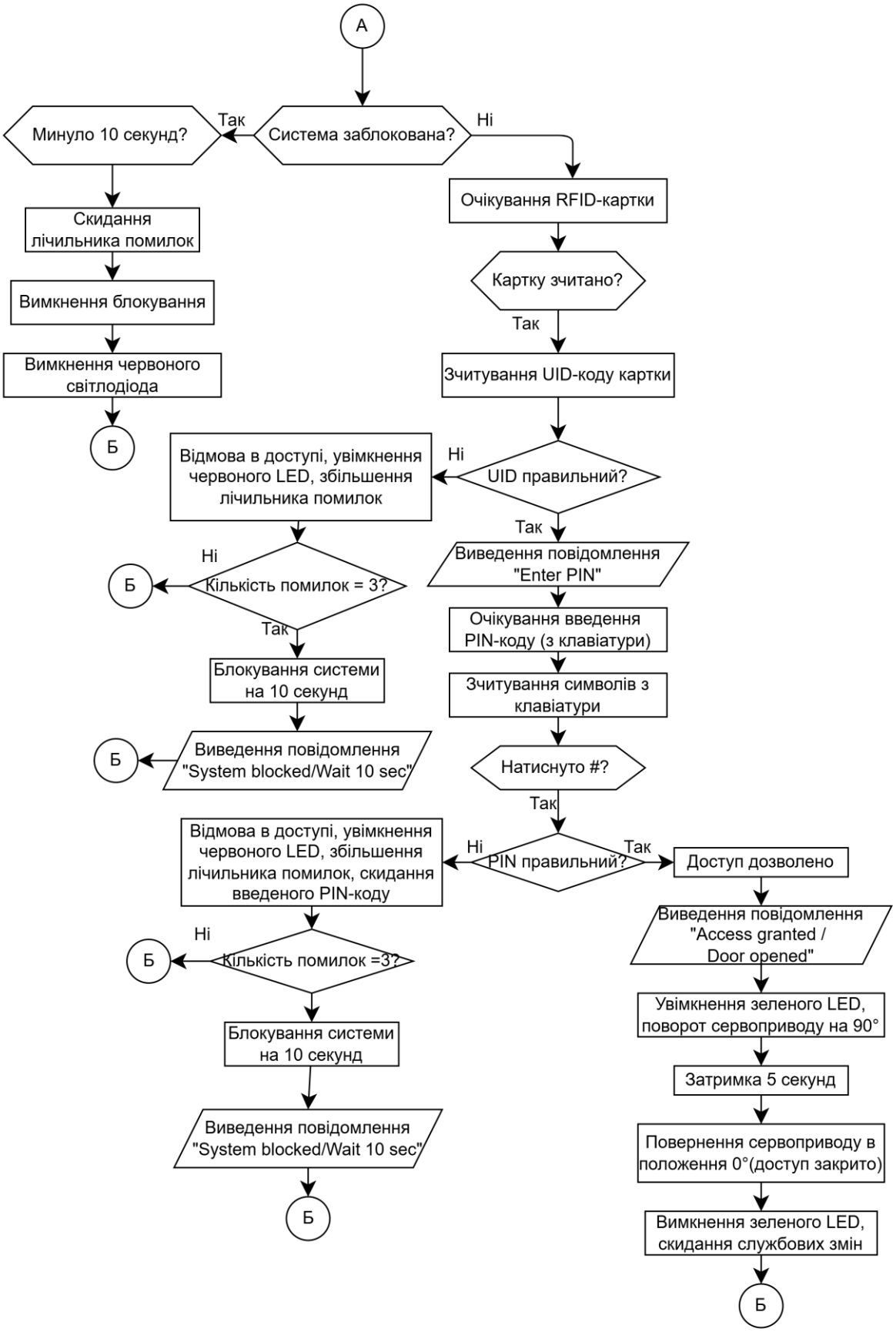


Рисунок 2.9 – Блок-схема алгоритму роботи програмно-технічного засобу контролю доступу



Кінець рисунка 2.9

Основні етапи алгоритму роботи системи можна подати у такій послідовності:

1. Ініціалізація компонентів системи.
2. Встановлення виконавчого механізму у початкове положення.
3. Перехід у режим очікування RFID-картки.
4. Зчитування UID-коду RFID-картки.
5. Порівняння UID-коду з дозволеним значенням.
6. У разі неправильного UID - відмова в доступі та повернення до початкового стану.
7. У разі правильного UID - перехід до введення PIN-коду.
8. Зчитування PIN-коду з клавіатури.
9. Підтвердження введення PIN-коду клавішею #.
10. Порівняння введеного PIN-коду з правильним значенням.
11. У разі правильного PIN-коду - надання доступу та активація виконавчого механізму.
12. У разі неправильного PIN-коду - відмова в доступі та збільшення лічильника помилок.
13. Блокування системи після трьох невдалих спроб автентифікації.
14. Скидання лічильника помилок після завершення часу блокування.
15. Повернення системи до режиму очікування RFID-картки.

Таким чином, алгоритм функціонування системи забезпечує послідовну перевірку RFID-ідентифікатора та PIN-коду, керування станами доступу, обробку помилкових спроб і тимчасове блокування після перевищення допустимої кількості помилок. Це дозволяє реалізувати автономний програмно-технічний засіб контролю доступу з підвищеним рівнем захищеності.

Описаний алгоритм є основою для побудови програмної логіки пристрою. Кожен етап роботи системи реалізується окремими програмними функціями, що відповідають за зчитування RFID-картки, обробку введеного PIN-коду, керування індикацією, активацію виконавчого механізму та блокування після

невдалих спроб доступу. Такий поділ дозволяє зробити програму більш структурованою та спростити перевірку правильності її роботи.

Для реалізації наведеного алгоритму в програмі передбачено основні функції, що відповідають за окремі етапи роботи системи: перевірку RFID-картки, обробку PIN-коду, надання або відмову в доступі та тимчасове блокування. Завдяки цьому програмна логіка відповідає послідовності станів, поданій на блок-схемі алгоритму.

Першим етапом роботи системи є перевірка RFID-картки, реалізована у функції checkRFID()[27]. Вона перевіряє наявність нової картки в зоні дії зчитувача. Якщо картка відсутня, функція завершує роботу без подальших дій, що дозволяє системі постійно перебувати в режимі очікування RFID-картки.

Після виявлення картки RFID-зчитувач RC522 зчитує її серійний номер. Отримані байти UID-коду послідовно об’єднуються в один текстовий рядок. Для коректного порівняння значення UID приводиться до однакового формату: якщо байт має значення менше 0x10, перед ним додається нуль, а весь рядок переводиться у верхній регістр. Це необхідно для того, щоб отриманий UID мав такий самий вигляд, як і дозволене значення, записане у програмі.

Після формування UID-коду програма виводить його у Serial Monitor та на LCD-дисплей. Це дає змогу під час моделювання перевірити, який саме ідентифікатор було зчитано. Далі отриманий UID порівнюється зі змінною allowedUID. Якщо значення збігаються, змінна rfidAccepted набуває значення true, а система переходить до наступного етапу -введення PIN-коду. Якщо UID не відповідає дозволеному значенню, викликається функція accessDenied() із причиною відмови Wrong RFID.

Обробка введення PIN-коду реалізована у функції checkPIN()[29]. Ця функція активується лише після успішного проходження RFID-ідентифікації, тобто коли змінна rfidAccepted має значення true. Такий підхід забезпечує послідовність двофакторної автентифікації: користувач не може перейти до введення PIN-коду без попереднього зчитування дозволеної RFID-картки.

У функції checkPIN() програма зчитує натискання клавіш матричної клавіатури. Якщо користувач натискає цифрову клавішу від 0 до 9, символ додається до рядка enteredPIN. Для обмеження довжини введення використовується перевірка кількості символів, тому у змінну додається не більше чотирьох цифр. Під час введення на LCD-дисплеї відображаються не самі цифри, а символи *, що дозволяє приховати PIN-код від сторонніх осіб [31].

У програмі також передбачено обробку службових клавіш. Клавіша * використовується для очищення введеної комбінації. Після її натискання змінна enteredPIN скидається, а на дисплеї з’являється повідомлення про очищення PIN-коду. Клавіша # використовується для підтвердження введення. Після її натискання програма порівнює введене значення enteredPIN зі змінною correctPIN. Якщо значення збігаються, викликається функція accessGranted(). Якщо введений код неправильний, викликається функція accessDenied() із причиною відмови Wrong PIN.

Функція accessGranted() відповідає за дії системи у випадку успішного проходження двох етапів автентифікації. Після її виклику на LCD-дисплей виводиться повідомлення про надання доступу, зелений світлодіод вмикається, а червоний вимикається. Після цього сервопривід повертається у положення 90°, що в межах моделі відповідає відкриттю доступу до приміщення.

Доступ залишається відкритим протягом п’яти секунд. Це реалізовано за допомогою затримки delay(5000) [38]. Після завершення цього часу сервопривід повертається у початкове положення 0°, зелений світлодіод вимикається, а система скидає службові змінні rfidAccepted, enteredPIN і failedAttempts. Після цього на LCD-дисплей виводиться повідомлення про повернення системи до очікування RFID-картки. Таким чином, після успішного циклу доступу система автоматично переходить у початковий стан і готова до наступної автентифікації.

Функція accessDenied() реалізує реакцію системи на помилкову автентифікацію. Вона використовується у двох випадках: якщо RFID-картка не відповідає дозволеному UID або якщо після правильної RFID-картки введено

неправильний PIN-код. Функція приймає текстову змінну reason, у якій зазначається причина відмови. Завдяки цьому на LCD-дисплеї та у Serial Monitor можна вивести конкретне повідомлення, наприклад Wrong RFID або Wrong PIN.

Після виклику accessDenied() на дисплеї відображається повідомлення про заборону доступу, вмикається червоний світлодіод, а лічильник невдалих спроб збільшується на одиницю. Також скидаються поточні дані автентифікації, тому після помилки користувач повинен знову починати перевірку з RFID-картки.

Якщо кількість невдалих спроб менша за встановлене обмеження, система повертається до очікування RFID-картки. Якщо ж лічильник досягає максимально допустимого значення, викликається функція blockSystem(), яка переводить пристрій у режим тимчасового блокування.

Функція blockSystem() використовується для захисту від багаторазових невдалих спроб автентифікації. Під час її виконання система переходить у заблокований стан, фіксує час початку блокування, виводить на LCD-дисплей повідомлення System blocked та Wait 10 sec, а червоний світлодіод залишається увімкненим.

Завершення блокування перевіряється функцією checkBlockState(). Вона порівнює поточний час із моментом початку блокування [39]. Якщо встановлений період минув, блокування вимикається, лічильник помилок скидається, червоний світлодіод вимикається, а система повертається до очікування RFID-картки.

Контроль часу блокування здійснюється на основі системного часу мікроконтролера [39]. У розробленій програмі тривалість блокування становить 10 секунд, що достатньо для демонстрації захисного механізму під час моделювання.

Таким чином, основні програмні функції забезпечують повний цикл роботи програмно-технічного засобу контролю доступу: зчитування RFID-картки, перевірку UID-коду, введення та перевірку PIN-коду, надання або заборону доступу, а також тимчасове блокування після кількох помилкових

спроб. Реалізація програми у вигляді окремих функціональних блоків робить її логічною, зрозумілою та придатною для подальшої програмно-апаратної реалізації й перевірки роботи системи.

2.5 Висновки до другого розділу

У другому розділі було визначено та обґрунтовано структурні частини програмно-технічного засобу контролю доступу до приміщення. На основі поставлених вимог сформовано апаратну структуру пристрою, до складу якої входять мікроконтролерний блок керування, RFID-зчитувач, матрична клавіатура, LCD-дисплей, виконавчий механізм та засоби світлової індикації.

Як центральний керуючий блок обрано платформу Arduino Uno, оскільки вона має достатню кількість виводів, підтримує необхідні інтерфейси SPI та I2C, сумісна з обраними модулями й дозволяє реалізувати автономну систему без використання серверної інфраструктури. Для ідентифікації користувача обґрунтовано застосування RFID-зчитувача RC522 та матричної клавіатури 4x4, що забезпечує реалізацію комбінованої автентифікації RFID + PIN-код.

Для відображення стану системи передбачено LCD-дисплей 16x2 з I2C-інтерфейсом і світлодіодну індикацію. Як умовний виконавчий механізм у моделі використано сервопривід, який дозволяє наочно продемонструвати реакцію системи на успішну або помилкову автентифікацію. Розроблена схема підключення компонентів до Arduino Uno забезпечує взаємодію всіх структурних частин пристрою та раціональне використання доступних виводів мікроконтролера.

Отже, у результаті виконання другого розділу сформовано апаратну основу автономного засобу контролю доступу до приміщення. Обрані компоненти та схема їх підключення створюють підґрунтя для подальшої програмно-апаратної реалізації пристрою, розроблення алгоритму роботи та перевірки системи у середовищі Wokwi.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

3.1 Схема підключення компонентів пристрою

Для узгодження роботи всіх структурних частин програмно-технічного засобу контролю доступу було розроблено схему підключення компонентів до мікроконтролерної плати Arduino Uno у середовищі Wokwi [40]. Схема відображає практичну реалізацію апаратної структури пристрою та показує, які виводи мікроконтролера використовуються для взаємодії з RFID-зчитувачем, клавіатурою, LCD-дисплеєм, сервоприводом і світлодіодами.

До складу схеми входять Arduino Uno, RFID-зчитувач RC522, матрична клавіатура 4x4, LCD-дисплей 16x2 з I2C-інтерфейсом, сервопривід, зелений і червоний світлодіоди та обмежувальні резистори. Загальний вигляд підключення компонентів пристрою у середовищі Wokwi наведено на рисунку 3.1.

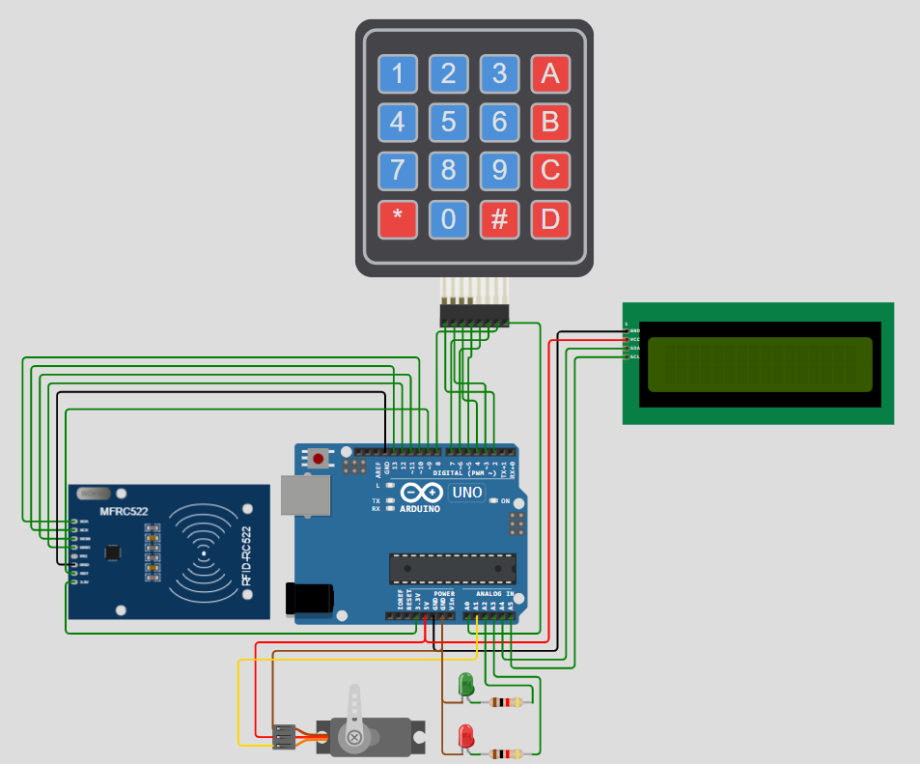


Рисунок 3.1 – Схема підключення компонентів програмно-технічного засобу контролю доступу у середовищі Wokwi

У розробленій схемі Arduino Uno виконує функцію центрального керуючого блока. До нього підключено всі периферійні елементи, які забезпечують введення даних, відображення стану системи, світлову індикацію та керування виконавчим механізмом. Такий підхід дозволяє реалізувати автономну роботу пристрою без використання додаткової серверної інфраструктури.

RFID-зчитувач RC522 підключено до Arduino Uno через SPI-інтерфейс [28]. Для обміну даними використовуються виводи D10, D11, D12 та D13, а також окремий вивід D9 для сигналу скидання модуля. Живлення RFID-зчитувача здійснюється від виводу 3.3V, оскільки модуль RC522 розрахований на роботу з напругою 3,3 В.

LCD-дисплей 16x2 з I2C-інтерфейсом підключено до виводів A4 та A5 Arduino Uno, які відповідають лініям SDA та SCL [24]. Використання I2C-інтерфейсу є доцільним, оскільки для обміну даними з дисплеєм потрібно лише дві сигнальні лінії. Це дозволяє залишити більше виводів мікроконтролера для підключення інших компонентів системи.

Матрична клавіатура 4x4 підключена до цифрових виводів D2–D8 та аналогового входу A0, який у цій схемі використовується як цифровий вивід. Сервопривід підключено до виводу A1, з якого формується керуючий PWM-сигнал. Зелений світлодіод підключено до виводу A2 через обмежувальний резистор, а червоний - до виводу A3 через резистор. Катоди світлодіодів підключені до загального проводу GND.

Загальне підключення компонентів до Arduino Uno наведено в таблиці 3.1.

Таблиця 3.1 – Підключення компонентів пристрою до Arduino Uno

Компонент	Вивід компонента	Вивід Arduino Uno	Призначення
RFID RC522	SDA	D10	Вибір пристрою на SPI-шині
RFID RC522	SCK	D13	Тактовий сигнал SPI

Продовження таблиці 3.1

RFID RC522	MOSI	D11	Передавання даних від Arduino до RC522
RFID RC522	MISO	D12	Передавання даних від RC522 до Arduino
RFID RC522	RST	D9	Скидання модуля
RFID RC522	GND	GND	Загальний провід
RFID RC522	3.3V	3.3V	Живлення модуля
Клавіатура 4x4	R1	D2	Рядок 1
Клавіатура 4x4	R2	D3	Рядок 2
Клавіатура 4x4	R3	D4	Рядок 3
Клавіатура 4x4	R4	D5	Рядок 4
Клавіатура 4x4	C1	D6	Стовпець 1
Клавіатура 4x4	C2	D7	Стовпець 2
Клавіатура 4x4	C3	D8	Стовпець 3
Клавіатура 4x4	C4	A0	Стовпець 4
LCD 16x2 I2C	GND	GND	Загальний провід
LCD 16x2 I2C	VCC	5V	Живлення дисплея
LCD 16x2 I2C	SDA	A4	Лінія даних I2C
LCD 16x2 I2C	SCL	A5	Лінія тактування I2C
Сервопривід	GND	GND	Загальний провід

Кінець таблиці 3.1

Сервопривід	V+	5V	Живлення сервоприводу
Сервопривід	Signal	A1	Керуючий PWM-сигнал
Зелений LED	Анод через резистор	A2	Індикація дозволеного доступу
Зелений LED	Катод	GND	Загальний провід
Червоний LED	Анод через резистор	A3	Індикація заборони доступу або блокування
Червоний LED	Катод	GND	Загальний провід

Схема підключення забезпечує раціональне використання виводів Arduino Uno. Для RFID-зчитувача використано апаратні SPI-виводи, для LCD-дисплея - I2C-інтерфейс, а для клавіатури, сервоприводу та світлодіодів -виводи загального призначення. Це дозволяє реалізувати всі необхідні функції пристрою без застосування додаткових розширювальних плат.

Важливою умовою коректної роботи схеми є наявність спільного загального проводу GND для всіх компонентів. LCD-дисплей і сервопривід живляться від виводу 5V Arduino Uno, тоді як RFID-зчитувач RC522 підключено до виводу 3.3V відповідно до його вимог щодо напруги живлення.

Таким чином, розроблена схема підключення забезпечує узгоджену взаємодію всіх структурних частин пристрою. Вона створює апаратну основу для подальшої програмно-апаратної реалізації системи контролю доступу та перевірки її роботи у середовищі Wokwi.

3.2 Опис програмної реалізації

Програмна реалізація програмно-технічного засобу контролю доступу виконана для мікроконтролерної платформи Arduino Uno [41]. Основним завданням програмної частини є керування послідовністю автентифікації користувача, обробка даних від RFID-зчитувача та клавіатури, формування

сигналів індикації, керування виконавчим механізмом і реалізація блокування після кількох невдалих спроб доступу.

Програма побудована за модульним принципом. Окремі програмні функції відповідають за роботу з RFID-зчитувачем, обробку PIN-коду, індикацію результатів перевірки, надання доступу, відмову в доступі та тимчасове блокування системи. Такий підхід спрощує структуру програми та дозволяє окремо перевіряти роботу кожної функціональної частини.

Для взаємодії з апаратними модулями використано стандартні та спеціалізовані бібліотеки Arduino [42–47]. Бібліотека SPI.h забезпечує обмін даними з RFID-зчитувачем через SPI-інтерфейс, а MFRC522.h використовується для роботи з модулем RC522 і зчитування UID-коду RFID-картки. Бібліотека Keypad.h відповідає за обробку натискань клавіш матричної клавіатури. Керування сервоприводом реалізовано за допомогою Servo.h, а для роботи з LCD-дисплеєм через I2C-інтерфейс використовуються Wire.h та LiquidCrystal_I2C.h.

На початку програми визначаються виводи Arduino Uno, до яких підключено основні компоненти системи. RFID-зчитувач RC522 використовує виводи SS_PIN і RST_PIN, сервопривід підключено до виводу A1, зелений світлодіод – до A2, а червоний – до A3. Також створюються програмні об’єкти для роботи з RFID-зчитувачем, сервоприводом, LCD-дисплеєм і клавіатурою.

У програмі задано дозволений UID RFID-картки та правильний PIN-код. У моделі Wokwi як дозволений RFID-ідентифікатор використовується значення 01 02 03 04, а правильним PIN-кодом є 1234. Для збереження введеного користувачем коду використовується змінна enteredPIN. Кількість неправильних спроб зберігається у змінній failedAttempts, а максимально допустима кількість помилок визначається сталою maxAttempts.

Окремо у програмі передбачено змінні стану системи. Змінна rfidAccepted визначає, чи успішно пройдено перший етап автентифікації. Якщо її значення дорівнює true, система переходить до введення PIN-коду. Змінна systemBlocked

показує, чи перебуває система у режимі тимчасового блокування. Для контролю тривалості блокування використовується змінна blockStartTime, а тривалість блокування задано сталою blockDuration.

Функція setup() виконується один раз після запуску системи. У ній ініціалізуються порт, SPI-інтерфейс, RFID-зчитувач, LCD-дисплей, сервопривід і світлодіоди. Сервопривід встановлюється у початкове положення, світлодіоди вимикаються, а на LCD-дисплей виводиться початкове повідомлення про очікування RFID-картки. Додатково в Serial Monitor виводяться службові повідомлення про запуск системи [48].

Основна логіка роботи програми реалізована у функції loop(). У ній спочатку перевіряється, чи не перебуває система у стані блокування. Якщо блокування активне, викликається функція checkBlockState(), а подальші дії користувача тимчасово не обробляються. Якщо система не заблокована, програма залежно від стану rfidAccepted або очікує RFID-картку, або переходить до обробки PIN-коду.

Функція checkRFID() реалізує перший етап автентифікації. Вона перевіряє наявність нової RFID-картки, зчитує її UID-код, формує його у вигляді рядка та порівнює з дозволеним значенням. Якщо UID збігається, змінна rfidAccepted набуває значення true, після чого система переходить до очікування введення PIN-коду. Якщо UID неправильний, викликається функція accessDenied() із причиною відмови Wrong RFID.

Функція checkPIN() відповідає за другий етап автентифікації. Вона обробляє натискання клавіш матричної клавіатури, додає цифрові символи до змінної enteredPIN, дозволяє очистити введення клавішею * та підтвердити введення клавішею #. Після натискання # введений PIN-код порівнюється з правильним значенням. Якщо код збігається, викликається функція accessGranted(), а якщо ні – accessDenied() із причиною Wrong PIN.

У разі успішної автентифікації виконується функція accessGranted(). Вона виводить на LCD-дисплей повідомлення про надання доступу, вмикає зелений

світлодіод, вимикає червоний і повертає сервопривід у положення 90°. Через п’ять секунд сервопривід повертається у початкове положення, зелений світлодіод вимикається, а службові змінні скидаються для переходу системи до нового циклу очікування RFID-картки.

Функція accessDenied() виконується у разі неправильного RFID-ідентифікатора або неправильного PIN-коду. Вона виводить повідомлення про заборону доступу, вмикає червоний світлодіод, збільшує лічильник невдалих спроб і скидає поточний стан автентифікації. Якщо кількість помилок досягає встановленого обмеження, викликається функція blockSystem().

Механізм тимчасового блокування реалізовано функціями blockSystem() та checkBlockState(). Функція blockSystem() переводить систему у заблокований стан, запам’ятовує час початку блокування, виводить відповідне повідомлення на LCD-дисплей і вмикає червоний світлодіод. Функція checkBlockState() перевіряє, чи минув встановлений час блокування. Після завершення цього періоду система скидає лічильник помилок, вимикає червоний світлодіод і повертається до початкового стану.

Отже, програмна реалізація розробленого пристрою забезпечує послідовне виконання всіх етапів двофакторної автентифікації та керування станами системи. Використання окремих функцій для зчитування RFID-картки, перевірки PIN-коду, надання або заборони доступу й блокування після невдалих спроб дозволяє забезпечити зрозумілу структуру програми та стабільну роботу програмно-технічного засобу.

3.3 Моделювання пристрою у середовищі Wokwi

Після визначення структурних частин програмно-технічного засобу контролю доступу було виконано його програмно-апаратну реалізацію у середовищі моделювання Wokwi [40]. Використання цього середовища дозволяє перевірити роботу мікроконтролерного пристрою без фізичного складання

макета, що є зручним на етапі розробки, тестування та відлагодження алгоритму роботи системи [49].

У другому розділі було розглянуто апаратну структуру пристрою та схему підключення його компонентів. У даному розділі основну увагу приділено не опису складових частин, а перевірці їх спільної роботи під керуванням програмного коду. Моделювання у Wokwi дало змогу відтворити основні режими функціонування системи: очікування RFID-картки, зчитування UID-коду, введення PIN-коду, надання або заборону доступу, а також тимчасове блокування після кількох неправильних спроб.

На рисунку 3.2 наведено роботу моделі програмно-технічного засобу контролю доступу у середовищі Wokwi в режимі очікування RFID-картки.

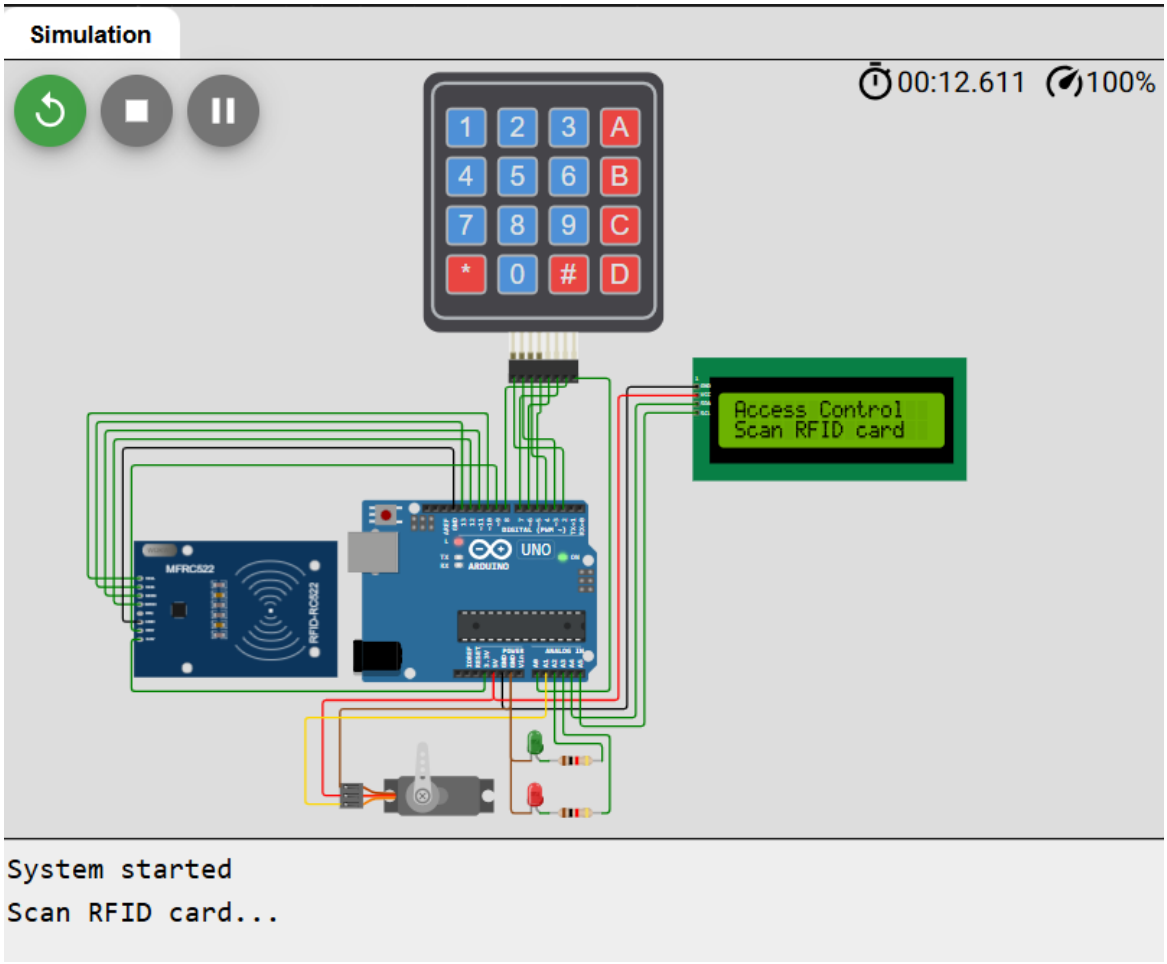


Рисунок 3.2 – Робота моделі програмно-технічного засобу контролю доступу у середовищі Wokwi в режимі очікування RFID-картки

У початковому стані система виконує ініціалізацію підключених модулів і переходить у режим очікування користувача. На LCD-дисплеї відображається повідомлення про необхідність піднести RFID-картку, а в Serial Monitor виводяться службові повідомлення про запуск системи та очікування зчитування картки. У цей момент виконавчий механізм перебуває у початковому положенні, а світлодіодна індикація не сигналізує про дозвіл або заборону доступу.

У середовищі Wokwi було перевірено реакцію системи на різні дії користувача. Під час імітації піднесення RFID-картки програма зчитує UID-код і порівнює його з дозволеним значенням. У разі успішної перевірки система переходить до введення PIN-коду. Якщо введений код відповідає заданому значенню, мікроконтролер формує керуючий сигнал на сервопривід, вмикає зелений світлодіод і виводить на дисплей повідомлення про надання доступу. Якщо RFID-картка або PIN-код не відповідають заданим значенням, система повідомляє про відмову, а виконавчий механізм залишається у початковому стані.

Окремо в моделі було перевірено роботу механізму тимчасового блокування. Після трьох неправильних спроб введення PIN-коду система переходить у заблокований стан на заданий проміжок часу. У цей період нові спроби доступу не обробляються, на дисплеї відображається повідомлення про блокування, а червоний світлодіод сигналізує про помилковий стан системи.

Під час моделювання використовувався Serial Monitor, який дав змогу контролювати внутрішні стани програми [48]. У ньому відображалися повідомлення про запуск системи, очікування RFID-картки, зчитаний UID, натиснуті клавіші, результат перевірки PIN-коду, дозвіл або заборону доступу та перехід у режим блокування. Це спростило перевірку правильності роботи алгоритму та дозволило виявляти помилки на етапі програмної реалізації.

Таким чином, середовище Wokwi було використано не лише для побудови схеми пристрою, а й для практичної перевірки взаємодії апаратної та програмної частин системи. Результати моделювання підтвердили можливість реалізації

алгоритму двофакторної автентифікації RFID + PIN-код, керування виконавчим механізмом, відображення стану системи та блокування після кількох невдалих спроб доступу.

3.4 Тестування роботи системи та аналіз результатів моделювання

Після створення схеми підключення та програмної реалізації було виконано тестування роботи програмно-технічного засобу контролю доступу у середовищі Wokwi [40]. Метою тестування була перевірка правильності роботи алгоритму двофакторної автентифікації, реакції системи на правильні та неправильні дані, функціонування виконавчого механізму, світлової індикації, LCD-дисплея та вікна Serial Monitor. Вікно Serial Monitor використовувалося для перегляду UID-кодів карток, натиснутих клавіш і службових повідомлень системи [48].

Під час тестування перевірялися такі основні режими роботи системи: очікування RFID-картки, зчитування дозволеного RFID-ідентифікатора, введення правильного PIN-коду, надання доступу, повернення системи до початкового стану, введення неправильного PIN-коду, тимчасове блокування після кількох невдалих спроб, а також реакція системи на недозволену RFID-картку. Такий набір перевірок дозволяє оцінити роботу пристрою як у штатному режимі, так і в ситуаціях помилкової або несанкціонованої спроби доступу.

Першим етапом тестування була перевірка зчитування дозволеної RFID-картки. У середовищі Wokwi для цього було використано віртуальну панель модуля MFRC522 RFID Reader, у якій обрано картку з UID-кодом, що відповідає дозволеному значенню, заданому в програмі [50]. Після натискання кнопки TAP система зчитала ідентифікатор картки та порівняла його з дозволеним UID. У результаті цього система перейшла до наступного етапу автентифікації та вивела на LCD-дисплей повідомлення з пропозицією ввести PIN-код.

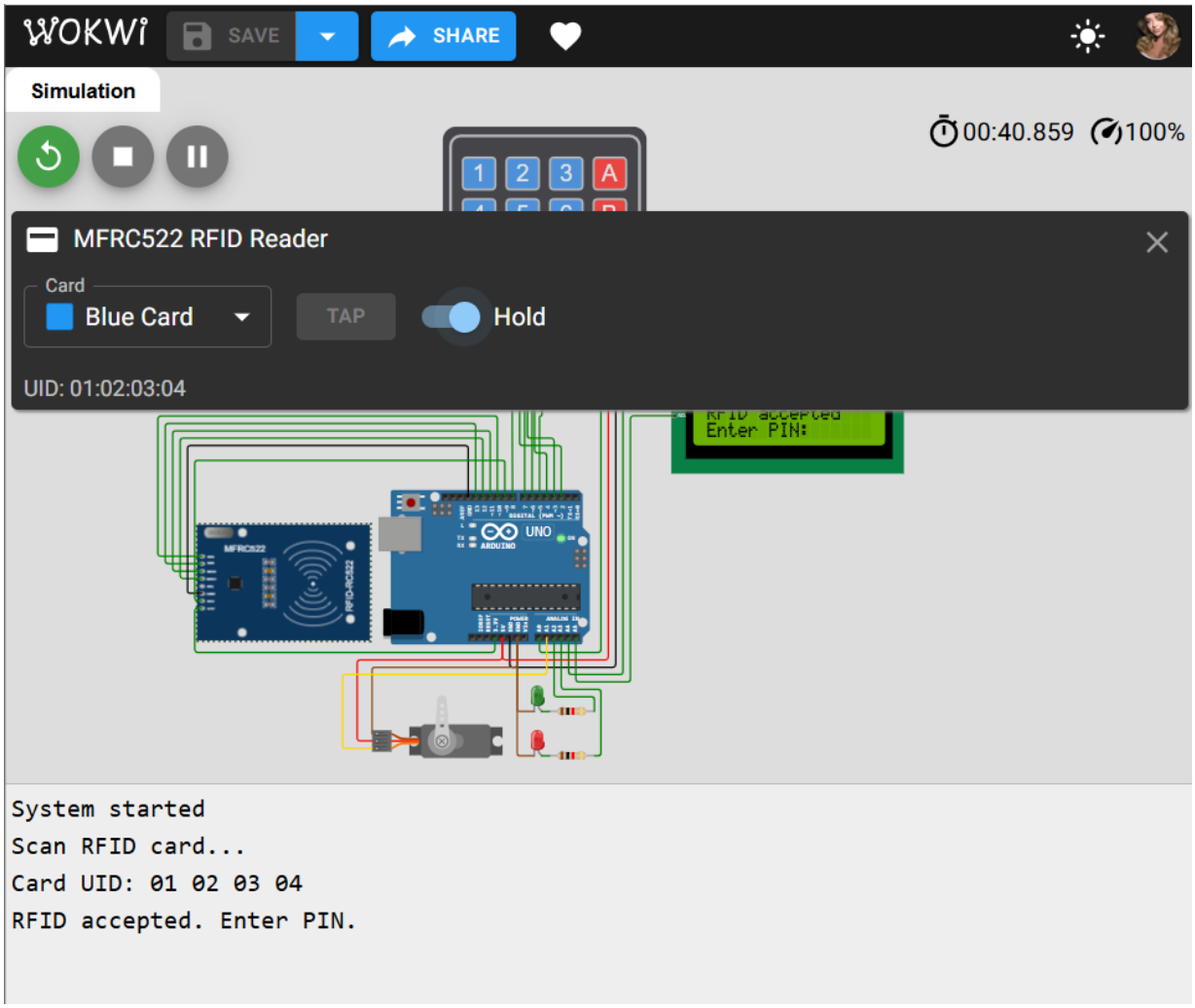


Рисунок 3.3 – Зчитування дозволеної RFID-картки у середовищі Wokwi

Як видно з рисунка 3.3, у Serial Monitor відображається зчитаний UID-код картки 01 02 03 04, після чого система виводить повідомлення про успішне проходження першого етапу автентифікації. На LCD-дисплеї з'являється повідомлення про необхідність введення PIN-коду. Це підтверджує, що RFID-зчитувач працює коректно, а програма правильно розпізнає дозволений ідентифікатор.

Додатково стан переходу до введення PIN-коду відображено на LCD-дисплеї. Після прийняття RFID-картки система не надає доступ одразу, а переходить до другого етапу автентифікації. Це відповідає логіці розробленого алгоритму, згідно з яким RFID-картка є лише першим фактором перевірки користувача.

Рисунок 3.4 – Повідомлення LCD-дисплея після прийняття RFID-картки

На рисунку 3.4 показано повідомлення RFID accepted / Enter PIN, яке інформує користувача про успішне зчитування картки та необхідність введення персонального коду. Такий результат підтверджує правильну роботу LCD-дисплея як засобу відображення поточного стану системи.

Наступним етапом було тестування введення правильного PIN-коду. Після прийняття RFID-картки на матричній клавіатурі було послідовно натиснуто клавіші 1, 2, 3, 4, після чого введення підтверджено клавішею #. Ця комбінація відповідає правильному PIN-коду, заданому в програмі.

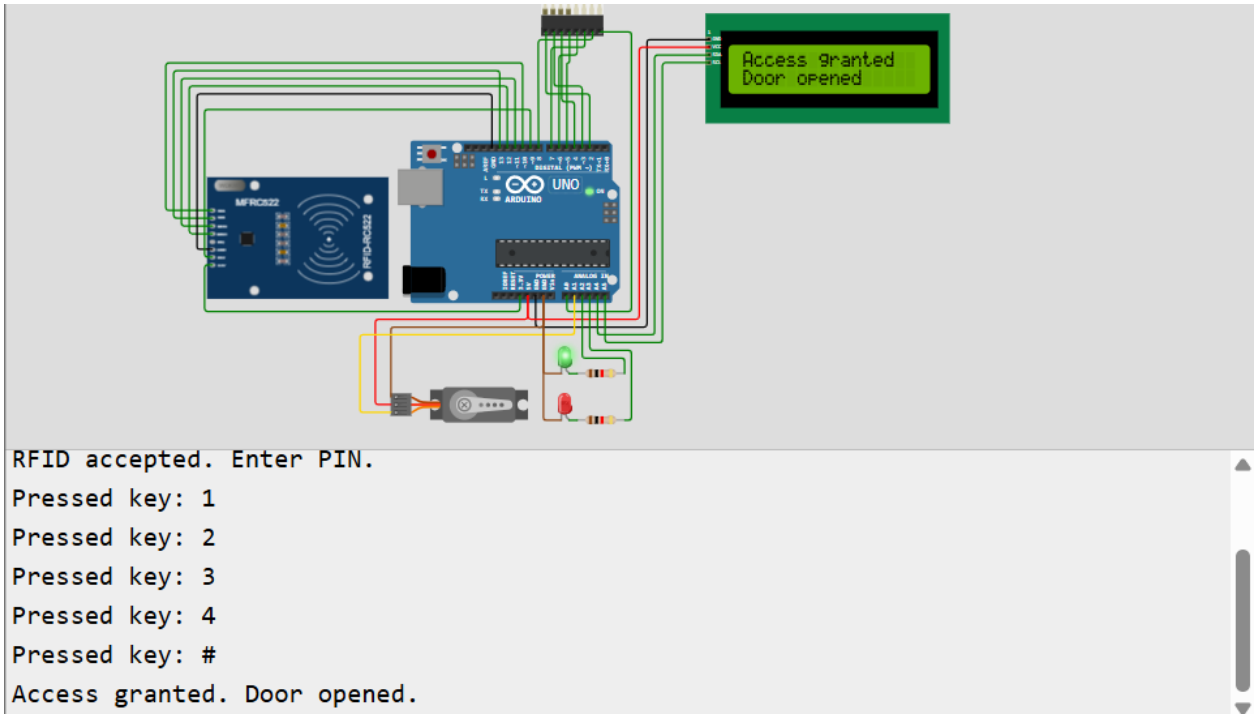


Рисунок 3.5 – Надання доступу після введення правильного PIN-коду

На рисунку 3.5 видно, що після введення правильного PIN-коду система сформувала повідомлення Access granted / Door opened. У Serial Monitor зафіксовано натискання клавіш та повідомлення про надання доступу. Одночасно вмикається зелений світлодіод, а сервопривід переходить у положення відкриття доступу. Це підтверджує, що обидва етапи автентифікації - RFID-картка та PIN-код - були успішно пройдені.

Після завершення встановленого часу відкриття виконавчий механізм повертається у початкове положення. У Serial Monitor відображається повідомлення про закриття доступу та повторний перехід системи до очікування RFID-картки.

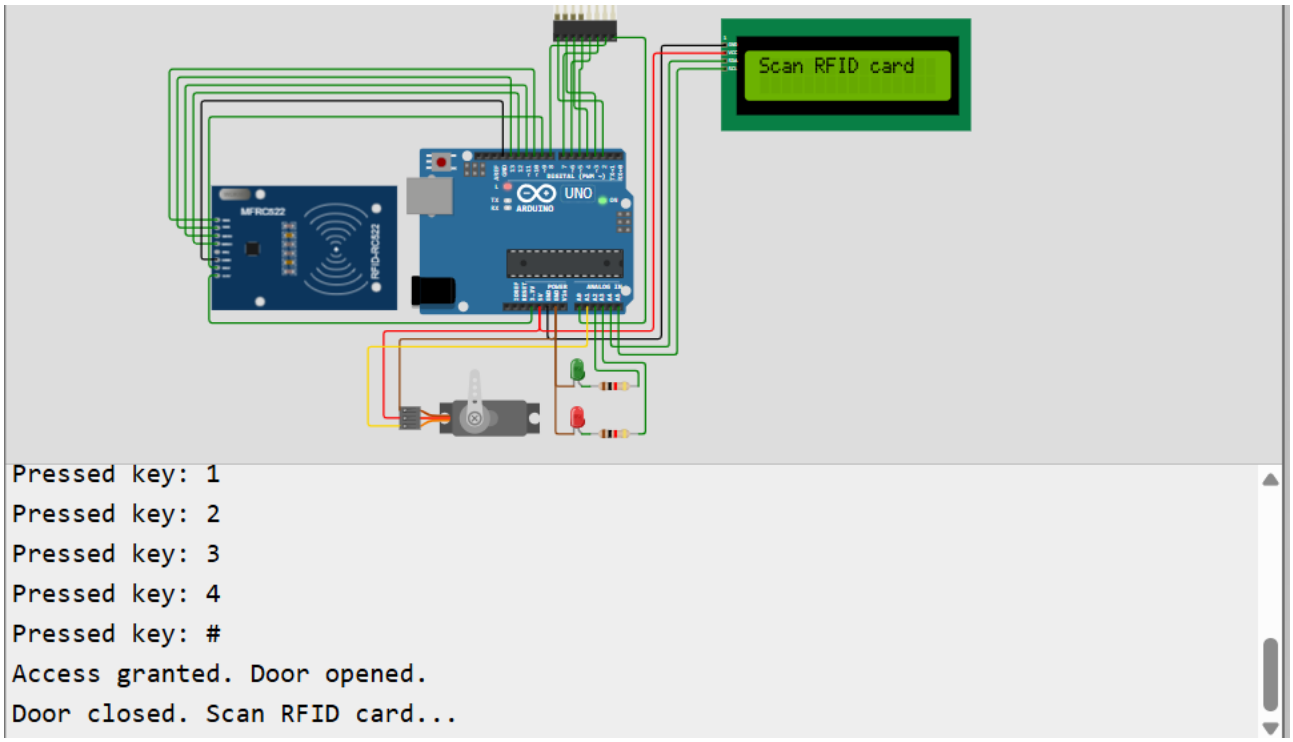


Рисунок 3.6 – Повернення системи до початкового стану після надання доступу

Результат, наведений на рисунку 3.6, підтверджує, що після успішної автентифікації система не залишається у стані відкритого доступу постійно. Сервопривід повертається у початкове положення, зелений світлодіод вимикається, а система знову готова до нового циклу перевірки користувача. Це є важливим для коректної роботи автономного засобу контролю доступу.

Наступним етапом тестування була перевірка реакції системи на неправильний PIN-код. Для цього після успішного зчитування дозволеної RFID-картки було введено неправильну цифрову комбінацію та підтверджено її клавішею #.

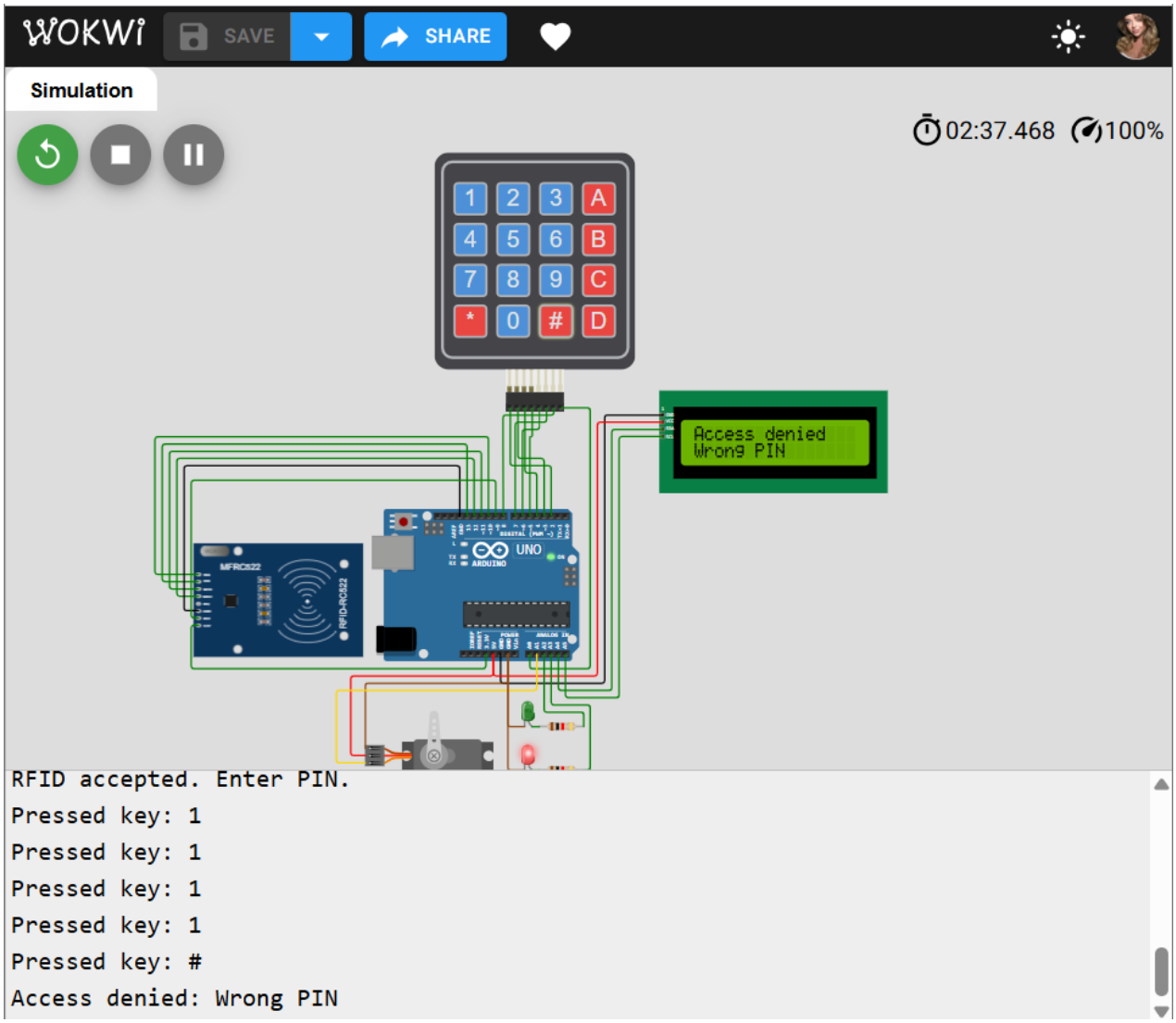


Рисунок 3.7 – Відмова в доступі після введення неправильного PIN-коду

На рисунку 3.7 видно, що після введення неправильного PIN-коду система сформувала повідомлення про відмову в доступі. У Serial Monitor відображено натиснуті клавіші та повідомлення Access denied: Wrong PIN. При цьому сервопривід залишається у початковому положенні, а червоний світлодіод сигналізує про помилку. Це підтверджує, що система не надає доступ за умови

правильного RFID-ідентифікатора, якщо другий фактор автентифікації не пройдено.

Після помилкового введення PIN-коду система скидає поточний стан автентифікації. Це означає, що наступна спроба доступу знову повинна починатися зі зчитування RFID-картки. Такий підхід підвищує захищеність системи, оскільки користувач не може необмежено підбирати PIN-код після одного успішного зчитування картки.

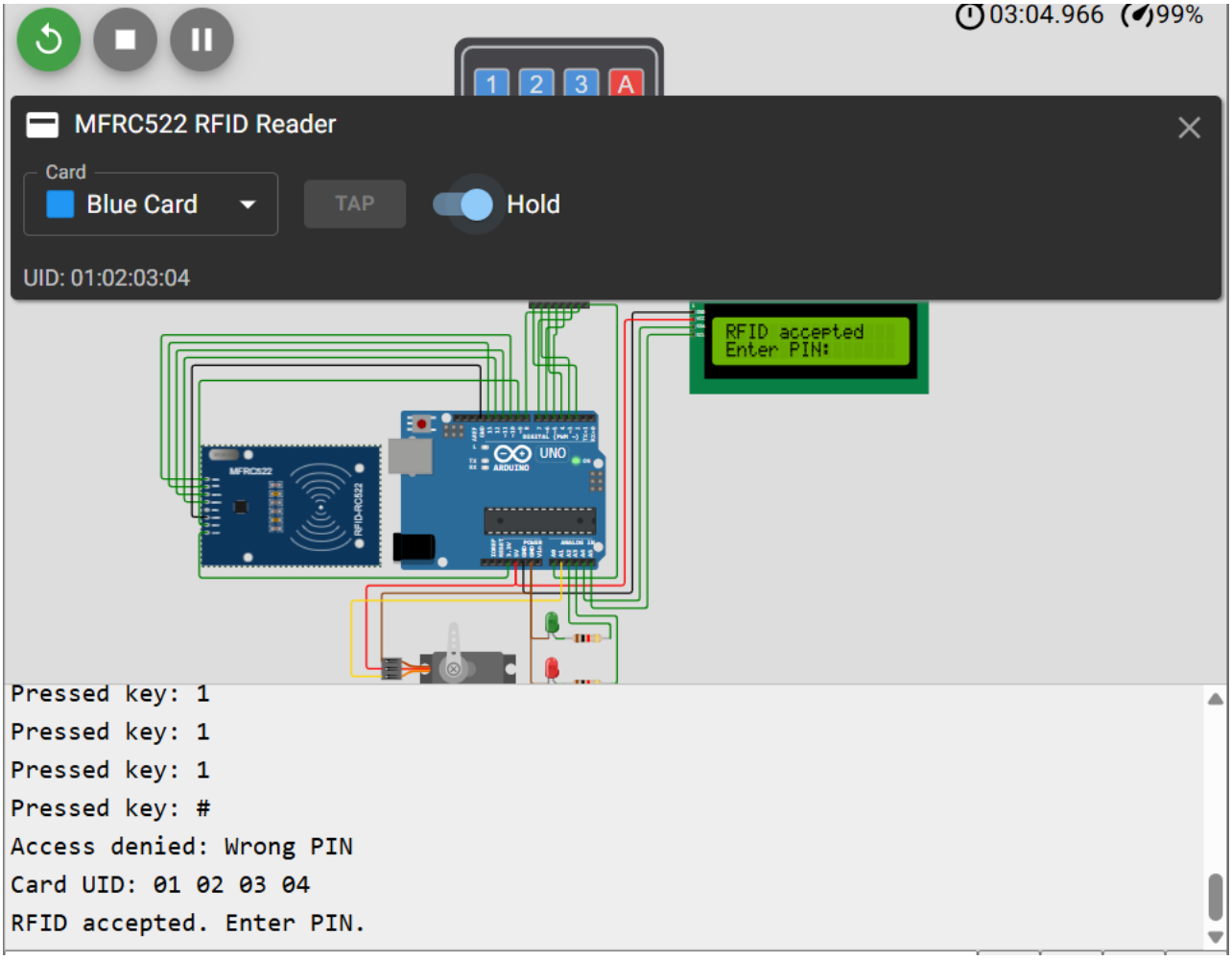


Рисунок 3.8 – Повторний перехід до введення PIN-коду після нової спроби автентифікації

На рисунку 3.8 показано, що після повторного зчитування дозволеної RFID-картки система знову переходить до очікування PIN-коду. Це підтверджує

правильну роботу логіки скидання станів після помилкової спроби та повернення до початкового етапу автентифікації.

Для перевірки механізму захисту від підбору PIN-коду було виконано три послідовні неправильні спроби введення коду. Після кожної помилки система збільшувала лічильник невдалих спроб і формувала повідомлення про відмову в доступі. До моменту досягнення третьої помилки система дозволяла повторити автентифікацію, однак після третьої неправильної спроби автоматично переходила у режим тимчасового блокування.

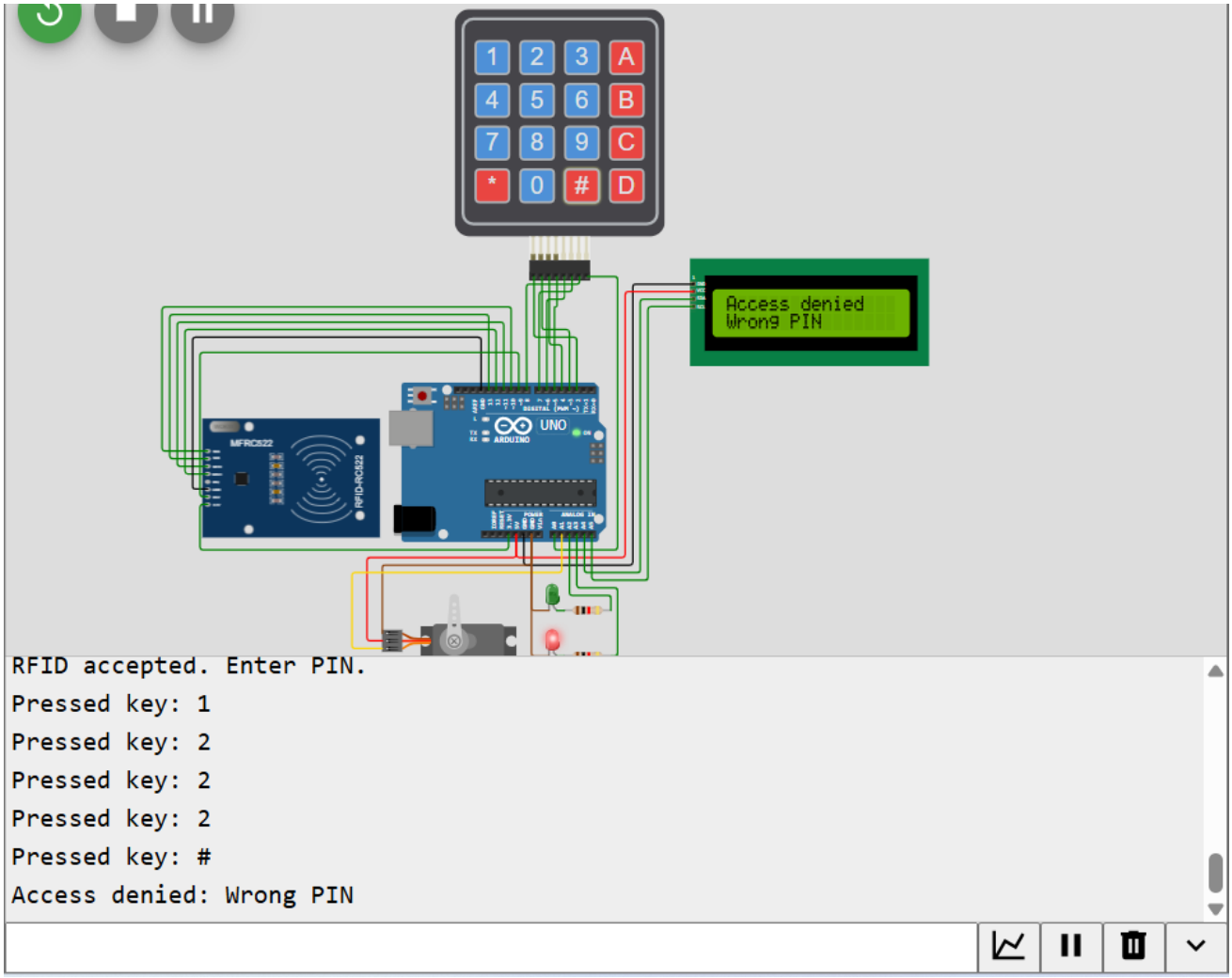


Рисунок 3.9 – Повторне введення неправильного PIN-коду

На рисунку 3.9 наведено приклад чергової неправильної спроби введення PIN-коду. У Serial Monitor відображено натиснуті клавіші та повідомлення про

помилку. Сервопривід не змінює положення, доступ не відкривається, а система фіксує помилкову спробу. Це підтверджує правильну роботу лічильника невдалих спроб.

Після третьої неправильної спроби введення PIN-коду система переходить у режим тимчасового блокування на 10 секунд. У цьому стані нові спроби автентифікації не обробляються, а користувач отримує відповідне повідомлення на LCD-дисплеї.

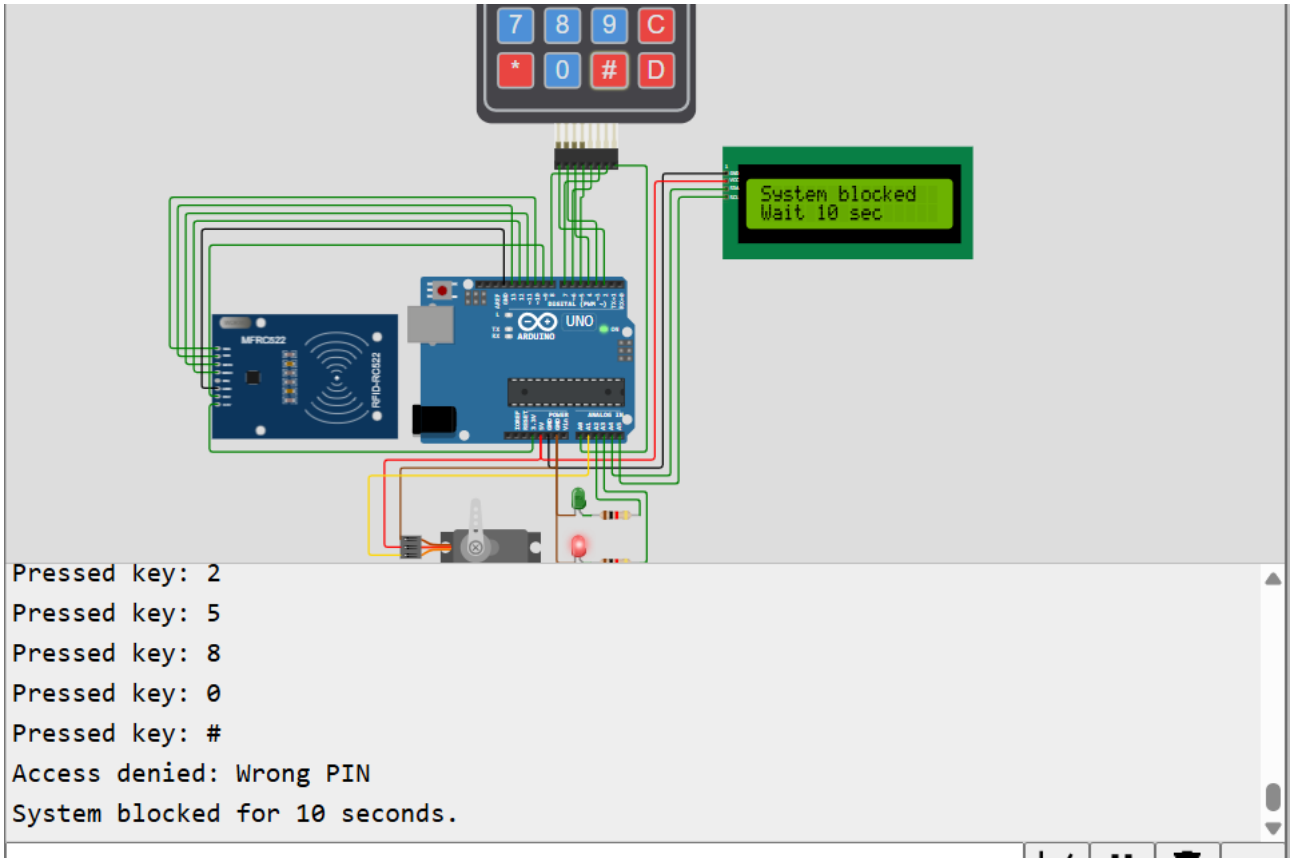


Рисунок 3.10 – Тимчасове блокування системи після трьох невдалих спроб введення PIN-коду

Як видно з рисунка 3.10, на LCD-дисплеї відображається повідомлення System blocked / Wait 10 sec, а в Serial Monitor виводиться повідомлення про блокування системи на 10 секунд. Червоний світлодіод сигналізує про помилковий стан системи. Це підтверджує, що механізм блокування спрацьовує саме після трьох невдалих спроб введення PIN-коду та працює відповідно до

заданого алгоритму. Після завершення часу блокування система скидає лічильник помилок і повертається до режиму очікування RFID-картки.

Окремо було перевірено реакцію системи на недозволену RFID-картку. Для цього у віртуальному зчитувачі MFRC522 було обрано картку, UID-код якої не відповідає дозволеному значенню 01 02 03 04, заданому в програмі. Метою цього тесту було перевірити, чи блокує система подальшу автентифікацію у випадку неправильного першого фактора. Під час такого сценарію система не переходить до етапу введення PIN-коду, а одразу формує відмову в доступі, вмикає червоний світлодіод і збільшує лічильник невдалих спроб.

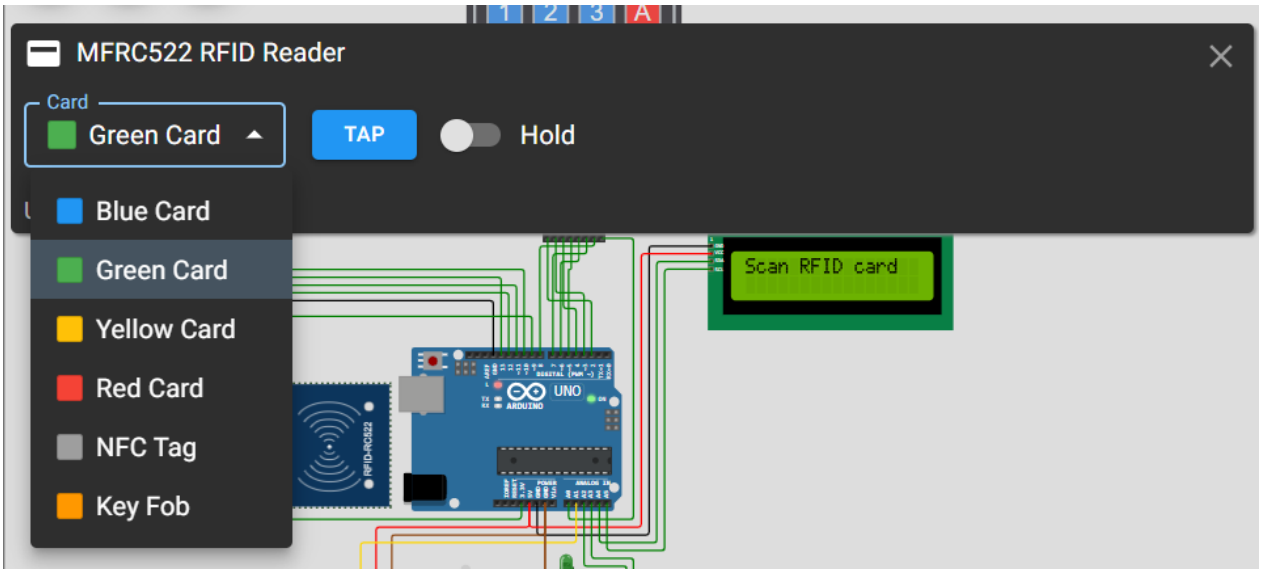


Рисунок 3.11 – Вибір недозволеної RFID-картки у середовищі Wokwi

На рисунку 3.11 показано вибір іншої RFID-картки у віртуальній панелі зчитувача. Після її піднесення до RFID-зчитувача система зчитує UID-код і порівнює його з дозволеним значенням. Оскільки UID не збігається з дозволеним ідентифікатором, система не переходить до введення PIN-коду. У цьому випадку одразу формується відмова в доступі: на LCD-дисплей виводиться повідомлення про помилку, вмикається червоний світлодіод, а лічильник невдалих спроб збільшується на одиницю. Така реакція підтверджує, що перший етап

автентифікації є обов'язковим, а подальше введення PIN-коду можливе лише після зчитування дозволеної RFID-картки

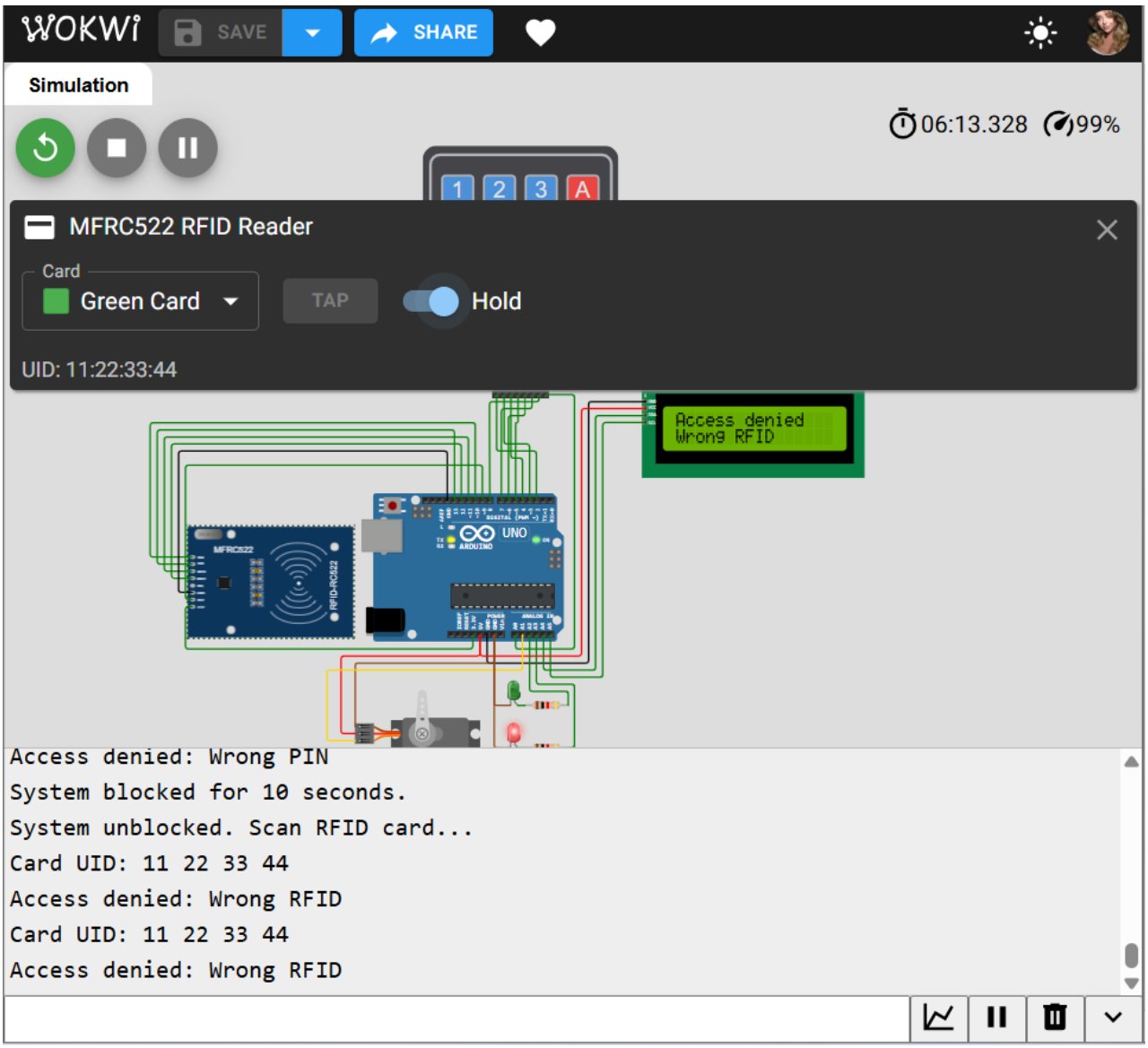


Рисунок 3.12 – Відмова в доступі після зчитування недозволеної RFID-картки

На рисунку 3.12 видно, що після зчитування недозволеної RFID-картки система формує повідомлення про помилку RFID-ідентифікатора. У Serial Monitor відображається UID-код картки, який не відповідає дозволеному значенню, після чого виводиться повідомлення Access denied: Wrong RFID. У цьому випадку сервопривід залишається у початковому положенні, доступ не відкривається, а введення PIN-коду не запитується. Це підтверджує, що перший

етап автентифікації є обов'язковим і без його успішного проходження система не дозволяє перейти до другого етапу перевірки.

Крім одноразової перевірки недозволеної RFID-картки, було протестовано реакцію системи на кілька послідовних неправильних RFID-ідентифікаторів. Для цього у середовищі Wokwi тричі було виконано зчитування картки з UID-кодом 11 22 33 44, який не відповідає дозволеному значенню 01 02 03 04.

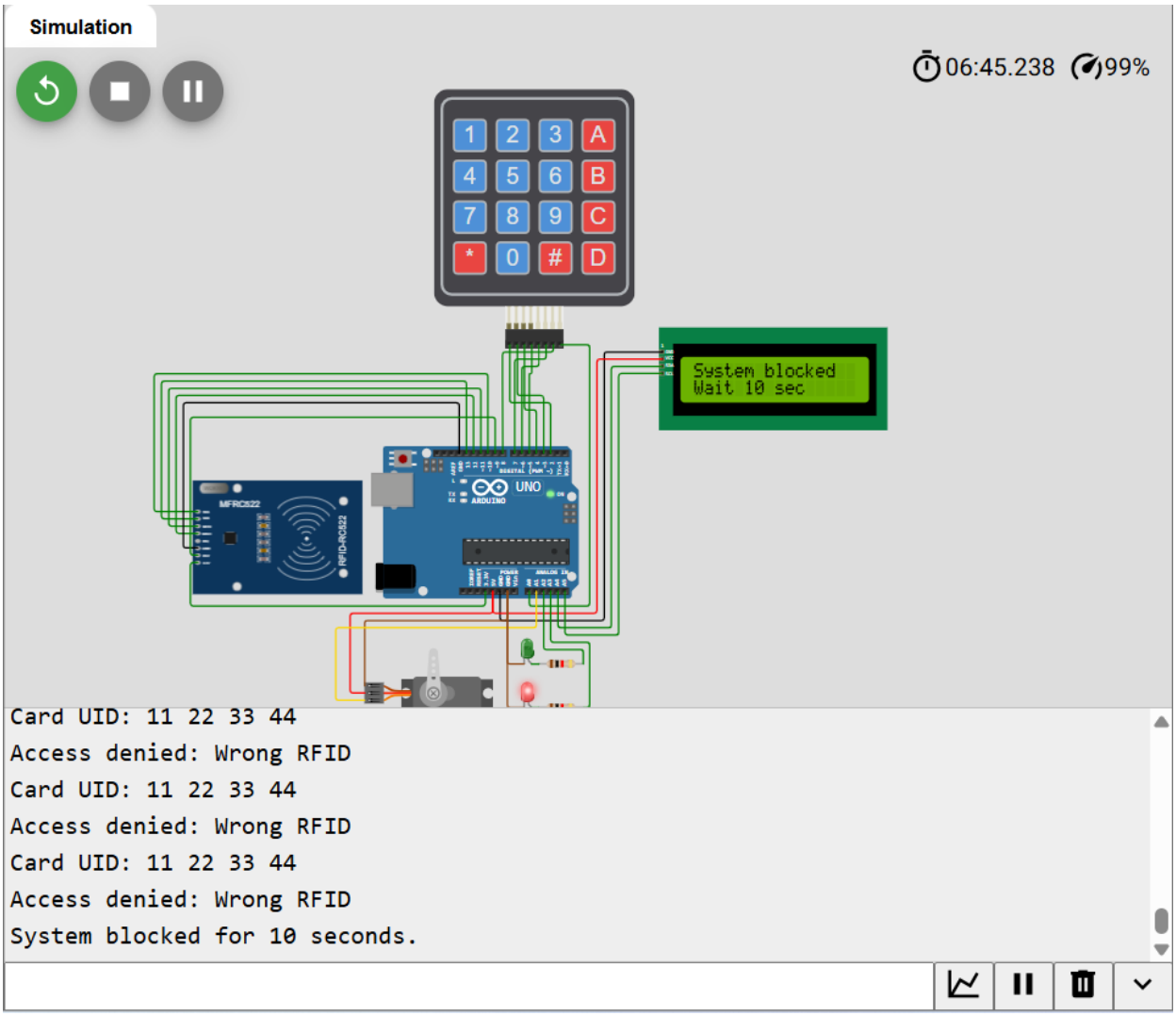


Рисунок 3.13 – Тимчасове блокування системи після трьох невдалих спроб зчитування RFID-картки

На рисунку 3.13 видно, що після кожного зчитування недозволеної RFID-картки у Serial Monitor відображається повідомлення Access denied: Wrong RFID.

Після третьої невдалої спроби система переходить у режим тимчасового блокування на 10 секунд. На LCD-дисплеї відображається повідомлення System blocked / Wait 10 sec, а червоний світлодіод сигналізує про помилковий стан системи. Це підтверджує, що механізм блокування спрацьовує не лише після трьох неправильних введень PIN-коду, а й після трьох невдалих спроб автентифікації за RFID-карткою. Після завершення часу блокування лічильник помилок скидається, а система знову переходить у режим очікування RFID-картки. Така поведінка забезпечує однакову реакцію системи на багаторазові помилки незалежно від того, на якому етапі автентифікації вони виникли.

Для узагальнення результатів тестування було перевірено декілька сценаріїв роботи системи, що охоплюють як успішну автентифікацію, так і помилкові дії користувача. Окремо перевірялися реакція системи на дозволену та недозволену RFID-картку, правильне і неправильне введення PIN-коду, а також спрацювання механізму тимчасового блокування після трьох невдалих спроб автентифікації. Результати перевірки наведено в таблиці 3.2.

Таблиця 3.2 – Результати тестування роботи програмно-технічного засобу контролю доступу

Сценарій тестування	Очікувана реакція системи	Отриманий результат
Початковий запуск системи	Ініціалізація компонентів і перехід у режим очікування RFID-картки	На LCD-дисплеї відображено повідомлення про очікування RFID-картки, у Serial Monitor виведено повідомлення про запуск системи
Піднесення дозволеної RFID-картки з UID 01 02 03 04	Прийняття RFID-картки та перехід до введення PIN-коду	Система зчитала дозволений UID, вивела повідомлення RFID accepted / Enter PIN і перейшла до другого етапу автентифікації

Продовження таблиці 3.2

Піднесення недозволеної RFID-картки з UID 11 22 33 44	Відмова в доступі без переходу до введення PIN-коду	Система вивела повідомлення Access denied: Wrong RFID, доступ не надала, введення PIN-коду не запитувалося
Три послідовні зчитування недозволеної RFID-картки з UID 11 22 33 44	Тимчасове блокування системи на 10 секунд	Після третьої невдалої RFID-спроби система перейшла у режим блокування, на LCD-дисплеї відображено System blocked / Wait 10 sec
Введення правильного PIN-коду 1234 після дозволеної RFID-картки	Надання доступу, активація сервоприводу та вмикання зеленого світлодіода	На LCD-дисплеї відображено повідомлення Access granted / Door opened, сервопривід перейшов у положення відкриття, зелений світлодіод увімкнувся
Повернення системи після успішного доступу	Виконавчий механізм повертається у початкове положення, система знову очікує RFID-картку	Сервопривід повернувся у положення закритого доступу, зелений світлодіод вимкнувся, система перейшла до початкового стану
Введення неправильного PIN-коду після дозволеної RFID-картки	Відмова в доступі, вмикання червоного світлодіода, збільшення лічильника помилок	Доступ не відкрито, у Serial Monitor виведено повідомлення Access denied: Wrong PIN, червоний світлодіод сигналізував про помилку

Кінець таблиці 3.2

Три послідовні неправильні спроби введення PIN-коду	Тимчасове блокування системи на 10 секунд	Після третьої невдалої PIN-спроби система перейшла у режим блокування, на LCD-дисплеї відображено System blocked / Wait 10 sec
Завершення часу блокування	Скидання лічильника помилок і повернення до режиму очікування RFID-картки	Після завершення 10 секунд блокування система повернулася до початкового стану та знову очікувала RFID-картку

Проведене тестування підтвердило правильність роботи основних режимів програмно-технічного засобу контролю доступу. Система коректно розпізнає дозволену RFID-картку з UID 01 02 03 04 і лише після цього переходить до другого етапу автентифікації — введення PIN-коду. Якщо RFID-картка має інший UID, зокрема 11 22 33 44, система одразу формує відмову в доступі, не активує виконавчий механізм і не запитує введення PIN-коду.

Успішна автентифікація відбувається тільки за умови послідовного виконання двох етапів: зчитування дозволеної RFID-картки та введення правильного PIN-коду 1234. У цьому випадку система вмикає зелений світлодіод, виводить на LCD-дисплей повідомлення про надання доступу та переводить сервопривід у положення відкриття доступу. Після завершення заданого часу сервопривід повертається у початкове положення, а система знову переходить до очікування RFID-картки.

У разі введення неправильного PIN-коду або зчитування недозволеної RFID-картки доступ не надається. Система виводить повідомлення про помилку, вмикає червоний світлодіод і збільшує лічильник невдалих спроб. Після трьох послідовних невдалих спроб автентифікації система переходить у режим

тимчасового блокування на 10 секунд. Це стосується як помилок введення PIN-коду, так і неправильних RFID-ідентифікаторів.

Отже, результати тестування у середовищі Wokwi підтвердили працездатність розробленого програмно-технічного засобу контролю доступу. Реалізована система забезпечує послідовну двофакторну автентифікацію RFID + PIN-код, коректно реагує на дозволені й недозволені RFID-картки, розрізняє правильне та неправильне введення PIN-коду, керує виконавчим механізмом, відображає стан системи на LCD-дисплеї та виконує тимчасове блокування після трьох невдалих спроб автентифікації.

3.5 Висновки до третього розділу

У третьому розділі було виконано програмно-апаратну реалізацію програмно-технічного засобу контролю доступу до приміщення. На основі обраної структури пристрою було розроблено схему підключення компонентів до мікроконтролерної плати Arduino Uno та визначено призначення використаних виводів для RFID-зчитувача RC522, матричної клавіатури, LCD-дисплея, сервоприводу та світлодіодної індикації.

Описано програмну реалізацію пристрою, яка забезпечує послідовне виконання алгоритму двофакторної автентифікації. Програмна частина побудована за модульним принципом і включає функції для зчитування RFID-картки, перевірки PIN-коду, надання або заборони доступу, керування виконавчим механізмом, відображення повідомлень на LCD-дисплеї та блокування системи після невдалих спроб автентифікації.

Моделювання роботи пристрою було виконано у середовищі Wokwi. У процесі моделювання перевірено початковий стан системи, зчитування дозволеної та недозволеної RFID-картки, введення правильного й неправильного PIN-коду, надання доступу, повернення виконавчого механізму у початкове положення та перехід системи в режим тимчасового блокування.

За результатами тестування встановлено, що доступ до приміщення надається лише після успішного проходження двох етапів автентифікації: зчитування дозволеної RFID-картки з UID 01 02 03 04 та введення правильного PIN-коду 1234. У разі використання недозволеної RFID-картки або неправильного PIN-коду система формує відмову в доступі, не активує виконавчий механізм і повідомляє користувача про помилку.

Також підтверджено роботу механізму тимчасового блокування. Після трьох послідовних невдалих спроб автентифікації система переходить у заблокований стан на 10 секунд. Блокування спрацьовує як у випадку неправильного введення PIN-коду, так і в разі повторного зчитування недозволеної RFID-картки. Це підвищує захищеність пристрою від підбору коду або багаторазового використання недозволеного ідентифікатора.

Отже, результати програмно-апаратної реалізації та моделювання підтвердили працездатність розробленого програмно-технічного засобу контролю доступу. Система забезпечує послідовну автентифікацію RFID + PIN-код, керування виконавчим механізмом, відображення стану на LCD-дисплеї, світлову індикацію результатів перевірки та тимчасове блокування після трьох невдалих спроб доступу. Таким чином, поставлене завдання розроблення автономного засобу контролю доступу до приміщення в межах програмно-апаратної реалізації було виконано.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень було розроблено програмно-технічний засіб контролю доступу до приміщення з використанням комбінованої автентифікації користувача. Розроблена система передбачає послідовну перевірку двох факторів доступу: RFID-картки та PIN-коду. Такий підхід дозволяє підвищити рівень захищеності порівняно з рішеннями, у яких використовується лише один спосіб ідентифікації користувача.

У першому розділі проведено аналіз теоретичних основ систем контролю доступу. Розглянуто їх призначення, принцип функціонування, основні структурні компоненти та класифікацію за способом ідентифікації, архітектурою побудови й рівнем функціональної складності. Також проаналізовано промислові системи контролю доступу та приклади готових рішень. Встановлено, що промислові мережеві системи мають широкий функціонал і високу масштабованість, однак для контролю доступу до одного приміщення є надлишковими через складність впровадження, вартість і потребу в додатковій інфраструктурі. У результаті обґрунтовано доцільність використання автономного засобу з комбінованою автентифікацією RFID + PIN-код.

У другому розділі проведено обґрунтування структури розроблюваного пристрою та вибір його основних апаратних компонентів. Як центральний блок керування обрано мікроконтролерну платформу Arduino Uno, яка має достатню кількість виводів, підтримує необхідні інтерфейси SPI та I2C і є придатною для реалізації автономної системи контролю доступу. До складу пристрою включено RFID-зчитувач RC522, матричну клавіатуру 4x4, LCD-дисплей 16x2 з I2C-інтерфейсом, сервопривід як умовний виконавчий механізм, а також зелений і червоний світлодіоди для індикації стану системи.

У цьому ж розділі описано алгоритм функціонування програмно-технічного засобу. Алгоритм передбачає початкову ініціалізацію компонентів,

очікування RFID-картки, перевірку UID-коду, перехід до введення PIN-коду лише після прийняття дозволеної картки, перевірку введеного коду та формування рішення про дозвіл або заборону доступу. Для підвищення рівня захисту передбачено тимчасове блокування системи після трьох невдалих спроб автентифікації.

У третьому розділі виконано програмно-апаратну реалізацію розробленого засобу контролю доступу. Розроблено схему підключення компонентів до Arduino Uno, описано призначення використаних виводів та особливості взаємодії RFID-зчитувача, клавіатури, LCD-дисплея, сервоприводу і світлодіодів. Програмна реалізація побудована за модульним принципом: окремі функції відповідають за зчитування RFID-картки, обробку PIN-коду, надання доступу, відмову в доступі, керування блокуванням і повернення системи до початкового стану.

Моделювання та тестування пристрою виконано у середовищі Wokwi. Перевірено основні сценарії роботи системи: дозволена та недозволена RFID-картка, правильний і неправильний PIN-код, надання й відмова в доступі, робота LCD-дисплея, світлодіодної індикації, сервоприводу та механізму блокування. Результати підтвердили, що доступ надається лише після успішного проходження двох етапів автентифікації, а після трьох невдалих спроб система переходить у режим блокування на 10 секунд.

Отже, поставлену мету кваліфікаційної роботи досягнуто. Розроблено працездатну модель автономного програмно-технічного засобу контролю доступу до приміщення, яка забезпечує двофакторну автентифікацію RFID + PIN-код, керування виконавчим механізмом, відображення стану системи, світлову індикацію та захист від багаторазових помилкових спроб. Запропоноване рішення може бути основою для подальшої фізичної реалізації або вдосконалення системи контролю доступу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Veľas A., Boroš M., Kuffa R., Lenko F. Testing of Permeability of RFID Access Control System for the Needs of Security Management. *Applied Sciences*. 2024. Vol. 14, No. 10. Article 4227. URL: https://doi.org/10.3390/app14104227 (дата звернення: 03.05.2026).

2. Kassim S. O., Idriss A. S., Ahmed A. I. Implementation of a Sustainable Security Architecture using Radio Frequency Identification (RFID) Technology for Access Control. *arXiv*. 2023. URL: https://arxiv.org/abs/2304.04628 (дата звернення: 06.05.2026).

3. Ishaq K., Bibi S. IoT Based Smart Attendance System Using RFID: A Systematic Literature Review. *arXiv*. 2023. URL: https://arxiv.org/abs/2308.02591 (дата звернення: 03.05.2026).

4. Багатофакторна автентифікація. iIT Distribution. URL: https://iitd.ua/bagatofaktorna-avtentifikacziya/ (дата звернення: 10.05.2026).

5. Rusten-Andrei I., Bizon N., Dragusin S.-A. Design of an Arduino-Based Intelligent Access Control System with Priority Levels. *Journal of Electrical Engineering, Electronics, Control and Computer Science*. 2025. Vol. 11, No. 3. URL: https://jeeeccs.net/index.php/journal/article/view/400 (дата звернення: 10.05.2026).

6. Як створити зчитувач RFID на Arduino. Transfer Multisort Elektronik. URL: https://www.tme.eu/ua/news/library-articles/diy/page/70872/iak-stvoriti-zchituvach-rfid-na-arduino/ (дата звернення: 30.05.2026).

7. RFID-модуль RC522: повний посібник з опису, підключення і перших кроків у розробці. ID Card. URL: https://idcard.com.ua/ua/blog/rfid-modul-rc522-polnoe-rukovodstvo-po-opisaniyu-podklyucheniyu-i-pervym-shagam-v-razrabotke/ (дата звернення: 11.05.2026).

8. Double-Layered Authentication Door-Lock System Utilizing Hybrid RFID and Keypad Verification. *Engineering Proceedings*. 2025. Vol. 23, No. 1. Article 19. URL: https://www.mdpi.com/2673-4605/23/1/19 (дата звернення: 11.05.2026).

9. Bolid S2000-K User Manual. Orion Integrated Security System. ManualsLib. URL: https://www.manualslib.com/manual/1183473/Bolid-S2000-K.html (дата звернення: 17.05.2026).

10. Bolid S2000-2 User Manual. Access Controller. ManualsLib. URL: https://www.manualslib.com/manual/740416/Bolid-S2000-2.html (дата звернення: 14.05.2026).

11. Системи контролю доступу. Українські Інфосистеми. URL: https://ukrinfosystems.com.ua/uk/design-and-construction/access-control-systems (дата звернення: 19.05.2026).

12. Access Control Products. Hikvision. URL: https://www.hikvision.com/en/products/Access-Control-Products/ (дата звернення: 10.05.2026).

13. Access Control. ZKTeco. URL: https://www.zkteco.com/en/AccessControl (дата звернення: 23.05.2026).

14. RFID зчитувач для карток 13.56 MHz на базі ARDUINO Pro Micro. Arduino.ua. URL: https://arduino.ua/art138-rfid-zchityvach-dlya-kartok-13-56-mhz-na-bazi-arduino-pro-micro (дата звернення: 19.05.2026).

15. ESP32 Series Datasheet. Espressif Systems. URL: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf (дата звернення: 15.05.2026).

16. Комплекти контролю доступу. SEVEN Systems. URL: https://seven-systems.com.ua/ua/g83640007-komplekty-kontrolya-dostupa (дата звернення: 19.05.2026).

17. Зчитувачі карт доступу Варта. ROZETKA. URL: https://rozetka.com.ua/ua/schitivateli-kart-dostupa/c4650471/producer%3Dvarta-systems/ (дата звернення: 15.05.2026).

18. ATIS — передові технології безпеки. URL: https://atis-security.com/ua/ (дата звернення: 14.05.2026).

19. Зчитувачі карт доступу ATIS. ROZETKA. URL: https://rozetka.com.ua/ua/schitivateli-kart-dostupa/c4650471/producer%3Datis/ (дата звернення: 03.05.2026).

20. Як використовувати модуль зчитування RFID RC522 з Arduino для контролю доступу. Hardware Libre. URL: https://uk.hwlibre.com/як-використовувати-модуль-зчитування-RFID-rc522-з-arduino-для-контролю-доступу/ (дата звернення: 01.05.2026).

21. Що таке двофакторна автентифікація? Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa (дата звернення: 07.05.2026).

22. Arduino Uno Rev3. Arduino Documentation. URL: https://docs.arduino.cc/hardware/uno-rev3/ (дата звернення: 07.05.2026).

23. Arduino & Serial Peripheral Interface. Arduino Documentation. URL: https://docs.arduino.cc/learn/communication/spi/ (дата звернення: 20.05.2026).

24. Inter-Integrated Circuit (I2C) Protocol. Arduino Documentation. URL: https://docs.arduino.cc/learn/communication/wire/ (дата звернення: 20.05.2026).

25. Arduino Docs. Arduino Documentation. URL: https://docs.arduino.cc/ (дата звернення: 20.05.2026).

26. Мікроконтролер ESP32. IT Master. URL: https://itmaster.biz.ua/directory/microcontrollers/esp32.html (дата звернення: 21.05.2026).

27. MFRC522 RFID Reader. Wokwi Docs. URL: https://docs.wokwi.com/parts/board-mfrc522 (дата звернення: 14.05.2026).

28. SPI. Arduino Documentation. URL: https://docs.arduino.cc/language-reference/en/functions/communication/SPI/ (дата звернення: 17.05.2026).

29. Keypad. Arduino Documentation. URL: https://docs.arduino.cc/libraries/keypad/ (дата звернення: 13.05.2026).

30. Arduino Keypad Tutorial. ArduinoGetStarted. URL: https://arduinogetstarted.com/tutorials/arduino-keypad (дата звернення: 03.05.2026).

31. LCD 1602 I2C. Wokwi Docs. URL: https://docs.wokwi.com/parts/wokwi-lcd1602 (дата звернення: 03.05.2026).

32. LiquidCrystal I2C. Arduino Documentation. URL: https://docs.arduino.cc/libraries/liquidcrystal-i2c/ (дата звернення: 05.05.2026).

33. Servo Motor. Wokwi Docs. URL: https://docs.wokwi.com/parts/wokwi-servo (дата звернення: 05.05.2026).

34. Servo Motor Basics with Arduino. Arduino Documentation. URL: https://docs.arduino.cc/learn/electronics/servo-motors/ (дата звернення: 05.05.2026).

35. digitalWrite(). Arduino Documentation. URL: https://docs.arduino.cc/language-reference/en/functions/digital-io/digitalwrite/ (дата звернення: 20.05.2026).

36. Arduino Language Reference. Arduino Documentation. URL: https://docs.arduino.cc/language-reference/ (дата звернення: 04.05.2026).

37. Servo. Arduino Documentation. URL: https://docs.arduino.cc/libraries/servo/ (дата звернення: 15.05.2026).

38. delay(). Arduino Documentation. URL: https://docs.arduino.cc/language-reference/en/functions/time/delay/ (дата звернення: 15.05.2026).

39. millis(). Arduino Documentation. URL: https://docs.arduino.cc/language-reference/en/functions/time/millis/ (дата звернення: 08.05.2026).

40. Wokwi Docs. URL: https://docs.wokwi.com/ (дата звернення: 21.05.2026).

41. Arduino IDE 2. Arduino Documentation. URL: https://docs.arduino.cc/software/ide-v2/ (дата звернення: 17.05.2026).

42. SPI. Arduino Documentation. URL: https://docs.arduino.cc/language-reference/en/functions/communication/SPI/ (дата звернення: 13.05.2026).

43. MFRC522. Arduino Libraries. URL: https://docs.arduino.cc/libraries/mfrc522/ (дата звернення: 21.05.2026).

44. Wire. Arduino Documentation. URL: https://docs.arduino.cc/language-reference/en/functions/communication/wire/ (дата звернення: 21.05.2026).

45. Keypad. Arduino Libraries. URL: https://docs.arduino.cc/libraries/keypad/ (дата звернення: 17.05.2026).

46. LiquidCrystal I2C. Arduino Libraries. URL: https://docs.arduino.cc/libraries/liquidcrystal-i2c/ (дата звернення: 15.05.2026).

47. Servo. Arduino Libraries. URL: https://docs.arduino.cc/libraries/servo/ (дата звернення: 20.05.2026).

48. The Serial Monitor. Wokwi Docs. URL: https://docs.wokwi.com/guides/serial-monitor (дата звернення: 20.05.2026).

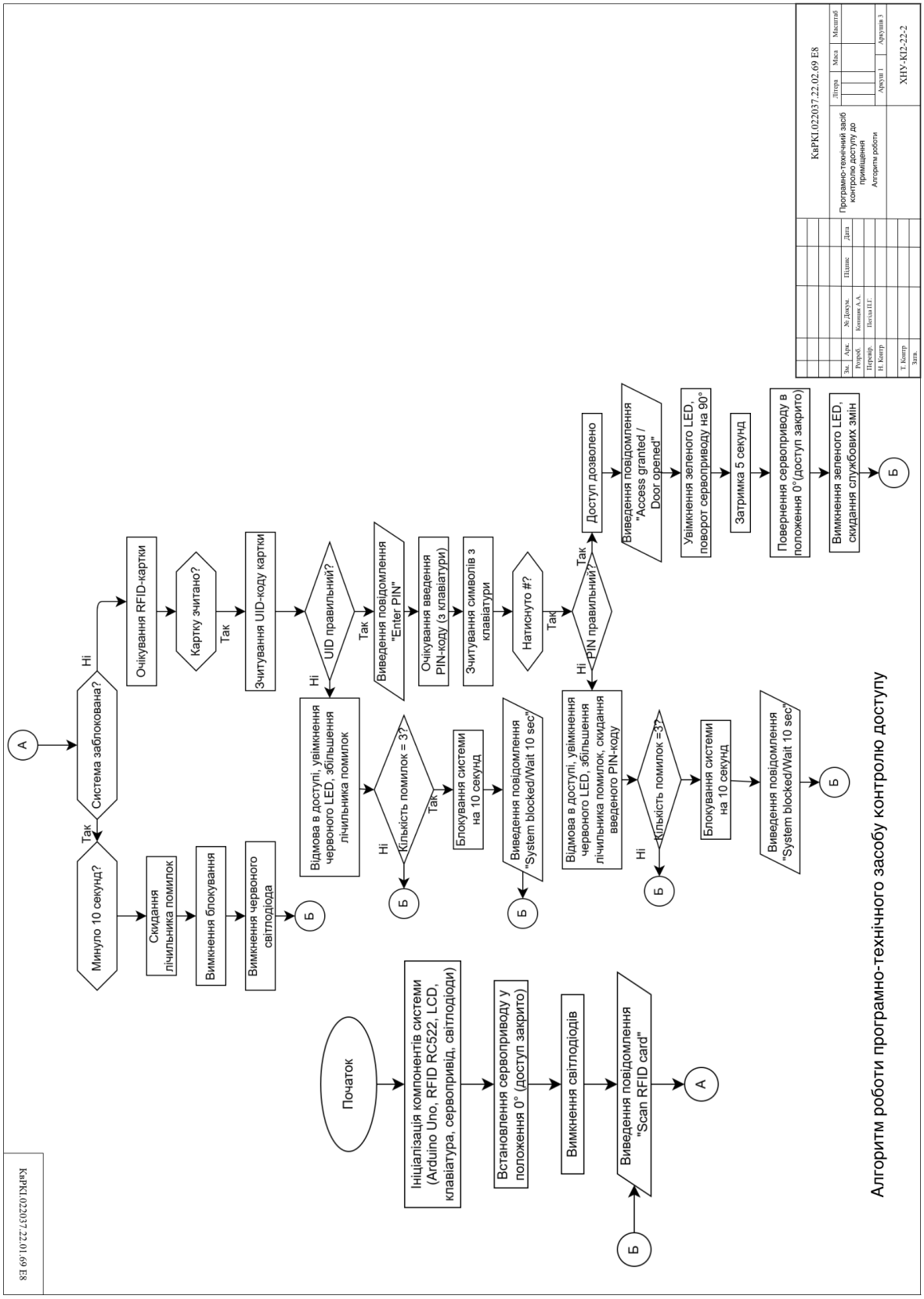
49. Arduino Uno. Wokwi Docs. URL: https://docs.wokwi.com/parts/wokwi-arduino-uno (дата звернення: 21.05.2026).

50. Intelligent Door Entry: RFID-Based Authentication with PIN and Keystroke Profiling. *Proceedings of ICCSCE* 2025. Atlantis Press. 2025. URL: https://www.atlantis-press.com/proceedings/iccsce-25/126017312 (дата звернення: 23.05.2026).

ДОДАТОК А

(обов’язковий)

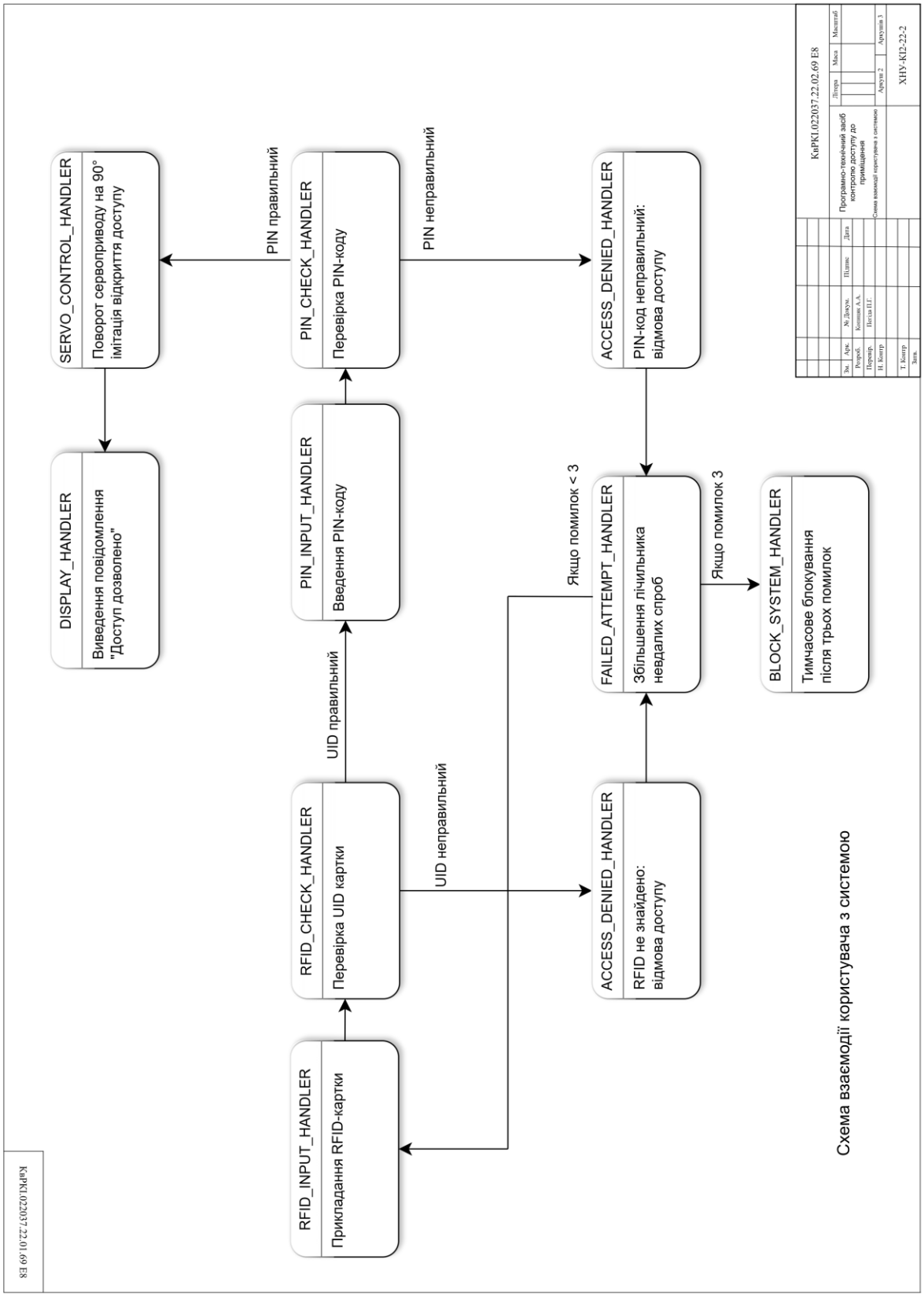
Копія креслення «Алгоритм роботи»



ДОДАТОК Б

(обов’язковий)

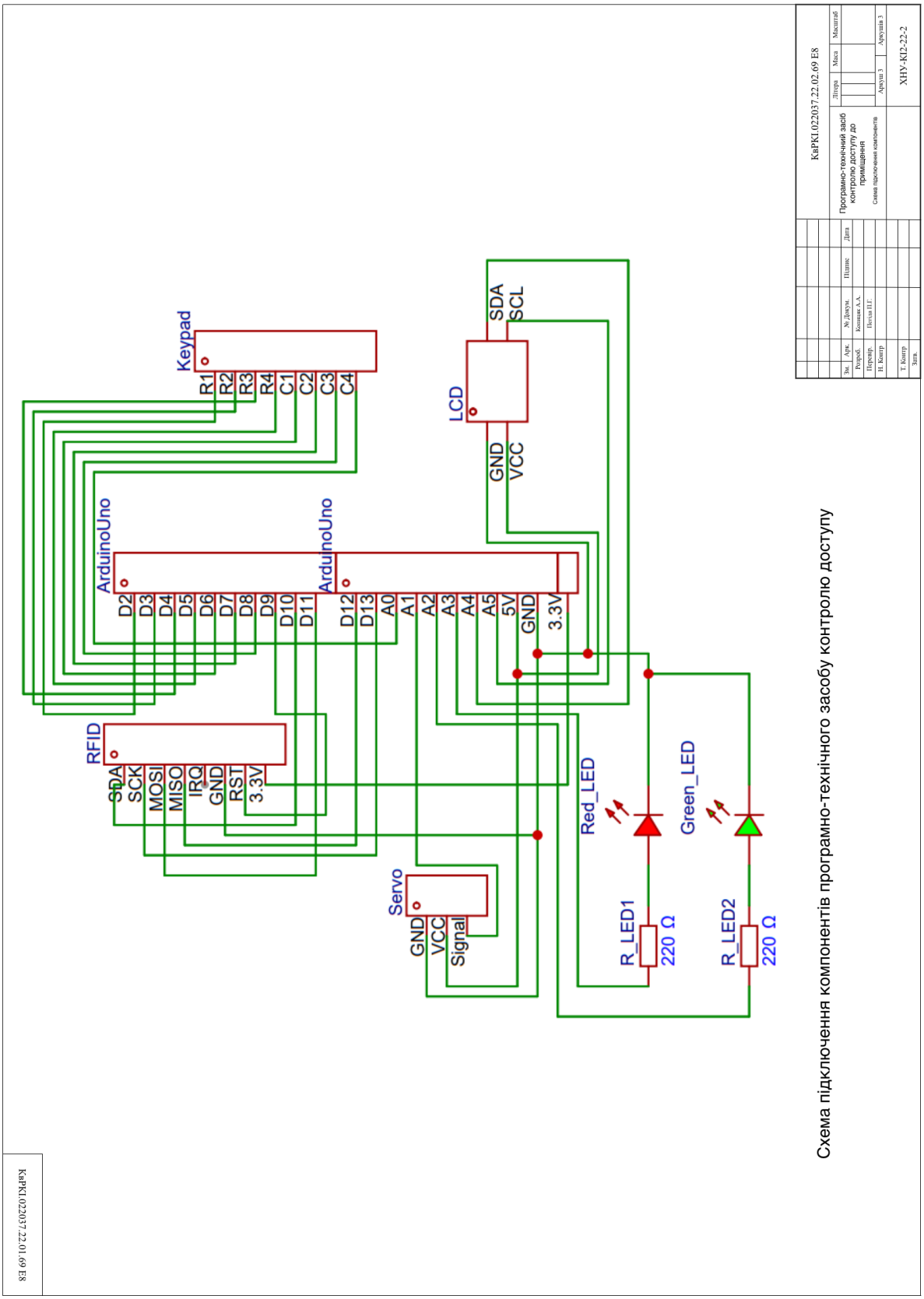
Копія креслення «Схема взаємодії користувача з системою»



ДОДАТОК В

(обов’язковий)

Копія креслення «Схема підключення компонентів»



ДОДАТОК Г

(обов’язковий)

Лістинг коду

```
#include <SPI.h>
#include <MFRC522.h>
#include <Keypad.h>
#include <Servo.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#define SS_PIN 10
#define RST_PIN 9
#define SERVO_PIN A1
#define GREEN_LED A2
#define RED_LED A3

MFRC522 rfid(SS_PIN, RST_PIN);
Servo doorServo;
LiquidCrystal_I2C lcd(0x27, 16, 2);

const byte ROWS = 4;
const byte COLS = 4;

char keys[ROWS][COLS] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};

byte rowPins[ROWS] = {2, 3, 4, 5};
byte colPins[COLS] = {6, 7, 8, A0};
```

```
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS,
COLS);

String allowedUID = "01 02 03 04";

String correctPIN = "1234";
String enteredPIN = "";

int failedAttempts = 0;
const int maxAttempts = 3;

bool rfidAccepted = false;
bool systemBlocked = false;

unsigned long blockStartTime = 0;
const unsigned long blockDuration = 10000;

void setup() {
  Serial.begin(9600);

  SPI.begin();
  rfid.PCD_Init();

  lcd.init();
  lcd.backlight();

  doorServo.attach(SERVO_PIN);
  doorServo.write(0);

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

  digitalWrite(GREEN_LED, LOW);
  digitalWrite(RED_LED, LOW);
```

```
  lcd.setCursor(0, 0);
  lcd.print("Access Control");
  lcd.setCursor(0, 1);
  lcd.print("Scan RFID card");

  Serial.println("System started");
  Serial.println("Scan RFID card...");
}

void loop() {
  if (systemBlocked) {
    checkBlockState();
    return;
  }

  if (!rfidAccepted) {
    checkRFID();
  } else {
    checkPIN();
  }
}

void checkRFID() {
  if (!rfid.PICC_IsNewCardPresent()) {
    return;
  }

  if (!rfid.PICC_ReadCardSerial()) {
    return;
  }

  String uid = "";

  for (byte i = 0; i < rfid.uid.size; i++) {
    if (rfid.uid.uidByte[i] < 0x10) {
```

```
    uid += "0";
  }

  uid += String(rfid.uid.uidByte[i], HEX);

  if (i < rfid.uid.size - 1) {
    uid += " ";
  }
}

uid.toUpperCase();

Serial.print("Card UID: ");
Serial.println(uid);

lcd.clear();
lcd.setCursor(0, 0);
lcd.print("UID:");
lcd.setCursor(0, 1);
lcd.print(uid);

delay(1500);

if (uid == allowedUID) {
  rfidAccepted = true;
  enteredPIN = "";

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("RFID accepted");
  lcd.setCursor(0, 1);
  lcd.print("Enter PIN:");

  Serial.println("RFID accepted. Enter PIN.");
} else {
```

```
    accessDenied("Wrong RFID");
  }

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

void checkPIN() {
  char key = keypad.getKey();

  if (key) {
    Serial.print("Pressed key: ");
    Serial.println(key);

    if (key >= '0' && key <= '9') {
      if (enteredPIN.length() < 4) {
        enteredPIN += key;

        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Enter PIN:");
        lcd.setCursor(0, 1);
        lcd.print("PIN: ");

        for (int i = 0; i < enteredPIN.length(); i++) {
          lcd.print("*");
        }
      }
    }

    if (key == '*') {
      enteredPIN = "";

      lcd.clear();
      lcd.setCursor(0, 0);
```

```
      lcd.print("PIN cleared");
      lcd.setCursor(0, 1);
      lcd.print("Enter again");

      delay(1000);

      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("RFID accepted");
      lcd.setCursor(0, 1);
      lcd.print("Enter PIN:");
    }

    if (key == '#') {
      if (enteredPIN == correctPIN) {
        accessGranted();
      } else {
        accessDenied("Wrong PIN");
      }
    }
  }
}

void accessGranted() {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Access granted");
  lcd.setCursor(0, 1);
  lcd.print("Door opened");

  Serial.println("Access granted. Door opened.");

  digitalWrite(GREEN_LED, HIGH);
  digitalWrite(RED_LED, LOW);
```

```
  doorServo.write(90);
  delay(5000);

  doorServo.write(0);
  digitalWrite(GREEN_LED, LOW);

  rfidAccepted = false;
  enteredPIN = "";
  failedAttempts = 0;

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Door closed");
  delay(1000);

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Scan RFID card");

  Serial.println("Door closed. Scan RFID card...");
}

void accessDenied(String reason) {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Access denied");
  lcd.setCursor(0, 1);
  lcd.print(reason);

  Serial.print("Access denied: ");
  Serial.println(reason);

  digitalWrite(RED_LED, HIGH);
  digitalWrite(GREEN_LED, LOW);
```

```
  delay(2000);

  digitalWrite(RED_LED, LOW);

  failedAttempts++;
  rfidAccepted = false;
  enteredPIN = "";

  if (failedAttempts >= maxAttempts) {
    blockSystem();
  } else {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Try again");
    lcd.setCursor(0, 1);
    lcd.print("Attempts: ");
    lcd.print(failedAttempts);

    delay(1500);

    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Scan RFID card");
  }
}

void blockSystem() {
  systemBlocked = true;
  blockStartTime = millis();

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("System blocked");
  lcd.setCursor(0, 1);
  lcd.print("Wait 10 sec");
```

```
  Serial.println("System blocked for 10 seconds.");

  digitalWrite(RED_LED, HIGH);
}

void checkBlockState() {
  if (millis() - blockStartTime >= blockDuration) {
    systemBlocked = false;
    failedAttempts = 0;

    digitalWrite(RED_LED, LOW);

    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("System ready");
    delay(1000);

    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Scan RFID card");

    Serial.println("System unblocked. Scan RFID card...");
  }
}
```

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: Анастасія КОПИЦЯК

Співавтор:

Назва: Програмно-технічний засіб контролю доступу до приміщення

Експерт: Павло РЕГІДА

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:3.11%

Коефіцієнт подібності 2:1.12%

Мікропробіли: 3

Заміна букв: 0

Інтервали: 0

Білі знаки: 10

Дата створення звіту: 2026-06-01 19:49:39.0

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:

2026-06-01 Доцент Андрій Нічепорук

Дата експерт

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: 12%**

	Документ		Сумарний збіг по Базі Даних	
ID: 272927 Назва: БКР Програмно-технічний засіб контролю доступу до приміщення Додано в БД: 2026-06-01 Автора: Анастасія КОПИЦЯК Керівники: Павло РЕГІДА Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	100206	811	2652 (3%)	37 (5%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Копицяк Анастасія Андріївна

Тема: Програмно-технічний засіб контролю доступу до приміщення

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___79___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є розроблення програмно-технічного засобу контролю доступу до приміщення з використанням RFID-картки та PIN-коду.

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: У першому розділі кваліфікаційної роботи розглянуто теоретичні основи систем контролю доступу, їх актуальність, принципи функціонування та класифікацію. Проведено аналіз промислових і автономних рішень контролю доступу, визначено їхні переваги та недоліки, а також обґрунтовано доцільність використання комбінованої автентифікації RFID + PIN-код для підвищення рівня безпеки. У другому розділі обґрунтовано структуру програмно-технічного засобу контролю доступу до приміщення. Розглянуто вибір мікроконтролерної платформи Arduino Uno та основних апаратних компонентів системи: RFID-зчитувача RC522, матричної клавіатури 4x4, LCD-дисплея з I2C-інтерфейсом, сервоприводу та світлодіодної індикації. Також описано алгоритм роботи пристрою, який передбачає послідовну перевірку RFID-картки та PIN-коду, надання або заборону доступу і блокування після трьох невдалих спроб. У третьому розділі виконано програмно-апаратну реалізацію розробленого засобу контролю доступу. Розроблено схему підключення компонентів, описано програмну логіку роботи системи та виконано моделювання пристрою у середовищі Wokwi. Проведене тестування підтвердило правильність

роботи двофакторної автентифікації, виконавчого механізму, LCD-дисплея та світлодіодної індикації.

4. Позитивні сторони роботи: актуальність теми, практична спрямованість, використання двофакторної автентифікації RFID + PIN-код, наявність блокування після трьох невдалих спроб та моделювання роботи пристрою.

5. Негативні сторони роботи: недостатньо уваги приділено реалізації фізичного макета пристрою та розширенню системи для роботи з кількома користувачами.

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 високому технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: відмінно(A/92)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Гетман Наталія Сергіївна, д-р філософії

доцент кафедри КБ

"4" 06 2026 р. _____(підпис)

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Анастасія КОПИЦЯК
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-22-2

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 Програмно-технічний засіб контролю доступу до приміщення
Автор Анастасія КОПИЦЯК
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: д.ф., доцент Павло РЕГІДА

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 3,11%; та системою Anti-Plagiarism складає 1,0%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

01.06.2026

Завідувач кафедри _____ Підпис — Ольга ПАВЛОВА (Ім'я, ПРІЗВИЩЕ)

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

Керівник кваліфікаційної роботи _____ Підпис — Павло РЕГІДА (Ім'я, ПРІЗВИЩЕ)