МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Безпека комп'ютерних систем і мереж»

Група: 4КБ-02

Дипломний проект

здобувача освіти денної форми навчання
КБ.02.02.000.ДП

БАРОЛІСА
ОЛЕКСАНДРА ЮРІЙОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: «**Безпека комп'ютерних систем і мереж»**

Група: **4КБ-02**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту на тему:

Розробка системи моніторингу та контролю доступу до офісу на основі RFID

Проектний матеріал складається з пояснювальної записки на 76 сторінках
та графічного (презентаційного) матеріалу на 16 аркушах (слайдах)

Дипломник _____ (Бароліс О. Ю.)
Керівник _____ (Кільдішев В. Й.)

Консультанти:

з економічного розділу _____ (Канський М. Ю.)
з розділу охорони праці та техніки безпеки _____ (Чорновол Н. І.)
з нормоконтролю _____ (Петрашова В. І.)
старший консультант _____ (Кривченко Ю. В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю. В.)
Завідувач відділення _____ (Краснокутська К. Г.)

Захист «26» червня 2025 р. Протокол ЕК № 5
Оцінка ЕК 5 (відмінно) / 90 б.

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ІІІ*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Безпека комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР _____

Беркань І. В.

"19" 05 2025 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві (здобувачці) освіти *Бароліса Олександра Юрійовича*

(прізвище, ім'я, по батькові)

1. Тема проекту *Розробка системи моніторингу та контролю доступу до офісу на основі RFID*

затверджена наказом по коледжу від "14" листопада 2024 р. № 246

2. Термін здачі закінченого проекту 16.06.25 р.

3. Вихідні дані до проекту *1. Аналіз сучасних підходів до реалізації систем контролю доступу, їх переваг і недоліків; 2. Складові елементи системи на основі RFID-технологій; 3. Можливості застосування платформи Arduino для побудови систем доступу; 4. Проєктування архітектури системи та алгоритмів її функціонування; 5. Реалізація проєкту за допомогою симулятора Wokwi та аналіз працездатності системи.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Основні завдання систем моніторингу доступу; Принцип дії та типи RFID-датчиків; Підключення та використання компонентів з Arduino; Розробка електричної схеми системи; Вибір та обґрунтування контролера Arduino Mega 2560; Сценарії роботи системи: авторизація, блокування, сигналізація; Реалізація проєкту у Wokwi; Вивід повідомлень на LCD-дисплей; Використання SD-карт; Управління сервоприводом та звуковим бузером; Обмеження доступу та блокування після помилкових спроб; Економічні аспекти впровадження; Заходи з безпеки праці.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Схема підключення компонентів системи контролю доступу; Робота системи в режимі очікування дій користувача; Сценарій надання доступу при правильній авторизації; Сценарій відмови в доступі при неправильному вводі; Сценарій блокування системи після трьох помилкових спроб; Перевірка UID-коду RFID-мітки та PIN-коду користувача; Надання або заборона доступу залежно від результатів авторизації; Зовнішній вигляд пристрою; Використані бібліотеки Arduino та структура списку авторизованих осіб; Реакція системи та результати тестування.

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	*Кільдішев В. Й.*		
Економічний розділ	*Канський М. Ю.*		
Розділ охорони праці	*Чорновол Н. І.*		
Нормоконтроль	*Петрашова В. І.*		
Старший консультант	*Кривченко Ю. В.*		

7. Дата видачі завдання 15.05.25р.

Керівник *Кільдішев В. Й.* _____
(підпис)

Завдання прийняв до виконання *Бароліс О. Ю.* _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	Вступ. Постановка мети та завдань проєкту.	16.05.25	Виконав
2	Аналіз вимог до систем моніторингу та контролю доступу.	17.05.25	Виконав
3	Вивчення RFID-технологій та їх застосування в СКУД.	19.05.25	Виконав
4	Аналіз платформи Arduino та сумісних модулів.	22.05.25	Виконав
5	Дослідження роботи компонентів з Arduino.	23.05.25	Виконав
6	Розробка алгоритму функціонування системи доступу.	25.05.25	Виконав
7	Вибір компонентів для створення апаратної частини проєкту.	27.05.25	Виконав
8	Створення електричної схеми підключення пристроя.	30.05.25	Виконав
9	Розробка програмного забезпечення для Arduino.	02.06.25	Виконав
10	Тестування роботи RFID-карти, LCD-дисплея, SD-карта, сервоприводу, бузера та RGB-світлодіода.	05.06.25	Виконав
11	Аналіз результата моделювання в середовищі Wokwi.	08.06.25	Виконав
12	Виконання економічних розрахунків пристроя.	10.06.25	Виконав
13	Розгляд питань з охорони праці.	12.06.25	Виконав
14	Підготовка графічного матеріалу.	14.06.25	Виконав
15	Підготовка до захисту дипломного проєкту.	16.06.25	Виконав

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КБ 02. 02 000. 00 ДП	Дипломний проект		
А4			КБ 02. 02 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 02. 02 000. 00 ДП		
Розробив		Бароліс О.Ю.		18.06	Розробка системи моніторингу та контролю доступу до офісу на основі RFID	Літ.	Аркуш 4 / Аркушів 84
Перевірив		Кільдішев В.Й.		18.06		Н Д П	
Н. Контр.		Петрашова В.І.		18.06		ВСП "ОТФК ОНТУ" гр.4КБ-02	
Затверд.		Кривченко Ю.В.		18.06			

ЗМІСТ

ВСТУП

На сьогоднішній день у галузі інформаційних технологій актуальною темою є пошук і впровадження нових можливостей безпеки та автоматизації доступу до приміщень, зокрема офісів. Одним із сучасних рішень у цьому напрямі є використання RFID-технологій у поєднанні з мікроконтролерами типу Arduino, що дозволяє створювати надійні та доступні системи контролю доступу.

Популярність застосування RFID-технологій стрімко зросла завдяки їх простоті, швидкодії та можливості ідентифікації користувачів без прямого фізичного контакту. Такі системи широко використовуються для організації доступу в офісні приміщення, навчальні заклади, склади та інші об'єкти, де необхідно контролювати переміщення осіб. Особливо корисними є рішення, які поєднують RFID-модулі, клавіатури, серводвигуни, звукову та світлову індикацію, що забезпечує перевірку та зручність у користуванні.

Проте, незважаючи на доступність окремих компонентів, ефективна реалізація такої системи вимагає правильного підбору апаратного забезпечення, написання надійного програмного коду та врахування можливостей розширення функціоналу. Це дає змогу забезпечити як безпеку, так і гнучкість у подальшому використанні та адаптації системи.

Окрім технічних переваг, такі системи також сприяють підвищенню рівня дисципліни та обліку персоналу в організаціях. Вони можуть інтегруватися з базами даних, вести журнали відвідувань та формувати звіти, що є корисним для керівництва та служби безпеки підприємства.

У даній дипломній роботі розглядаються принципи побудови системи контролю доступу до офісу на основі технології RFID, описуються основні апаратні та програмні засоби, алгоритми роботи, а також реалізація повноцінного прототипу з можливістю ведення логів подій та блокування після несанкціонованих спроб доступу.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Аналіз сучасних технологій контролю доступу

У наш час питання безпеки набуло нового значення. Раніше достатньо було звичайного ключа від замка, але сьогодні це вже не працює — потрібні більш «розумні» рішення. Особливо це актуально для офісів, навчальних закладів, складів і навіть житлових будинків. Саме тому активно розвиваються технології контролю доступу — тобто системи, які визначають, хто має право заходити в приміщення, а хто ні.

Сучасні технології контролю доступу можна умовно поділити на кілька типів: фізичні (ключі, магнітні картки), цифрові (PIN-коди, мобільні додатки), біометричні (відбитки пальців, розпізнавання обличчя) та радіочастотні (RFID, NFC, Bluetooth). Кожна з цих технологій має свої переваги і недоліки, тому вибір залежить від конкретних потреб та бюджету.

Рисунок 1.1. Види контролю доступу

Біометричні системи вважаються одними з найбільш надійних, адже базуються на унікальних особливостях кожної людини — наприклад, відбитках пальців або формі обличчя. Такі системи складно підробити, але вони дорогі, і не завжди спрацьовують у несприятливих умовах — наприклад, вологість або бруд можуть заважати зчитуванню.

Системи з PIN-кодами — це простий і бюджетний варіант. З одного боку, вони легко реалізуються на базі Arduino, з іншого — користувач може забути код, або його можуть підглянути сторонні.

Bluetooth і NFC дозволяють використовувати смартфон як ключ доступу, що досить зручно, адже телефон завжди з собою. Проте тут вже є ризики — якщо телефон втрачено, доступ до системи може отримати стороння особа. Також потрібне окреме програмне забезпечення.

І нарешті — RFID-технологія. Це, на мою думку, один із найкращих варіантів для навчального проєкту чи невеликої офісної системи. RFID забезпечує швидке та безконтактне зчитування даних, картки або брелоки мають невисоку ціну, а підключити модуль RC522 до Arduino досить просто. Більш того, RFID-карти можна записувати, змінювати права доступу, і навіть вести журнал доступу, якщо додати SD-карту до системи.

Крім того, RFID легко масштабувати — тобто додавати нових користувачів, змінювати алгоритми доступу або поєднувати з іншими пристроями (дисплеями, серво, звуковими сигналами тощо). Окрім цього, RFID-системи чудово підходять для інтеграції в навчальні або демонстраційні проєкти, оскільки дозволяють студентам опанувати принципи роботи електроніки, мікроконтролерів та систем безпеки.

Підсумовуючи, можна сказати, що на сьогодні найперспективнішими є RFID та біометричні технології, хоча у кожної є свої особливості. Для мого проєкту я вибрав RFID саме через її доступність, простоту реалізації, і тому, що вона ідеально підходить для Arduino-платформи.

1.2 Загальна характеристика СКУД

Системи контролю та управління доступом, або скорочено СКУД, — це такі собі «розумні охоронці», які вирішують, кого пускати в приміщення, а кого — ні. Їх можна зустріти в офісах, школах, гуртожитках, на складах і навіть у звичайних під'їздах. Головна мета СКУД — забезпечити безпечний і зручний доступ до певних зон тільки для дозволених осіб.

СКУД — це не просто один пристрій. Зазвичай це ціла система, яка складається з кількох частин. Наприклад, є засоби ідентифікації (це можуть бути RFID-картки, брелоки, або навіть обличчя чи відбитки пальців), контролер (який приймає рішення — впустити чи ні), виконавчі механізми (типу електрозамків або серво), а також інтерфейси для користувача — дисплеї, кнопки, звукові сигнали тощо.

Принцип роботи СКУД виглядає приблизно так: користувач підносить картку до зчитувача → контролер перевіряє дані → якщо все збігається — двері відкриваються, якщо ні — система або подає сигнал про помилку, або блокує доступ. Все це займає буквально секунду, але дозволяє уникнути купи проблем, особливо в місцях з обмеженим доступом.

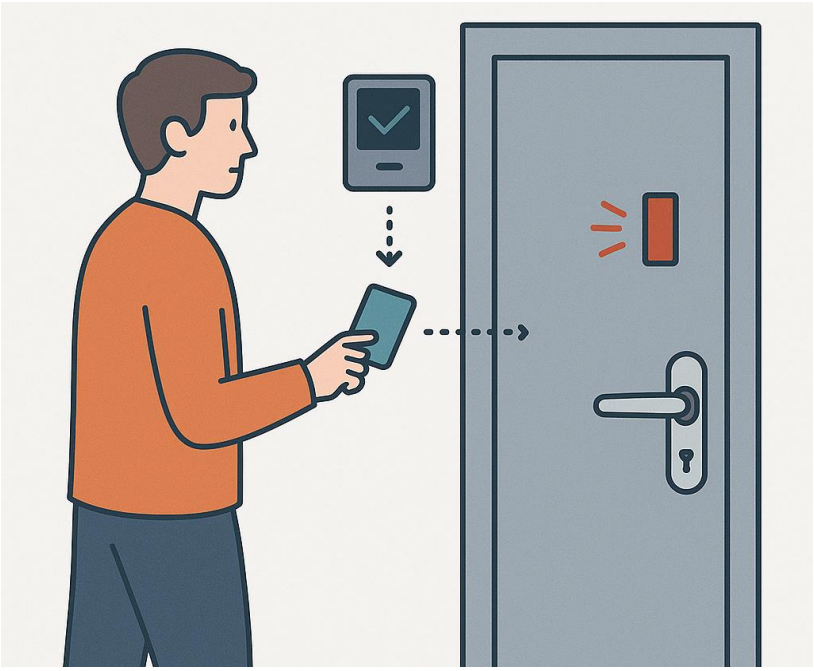


Рисунок 1.2. Принцип роботи СКУД

Ще одна перевага сучасних СКУД — гнучкість. Їх можна легко адаптувати до будь-яких умов. Наприклад, можна зробити різні рівні доступу — щоб одні могли входити тільки вдень, інші — цілодобово. Або додати клавіатуру для введення PIN-коду, якщо картка втрачена. Деякі системи навіть надсилають повідомлення адміністратору при спробі несанкціонованого доступу.

СКУД бувають автономними і мережевими. Автономні працюють самі по собі — без підключення до комп'ютера чи серверу, всі дані зберігаються всередині контролера. Це зручно для невеликих об’єктів. Натомість мережеві СКУД — більш «просунуті», вони дозволяють вести облік подій, керувати доступом з комп’ютера, переглядати логі активності та змінювати налаштування в реальному часі.

В моєму проєкті я вирішив реалізувати СКУД на базі Arduino, бо це чудовий варіант для практики. Він дозволяє краще зрозуміти, як працюють логіка контролю, обробка даних з RFID-модуля, робота з пристроями виводу, і взагалі — як можна самостійно зібрати повноцінну систему безпеки.

1.3 Порівняння технологій RFID

RFID-технологія насправді не така вже й нова, але останніми роками вона отримала друге дихання завдяки широкому використанню у системах контролю доступу, логістиці, роздрібній торгівлі та навіть у медичній сфері. У загальному сенсі, RFID (Radio Frequency Identification) — це спосіб безконтактної ідентифікації об’єктів або осіб за допомогою радіохвиль. Але, як виявилось під час аналізу, RFID не є якоюсь єдиною технологією — існує декілька її варіантів, які суттєво відрізняються за характеристиками, частотами та сценаріями використання.

По-перше, RFID-системи поділяються на три основні типи за частотою роботи:

1. Низькочастотні (LF, 125–134 кГц) — це найстаріший і найдешевший тип. Такі картки мають обмежену швидкість обміну даними та невеликий радіус дії (до 10 см), але водночас вони стійкі до завад та добре працюють навіть через вологі або металеві середовища. Часто використовуються в тваринництві або в простих офісних системах, де не потрібно великої швидкості або складної безпеки.

2. Високочастотні (HF, 13,56 МГц) — саме до цього типу належить RC522, який використовується у моєму проєкті. Його перевага — більша швидкість передавання даних, підтримка шифрування (наприклад, стандарт ISO/IEC 14443), можливість читати картки на відстані до 10–15 см та більший обсяг пам’яті на самій мітці. Цей тип широко застосовується в проїзних квитках, студентських ID, пропусках у будівлі та в сучасних офісних СКУД.

3. Ультрависокочастотні (UHF, 860–960 МГц) — мають найбільший радіус зчитування (іноді до кількох метрів!) і здатні зчитувати десятки тегів одночасно. Але такі системи чутливі до завад, вимагають кращого розташування антен і зазвичай використовуються там, де треба швидко і масово ідентифікувати об'єкти — наприклад, на складах або в супермаркетах.

Класифікації за частотними діапазонами, важливо також враховувати специфіку використання RFID-систем у конкретному середовищі. Наприклад, для невеликих офісів або навчальних закладів оптимальним вибором буде HF-система з RC522, оскільки вона поєднує помірну вартість із хорошими характеристиками безпеки. Правильне налаштування модуля і вибір типу тегів дозволяє досягти балансу між зручністю, швидкістю і надійністю доступу.

Щодо безпеки, HF-технологія, яку я застосував у проєкті, є кращою за LF, бо підтримує автентифікацію і криптографію.

Також варто згадати, що існують активні і пасивні RFID-мітки. У моєму випадку використовується пасивна система — тобто, картка не має власного джерела живлення і активується тільки тоді, коли потрапляє в зону дії зчитувача. Це робить систему енергоефективною і дешевою у впровадженні. Активні ж мітки мають батареї і можуть передавати сигнал на великі відстані, але їх використання обґрунтоване лише в специфічних галузях.

Отже, як показав мій аналіз з RC522, для локальних офісних систем контролю доступу найбільш зручною, збалансованою за ціною, захистом і зручністю інтеграції є HF-RFID. Вона ідеально підходить для мого проєкту: швидке зчитування картки, перевірка UID, простота програмної реалізації на Arduino — все це дозволяє створити надійну і зручну систему доступу.

1.4 Вибір RFID як основної технології

Коли переді мною постало завдання розробити систему контролю доступу для офісу, я почав із найголовнішого питання — яку саме технологію ідентифікації обрати? Варіантів насправді чимало: від класичних магнітних карток, кодових замків, біометрії до сучасних рішень на базі NFC, Bluetooth або навіть розпізнавання обличчя. Проте серед усього цього різноманіття саме RFID виявився найбільш логічним, практичним і збалансованим вибором для реалізації мого проєкту.

Найперше, що привернуло увагу — простота реалізації. На відміну від, скажімо, систем з розпізнаванням облич або відбитків пальців, RFID-системи не потребують складного обладнання чи спеціального калібрування. Все, що потрібно — це зчитувач і невеличка картка або брелок. При цьому процес зчитування відбувається швидко і безконтактно, що дуже зручно для щоденного використання в офісі.

Ще одна важлива причина вибору RFID — оптимальне співвідношення між безпекою та вартістю. У рамках проєкту я використовую зчитувач RC522, який працює на частоті 13,56 МГц і підтримує стандарт ISO/IEC 14443. Цей модуль може працювати з картками типу MIFARE, де кожна має унікальний ідентифікатор (UID), що дозволяє швидко перевіряти, чи має людина доступ до приміщення.

З погляду практичного застосування, RFID виявився дуже зручним: співробітник може просто прикласти картку до зчитувача — і замок миттєво відкриється. Ніяких кодів, які можна забути, чи фізичного контакту, що зношує механізми.

Більше того, RFID легко масштабувати: якщо потрібно — можна додати десятки карток, або ж навпаки — видалити доступ окремим користувачам без перепрошивки всієї системи.

Окремо варто згадати про енергоефективність. У проєкті використовуються пасивні RFID-картки, які не потребують власного живлення — усю необхідну енергію вони отримують від поля зчитувача. Завдяки цьому споживання енергії системи загалом зменшується, що дозволяє використовувати її навіть у поєднанні з резервними або автономними джерелами живлення, забезпечуючи безперервну роботу навіть у разі перебоїв з електропостачанням.

Ще один важливий плюс — універсальність і гнучкість інтеграції. Існують перевірені бібліотеки для роботи з RC522 у середовищі Arduino, а сам модуль легко підключається через SPI-інтерфейс. Усі ці фактори дозволяють швидко інтегрувати RFID у проєкт без значних витрат часу на налаштування або вирішення проблем сумісності. У майбутньому можливе подальше вдосконалення системи: додавання журналу подій, інтеграція з базою даних, використання Wi-Fi-модулів для віддаленого моніторингу або повна автоматизація обліку доступу.

Таким чином, вибір RFID як основної технології в моїй системі є цілком обґрунтованим: це надійне, зручне, безконтактне рішення, яке чудово підходить для офісного середовища. Воно поєднує в собі зручність для користувача, доступну вартість для розробника і достатній рівень безпеки для захисту доступу до приміщення. Тому RFID і став центральним елементом розробленої мною системи контролю.

1.5 Огляд апаратних засобів

Для реалізації системи контролю доступу я підібрав набір компонентів, які не тільки сумісні між собою, але й максимально доступні, надійні та прості в інтеграції. Метою було створити повноцінний пристрій, який би реагував на RFID-картки, дозволяв вводити PIN-код, показував повідомлення на екрані, керував замком через сервопривід і сповіщав користувача про результат за допомогою світла або звуку. У цьому розділі я хочу коротко розповісти про кожен елемент, який увійшов до складу системи.

Найперше, що привернуло увагу — простота реалізації. На відміну від, скажімо, систем з розпізнаванням облич або відбитків пальців, RFID-системи не потребують складного обладнання чи спеціального калібрування. Все, що потрібно — це зчитувач і невеличка картка або брелок. При цьому процес зчитування відбувається швидко і безконтактно, що дуже зручно для щоденного використання в офісі.

Крім того, кожен компонент легко програмується і має велику кількість прикладів у відкритому доступі, що значно прискорило розробку. А використання Arduino Mega 2560 дозволяє без проблем підключити одразу декілька модулів, не обмежуючи себе кількістю входів/виходів. Завдяки цьому, система вийшла не лише функціональною, а й відкритою для майбутніх покращень.

1.5.1 Модуль RFID-RC522

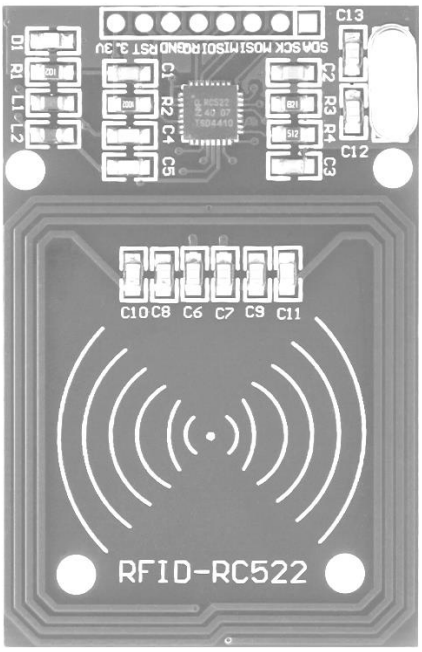


Рисунок 1.3. Фізичний вигляд модуля RFID-RC522

Модуль RFID-RC522 є одним із ключових елементів в моєму проєкті, оскільки саме він відповідає за зчитування RFID-міток — карток або брелоків, які використовуються користувачами для авторизації. Саме завдяки цьому модулю система контролю доступу може безконтактно розпізнавати особу та приймати рішення про дозвіл або заборону доступу. Без перебільшення — RFID-RC522 виконує функцію «очей» системи, що розпізнають, хто намагається увійти до офісу.

В основі модуля лежить мікросхема MFRC522, яка працює на частоті 13,56 МГц і підтримує стандарт ISO/IEC 14443 Type A — це саме той стандарт, який використовується у більшості сучасних RFID-карт і NFC-пристроїв. Ще однією перевагою є підтримка двостороннього зв’язку з RFID-міткою, в проєкті реалізована функція зчитування UID (унікального ідентифікатора), що реалізовано для завдань контролю доступу.

RFID-RC522 є досить компактним модулем і має сім основних виводів:

- SDA (SS) — вибір пристрою (Slave Select);
- SCK — тактова лінія (Serial Clock);

- MOSI — передача даних (Master Out Slave In);
- MISO — прийом даних (Master In Slave Out);
- IRQ — переривання (не використовується у проєкті);
- GND — земля;
- 3.3V — живлення.

У проєкті модуль підключений до Arduino через SPI-інтерфейс, який забезпечує швидкий і надійний обмін даними. Це особливо важливо, оскільки зчитування UID повинно відбуватися максимально швидко, щоб не створювати затримок у роботі системи.

Що стосується практичного застосування — RFID-RC522 здатний зчитувати RFID-картки на відстані приблизно від 2 до 5 см. Така невелика дистанція — це не недолік, а, скоріше, перевага, оскільки вона запобігає випадковому зчитуванню карток користувачів, які просто проходять повз.

У віртуальному середовищі Wokwi, яке використовується для реалізації проєкту, модуль RFID-RC522 підключається аналогічно, як у реальному житті, але без ризику пошкодження компонентів або проблем з живленням. Тут зручно експериментувати з логікою роботи та алгоритмами перевірки UID. Також у бібліотеці передбачено можливість роботи з кількома секторами пам’яті картки, що дозволяє реалізувати додаткові рівні безпеки.

Для роботи з модулем використовується бібліотека MFRC522.h, яка значно спрощує програмування. Завдяки їй я можу легко ініціалізувати модуль, шукати наявність карти в полі дії, зчитувати її UID, порівнювати цей UID із попередньо збереженим «білим списком» і приймати рішення про доступ. Якщо UID збігається з дозволеним, система подає сигнал на сервопривід і відкриває доступ. У разі невідповідності — блокує прохід, супроводжуючи це звуковим сигналом і відповідним повідомленням на LCD-дисплеї.

Ще одна важлива деталь: RFID-RC522 працює тільки від 3.3 В, і це слід враховувати при підключенні в реальному середовищі, інакше можна спалити модуль. У моєму проєкті це питання вирішується через використання безпечного підключення через Arduino Mega, яка має вивід на 3.3 В.

Окрім того, сам модуль підключається через інтерфейс SPI, що дозволяє досягти швидкої та стабільної передачі даних. Завдяки цьому система оперативно реагує на кожну спробу доступу — без затримок чи збоїв.

Також можливе об’єднання RFID-модуля з іншими модулями, такими як модуль годинника реального часу (RTC) або SD-карта, що дозволяє створити журнал доступу з точним часом кожної авторизації. У перспективі така система може бути повноцінно інтегрована до централізованої мережі офісного обліку, де кожен прохід фіксується, а аналітика використовується для звітності або оптимізації доступу.

Завдяки гнучкості цієї технології, RFID-RC522 можна не лише легко реалізувати у рамках студентського чи аматорського проєкту, а й масштабувати до напівпрофесійної системи, яка здатна вирішувати конкретні завдання підприємства або організації.

Важливо враховувати, що RC522 дозволяє реалізувати багаторівневу перевірку доступу, комбінуючи RFID-автентифікацію з іншими методами — наприклад, введенням PIN-коду або перевіркою часу. Такий підхід робить систему адаптованою до реальних потреб та здатною еволюціонувати разом із вимогами безпеки об’єкта.

Загалом, RFID-RC522 — це ідеальний варіант для побудови системи контролю доступу. Він недорогий, надійний, має хорошу підтримку в середовищі Arduino, простий у використанні та сумісний з іншими компонентами проєкту. Саме тому я обрав цей модуль як основний засіб ідентифікації користувачів у своєму проєкті.

1.5.2 Контролер Arduino MEGA 2560

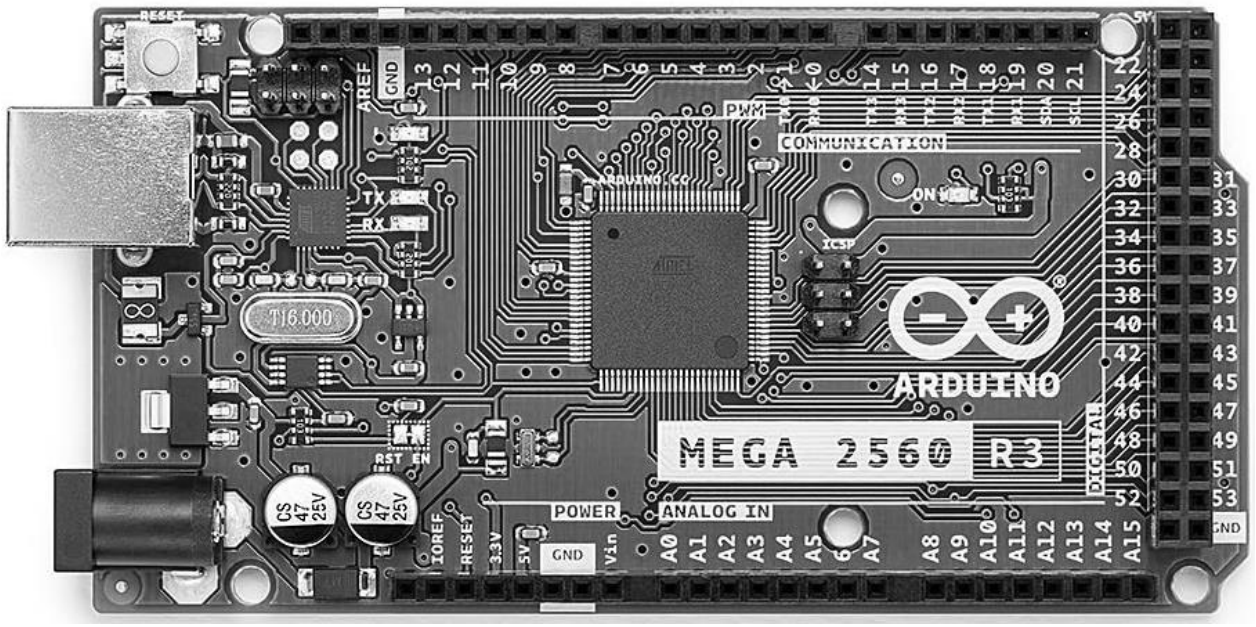


Рисунок 1.4. Фізичний вигляд контролера Arduino MEGA 2560

У моєму проєкті головну роль відіграє Arduino MEGA 2560 — це свого роду "мозок" всієї системи, який координує роботу всіх підключених компонентів: RFID-модуля RC522, LCD-дисплея, клавіатури, сервоприводу, бузера, світлодіодів та навіть SD-карти. Без нього проєкт просто не зміг би функціонувати, адже саме Arduino виконує всі обчислення, перевірки та керує зовнішніми пристроями.

Однією з головних причин, чому я обрав саме MEGA 2560, є велика кількість входів/виходів. На відміну від популярнішої, але обмеженої Arduino UNO, плата MEGA має аж 54 цифрові пінов (із яких 15 можуть працювати як ШІМ), а також 16 аналогових входів. Для складного проєкту з великою кількістю підключених модулів це критично важливо. Наприклад, лише RFID-модуль потребує 5 пінів, LCD — ще 6, клавіатура — 8, плюс додатково потрібні пін для сервоприводу, для бузера, для RGB-світлодіода, кнопок та інших елементів. Arduino MEGA 2560 без проблем справляється з цим навантаженням.

Arduino MEGA 2560 чудово підходить для реалізації мого дипломного проєкту на базі RFID.

1.5.3 Сервопривід SG90

Рисунок 1.5. Фізичний вигляд сервоприводу SG90

Сервопривід SG90 — це один із найпопулярніших мікросервомоторів, який часто використовується в освітніх та прототипувальних проєктах, зокрема на базі Arduino.

У контексті системи моніторингу та контролю доступу SG90 виконує ключову функцію — фізичне відкриття або закриття замка (наприклад, за допомогою повороту важеля або блокувального механізму). Після успішної автентифікації користувача за допомогою RFID або введення PIN-коду, сервомотор отримує сигнал і повертає вал, імітуючи дію замка. Такий підхід дозволяє реалізувати реалістичну модель дверного контролю в компактному та безпечному форматі.

Важливо зазначити, що сервомотор SG90 має компактні розміри та низьке енергоспоживання, що дозволяє використовувати його в автономних системах. У поєднанні з мікроконтролером Arduino, він забезпечує стабільну роботу навіть у випадку багаторазових циклів відкриття-закриття, що робить його практичним рішенням для реального застосування

Сервопривід SG90 надійний і зручний компонент для проєктів для системи доступу, де потрібна проста, але функціональна форма фізичного управління.

1.5.4 Додаткові компоненти (дисплей, бузер, SD-карта, RGB-світлодіод, матрична клавіатура)

1. Матрична клавіатура 4x4.

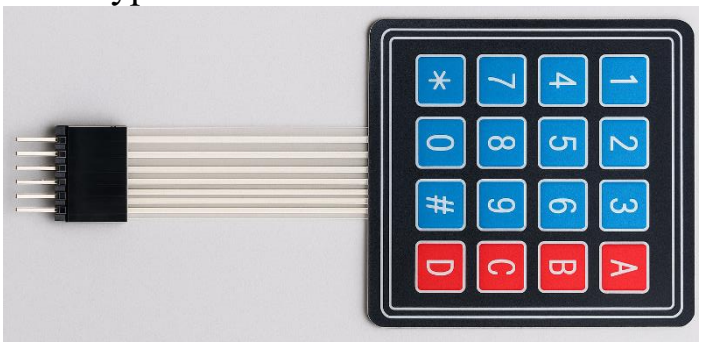


Рисунок 1.6. Фізичний вигляд матричної клавіатури 4x4

Використовується для введення PIN-коду як додатковий рівень безпеки. Користувач після прикладання RFID-картки може підтвердити свою особу, ввівши персональний код. Клавіатура підключена до Arduino через 8 цифрових пінів та дозволяє зчитувати натискання в реальному часі.

2. LCD-дисплей 16x2 з I2C-модулем.

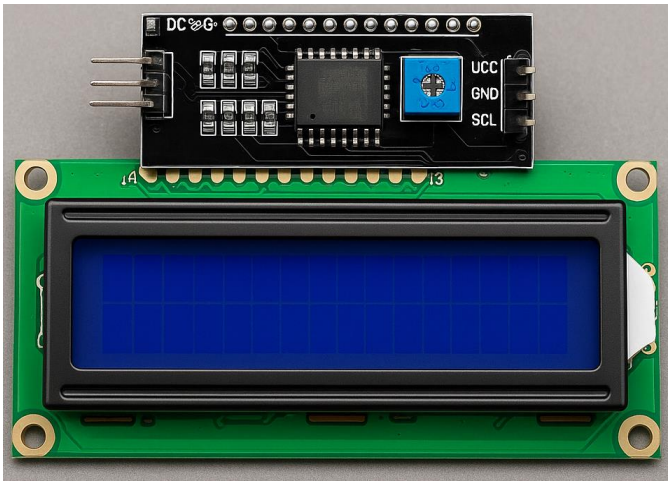


Рисунок 1.7. Фізичний вигляд LCD-дисплея 16x2 I2C

Дисплей відіграє роль інтерфейсу між користувачем і системою. На ньому відображається інформація: наприклад, "Очікується картка", "Доступ дозволено", "Невірний PIN" тощо. Завдяки модулю I2C дисплей використовує всього два пінів для зв'язку з Arduino, що дуже зручно при великій кількості підключень.

3. Активний бузер.

Рисунок 1.8. Фізичний вигляд активного бузера

Бузер використовується для звукового супроводу подій. Наприклад, при успішному вході подається короткий сигнал, а при помилці — кілька тривожних біпів. Така звукова індикація покращує зручність користування системою.

4. RGB-світлодіод.

Рисунок 1.9. Фізичний вигляд RGB-світлодіода

Це триколірний світлодіод, який змінює колір залежно від ситуації. Зелений — доступ дозволено, червоний — відмова, синій — очікування введення PIN-коду. Це додатковий візуальний рівень зворотного зв’язку, що особливо зручно у шумному офісі.

5. Модуль для SD-картки.

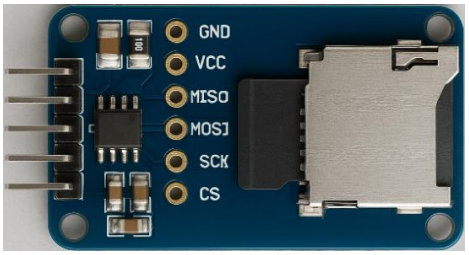


Рисунок 1.10. Фізичний вигляд модуля SD-картки

SD-карта для логування подій — хто коли заходив, які UID використовувалися, і скільки було невдалих спроб.

У результаті всі ці апаратні засоби створюють повноцінну інтерактивну систему, яка не просто відкриває двері, а й комунікує з користувачем, реагує на помилки і навіть дає змогу в майбутньому інтегрувати інші можливості.

1.5.5 Вибір альтернативних варіантів компонентів

У процесі розробки будь-якої апаратної системи, зокрема системи контролю доступу на базі Arduino, важливо не лише підібрати оптимальні компоненти, але й оцінити наявні альтернативи. Це дозволяє врахувати доступність обладнання, або ж покращити функціональність.

Почнемо з головного контролера — Arduino MEGA 2560. Його перевага полягає у великій кількості цифрових і аналогових входів/виходів, що дозволяє легко підключити багато компонентів одночасно. Проте якщо проєкт потребує меншої кількості портів і простішої логіки, можна розглядати Arduino Uno або Nano як більш компактні й економічні альтернативи. У випадках, коли потрібно використовувати бездротовий зв’язок або більше обчислювальної потужності, підійде ESP32 — він має вбудований Wi-Fi, Bluetooth та більшу швидкість обробки даних.

Щодо модуля RFID RC522, який використовується для зчитування безконтактних карток, його альтернативами є PN532 або RDM6300. PN532 підтримує більше протоколів (NFC, наприклад) і має ширші можливості зв'язку (I2C, SPI, UART), що корисно в проєктах із більш складною логікою. RDM6300, натомість, — простіший та дешевший модуль, який працює лише з 125 кГц картами, але може бути чудовим варіантом для базових задач.

У випадку сервопривода SG90, альтернативами можуть бути MG90S (з металевими шестернями, витриваліший варіант) або Tower Pro MG996R, якщо потрібна більша сила крутного моменту, наприклад, для управління реальним замком. Проте SG90 залишається лідером серед недорогих і компактних сервоприводів для навчальних макетів.

Бузер, який відповідає за звукову індикацію, має теж декілька варіантів — активні та пасивні. Якщо потрібно мати більше контролю над звуком (мелодії, частота), краще використовувати пасивний бузер або навіть динамік, підключений через підсилювач.

Якщо говорити про LCD-дисплей 16x2 (на базі контролера HD44780), поширеною альтернативою є OLED-дисплеї (наприклад, 0.96" на SSD1306). Вони компактніші, енергоефективніші та можуть відображати графіку, а не тільки текст. Для проєктів, де потрібно показувати більше інформації, підходять також TFT-дисплеї з кольоровою графікою.

Замість стандартного RGB-світлодіода (де кожен канал потрібно підключати окремо), можна використовувати інтелектуальні світлодіоди WS2812 (NeoPixel), які дозволяють керувати кольором і яскравістю через один цифровий пін, а також об’єднувати багато таких діодів у послідовність.

Для збереження логів або доступу до журналів у проєкті використовується модуль SD-карти. Якщо потрібно зберігати більший обсяг даних або організувати бездротову передачу, замість цього можна використати ESP32 з доступом до хмарних сервісів.

Матрична клавіатура 4x4 — ще один важливий елемент. Якщо потрібно спростити взаємодію з користувачем, можна замінити її на сенсорну панель, мембранну клавіатуру 3x4, або навіть використати мобільний додаток як інтерфейс (через Bluetooth або Wi-Fi).

Знання та використання альтернатив дозволяє не лише розширити функціональність, а й зробити систему більш стійкою до змін — наприклад, у разі дефіциту певного модуля його легко замінити аналогом без суттєвої перебудови всієї архітектури. Це особливо важливо для проєктів, які розвиваються поступово або створюються в умовах обмеженого доступу до комплектуючих.

Таким чином, дає змогу адаптувати систему під конкретні вимоги проєкту, бюджету, доступності обладнання або технічних обмежень. Це підвищує надійність та універсальність системи й дозволяє в майбутньому масштабувати або модернізувати її з мінімальними витратами.

1.5.6 Практичний досвід використання елементної бази

У процесі створення системи моніторингу та контролю доступу на основі RFID-технологій дуже важливо не лише теоретично ознайомитися з обраними компонентами, а й отримати практичний досвід роботи з ними. Саме під час налаштування, тестування та інтеграції різних модулів проявляються як переваги, так і недоліки елементної бази. Усі компоненти, обрані для реалізації проєкту, були перевірені за допомогою середовища веб-сайта Wokwi, що дозволило швидко тестувати взаємодію елементів без потреби в реальному обладнанні.

Рисунок 1.11. Веб-сайт Wokwi

Контролер Arduino MEGA 2560 у ході симуляції показав високу стабільність роботи навіть за умови паралельної взаємодії з великою кількістю периферії: RFID-модулем, LCD-дисплеєм, SD-картою, сервоприводом, бузером, клавіатурою та RGB-світлодіодом. Завдяки великій кількості цифрових пінів не виникало необхідності в мультиплексорах або використанні нестандартних схем підключення, що значно спрощує структуру проєкту.

У симуляції з Wokwi дисплей не мав затримок, однак у реальному проєкті бажано використовувати не блокуючі функції оновлення виводу, щоб не уповільнювати інші процеси.

Сервопривід SG90 показав себе як надійний виконавчий пристрій для моделювання механічного відкривання дверей. У віртуальному середовищі було змодельовано поворот на 90° при успішній аутентифікації, що імітує відкриття замка. Важливо контролювати тривалість подачі сигналу, щоб уникнути перегріву або деренчання у фізичній реалізації.

Бузер і RGB-світлодіод відіграли роль елементів індикації. На практиці було реалізовано зміну кольору діода відповідно до статусу (червоний – відмова доступу, зелений – дозвіл, синій – очікування), а також звуковий супровід дій користувача. Це значно покращило інтуїтивність взаємодії з системою.

Матрична клавіатура 4x4 дозволила вводити PIN-коди. Важливо було правильно обробляти натискання клавіш і запобігати дублюванню введення. У ході тестування реалізовано алгоритм з обмеженням кількості спроб введення, що додатково зміцнило безпеку системи.

Також виявилося корисним додати SD-карту для зберігання логів. Віртуальна симуляція на Wokwi дозволила протестувати лише базову логіку роботи з файлами, однак у реальному пристрої це стане ключовим для збереження історії доступу.

У підсумку, практичний досвід роботи з елементною базою підтвердив, що обрані компоненти не лише сумісні між собою, але й утворюють стійку систему, здатну до масштабування. Кожен елемент вніс свій вклад у надійність і функціональність системи, а середовище симуляції дозволило глибше зрозуміти їхню поведінку без додаткових витрат на фізичне тестування.

1.6 Архітектура системи та алгоритм роботи

Система моніторингу та контролю доступу до офісу, побудована на основі RFID-технологій, є багатокомпонентною інтерактивною платформою, яка поєднує в собі елементи зчитування, обробки, індикації та керування. Архітектура системи спроєктована таким чином, щоб забезпечити не лише перевірку права доступу користувача, а й зберігати гнучкість для розширення функціоналу у майбутньому.

1.6.1 Структура системи

Структура розробленої системи моніторингу та контролю доступу до офісу базується на поєднанні декількох апаратних та програмних компонентів, які взаємодіють між собою для реалізації логіки перевірки прав доступу, сигналізації подій і збереження інформації. Уся конструкція спроєктована у віртуальному середовищі Wokwi, що дозволило не лише зекономити ресурси, але й максимально гнучко змоделювати й протестувати роботу всієї системи без потреби у фізичному збиранні пристрою.

У центрі структури знаходиться контролер Arduino Mega 2560, який забезпечує взаємодію всіх модулів. Завдяки великій кількості портів введення/виведення Arduino Mega здатен одночасно керувати кількома модулями, що мають різні інтерфейси (SPI, I2C, цифрові входи/виходи).

Завдяки модульній структурі система легко піддається розширенню, за потреби можна додати нові компоненти, наприклад, модуль Wi-Fi для віддаленого моніторингу, або біометричний сенсор для багатофакторної автентифікації.

Основні компоненти структури системи:

- RFID-модуль RC522 — зчитує унікальний ідентифікаційний код (UID) кожної картки. Підключений через SPI-інтерфейс, цей модуль виконує роль етапу перевірки користувача.

- Матрична клавіатура 4×4 — використовується для введення PIN-коду після успішного зчитування RFID. Завдяки своїй компактності і надійності, вона ідеально підходить для інтерактивних систем контролю.

- LCD-дисплей з інтерфейсом I2C — інформує користувача про стан системи: очікування картки, запит на введення PIN-коду, результат доступу. Завдяки інтерфейсу I2C дисплей займає лише два піни на Arduino.

- Сервопривід SG90 — виконує функцію електрозамка: при наданні доступу повертається, імітуючи відкриття дверей.

- Бузер — використовується для звукової сигналізації подій: неправильний PIN, блокування доступу, успішне відкриття.

- RGB-світлодіод — виконує роль візуального індикатора. Світло різних кольорів (зелений, червоний, синій) інформує про результат перевірки.

- Модуль SD-карти — відповідає за збереження логів подій: UID карток, час доступу, результат (доступ дозволено/заборонено/заблоковано).

Уся структура системи логічно поділяється на три рівні:

1. Вхідний рівень: RFID-модуль або клавіатура, які отримують дані від користувача.

2. Логічний рівень: Arduino Mega аналізує отримані дані, порівнює їх з попередньо заданими UID або PIN-кодами, обробляє кількість спроб, формує відповідь.

3. Вихідний рівень: інформує користувача через дисплей, бузер і світлодіод, а також фізично відкриває замок (сервопривід) і записує подію на SD-карту.

Важливо, що структура проєкту враховує можливість блокування системи після декількох невдалих спроб входу. Це додає рівень захисту від перебору UID/PIN-кодів.

1.6.2 Опис сценаріїв доступу та блокуванні

У створеній системі контролю доступу реалізовано кілька типових сценаріїв взаємодії користувача з пристроєм, що дозволяють забезпечити надійний контроль за входом в офісне приміщення. Ці сценарії охоплюють як успішні, так і помилкові ситуації, включаючи відповідне блокування, що є важливою частиною безпеки.

Сценарій 1: Успішний доступ.

1. Користувач підносить RFID-картку до зчитувача RC522, або вводить правильний PIN-код.

2. Arduino Mega 2560 перевіряє UID картки або PIN-кодів. Якщо UID або PIN співпадає з одним із заздалегідь дозволених значень, на LCD-дисплей виводиться повідомлення: “Access Granted”, RGB-світлодіод загоряється зеленим, бузер подає короткий сигнал підтвердження, і сервомотор SG90 відкриває замок на 5 секунд (наприклад, двері).

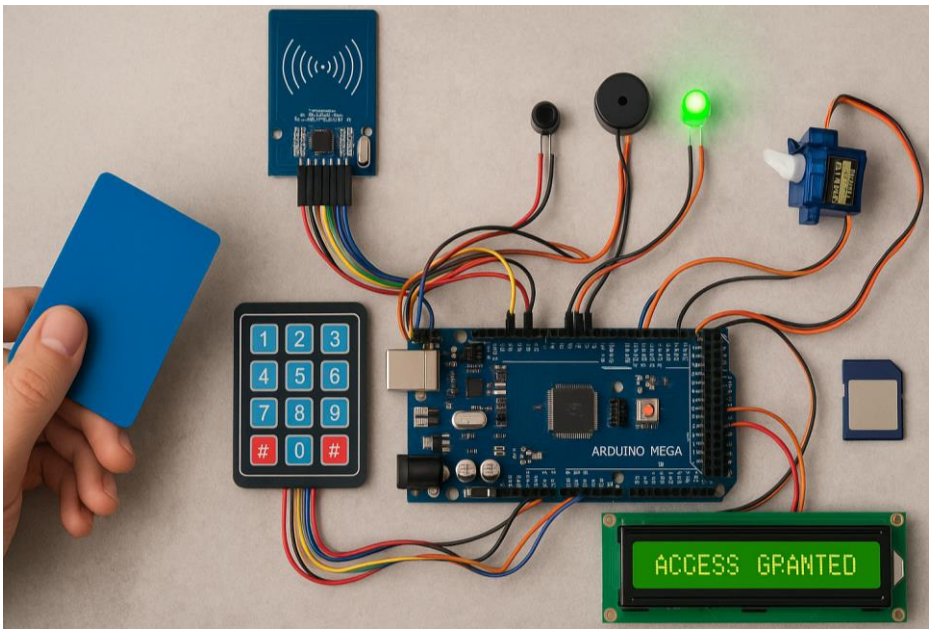


Рисунок 1.12. Приклад виконання сценарію 1

Цей сценарій — стандартний шлях для авторизованого користувача. При кожному вході система реєструє подію (UID або PIN, час, статус) на SD-картці.

Сценарій 2: Відмова в доступі.

1. Користувач підносить неправильну RFID-картку до зчитувача RC522, або вводить неправильний PIN-код.

2. Система миттєво виводить повідомлення: “Access Denied”, RGB-світлодіод блимає червоним, бузер сигналізує про помилку.

3. Жоден наступний крок не виконується — доступ заборонено.

Це захищає систему від спроб входу сторонніми особами, які мають невірну RFID-картку або PIN-код. При кожному помилки система реєструє подію (UID або PIN, час, статус) на SD-картці.

Сценарій 3: Блокування після 3 помилкових спроб.

1. Після трьох невдалих спроб введення PIN-коду або UID картки система автоматично блокує доступ.

2. Виводиться повідомлення: “SYSTEM LOCKED Wait: 30 sec”.

3. Всі інші дії (навіть правильна картка) тимчасово ігноруються. RGB-світлодіод блимає різними кольорами, бузер видає тривалий звук.

4. Розблокування можливе по завершенні встановленого часу очікування (32 секунд).

Цей сценарій підвищує рівень безпеки і захищає систему від підбору коду або несанкціонованого доступу. При кожному блокуванні система реєструє подію (UID або PIN, час, статус) на SD-картці.

Усі ці сценарії наочно демонструють, як компоненти системи злагоджено працюють у різних умовах.

Ще однією перевагою реалізації таких сценаріїв є можливість подальшого розширення логіки — наприклад, додавання нових режимів доступу, створення розкладу доступу для окремих користувачів. Це дозволяє адаптувати систему до потреб конкретного офісу та підвищити її функціональність у майбутньому.

1.7 Програмна реалізація системи

1.7.1 Використання мови програмування C++

У розробці системи моніторингу та контролю доступу на базі Arduino MEGA 2560 використано мову програмування C++. Це рішення є логічним, адже саме ця мова лежить в основі всієї системи Arduino та підтримується офіційною середою розробки Arduino IDE.

C++ дає змогу легко працювати з бібліотеками для всіх необхідних компонентів: RFID-модуля RC522, LCD-дисплея, сервоприводу SG90, клавіатури 4×4, бузера, RGB-світлодіода та інших.

Особливу роль відіграє об’єктно-орієнтований підхід, який дозволяє зручно організовувати код: кожен пристрій працює як окремий об’єкт із власними методами керування. Це робить структуру програми зрозумілою, полегшує налагодження та додає гнучкості у разі подальших змін або доповнень.

Ще одна важлива перевага C++ — це ефективне використання ресурсів мікроконтролера. У системах на базі Arduino, де кожен байт пам’яті має значення, можливість точно контролювати роботу з оперативною пам’яттю та портами вводу-виводу є критичною. C++ надає цей рівень контролю, дозволяючи реалізувати швидку й стабільну реакцію на події, такі як зчитування RFID-картки або введення PIN-коду.

І, нарешті, код, написаний на C++, у майбутньому можна адаптувати для інших мікроконтролерів або платформ, таких як ESP32 чи STM32, що відкриває шлях до масштабування або модернізації проєкту.

Таким чином, вибір мови C++ у цьому проєкті це не лише зручність і стандарт для Arduino, а й практичний шлях до створення стабільної, масштабованої та ефективної системи.

1.7.2 Програмне втілення системи

Програмне забезпечення для системи контролю доступу реалізовано на мові програмування C++ для платформи Arduino, з використанням популярних бібліотек, що забезпечують взаємодію з периферійними пристроями: RFID-модулем, клавіатурою, LCD-дисплеєм, SD-картою, RGB-світлодіодом, бузером та сервомотором. Основна мета — забезпечення надійного контролю доступу до офісного приміщення за допомогою RFID-карток або PIN-коду, з можливістю журналювання подій на SD-карті та системою блокування при несанкціонованих спробах входу.

Ініціалізація бібліотек і компонентів. У першій частині коду підключаються бібліотеки, необхідні для роботи з апаратними компонентами. Це забезпечує доступ до методів управління RFID-модулем, клавіатурою, дисплеєм, сервоприводом, SD-картою та RGB-світлодіодом.

```
#include <Keypad.h>              // Бібліотека для роботи з матричною клавіатурою
#include <SPI.h>                 // Бібліотека для SPI-зв'язку (потрібна для RFID і SD)
#include <MFRC522.h>             // Бібліотека для RFID-модуля RC522
#include <Servo.h>               // Бібліотека для роботи з сервоприводом
#include <LiquidCrystal_I2C.h>   // Бібліотека для LCD-дисплея через I2C
#include <SD.h>                  // Бібліотека для SD-карти
```

Рисунок 1.13. Ініціалізація бібліотек і компонентів

Функція RGBWrite(). Використовується для керування кольором RGB-світлодіода. Колір змінюється в залежності від статусу доступу.

```
// Функція керування кольором RGB-світлодіода
void RGBWrite(int r, int g, int b)
{
  analogWrite(ledRed, r);
  analogWrite(ledGreen, g);
  analogWrite(ledBlue, b);
}
```

Рисунок 1.14. Керування кольором RGB-світлодіода

Налаштування основних змінних і пінів. Задано пін-коди для всіх підключених пристроїв — RFID-модуля (SDA, RST), SD-карти (CS), RGB-світлодіода, сервопривода та бузера. Ініціалізовано масиви з дозволеними UID RFID-карт і PIN-кодами.

```
// Ініціалізація LCD-дисплея (адреса 0x27, 16 символів на 2 рядки)
LiquidCrystal_I2C lcd(0x27, 16, 2);

// Піни для підключення RFID RC522
#define SS_PIN 53
#define RST_PIN 5
MFRC522 mfrc522(SS_PIN, RST_PIN); // Створення об'єкта RFID

// SD-карта (пін CS)
#define SD_CS 10
File logFile; // Об'єкт для роботи з файлом на SD-карті

// Список авторизованих UID-карток та PIN-кодів
String validUIDs[] = {"12AB74", "DB0582"};
String pins[] = {"12AB74", "DB0582"};

// Піни для RGB-світлодіода, бузера і сервопривода
int ledRed = 3;
int ledGreen = 6;
int ledBlue = 7;
int buzzer = 4;
int servoPin = 8;
Servo myServo; // Об'єкт для керування сервоприводом
```

Рисунок 1.15. Налаштування пінів та масивів

Конфігурація клавіатури. Вказано розкладку клавіш та їхнє апаратне підключення до Arduino. Це дозволяє зчитувати натискання користувача під час введення PIN-коду.

```
// Піни для клавіатури
byte rowPins[4] = {22, 23, 24, 25};
byte colPins[4] = {26, 27, 28, 29};
// Карта клавіш (4x4)
char keymap[4][4] =
{
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};

// Ініціалізація об'єкта клавіатури
Keypad keypad = Keypad(makeKeymap(keymap), rowPins, colPins, 4, 4);
```

Рисунок 1.16. Конфігурація клавіатури

Блок змінних для логіки блокування. Визначено змінні, що відповідають за фіксацію невдалих спроб входу та за активацію тимчасового блокування системи.

```
// Змінні для логіки блокування
int failedAttempts = 0;
bool isLocked = false;
unsigned long lockStart = 0;
const unsigned long lockDuration = 32000;  // Тривалість блокування — 32 секунди
```

Рисунок 1.17. Змінні для блокування

Функція ShowIdleScreen(). Виводить на LCD повідомлення в очікуванні дій користувача —сканування RFID-картки, або введення PIN-коду.

```
// Функція показу стартового повідомлення
void ShowIdleScreen()
{
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("  Scan card or  ");
  lcd.setCursor(0, 1);
  lcd.print("Press '#' to PIN");
}
```

Рисунок 1.18. Старт роботи повідомлення на LCD-дисплея

Функція logEvent(). Записує усі дії до SD-карти та серійного монітора. Фіксуються джерело (RFID чи PIN), значення (UID чи введений код), часу і результат (успіх або відмова).

```
// Функція запису подій у файл журналу
void logEvent(String source, String value, String status)
{
  String timestamp = String(millis() / 1000); // Мітка часу в секундах
  String entry = timestamp + " | " + source + ": " + value + " | " + status;
  Serial.println(entry);      // Вивід у серійний монітор
  if (logFile)
  {
    logFile.println(entry);  // Запис у файл
    logFile.flush();         // Одразу зберегти зміни
  }
}
```

Рисунок 1.19. Записування дії до SD-карти

Функція lockSystem(). Активує блокування системи на певний час (32 сек), якщо користувач тричі помилився при введенні даних. Виводиться таймер блокування, блимає світлодіод та активується звук.

```
// Функція блокування системи
void lockSystem()
{
  lockStart = millis();
  isLocked = true;
  logEvent("Система", "Закрито", "Доступ закрито на 30 секунд...");
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(" SYSTEM LOCKED ");
  RGBWrite(0, 0, 0);
  tone(buzzer, 1500); // Звук блокування
  delay(1000);
  noTone(buzzer);
}
```

Рисунок 1.20. Активація блокування системи

Функція setup(). Основна ініціалізація пристроїв: RFID, дисплея, SD-карти, сервопривода, RGB-світлодіода. Також відкривається файл для журналу подій.

```
void setup() //  ініціалізація пристроїв: RFID, дисплея, SD-карти, сервопривода, RGB-світлодіода
{
  Serial.begin(9600);
  SPI.begin();           // Старт SPI-зв'язку
  mfrc522.PCD_Init();    // Ініціалізація RFID

  // Налаштування виходів
  pinMode(ledRed, OUTPUT);
  pinMode(ledGreen, OUTPUT);
  pinMode(ledBlue, OUTPUT);
  pinMode(buzzer, OUTPUT);

  // Підключення сервопривода
  myServo.attach(servoPin);
  myServo.write(0); // Початкова позиція

  // Ініціалізація LCD
  lcd.init();
  lcd.backlight();
  ShowIdleScreen();

  RGBWrite(0, 0, 255); // Синє світло на старті
  Serial.println("Прикладіть картку або натисніть '#' для введення PIN-коду");

  // Ініціалізація SD-карти
  if (!SD.begin(SD_CS))
  {
    Serial.println("Помилка ініціалізації SD-карти!");
  }
  else
  {
  logFile = SD.open("log.txt", FILE_WRITE);
    if (logFile)
    {
      logFile.println("--- Нова сесія ---");
      logFile.flush();
    }
  }
}
```

Рисунок 1.21. Ініціалізація пристроїв

Функція loop(). Цикл, що безперервно виконується. Він містить головну логіку системи доступу.

1. Обробка режиму блокування: Якщо система заблокована, на дисплеї відображається зворотний відлік, а RGB-світлодіод блимає різними кольорами.

```
void loop() // Дії системи доступу та блокування
{
  if (isLocked)
  {
    // Обробка режиму блокування
    unsigned long elapsed = millis() - lockStart;
    if (elapsed >= lockDuration)
    {
      isLocked = false;
      failedAttempts = 0;
      ShowIdleScreen();
      RGBWrite(0, 0, 255);
    }
    else
    {
      // Відлік часу блокування
      int remaining = (lockDuration - elapsed) / 1000;
      lcd.setCursor(0, 0);
      lcd.print(" SYSTEM LOCKED ");
      lcd.setCursor(0, 1);
      lcd.print("  Wait: ");
      lcd.print(remaining);
      lcd.print(" sec ");

      // Блимання RGB під час блокування
      static int colorState = 0;
      static unsigned long lastBlink = 0;
      if (millis() - lastBlink > 300)
      {
        lastBlink = millis();
        colorState = (colorState + 1) % 3;
        if (colorState == 0) RGBWrite(255, 0, 0);
        if (colorState == 1) RGBWrite(0, 255, 0);
        if (colorState == 2) RGBWrite(0, 0, 255);
      }
      delay(20);
    }
    return;
  }
```

Рисунок 1.22. Дії під час блокування системи

2. Обробка введення PIN-коду: Якщо натиснута клавіша #, користувачеві пропонується ввести PIN-код. Введення відображається у вигляді зірочок на дисплеї.

```
// Введення PIN-коду
if (keypad.getKey() == '#')
{
  String pin = "";
  char key;
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("   Enter PIN:   ");
  Serial.print("Введіть PIN: ");

  while (true)
  {
    key = keypad.getKey();
    if (isLocked) return;
    if (key)
    {
      if (key == '#') break;

      if (key == '*')
      {
        pin = "";
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("   Enter PIN:   ");
        lcd.setCursor(0, 1);
        lcd.print("                ");
        lcd.setCursor(0, 1);
        Serial.println("\nPIN скинуто");
        Serial.print("Введіть PIN: ");
        continue;
      }
```

Рисунок 1.23. Перша частина кода обробки PIN-коду

```
    if (pin.length() < 15)
    {
      pin += key;
      Serial.print("*");
      int index = pin.length() - 1;
      int col = index % 16;
      int row = index / 16;
      lcd.setCursor(col, row + 1);
      lcd.print("*");
    }
  }
}

// Перевірка PIN-коду
Serial.println();
for (String validPin : pins)
{
  if (pin == validPin)
  {
    logEvent("PIN", pin, "Доступ надано");
    accessGranted();
    failedAttempts = 0;
    return;
  }
}

// Невірний PIN-код
logEvent("PIN", pin, "Доступ заборонено");
failedAttempts++;
(failedAttempts >= 3) ? lockSystem() : accessDenied();
return;
}
```

Рисунок 1.24. Друга частина кода обробки PIN-коду

3. Зчитування RFID-картки: Якщо виявлено картку, зчитується її UID. Якщо UID авторизовано — відкривається замок, і подія фіксується. Інакше — фіксується помилка.

```
// Зчитування RFID-картки
if (!mfrc522.PICC_IsNewCardPresent() || !mfrc522.PICC_ReadCardSerial()) return;

String uid = "";
for (byte i = 0; i < mfrc522.uid.size; i++)
{
  if (mfrc522.uid.uidByte[i] < 0x10) uid += "0";
  uid += String(mfrc522.uid.uidByte[i], HEX);
}
uid.toUpperCase();
Serial.print("UID: ");
Serial.println(uid);

// Перевірка UID
for (String valid : validUIDs)
{
  if (uid == valid)
  {
    logEvent("RFID", uid, "Доступ надано");
    accessGranted();
    failedAttempts = 0;
    mfrc522.PICC_HaltA();
    mfrc522.PCD_StopCrypto1();
    return;
  }
}

// Невірний UID
logEvent("RFID", uid, "Доступ заборонено");
failedAttempts++;
(failedAttempts >= 3) ? lockSystem() : accessDenied();
mfrc522.PICC_HaltA();
mfrc522.PCD_StopCrypto1();
}
```

Рисунок 1.25. Зчитування дії для RFID-картки

У симуляції з Wokwi дисплей не мав затримок, однак у реальному проєкті бажано використовувати не блокуючі функції оновлення виводу, щоб не уповільнювати інші процеси.

```
// Доступ надано – відкриття замка
void accessGranted()
{
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(" Access Granted ");
  RGBWrite(0, 255, 0);
  tone(buzzer, 1000);
  delay(200);
  noTone(buzzer);
  myServo.write(90);    // Відкрити замок

  // Таймер відкриття 5 секунд
  for (int i = 5; i > 0; i--)
  {
    lcd.setCursor(0, 1);
    lcd.print("  Open: ");
    lcd.print(i);
    lcd.print(" sec ");
    delay(1000);
  }

  myServo.write(0);     // Закрити замок
  RGBWrite(0, 0, 255);
  ShowIdleScreen();
}
```

Рисунок 1.26. Дії відкриття замка

Функція accessDenied(). При невірному UID або PIN-коді виводиться повідомлення про відмову в доступі, RGB світлодіод блимає червоним, бузер подає сигнал.

```
// Доступ заборонено – сигналізація
void accessDenied()
{
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(" Access Denied ");
  RGBWrite(255, 0, 0);
  for (int i = 0; i < 2; i++)
  {
    tone(buzzer, 800);
    delay(200);
    noTone(buzzer);
    delay(200);
  }
  RGBWrite(0, 0, 255);
  ShowIdleScreen();
}
```

Рисунок 1.27. Дії відмови пристрою

1.8 Моделювання та тестування на сайті Wokwi

Однією з важливих складових у створенні системи контролю доступу стала можливість проведення повноцінного моделювання безпосередньо онлайн, без потреби у фізичному збиранні схеми. Для цього був обраний симулятор Wokwi — інструмент, який дозволяє перевіряти роботу Arduino-проєктів у режимі реального часу, використовуючи віртуальні компоненти та схеми.

Для мого проєкту, Wokwi став ідеальним середовищем для тестування всіх логічних зв'язків між компонентами. Він дозволив без ризику пошкодження плати або модулів перевірити, як саме система реагує на введення RFID-карток, PIN-коду, неправильні спроби доступу та логіку блокування.

1.8.1 Проведення моделювання

У середовищі Wokwi я відтворив повну схему, використовуючи наступні віртуальні компоненти:

1. Arduino Mega 2560 — як основний контролер системи.

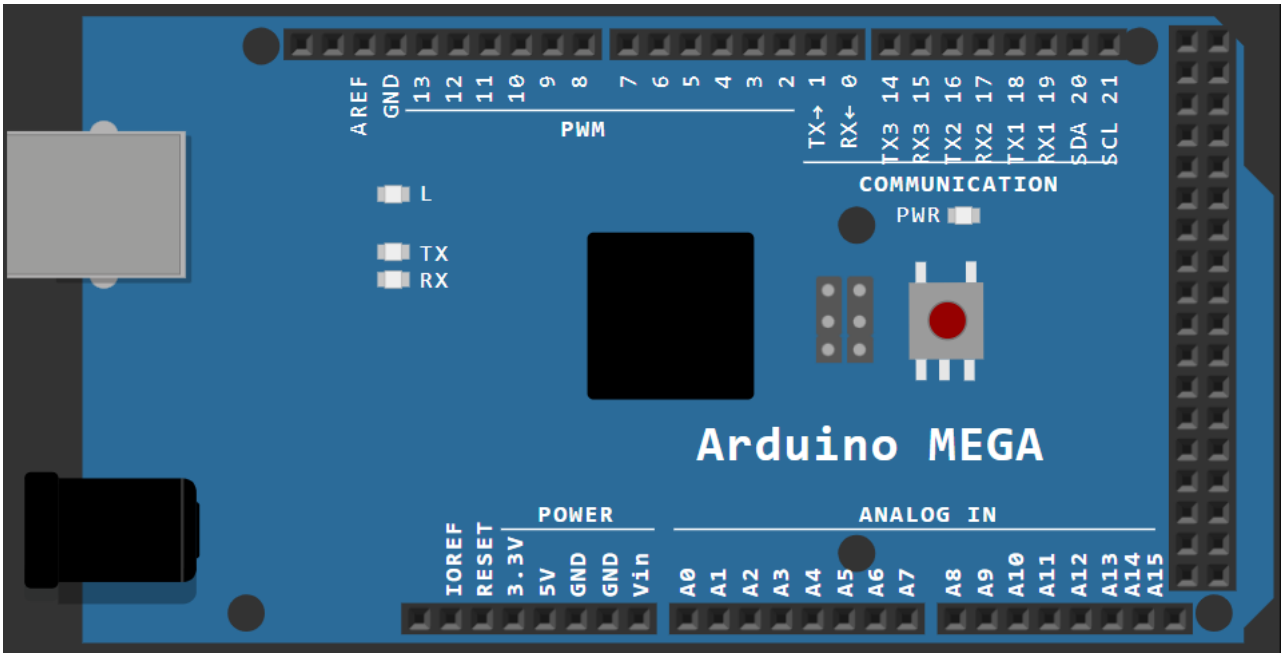


Рисунок 1.28. Віртульний вигляд компонента Arduino Mega

2. Модуль RFID RC522 — для зчитування UID карток.

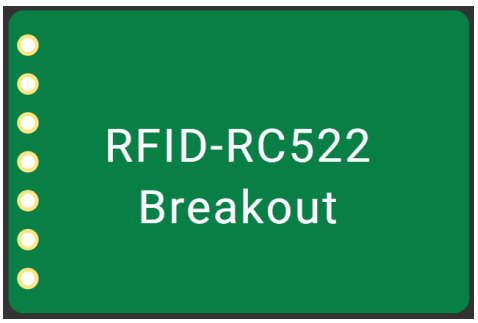


Рисунок 1.29. Віртульний вигляд компонента RFID RC522

3. Матрична клавіатура 4x4 — для введення PIN-коду.

Рисунок 1.30. Віртульний вигляд компонента матрична клавіатура

4. RGB-світлодіод — для візуального інформування (зелений = доступ дозволено, червоний = відмовлено, синій = стан очікування дії).

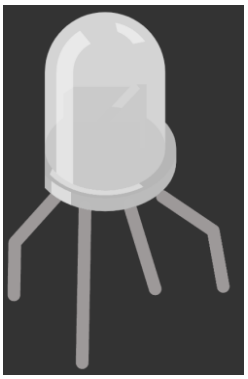


Рисунок 1.31. Віртульний вигляд компонента RGB-світлодіода

5. Активний бузер — для звукових сповіщень.

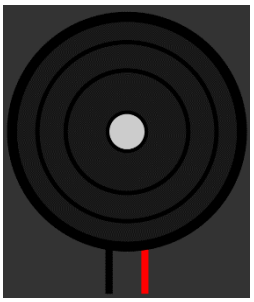


Рисунок 1.32. Віртульний вигляд компонента бузера

6. Сервомотор — для імітації відкриття або блокування дверей.

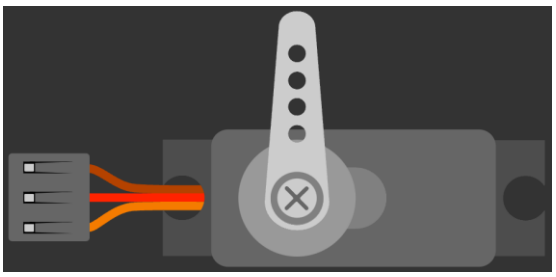


Рисунок 1.33. Віртульний вигляд компонента сервомотора

7. SD-карта — для зберігання логів входів та помилок.

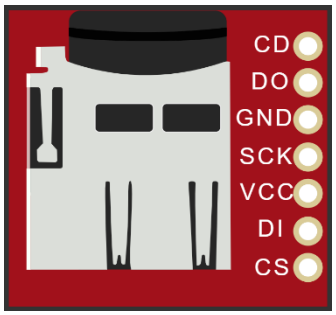


Рисунок 1.34. Віртульний вигляд компонента SD-карти

8. SD-карта — для зберігання логів входів та помилок.

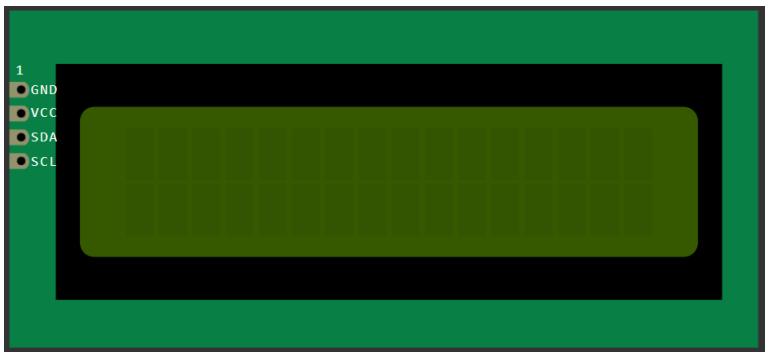


Рисунок 1.35. Віртульний вигляд компонента LCD-дисплея

1.8.2 Пояснення підключень пінів компонентів

У цьому розділі розглянемо конкретні підключення кожного апаратного елементу до плати Arduino Mega 2560, що використовується в системі моніторингу та контролю доступу до офісу. Схема реалізована у віртуальному середовищі Wokwi, що дозволяє безпечно й наочно протестувати всі функції системи ще до створення фізичного прототипу.

1. RC522 RFID-модуль.

Цей модуль підключено до Arduino за стандартним SPI-протоколом:

- SDA → пін 53;
- SCK → пін 52;
- MOSI → пін 51;
- MISO → пін 50;
- RST → пін 5;
- VCC → 3.3V;
- GND → GND.2.

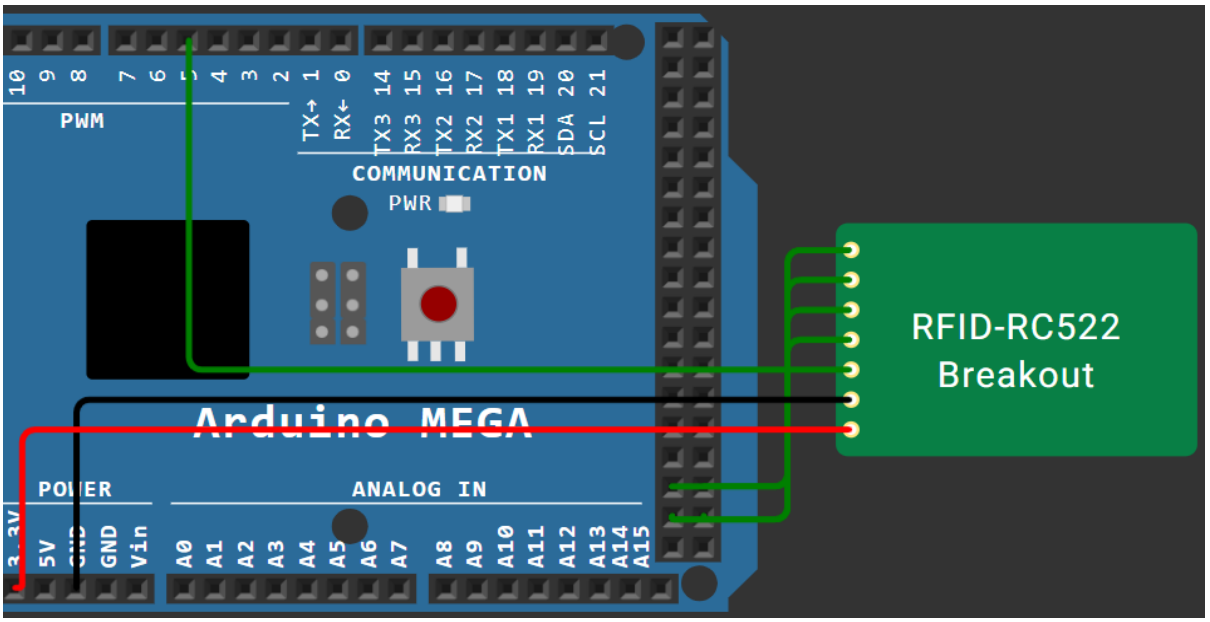


Рисунок 1.36. Підключення пінів RFID RC522

Такий спосіб забезпечує швидкий обмін UID-даними картки з мікроконтролером. Живлення здійснюється через 3.3V, як вимагає модуль.

2. LCD-дисплей 16×2 з модулем I2C.

Дисплей підключено через I2C-інтерфейс пінів на Arduino:

- SDA → пін 20;
- SCL → пін 21;
- VCC → 5V;
- GND → GND.5.

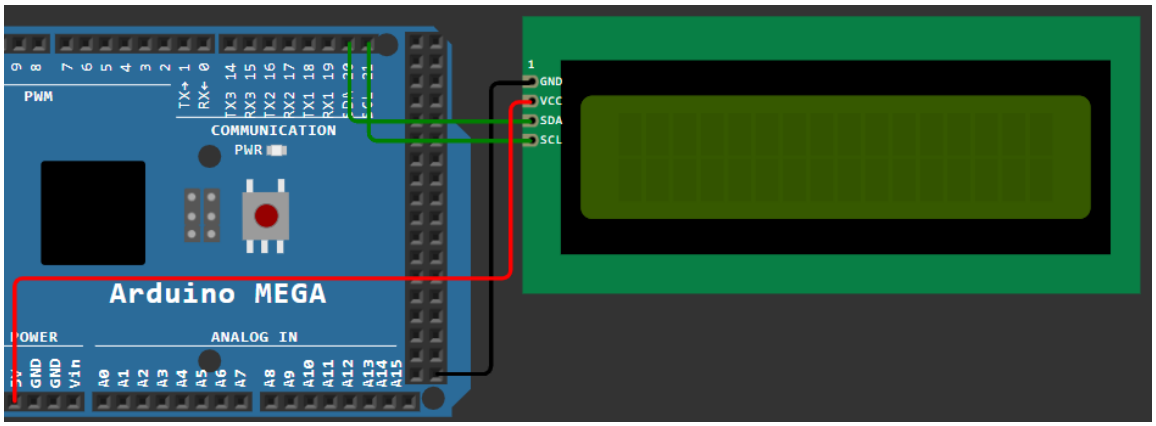


Рисунок 1.37. Підключення пінів LCD-дисплея

Це дозволяє використовувати лише два піни замість шести, як у звичайному підключенні без I2C.

3. Бузер.

Звуковий сигнал допомагає інформувати користувача:

- Сигнальний пін → пін 4;
- GND → GND.1.

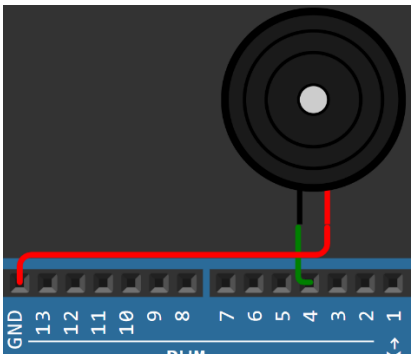


Рисунок 1.38. Підключення пінів бузера

Подає короткий або довгий сигнал, залежно від сценарію — успішний доступ, помилка або блокування.

4. Матрична клавіатура 4×4.

До введення PIN-коду використовується матрична клавіатура, підключена до цифрових пінів Arduino:

- Піни клавіатури R1–R4, C1–C4 → піни 22 до 29.

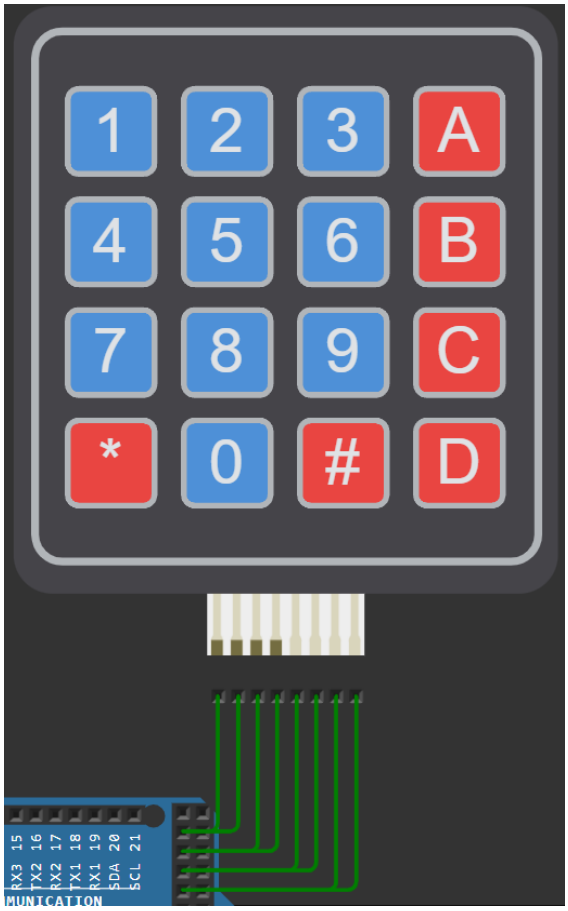


Рисунок 1.39. Підключення пінів матричної клавіатури

Її підключення дозволяє зчитувати натискання клавіш за допомогою спеціальної бібліотеки Keypad.

5. SD-картка.

Використовується для збереження логів доступу:

- DO → пін 50;
- DI → пін 51;
- CS → пін 10;
- VCC → 5V;
- GND → GND.5.

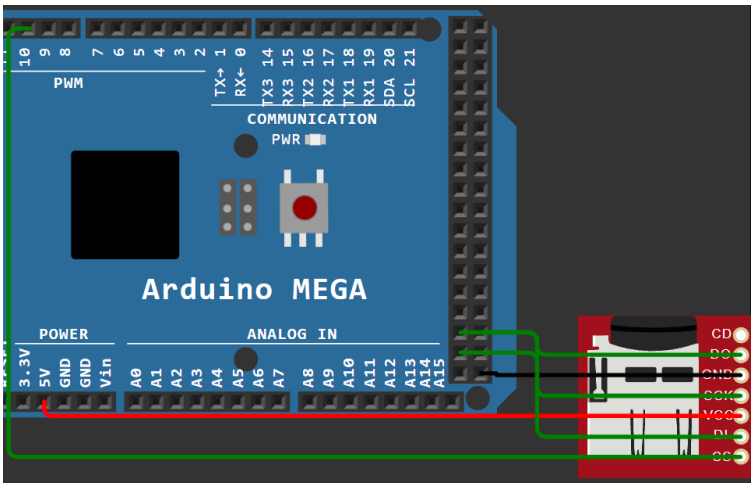


Рисунок 1.40. Підключення пінів SD-карти

Для одночасної роботи з кількома SPI-пристроями використовуються різні пінів CS (Chip Select), тому RC522 працює через пін 53.

6. RGB-світлодіод.

Цей компонент надає візуальне зворотне повідомлення:

- Червоний (R) → пін 3;
- Зелений (G) → пін 6;
- Синій (B) → пін 7;
- COM → через спільний катод до GND.4.

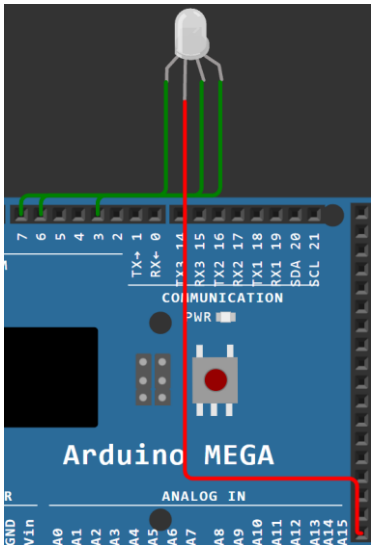


Рисунок 1.41. Підключення пінів RGB-світлодіода

Індикація: червоний — відмова в доступі, зелений — дозвіл, синій — введення PIN або UID.

7. Сервомотор SG90.

Використовується для блокування/розблокування дверей:

- PWM → пін 8;
- V+ → 5V;
- GND → GND.3.

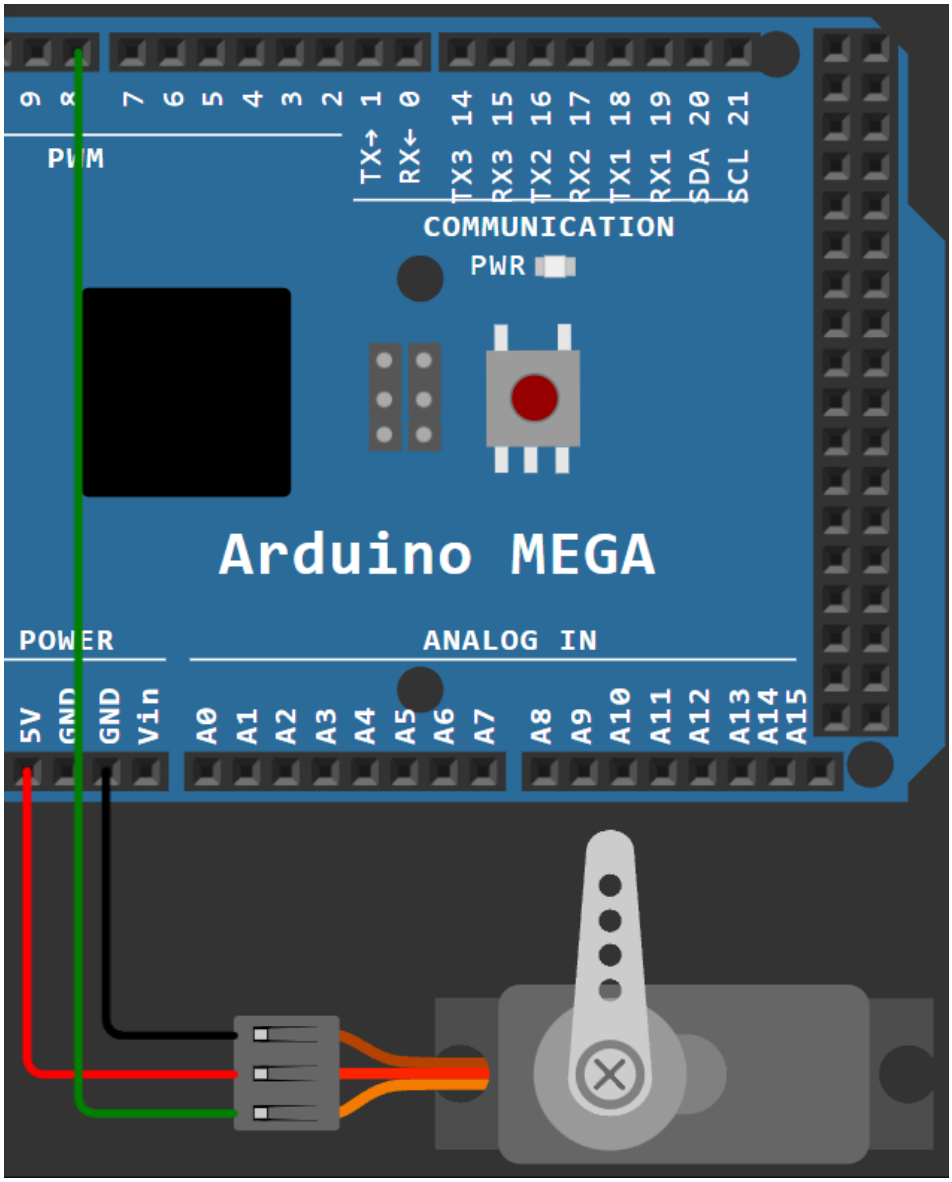


Рисунок 1.42. Підключення пінів сервомотора

Керування здійснюється через PWM-сигнал. При правильному доступі сервопривід повертається у відкрите положення. Повна реалізація підключення пінів з компонентами показано на рисунку.

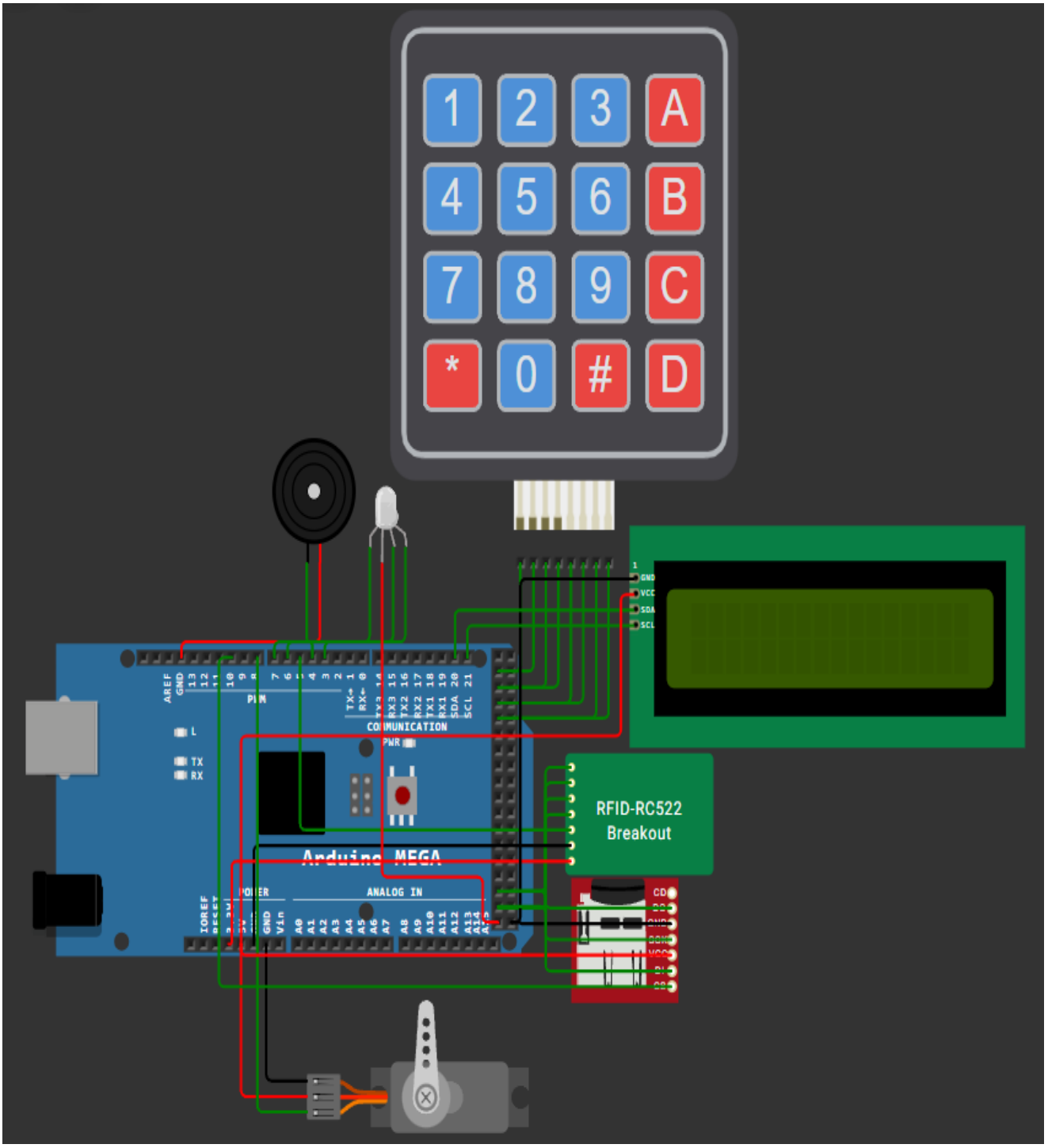


Рисунок 1.43. Віртуальний вигляд підключеного проекта

Усі компоненти підключені таким чином, щоб не конфліктувати між собою, з урахуванням специфікації Arduino Mega 2560, яка має велику кількість доступних цифрових ліній. Це дозволяє масштабувати систему або замінити частину пристроїв у майбутньому без складної перепрошивки.

1.8.3 Перевірка сценаріїв роботи

Після того як було завершено написання основного коду та зібрано віртуальну модель системи у середовищі Wokwi, настав етап перевірки ключових сценаріїв роботи. Це один із найважливіших моментів розробки, адже саме тут можна переконатися, що логіка системи відповідає поставленим цілям: контроль доступу до офісу з автентифікацією по RFID-картці та PIN-коду, інформування користувача через дисплей і світлові/звукові сигнали, а також запис дій на SD-карту.

Щоб упевнитися, що система поводиться правильно в усіх можливих ситуаціях, були змодельовані різні типи взаємодії користувача: від нормального входу до помилкових спроб та блокування. Всі перевірки проводилися в симуляторі Wokwi, що дозволило в режимі реального часу аналізувати поведінку пристроїв, переглядати серійну консоль та вміст SD-карти.

Сценарій 1: Стан очікування дій користувача.

Цей сценарій є вихідною точкою в роботі всієї системи. Саме з нього починається кожна сесія, і саме в ньому система перебуває більшість часу — чекаючи, поки користувач ініціює дію. Від того, наскільки грамотно реалізований цей стан, залежить зручність і стабільність роботи проєкту.

Умови:

1. Система щойно увімкнена або завершено попередню сесію;

2. Немає прикладених RFID-карт або натискань на клавіатурі;

3. Ніхто не взаємодіє з пристроєм.

Очікувана реакція:

- LCD-дисплей показує повідомлення: «Scan card or Press '#' to PIN»;
- Бузер мовчить (ніяких звуків);
- Сервомотор не активний, двері залишаються зачиненими;

- RGB-світлодіод засвічується синім кольором — як індикатор спокою або очікування;

- SD-карта не веде запис, бо немає дії.

Програма перебуває в циклі, де кожну мілісекунду сканує стан RFID-зчитувача.

Цей сценарій дає змогу користувачеві зрозуміти, що пристрій працює і готовий до використання, але водночас він економний по ресурсах: нічого не обробляється зайвого, ніяких таймерів не крутиться, лише спокійне очікування. Цей стан є базою для переходу до інших сценаріїв, описаних раніше. Як тільки прикладається картка — система автоматично переходить до перевірки UID та ініціює наступний сценарій. Якщо UID збігається — вибір запуска введення PIN-коду.

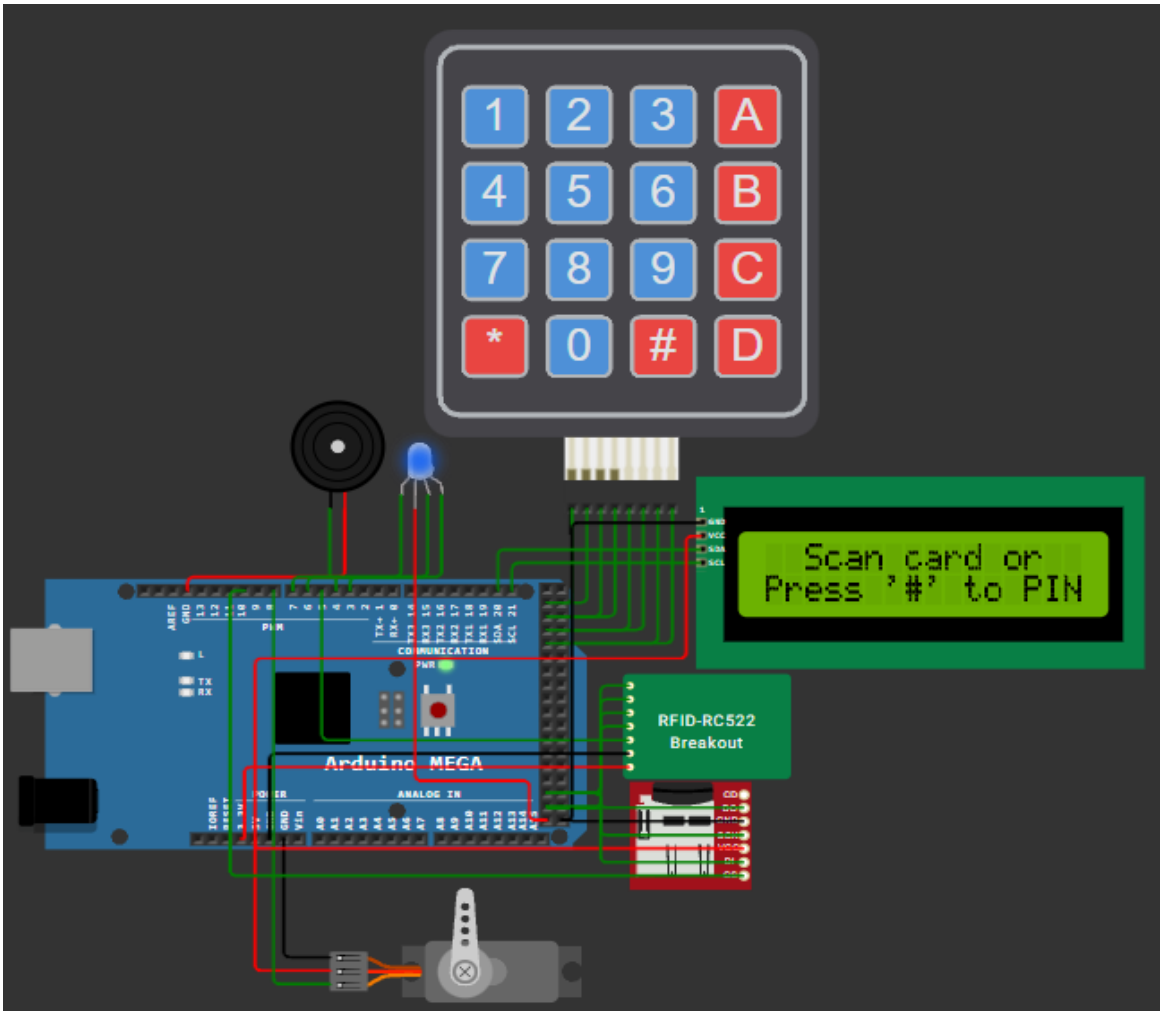


Рисунок 1.44. Стан очікування дії користувача

Сценарій 2: Дозволений доступ

Цей сценарій є базовим і демонструє стандартну взаємодію користувача з системою.

Умови:

1. Користувач прикладає дійсну RFID-картку з дозволеним UID або вводить дійсний PIN-код.

Очікувана реакція:

- LCD-дисплей вітає користувача.
- Зелений колір RGB-світлодіода засвічується.
- Бузер видає короткий приємний сигнал.
- Сервопривід відкриває двері (імітація).
- Усі дії записуються на SD-карту: UID або PIN, час доступу, статус "Доступ надано".

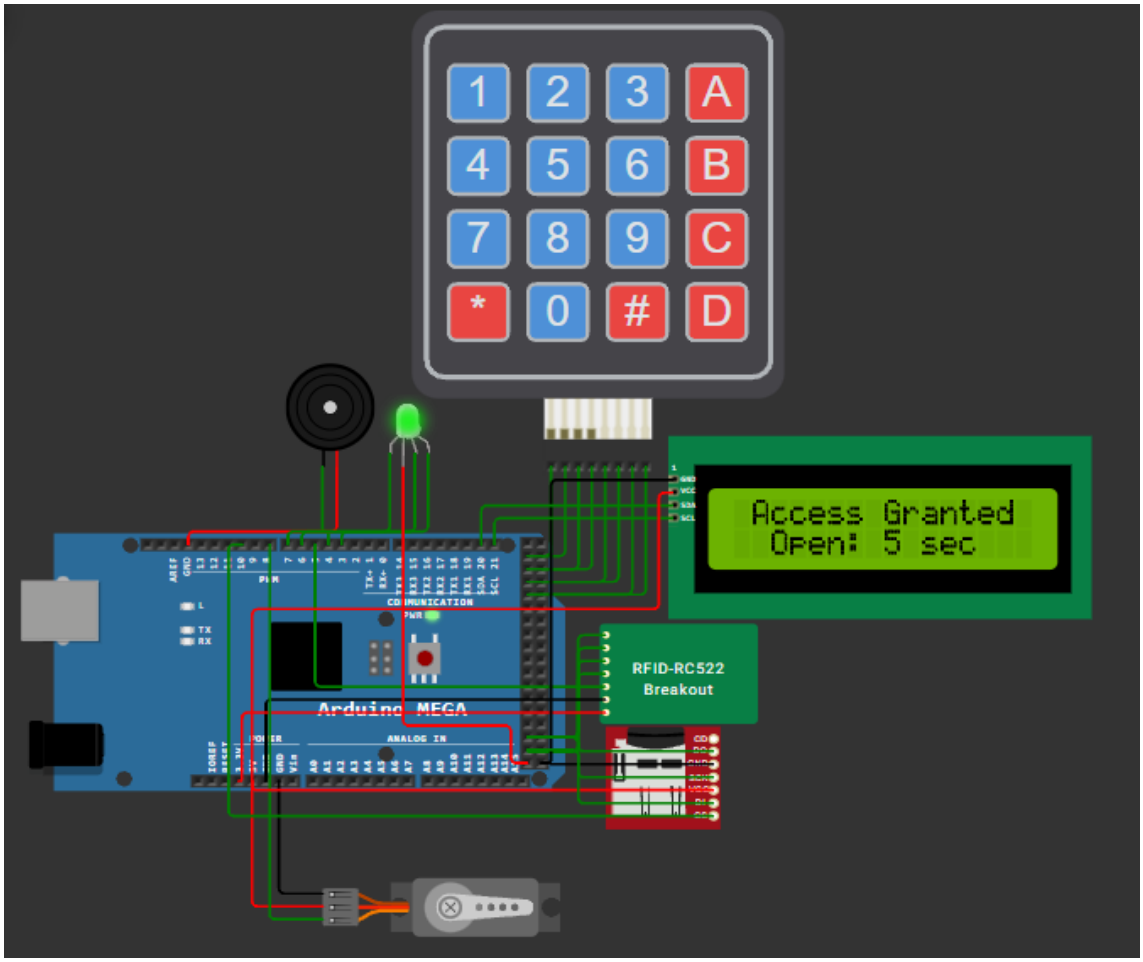


Рисунок 1.45. Дія пристрою при правильному доступі

Сценарій 3: Невірний RFID-картка або PIN-код.

Цей сценарій перевіряє здатність системи фільтрувати сторонні картки або PIN-коди, які не додані в список дозволених.

Умови:

1. Користувач прикладає невідому (недозволену) картку або вводить невірний PIN-код.

Очікувана реакція:

- На дисплеї з’являється повідомлення "Access Denied".
- Засвічується червоний колір RGB-світлодіода.
- Бузер видає довгий тривожний сигнал.
- Доступ не надається.
- Подія фіксується на SD-карті зі статусом "Доступ заборонено".

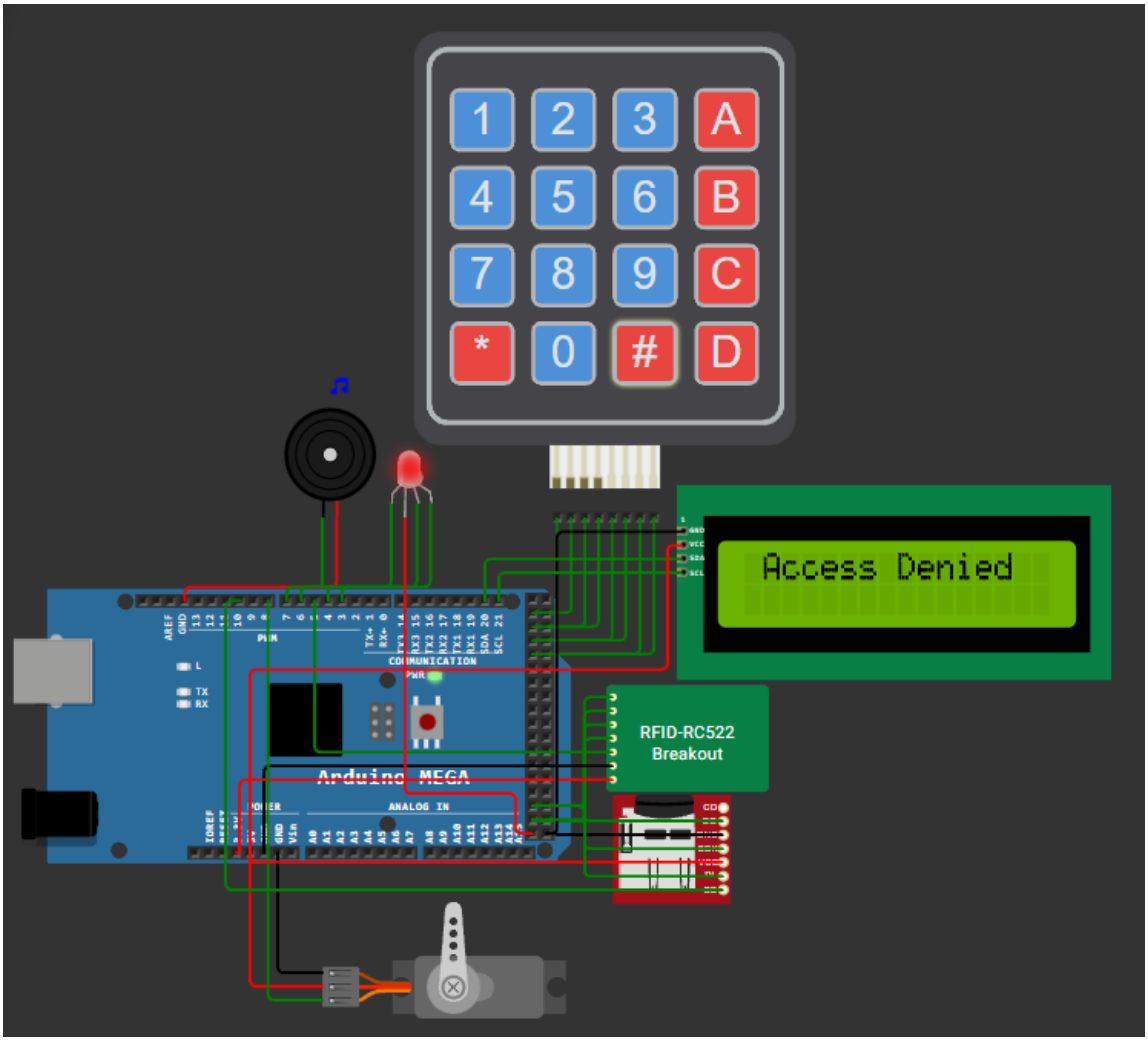


Рисунок 1.46. Дія пристрою при неправильному доступі

Сценарій 4: Блокування системи.

Цей сценарій перевіряє, чи працює механізм захисту при багаторазових спробах доступу з невірними даними.

Умови:

1. 3 рази підряд поспіль вводиться неправильний PIN або UID.

Очікувана реакція:

- Повідомлення на дисплеї "SYSTEM LOCKED Wait: ... sec".
- Пристрій не спрацьовує при взаємодії, поки таймер блокування не закінчиться (32 секунди).
- Різні кольори RGB-світлодіода і довгий звук бузера.
- Запис у лог-файл: час, "Система: Закрито".

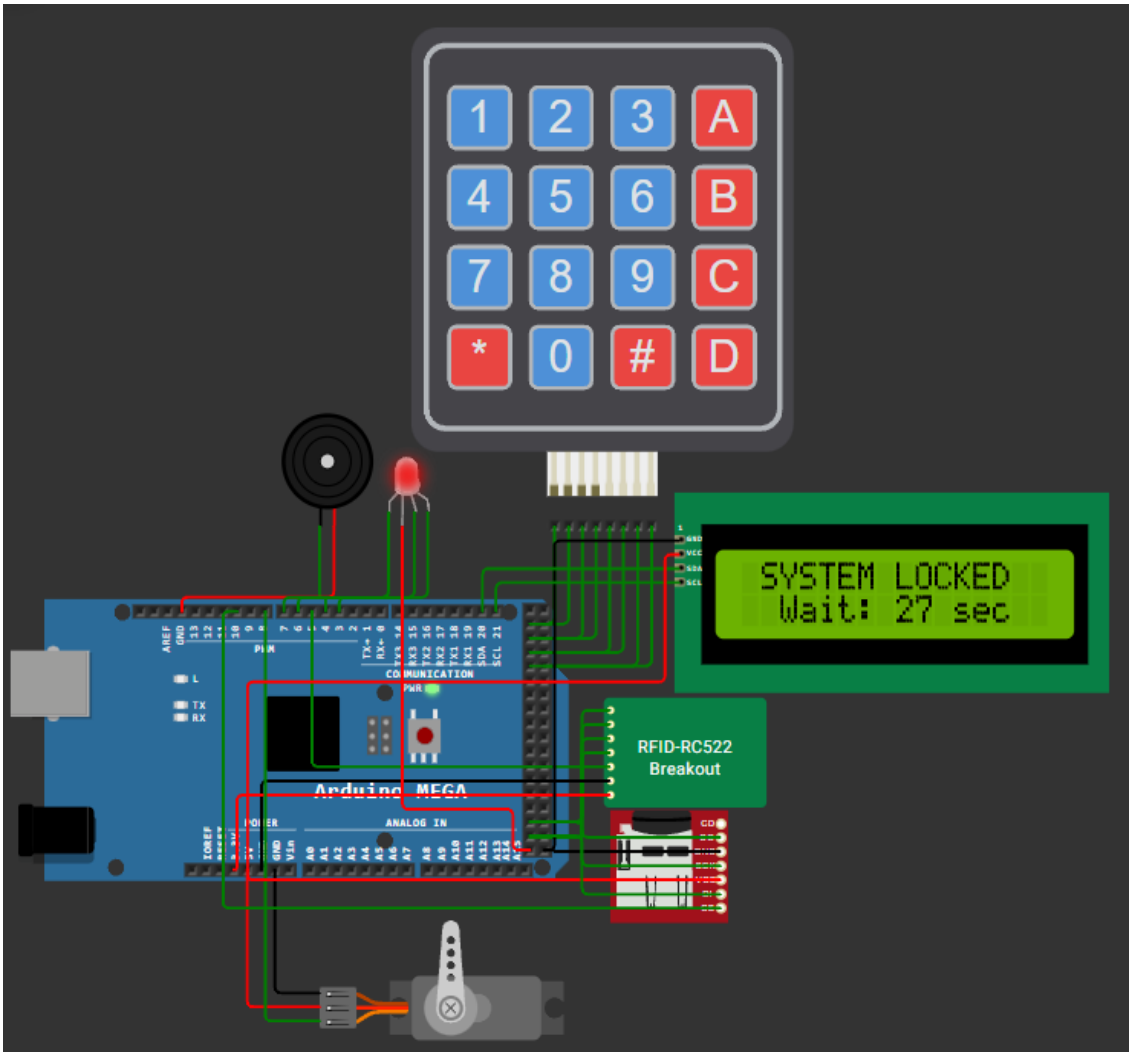


Рисунок 1.47. Дія пристрою при трьох поспіль помилках користувача

2 ЕКОНОМІЧНИЙ РОЗДІЛ

Темою даного проекту є розробка системи моніторингу та контролю доступу до офісу на основі RFID. Цей пристрій дозволяє ефективно керувати доступом до приміщення, забезпечуючи як безпеку, так і зручність користування. У проєкті реалізовано перевірку особи — за допомогою RFID-картки або введення PIN-коду на клавіатурі.

У даному розділі визначається вартісна оцінка розробленого пристрою. Спочатку визначається калькуляція розробленого виробу укрупненим методом через вартість покупних комплектуючих елементів і виробів, для визначення якої складаємо перерахування елементів і виробів на основі відомості специфікацій (принципової схеми) по формі, приведеної в таблиці 2.1

Таблиця 2.1. Розрахунок відомості покупних комплектуючих елементів

Найменування, тип, модель	Од.вим.	Норма витрат на виріб	Ціна, грн.	Вартість комплектуючих
Мікроконтролер Arduino Mega 2560	шт.	1	656,00	656,00
RFID-модуль RC522 + картка	шт.	1	61,00	61,00
4x4 Матрична клавіатура	шт.	1	40,00	40,00
LCD-дисплей 16x02 + I2C	шт.	1	168,00	168,00
Сервомотор SG90	шт.	1	50,00	50,00
Активний бузер KY-012	шт.	1	18,00	18,00
RGB-світлодіод	шт.	1	12,26	12,26
Модуль microSD (SPI)	шт.	1	29,00	29,00
Резистор 220 Ом	шт.	1	5,00	15,00
Макетна плата	шт.	1	120,00	120,00
З'єднувальні дроти	набір	1	70,00	70,00
Загальна вартість покупних комплектуючих елементів				1 239,26
Транспортні витрати (10%)				123,93
Всього ($В_{пк}$)				1 363,19

Калькуляцію планової собівартості розробленого виробу розраховуємо з використанням методу питомих ваг і структури собівартості аналогічної продукції (табл. 2.2).

Тому що, проектований виріб відноситься до радіоелектронної апаратури, то:

Питома вага матеріалу → $\alpha_м = 20\%$;

Питома вага покупних виробів → $\alpha_{пк} = 62\%$;

Питома вага основної заробітної плати → $\alpha_{озп} = 18\%$.

Таблиця 2.2. Калькуляція планової собівартості

Найменування статті витрат	Значення статті, грн.	Розрахунок
1. Сировина і матеріал	439,74	$В_м = \alpha_м * В_{пк} / \alpha_{пк}$ $В_м = 20\% * 1\ 363,19 / 62\%$
2. Комплектуючі вироби і покупні напівфабрикати	1 363,19	$В_{пк} = 1\ 363,19$
3. Основна заробітна плата	395,77	$В_{оз} = \alpha_{озп} * В_{пк} / \alpha_{пк}$ $В_{оз} = 18\% * 1\ 363,19 / 62\%$
4. Додаткова заробітна плата	158,31	$В_{дз} = 0,4 * В_{оз}$ $В_{дз} = 0,4 * 395,77$
5. Відрахування до єдиного соцфонду	121,90	$В_{єс} = (В_{оз} + В_{дз}) * 0,22$ $В_{єс} = (395,77 + 158,31) * 0,22$
6. Загально-виробничі витрати	514,50	$В_{заг.вир} = (1,2 \dots 1,5) * В_{оз}$ $В_{заг.вир} = 1,3 * 395,77$
7. Виробнича собівартість	2 993,41	$С_{вир} = В_м+В_{пк}+В_{оз}+В_{дз}+В_{єс}+ В_{заг.вир}$ $С_{вир} = 439,74 + 1\ 363,19 + 395,77 +$ $158,31 + 121,90 + 514,50$
8. Адміністративні витрати	118,73	$В_а = В_{оз} * 0,3$ $В_а = 395,77 * 0,3$
9. Витрати на збут	59,87	$В_{зб} = С_{вир} * 0,02$ $В_{зб} = 2\ 993,41 * 0,02$
10. Інші операційні витрати	29,93	$В_{оп} = С_{вир} * 0,01$ $В_{оп} = 2\ 993,41 * 0,01$
Повна собівартість	3 201,94	$С_{пов} = С_{вир} + В_а + В_{зб} + В_{оп}$ $С_{пов} = 2\ 993,41 + 118,73 + 59,87 + 29,93$

Розмір планового прибутку, що включається в ціну, визначаємо по формулі:

$$П = (С_{пов} * \rho) / 100\%, \qquad \text{(формула 2.1)}$$

де ρ-планова рентабельність продукції (10% ... 30%).

$$П = (3\ 201,94 * 25\%) / 100\% = 800,49$$

Оптову ціну виробу визначаємо по формулі:

$$Ц_о = С_{пов} + П \qquad \text{(формула 2.2)}$$

$$Ц_о = 3\ 201{,}94 + 800{,}49 = 4\ 002{,}43$$

Ціну реалізації виробу встановлюємо з урахуванням ПДВ:

$$Ц_р = Ц_о + П_з, \qquad \text{(формула 2.3)}$$

де $П_з$ - податкове зобов'язання з ПДВ:

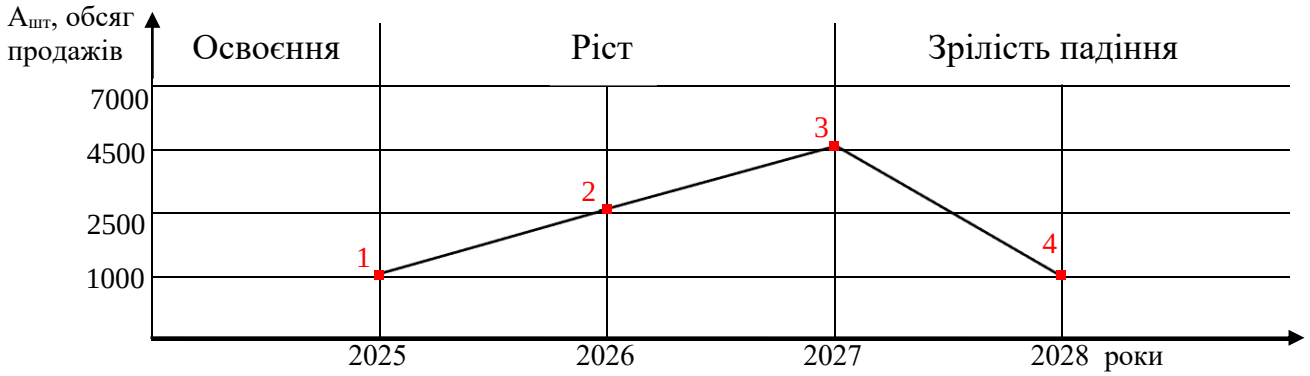
$$П_з = Ц_о * 0{,}2 \qquad \text{(формула 2.4)}$$

$$П_з = 4\ 002{,}43 * 0{,}2 = 800{,}49$$

$$Ц_р = 4\ 002{,}43 + 800{,}49 = 4\ 802{,}92$$

Прогноз обсягів продаж даного виробу:

Отримана в таблиці 2.2 повна собівартість являє собою витрати виготовлення ($С_{пк}$) одиниці виробу для даного року виробництва. Запропонуємо прогноз обсягів продажів даного виробу на другій стадії життєвого циклу виробу «Виробництво» з розподілом по роках (прогноз продажів передбачаємо на 4 роки). Характерні зони промислового випуску виробу представлені на малюнку:



В 2025 році обсяг продажів передбачається в розмірі 1000 шт. під замовлення. В наступному році прогнозується збільшення обсягу продажів, тому витрати виробництва визначаємо по формулі:

$$С_{пов\ i+1} = С_{пов i} \left(\frac{A_i}{A_{i=1}}\right)^{0.23}, \qquad \text{(формула 2.5)}$$

де A_i – обсяг продажів (виробництва) у 1 рік розрахункового періоду, шт.

A_{i+1} – обсяг продажів (i+1)-ом року, шт.;

0,23 – показник ступеня, що характеризує вплив росту обсягів виробництва на собівартість продукції. Звідси випливає, що

$$С_{пов\ 2026} = 3\ 201{,}94 * (2500/4500) \wedge 0{,}23 = 2\ 789{,}18$$

$$С_{пов\ 2027} = 2\ 789{,}18 * (4500/7000) \wedge 0{,}23 = 2\ 536{,}99$$

При відсутності росту обсягів виробництва, тобто якщо обсяг продажів або не змінюється, або зменшується в наступному році, витрати виробництва приймаються на ровне попереднього року.

$$С_{пов\ 2028} = 2\ 536,99$$

Плановий прибуток, що включається в оптову ціну підприємства, для наступного року при збільшенні обсягу продажів, визначаємо по формулі:

$$П_{i+1} = С_{пі+1} * \frac{\rho}{100} \qquad \text{(формула 2.6)}$$

$$П_{2026} = 2\ 789,18 * (25 / 100) = 697,30$$

$$П_{2027} = 2\ 536,99 * (25 / 100) = 634,25$$

$$П_{2028} = 2\ 536,99 * (25 / 100) = 634,25$$

Оптову ціну підприємства в наступні роки розрахункового періоду визначаємо по формулі:

$$Ц_{О_{i+1}} = С_{п_{i+1}} + П_{i+1} \qquad \text{(формула 2.7)}$$

$$Ц_{2026} = 2\ 789,18 + 697,30 = 3\ 486,48$$

$$Ц_{2027} = 2\ 536,99 + 634,25 = 3\ 171,24$$

$$Ц_{2028} = 2\ 536,99 + 634,25 = 3\ 171,24$$

Податкове зобов'язання визначається по формулі:

$$Пз_{i+1} = Ц_{О_{i+1}} * 0.2 \qquad \text{(формула 2.8)}$$

$$П_{з\ 2026} = 3\ 486,48 * 0,2 = 697,30$$

$$П_{з\ 2027} = 3\ 171,24 * 0,2 = 634,25$$

$$П_{з\ 2028} = 3\ 171,24 * 0,2 = 634,25$$

Ціну реалізації одиниці продукції в наступні роки визначаємо по формулі:

$$Ц_{Р_{i+1}} = Ц_{О_{i+1}} + Пз_{i+1} \qquad \text{(формула 2.9)}$$

$$Ц_{р\ 2026} = 3\ 486,48 + 697,30 = 4\ 183,78$$

$$Ц_{р\ 2027} = 3\ 171,24 + 634,25 = 3\ 805,49$$

$$Ц_{р\ 2028} = 3\ 171,24 + 634,25 = 3\ 805,49$$

Коефіцієнт α_i визначаємо по формулі:

$$\alpha_i = \left|1 + E_H\right|^{t_p - t_i} \qquad \text{(формула 2.10)}$$

$Е_н$ – норматив ефективності капітальних вкладень, $Е_н = 0,1$;

$t_р$ – розрахунковий рік розрахункового періоду;

$t_і$ – і-ій рік розрахункового періоду, витрати і результати якого приводяться до розрахункового року.

Вартісну оцінку результатів за розрахунковий період ($Р_т$) визначаємо по формулі:

$$P_T = \sum_{i=t_p}^{t_k} A_i * Ц_{P_i} * \alpha_i \qquad \text{(формула 2.11)}$$

де t_p, t_k – відповідно розрахунковий і кінцевий рік розрахункового періоду;

$Цр_i$ – ціна реалізації в і-тім році, грн.;

$А_i$ – обсяг продажів у і-тім році, грн.;

α_i – коефіцієнт, що включає фактор часу, тобто коефіцієнт приведення різночасних витрат і результатів до розрахункового року.

$$Р_{т\ 2025} = 1000 * 4\ 802{,}92 * 0{,}98 = 4\ 706\ 861{,}6$$

$$Р_{т\ 2026} = 2500 * 4\ 183{,}78 * 0{,}86 = 8\ 995\ 127$$

$$Р_{т\ 2027} = 4500 * 3\ 805{,}49 * 0{,}74 = 12\ 672\ 281{,}7$$

$$Р_{т\ 2028} = 1000 * 3\ 805{,}49 * 0{,}67 = 2\ 549\ 678{,}3$$

Вартісну оцінку за розрахунковий період визначаємо по формі, приведеної в таблиці 2.3.

Таблиця 2.3. Розрахунок вартісної оцінки результатів

Найменування показника	Позначення	Розрахунок виробничого періоду				Всього
		1-й	2-й	3-й	4-й	
Обсяг продажів, шт.	$А_i$	1000	2500	4500	1000	9000
Ціна реалізації, грн.	$Ц_{рі}$	4 802,92	4 183,78	3 805,49	3 805,49	16 597,68
Вартісна оцінка результатів, грн.	$А_i * Ц_{рі}$	4 802 920	10 459 450	17 124 705	3 805 490	36 192 565
Коефіцієнт, що враховує фактор часу	α_i	0,98	0,86	0,74	0,67	3,25
Вартісна оцінка результатів з урахування фактора часу, грн.	$А_i * Ц_{рі} * \alpha_i$	4 706 861,6	8 995 127	12 672 281,7	2 549 678,3	28 923 948,6

Виробництво дає змогу одержати дохід за 4 роки 28 923 948 грн.

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Охорона праці та техніки безпеки — один із найважливіших аспектів будь-якого технічного проєкту, особливо коли мова йде про розробку систем контролю та моніторингу доступу, таких як «Розробка системи моніторингу та контролю доступу до офісу на основі RFID». Під час проєктування, моделювання та тестування такої системи необхідно враховувати усі вимоги безпеки праці, які забезпечують здоров'я, комфорт і безпечне середовище для розробника або оператора.

3.1 Робоче приміщення та мікроклімат

Організація безпечного і комфортного робочого місця для реалізації проєкту «Розробка системи моніторингу та контролю доступу до офісу на основі RFID» є важливим компонентом охорони праці та техніки безпеки. Від якості мікроклімату, освітлення та ергономіки безпосередньо залежить ефективність роботи, а також зниження ризиків для здоров'я виконавця.

Робоче приміщення розміщене в окремому технічному кабінеті загальною площею не менше 6 м². Висота стелі становить 3 метри, що забезпечує об'єм повітря щонайменше 18 м³ на одну особу, але з урахуванням вентиляції та природного припливу повітря цей показник доведений до понад 20 м³, що відповідає вимогам ДСанПіН 3.3.6.042-99 щодо допустимого мікроклімату в робочих приміщеннях. Стіни приміщення пофарбовані в світло-сірий матовий колір, стеля — біла, підлога — лінолеум світлого кольору з антистатичним покриттям (рис. 3.1).

Важливу роль відіграє правильна організація робочого місця, а також зручне розташування інструментів і комп'ютера. Робоче місце обладнане меблями з регульованою висотою, що дозволяє мінімізувати навантаження під час тривалого перебування при макетуванні електронної схеми.

Рисунок 3.1. Приклад пофарбованого приміщення

Такий інтер’єр сприяє зниженню втомлюваності очей і збереженню нейтрального фону для роботи з електронними приладами.

Для підтримання комфортного стану робочого простору температурний режим утримується в межах +20…+24°C, що забезпечується за допомогою системи електричного опалення взимку та вентилятора/кондиціонера влітку. Вологість повітря підтримується в межах 40–60%, що є оптимальним для тривалого перебування людини та стабільної роботи електроніки.

Температура, вологість та швидкість руху повітря контролюються за допомогою настінного гігрометра-термометра, який розміщено у зоні постійної присутності виконавця.

Режим підтримання температури та вологість протягом доби показано на таблиці 3.1.

Таблиця 3.1. Температурно-вологісний режим протягом доби

Час доби	Температура повітря (°C)	Вологість повітря (%)	Швидкість руху повітря (м/с)
00:00 - 03:00	21	50	0,05
03:00 - 06:00	20	52	0,04
06:00 - 09:00	21	53	0,06
09:00 - 12:00	22	55	0,10
12:00 - 15:00	24	48	0,15
15:00 - 18:00	23	46	0,12
18:00 - 21:00	22	50	0,08
21:00 - 00:00	21	55	0,05

Значення температури та вологості відповідають нормативам ДСанПіН 3.3.6.042-99 для приміщень з роботою з електронним обладнанням.

3.2 Вентиляція та освітлення

Приміщення оснащено природною витяжною вентиляцією у вигляді повітряного каналу з решіткою вгорі стіни. Також передбачено можливість провітрювання через вікно, яке відкривається на провітрювану сторону будівлі.

Рисунок 3.2. Приклад використання вентиляції

Приміщення має вікно площею 1 м², розташоване з південного боку, що забезпечує природне освітлення протягом дня. Світлопропускна здатність скла — не менше 50%, що відповідає нормативам ДБН В.2.5-28:2018.

Для вечірньої та хмарної погоди передбачено штучне освітлення — це настільний LED-світильник потужністю 12 Вт з нейтральним білим світлом (4000K), а також стельовий світлодіодний світильник яскравістю не менше 500 лм, що забезпечує освітлення на рівні 400-500 лк на поверхні столу.

Освітлення в приміщенні регулюється залежно від часу доби. Вдень використовується природне світло з частковим або повним додатковим штучним освітленням, що забезпечує рівень 400–600 лк. Увечері та вночі, при відсутності природного освітлення, вмикається штучне світло, підтримуючи комфортний рівень 200–500 лк для безпечної роботи.

Для роботи системи контролю доступу рекомендовано підтримувати стабільний рівень освітлення не менше 400 лк для комфортного обслуговування мікрофонів, зчитувачів та дисплеїв.

3.3 Рівень шуму в робочому приміщенні

Робоче приміщення спроєктовано з урахуванням зниження шумового навантаження. Стіни мають базову звукоізоляцію, вікна — з подвійним склом, що зменшує проникнення зовнішніх звуків. Уся техніка, зокрема Arduino, працює безшумно, а сигнали від бузера короткочасні (до 65 дБ). Протягом дня рівень шуму залишається в межах 40–55 дБ, що відповідає нормам ДСанПіН і не викликає дискомфорту чи втоми.

Рівень шуму в робочому приміщенні протягом доби коливається в межах 30–55 дБ. Найвищі показники спостерігаються у години пік роботи обладнання (до 55 дБ), тоді як у нічний час рівень знижується до 30–35 дБ, що забезпечує комфортні умови для чергування або відпочинку систем.

3.4 Електробезпека та пожежна безпека в приміщенні

У приміщенні передбачено трьохконтактні розетки із заземленням, а також індивідуальний автоматичний вимикач, розташований у доступному місці. Усі блоки живлення системи проходять через мережевий фільтр з функцією відключення при перенапрузі. Для підключення пристроїв використовуються сертифіковані USB-кабелі та блоки живлення з захистом від короткого замикання. Для уникнення перегріву обладнання забезпечується належна вентиляція в зоні встановлення електроніки. Провідники розташовуються так, щоб уникнути натягу, зламів і перетину з джерелами тепла та встановлено таблички з попередженнями про напругу.

У робочому приміщенні забезпечено належний рівень пожежної безпеки відповідно до діючих норм. Усі використовувані матеріали, зокрема покриття підлоги, мають антистатичні та важкогорючі властивості, що знижує ризик загоряння. Електричне обладнання підключене через автоматичні вимикачі та мережеві фільтри з захистом від перенапруги, що запобігає коротким замиканням та перегріванню мережі.

У приміщенні встановлено вуглекислотний вогнегасник, розміщений у легкодоступному місці, а також наявні інструкції з пожежної безпеки та план евакуації. Робоча зона організована таким чином, щоб забезпечити вільний прохід до евакуаційного виходу. Завдяки цим заходам створено умови для безпечної експлуатації обладнання та мінімізації ризику виникнення пожежонебезпечних ситуацій.

У проєкті дотримано вимоги безпеки: забезпечено електрозахист, пожежну безпеку, оптимальний мікроклімат, природну вентиляцію та контроль рівня шуму. Усі умови відповідають чинним нормам для комфортної та безпечної роботи.

ВИСНОВКИ

У роботі здійснено всебічний аналіз сучасних технологій контролю доступу, серед яких особливу увагу приділено RFID-рішенням. Було порівняно кілька типів систем і на основі критеріїв ефективності, вартості, зручності реалізації та безпеки — обґрунтовано вибір RFID як основної технології для побудови системи контролю доступу.

Детально розглянуто апаратну складову системи: RFID-модуль RC522, контролер Arduino Mega 2560, сервопривід SG90, а також допоміжні елементи, такі як LCD-дисплей, звуковий сигналізатор, SD-карта, RGB-світлодіод і матрична клавіатура. Наведено технічні характеристики, принципи роботи, приклади застосування та можливі альтернативи.

Сформовано загальну архітектуру системи, логіку її роботи та сценарії взаємодії з користувачем, включаючи обробку успішної ідентифікації, відмову у доступі, блокування після кількох невдалих спроб. Програмну частину реалізовано мовою C++ з використанням відповідних бібліотек для керування кожним компонентом на віртуальній платформі Wokwi.

Окремий розділ присвячено економічній оцінці проєкту: визначено вартість обладнання, витрати на реалізацію та обґрунтовано доцільність використання компонентів з точки зору співвідношення «ціна-якість».

У контексті охорони праці проаналізовано умови організації робочого місця, рівень освітлення, вентиляцію, мікроклімат, шумове навантаження. Враховано вимоги до електробезпеки та пожежної безпеки — застосовано засоби захисту, сертифіковані кабелі, заземлення. Завдяки цьому забезпечено безпечну експлуатацію системи в реальному офісному середовищі.

У підсумку реалізована система контролю доступу є недорогим, функціональним і гнучким рішенням, що поєднує сучасні технології з високим рівнем безпеки та простотою використання.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Савчук О. С. Мікроконтролери Arduino в системах автоматизації: навч. посіб. – Київ: Ліра-К, 2021. – 256 с.
2. Шевченко І. В. Системи контролю доступу та ідентифікації користувачів: навч. посіб. – Харків: ХНУРЕ, 2020. – 288 с.
3. Романюк Т. І. RFID технології в безпеці об'єктів: монографія – Львів: ЛНУ імені І. Франка, 2022. – 214 с.
4. Войтенко М. М. Автоматизовані системи безпеки на базі Arduino: навч. посіб. – Одеса: ОНПУ, 2023. – 304 с.
5. Поліщук О. І. Автоматизовані системи управління і контролю вбудованими засобами – Запоріжжя: ЗНТУ, 2022. – 290 с.
6. Білик Ю. О. Мікропроцесорна техніка: Arduino, Raspberry Pi, STM – Київ: НТУУ «КПІ», 2020. – 312 с.
7. Ткаченко С. Л. Інтелектуальні системи моніторингу доступу: навч. посібник – Дніпро: ДНУ, 2021. – 274 с.
8. Кириленко П. В. Сенсорні технології та RFID у розумному середовищі – Харків: ХНАДУ, 2019. – 298 с.
9. Литвиненко С. М. Безконтактні технології ідентифікації: RFID, NFC, біометрія – Київ: Академвидав, 2023. – 248 с.
10. Гаврилюк Н. С. Інтернет речей з використанням Arduino: навчальний посібник – Тернопіль: ТНТУ, 2022. – 260 с.
11. Дяченко А. І. Основи побудови систем доступу з використанням мікроконтролерів – Чернівці: ЧНУ, 2023. – 310 с.
12. Яковенко М. С. Проєктування цифрових систем керування доступом – Вінниця: ВНТУ, 2021. – 232 с.
13. Wokwi. Онлайн-симулятор Arduino для моделювання систем доступу – [Електронний ресурс]. – Режим доступу: https://wokwi.com.

ДОДАТОК А. Програмні коди для системи пристрою

```
#include <Keypad.h>              // Бібліотека для роботи з матричною клавіатурою
#include <SPI.h>                 // Бібліотека для SPI-зв'язку (потрібна для RFID і SD)
#include <MFRC522.h>             // Бібліотека для RFID-модуля RC522
#include <Servo.h>               // Бібліотека для роботи з сервоприводом
#include <LiquidCrystal_I2C.h>   // Бібліотека для LCD-дисплея через I2C
#include <SD.h>                  // Бібліотека для SD-карти

// Ініціалізація LCD-дисплея (адреса 0x27, 16 символів на 2 рядки)
LiquidCrystal_I2C lcd(0x27, 16, 2);

// Піни для підключення RFID RC522
#define SS_PIN 53
#define RST_PIN 5
MFRC522 mfrc522(SS_PIN, RST_PIN); // Створення об'єкта RFID

// SD-карта (пін CS)
#define SD_CS 10
File logFile; // Об'єкт для роботи з файлом на SD-карті

// Список авторизованих UID-карток та PIN-кодів
String validUIDs[] = {"12AB74", "DB0582"};
String pins[] = {"12AB74", "DB0582"};

// Піни для RGB-світлодіода, бузера і сервопривода
int ledRed = 3;
int ledGreen = 6;
int ledBlue = 7;
int buzzer = 4;
int servoPin = 8;
Servo myServo; // Об'єкт для керування сервоприводом
```

```
// Піни для клавіатури
byte rowPins[4] = {22, 23, 24, 25};
byte colPins[4] = {26, 27, 28, 29};
// Карта клавіш (4x4)
char keymap[4][4] =
{
{'1','2','3','A'},
{'4','5','6','B'},
{'7','8','9','C'},
{'*','0','#','D'}
};

// Ініціалізація об'єкта клавіатури
Keypad keypad = Keypad(makeKeymap(keymap), rowPins, colPins, 4, 4);

// Функція керування кольором RGB-світлодіода
void RGBWrite(int r, int g, int b)
{
analogWrite(ledRed, r);
analogWrite(ledGreen, g);
analogWrite(ledBlue, b);
}

// Змінні для логіки блокування
int failedAttempts = 0;
bool isLocked = false;
unsigned long lockStart = 0;
const unsigned long lockDuration = 32000;  // Тривалість блокування — 32 секунди

// Функція показу стартового повідомлення
void ShowIdleScreen()
{
```

```
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("  Scan card or  ");
lcd.setCursor(0, 1);
lcd.print("Press '#' to PIN");
}

// Функція запису подій у файл журналу
void logEvent(String source, String value, String status)
{
String timestamp = String(millis() / 1000); // Мітка часу в секундах
String entry = timestamp + " | " + source + ": " + value + " | " + status;
Serial.println(entry);     // Вивід у серійний монітор
if (logFile)
{
logFile.println(entry);  // Запис у файл
logFile.flush();         // Одразу зберегти зміни
}
}

// Функція блокування системи
void lockSystem()
{
lockStart = millis();
isLocked = true;
logEvent("Система", "Закрито", "Доступ закрито на 30 секунд...");
lcd.clear();
lcd.setCursor(0, 0);
lcd.print(" SYSTEM LOCKED ");
RGBWrite(0, 0, 0);
tone(buzzer, 1500); // Звук блокування
delay(1000);
```

```
noTone(buzzer);
}

void setup() //  ініціалізація пристроїв: RFID, дисплея, SD-карти, сервопривода, RGB-світлодіода
{
Serial.begin(9600);
SPI.begin();           // Старт SPI-зв'язку
mfrc522.PCD_Init();    // Ініціалізація RFID

// Налаштування виходів
pinMode(ledRed, OUTPUT);
pinMode(ledGreen, OUTPUT);
pinMode(ledBlue, OUTPUT);
pinMode(buzzer, OUTPUT);

// Підключення сервопривода
myServo.attach(servoPin);
myServo.write(0); // Початкова позиція

// Ініціалізація LCD
lcd.init();
lcd.backlight();
ShowIdleScreen();

RGBWrite(0, 0, 255); // Синє світло на старті
Serial.println("Прикладіть картку або натисніть '#' для введення PIN-коду");

// Ініціалізація SD-карти
if (!SD.begin(SD_CS))
{
Serial.println("Помилка ініціалізації SD-карти!");
```

```
}
else
{
logFile = SD.open("log.txt", FILE_WRITE);
if (logFile)
{
logFile.println("--- Нова сесія ---");
logFile.flush();
}
}
}

void loop() // Дії системи доступу та блокування
{
if (isLocked)
{
// Обробка режиму блокування
unsigned long elapsed = millis() - lockStart;
if (elapsed >= lockDuration)
{
isLocked = false;
failedAttempts = 0;
ShowIdleScreen();
RGBWrite(0, 0, 255);
}
else
{
// Відлік часу блокування
int remaining = (lockDuration - elapsed) / 1000;
lcd.setCursor(0, 0);
lcd.print(" SYSTEM LOCKED ");
lcd.setCursor(0, 1);
```

```
lcd.print("  Wait: ");
lcd.print(remaining);
lcd.print(" sec ");

// Блимання RGB під час блокування
static int colorState = 0;
static unsigned long lastBlink = 0;
if (millis() - lastBlink > 300)
{
lastBlink = millis();
colorState = (colorState + 1) % 3;
if (colorState == 0) RGBWrite(255, 0, 0);
if (colorState == 1) RGBWrite(0, 255, 0);
if (colorState == 2) RGBWrite(0, 0, 255);
}
delay(20);
}
return;
}

// Введення PIN-коду
if (keypad.getKey() == '#')
{
String pin = "";
char key;
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("   Enter PIN:   ");
Serial.print("Введіть PIN: ");

while (true)
{
```

```
key = keypad.getKey();
if (isLocked) return;
if (key)
{
if (key == '#') break;

if (key == '*')
{
pin = "";
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("   Enter PIN:   ");
lcd.setCursor(0, 1);
lcd.print("                ");
lcd.setCursor(0, 1);
Serial.println("\nPIN скинуто");
Serial.print("Введіть PIN: ");
continue;
}

if (pin.length() < 15)
{
pin += key;
Serial.print("*");
int index = pin.length() - 1;
int col = index % 16;
int row = index / 16;
lcd.setCursor(col, row + 1);
lcd.print("*");
}
}
}
```

```
// Перевірка PIN-коду
Serial.println();
for (String validPin : pins)
{
if (pin == validPin) // Вірний PIN-код
{
logEvent("PIN", pin, "Доступ надано");
accessGranted();
failedAttempts = 0;
return;
}
}

// Невірний PIN-код
logEvent("PIN", pin, "Доступ заборонено");
failedAttempts++;
(failedAttempts >= 3) ? lockSystem() : accessDenied();
return;
}

// Зчитування RFID-картки
if (!mfrc522.PICC_IsNewCardPresent() || !mfrc522.PICC_ReadCardSerial()) return;

String uid = "";
for (byte i = 0; i < mfrc522.uid.size; i++)
{
if (mfrc522.uid.uidByte[i] < 0x10) uid += "0";
uid += String(mfrc522.uid.uidByte[i], HEX);
}
uid.toUpperCase();
Serial.print("UID: ");
Serial.println(uid);
```

```
// Перевірка UID
for (String valid : validUIDs)
{
if (uid == valid)
{
logEvent("RFID", uid, "Доступ надано");
accessGranted();
failedAttempts = 0;
mfrc522.PICC_HaltA();
mfrc522.PCD_StopCrypto1();
return;
}
}

// Невірний UID
logEvent("RFID", uid, "Доступ заборонено");
failedAttempts++;
(failedAttempts >= 3) ? lockSystem() : accessDenied();
mfrc522.PICC_HaltA();
mfrc522.PCD_StopCrypto1();
}

// Доступ надано — відкриття замка
void accessGranted()
{
lcd.clear();
lcd.setCursor(0, 0);
lcd.print(" Access Granted ");
RGBWrite(0, 255, 0);
tone(buzzer, 1000);
delay(200);
noTone(buzzer);
```

```
myServo.write(90);    // Відкрити замок

// Таймер відкриття 5 секунд
for (int i = 5; i > 0; i--)
{
lcd.setCursor(0, 1);
lcd.print("  Open: ");
lcd.print(i);
lcd.print(" sec ");
delay(1000);
}

myServo.write(0);     // Закрити замок
RGBWrite(0, 0, 255);
ShowIdleScreen();
}

// Доступ заборонено — сигналізація
void accessDenied()
{
lcd.clear();
lcd.setCursor(0, 0);
lcd.print(" Access Denied ");
RGBWrite(255, 0, 0);
for (int i = 0; i < 2; i++)
{
tone(buzzer, 800);
delay(200);
noTone(buzzer);
delay(200);
}
RGBWrite(0, 0, 255);
ShowIdleScreen();
}
```

ДОДАТОК Б. Слайди мультимедійної презентації

ДИПЛОМНА РОБОТА

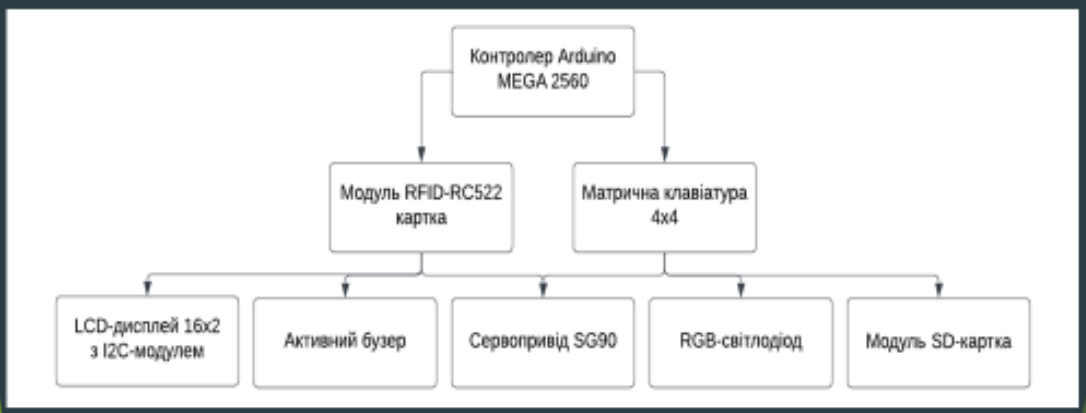
На тему:

«Розробка системи моніторингу та контролю доступу до офісу на основі RFID»

Виконав студент:
Бароліс Олександр

Група: 4КБ-02

Блок-схема компонентів системи пристрою



Блок-схема алгоритму роботи системи пристрою

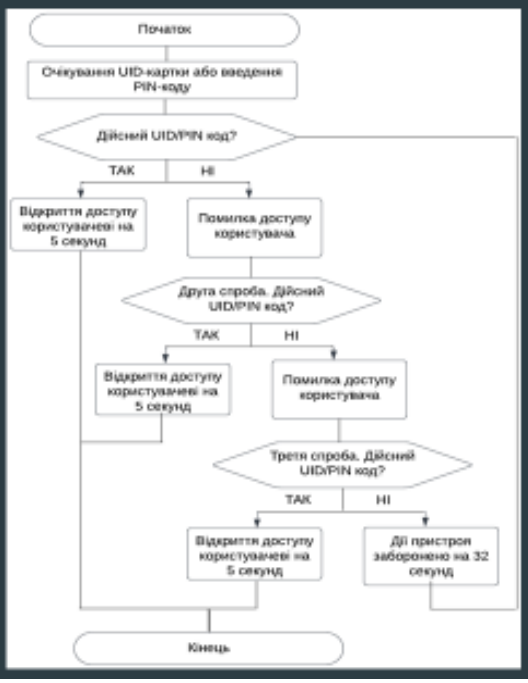


Схема дії структури системи

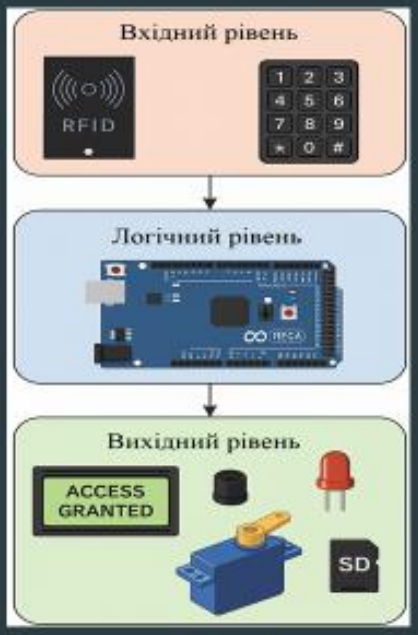
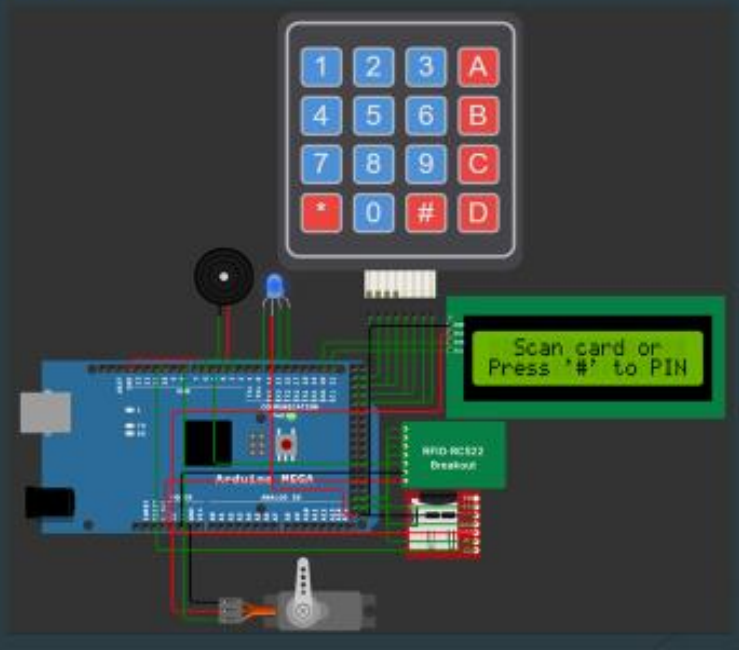
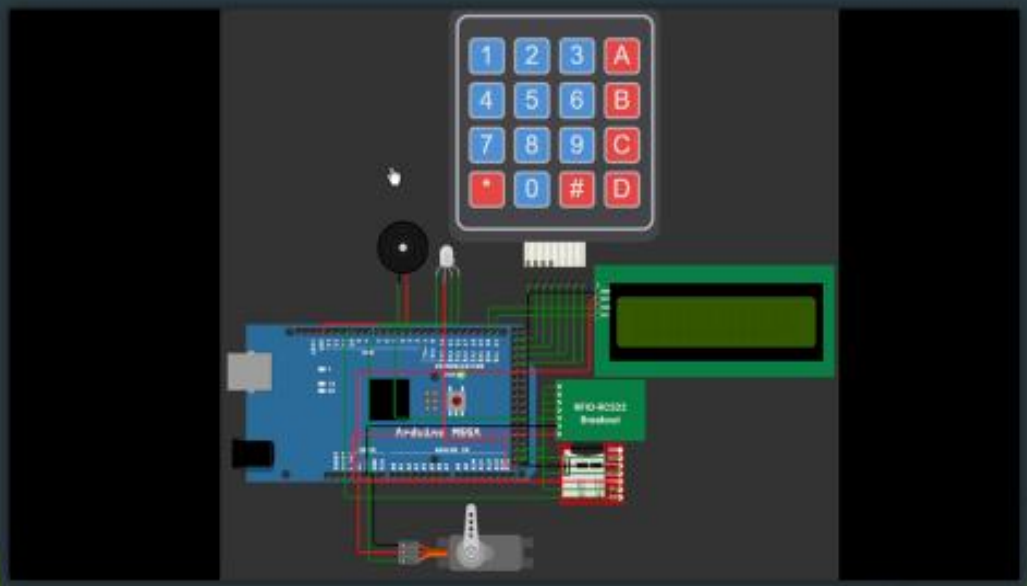


Схема проекта

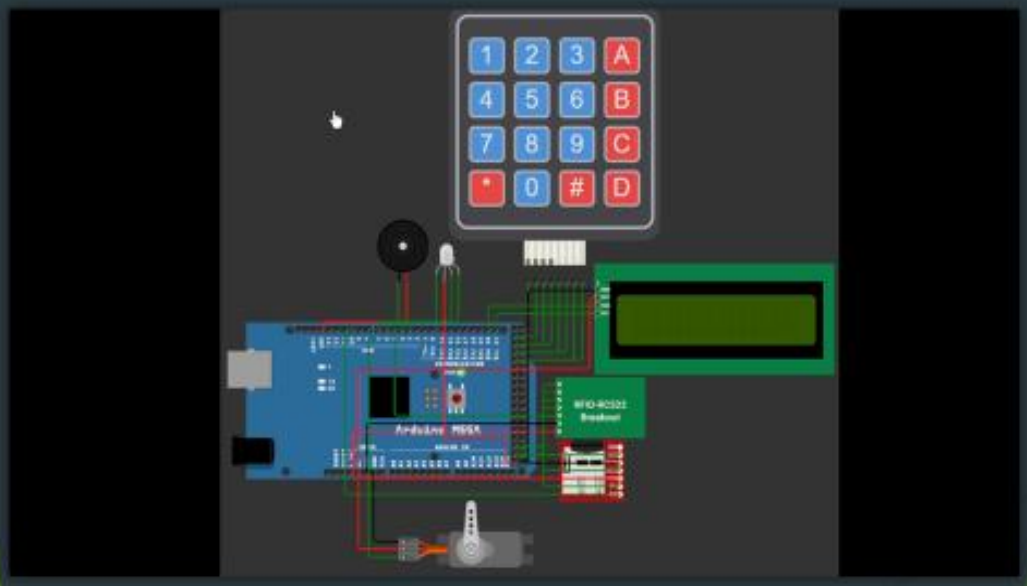
Перший сценарій: Стан очікування дій користувача.



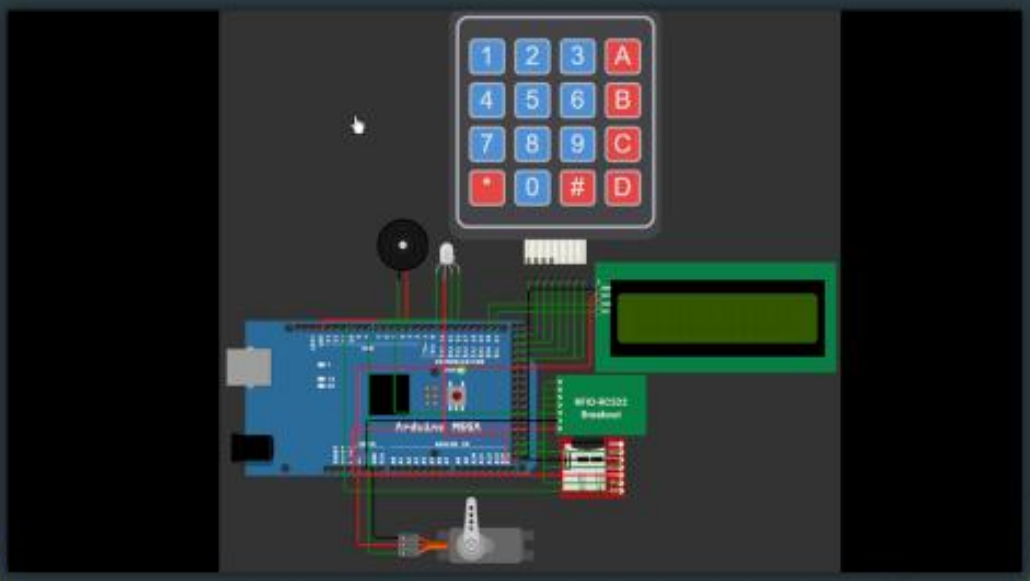
Другий сценарій: Доступ надано.



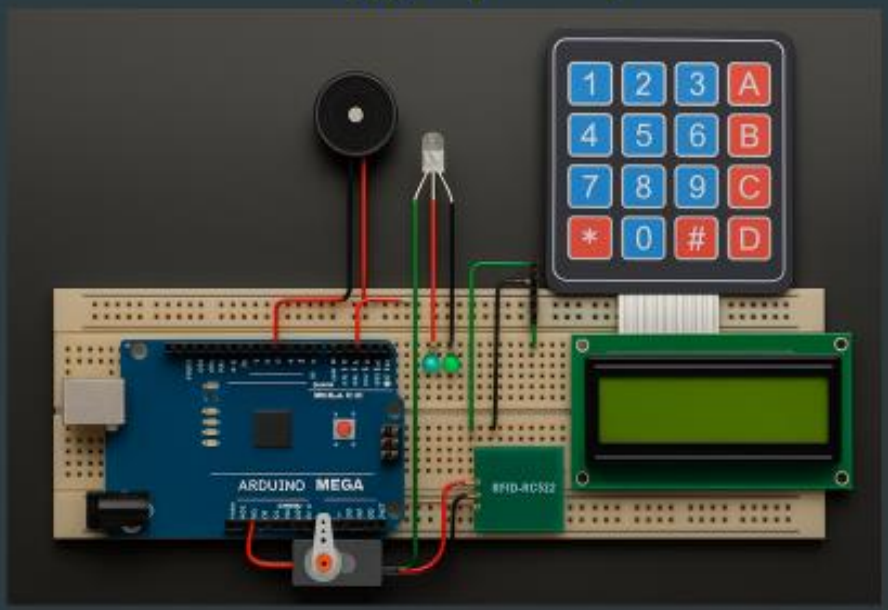
Третій сценарій: Доступ відказано.



Четвертий сценарій: Блокування системи.



Приклад зовнішнього вигляду пристрою



Використання бібліотек та авторизованих людей

```
#include <Keypad.h>                 // Бібліотека для роботи з матричною клавіатурою
#include <SPI.h>                    // Бібліотека для SPI-зв'язку (потрібна для RFID і SD)
#include <MFRC522.h>                // Бібліотека для RFID-модуля RC522
#include <Servo.h>                  // Бібліотека для роботи з сервоприводом
#include <LiquidCrystal_I2C.h>      // Бібліотека для LCD-дисплея через I2C
#include <SD.h>                     // Бібліотека для SD-карти
```

```
// Список авторизованих UID-карток та PIN-кодів
String validUIDs[] = {"12AB74", "DB0582"};
String pins[] = {"12AB74", "DB0582"};
```

Перевірка пристрою на пароль PIN-кода користувача

```
// Перевірка PIN-коду
Serial.println();
for (String validPin : pins)
{
  if (pin == validPin) // Вірний PIN-код
  {
    logEvent("PIN", pin, "Доступ надано");
    accessGranted();
    failedAttempts = 0;
    return;
  }
}

// Невірний PIN-код
logEvent("PIN", pin, "Доступ заборонено");
failedAttempts++;
(failedAttempts >= 3) ? lockSystem() : accessDenied();
return;
}
```

Перевірка пристрою на пароль UID-кода користувача

```
  // Перевірка UID
  for (String valid : validUIDs)
  {
    if (uid == valid)
    {
      logEvent("RFID", uid, "Доступ надано");
      accessGranted();
      failedAttempts = 0;
      mfrc522.PICC_HaltA();
      mfrc522.PCD_StopCrypto1();
      return;
    }
  }

  // Невірний UID
  logEvent("RFID", uid, "Доступ заборонено");
  failedAttempts++;
  (failedAttempts >= 3) ? lockSystem() : accessDenied();
  mfrc522.PICC_HaltA();
  mfrc522.PCD_StopCrypto1();
}
```

Надання доступу при правильному вводі пароля або UID-картки

```
// Доступ надано — відкриття замка
void accessGranted()
{
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(" Access Granted ");
  RGBWrite(0, 255, 0);
  tone(buzzer, 1000);
  delay(200);
  noTone(buzzer);
  myServo.write(90);     // Відкрити замок

  // Таймер відкриття 5 секунд
  for (int i = 5; i > 0; i--)
  {
    lcd.setCursor(0, 1);
    lcd.print("  Open: ");
    lcd.print(i);
    lcd.print(" sec ");
    delay(1000);
  }

  myServo.write(0);      // Закрити замок
  RGBWrite(0, 0, 255);
  ShowIdleScreen();
}
```

Заборона доступу при неправильному вводі пароля або UID-картки

```
// Доступ заборонено — сигналізація
void accessDenied()
{
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(" Access Denied ");
  RGBWrite(255, 0, 0);
  for (int i = 0; i < 2; i++)
  {
    tone(buzzer, 800);
    delay(200);
    noTone(buzzer);
    delay(200);
  }
  RGBWrite(0, 0, 255);
  ShowIdleScreen();
}
```

Блокування системи при неправильному вводі пароля або UID-картки 3 рази поспіль

```
// Змінні для логіки блокування
int failedAttempts = 0;
bool isLocked = false;
unsigned long lockStart = 0;
const unsigned long lockDuration = 32000;  // Тривалість блокування — 32 секунди
```

```
void loop() // Дії системи доступу та блокування
{
  if (isLocked)
  {
    // Обробка режиму блокування
    unsigned long elapsed = millis() - lockStart;
    if (elapsed >= lockDuration)
    {
      isLocked = false;
      failedAttempts = 0;
      ShowIdleScreen();
      RGBWrite(0, 0, 255);
    }
    else
    {
      // Відлік часу блокування
      int remaining = (lockDuration - elapsed) / 1000;
      lcd.setCursor(0, 0);
      lcd.print(" SYSTEM LOCKED ");
      lcd.setCursor(0, 1);
      lcd.print("  Wait: ");
      lcd.print(remaining);
      lcd.print(" sec ");
```

```
      // Блимання RGB під час блокування
      static int colorState = 0;
      static unsigned long lastBlink = 0;
      if (millis() - lastBlink > 300)
      {
        lastBlink = millis();
        colorState = (colorState + 1) % 3;
        if (colorState == 0) RGBWrite(255, 0, 0);
        if (colorState == 1) RGBWrite(0, 255, 0);
        if (colorState == 2) RGBWrite(0, 0, 255);
      }
      delay(20);
    }
    return;
  }
```

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Бароліса Олександра Юрійовича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Безпека комп'ютерних систем і мереж»*

Керівник дипломного проекту (роботи) *Кільдішев Віталій Йосипович*

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) *Система моніторінгу та контролю доступу до офісу на основі RFID-технологій з використанням Arduino*

Обсяг розрахунково-пояснювальної записки *84* сторінок

Обсяг графічної (презентаційної) частини *16* аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту завданню

Представлений дипломний проєкт відповідає затвердженій темі та виконаний відповідно технічному завданню. Дипломний проект присвячений моніторінгу та контролю доступу до офісу на основі RFID-технологій з використанням Arduino і складається з пояснювальної записки та мультимедійної презентації з відповідними схемами.

б) характеристика виконання кожного розділу дипломного проекту

Пояснювальна записка складається з основного розділу, економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту

Графічна частина складається з 16 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять структурні, принципові та функціональні схеми, структурні моделі, блок-схеми алгоритмів, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм. Якість виконання пояснювальної записки відмінна, розробку виконано у повному обсязі.

г) перелік позитивних якостей дипломного проекту

Чітка модульна архітектура: окремі блоки «зчитування RFID», «обробка PIN», «керування серво/бузером», «індикація» і «логування» спрощують підтримку та подальше розширення системи. Повний цикл розробки: від аналізу технологій RFID і порівняння з біометрією та NFC до докладної економічної оцінки та заходів з охорони праці.

д) основні недоліки дипломного проекту

Жорстко вшиті списки UID-карток і PIN-кодів у коді без механізму оновлення або захищеного зберігання. Використання численних delay() для звукових сигналів та роботи серво заблоковує головний цикл і не дозволяє оперативно реагувати на інші події. RC522 із стандартом MIFARE Classic працює без криптографії, отже система уразлива до клонування карток.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові рецензента *к.т.н. Шибаєва Наталя Олегівна*

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

Підпис:

« 23 » 06 2025 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проєкт здобувача освіти

відділення комп'ютерних систем

Бароліса Олександра Юрійовича

(прізвище, ім`я та по батькові здобувача/здобувачки освіти)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Безпека комп'ютерних систем і мереж»*

Тема дипломного проєкту: *«Розробка системи моніторингу та контролю доступу до офісу на основі RFID»*

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проєкту (графічного матеріалу і розрахунково-пояснювальної записки) Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проєкту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проєкті. Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над проєктом: Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Проведено аналіз існуючих систем моніторінгу та контролю доступу. Представлено принципи роботи систем з моніторінгу та контролю доступу. В рамках захисних заходів представлено проєктування з звуковим бузером та RGB-світлодіода. Проведено тестування та оцінка ефективності системи.

в) теоретична підготовка випускника Відповідає вимогам, що надаються здобувачу освіти зі спеціальності «Комп'ютерна інженерія»

г) вміння розв'язувати виробничі та конструкторські питання У дипломному проєкті розроблено, змодельовано та протестовано систему безпеки на базі платформи Arduino з використанням звукового бузера, LCD-дисплея та LCD-світлодіода. Система демонструє високу ефективність, стабільність функціонування та доступність для подальшої модернізації.

Оцінка розрахункової частини 5 (відмінно)

Оцінка графічної (презентаційної) частини 5 (відмінно)

Загальна оцінка 5 (відмінно)

Прізвище, ім'я, по батькові керівника роботи Кільдішев Віталій Йосипович

Місце роботи і посада керівника роботи к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

«18» червня 2025 р. _____ Кільдішев В. Й.

(підпис) (прізвище та ініціали керівника)

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
(ДИПЛОМНОГО ПРОЕКТУ)
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Бароліс Олександр Юрійович,
здобувач освіти гр. 4КБ-02, та

Кільдішев Віталій Йосипович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проєкту фахового молодшого бакалавра на тему:

«Розробка системи моніторингу та контролю доступу до офісу на основі RFID» (автор роботи – Бароліс О. Ю., керівник роботи – Кільдішев В. Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Бароліс О. Ю. /

Керівник _____ / Кільдішев В. Й. /

«16» червня 2025 р.

ДОВІДКА

циклової комісії КТ та ПІ
про допуск до захисту дипломного проєкту
здобувача (здобувачки) освіти IV курсу
відділення комп'ютерних систем групи 4КБ-02

Бароліса Олександра Юрійовича

на тему *Розробка системи моніторингу та контролю доступу до офісу на основі RFID*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до дипломного проєкту виконана з некритичними порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис) *18.06.2025* (дата) *Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 17.06.2025 р. значення коефіцієнту подібності в роботі становить 9,85%, коефіцієнт цитування – 1,70%.*

(підпис) *18.06.2025* (дата) *Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) дипломного проєкту

здобувача (здобувачки) освіти *Бароліса О.Ю.* (П.І.Б.)

проведена « *18* » *червня* 2025 р.

Висновки *Пояснювальна записка до дипломного проєкту виконана у повному обсязі. Випускна кваліфікаційна робота (дипломний проєкт) відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Голова ЦК КТ та ПІ (підпис) *Кривченко Ю.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 6/17/2025
Дата редагування 6/17/2025

Документ прийнятий

Звіт подібності

метадані

Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Розробка системи моніторингу та контролю доступу до офісу на основі RFID

Автор
Бароліс Олександр Юрійович
Науковий керівник / Експерт
Кільдішев Віталій Йосипович

підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

КЦ

25
Довжина фрази для коефіцієнта подібності 2

12123
Кількість слів

92192
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	23
Інтервали	A→	0
Мікропробіли	·	16
Білі знаки	ß	3
Парафрази (SmartMarks)	a	54

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз		Колір тексту
ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/server/api/core/bitstreams/c63b91ba-d04f-4715-890d-b16277695c7e/content	66 0.54 %
2	https://card-file.ontu.edu.ua/bitstreams/8999d5af-6274-44f4-ae78-d23e08048d38/download	62 0.51 %
3	https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download	52 0.43 %
4	https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download	47 0.39 %
5	https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download	43 0.35 %

6	https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download	35 0.29 %
7	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	34 0.28 %
8	https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download	33 0.27 %
9	https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download	32 0.26 %
10	https://card-file.ontu.edu.ua/bitstreams/f789da43-3034-4ad8-bf34-640a47414f93/download	32 0.26 %

з домашньої бази даних (0.40 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка системи авторизації користувача на web-сервері за допомогою nrf-модулю [redacted] 6/15/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	22 (2) 0.18 %
2	Розробка 3D-гри у жанрі survival-horror з налаштуваннями рівнів складності [redacted] 6/12/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	17 (2) 0.14 %
3	Створення web-застосунку цифрового помічника з використанням Open AI [redacted] 5/28/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	9 (1) 0.07 %

з програми обміну базами даних (0.72 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка WEB інтерфейсу для системи автоматизації макету розумного будинку [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	52 (5) 0.43 %
2	Розробка програмного забезпечення системи з кодовим доступом [redacted] 6/12/2024 National University "Zaporizhzhia Polytechnic" (Кафедра "Програмні засоби")	20 (2) 0.16 %
3	ФКНТ_2023_123м_Хлищибор_П.О [redacted] 7/11/2024 Ukrainian national aviation university (Ukrainian national aviation university)	15 (2) 0.12 %

з Інтернету (8.74 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	**https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download**	**341 (13) 2.81 %**
2	https://card-file.ontu.edu.ua/bitstreams/dfa57ac3-98fa-4c22-86e7-0549d1254d89/download	99 (16) 0.82 %
3	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/c63b91ba-d04f-4715-890d-b16277695c7e/content**	**91 (3) 0.75 %**
4	https://card-file.ontu.edu.ua/bitstreams/63ee88cb-a3d0-4005-9cf2-0cff89f28c0d/download	73 (9) 0.60 %

5	https://card-file.ontu.edu.ua/bitstreams/f789da43-3034-4ad8-bf34-640a47414f93/download	66 (4) 0.54 %
6	https://card-file.ontu.edu.ua/bitstreams/8999d5af-6274-44f4-ae78-d23e08048d38/download	62 (1) 0.51 %
7	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	60 (4) 0.49 %
8	https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download	54 (2) 0.45 %
9	https://card-file.ontu.edu.ua/bitstreams/bbaf3f38-16a8-4070-bead-5562769b7c71/download	47 (2) 0.39 %
10	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	35 (2) 0.29 %
11	https://card-file.ontu.edu.ua/server/api/core/bitstreams/21ac499a-a9e9-4137-810c-5f21a0318048/content	25 (3) 0.21 %
12	https://card-file.ontu.edu.ua/bitstreams/d170b7e7-9f64-4cae-8636-2f0a585386fa/download	24 (2) 0.20 %
13	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	22 (1) 0.18 %
14	https://forum.arduino.cc/t/change-a-stepping-value-with-4x4-keypad/480319	19 (2) 0.16 %
15	https://card-file.ontu.edu.ua/bitstreams/21173711-5b67-4b87-b17f-6302c25e7a31/download	15 (2) 0.12 %
16	https://wokwi.com/projects/381828262849664001	12 (1) 0.10 %
17	https://card-file.ontu.edu.ua/server/api/core/bitstreams/3302e08a-9549-43ba-8861-728bff7dc7ff/content	8 (1) 0.07 %
18	https://card-file.ontu.edu.ua/bitstreams/f4578adb-a317-40e4-97dd-5047e095641c/download	6 (1) 0.05 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: **«Безпека комп'ютерних систем і мереж» Група:** 4КБ- 02

Дипломний **проект здобувача освіти денної форми навчання КБ.** 02.02.000.ДП

БАРОЛІСА
ОЛЕКСАНДРА ЮРІЙОВИЧА

м. Одеса
2025 **р.**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: **«Безпека** комп'ютерних **систем і мереж** Група: 4 КБ-02

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломного проекту на тему:

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на _____ аркушах (слайдах) Дипломник _____ (Бароліса О. Ю.)
_____ Керівник _____ **(Кільдишев В. Й.) Консультанти: з** економічного розділу_____ (Канський М. Ю.)