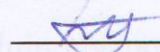


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

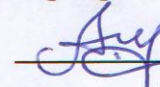
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект інтегрованої системи контролю та
управління доступом медичного закладу»

Виконала: студентка 4-го курсу групи КБ-22-2
спеціальності 125 «Кібербезпека»

 Марина НІКОЛАЄНКО

Керівник: доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

Рецензент: доцент кафедри КІ та КБ, к.т.н.

 Олександр ПІРОГ

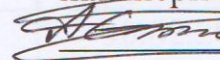
Розділ	Консультант	Закордонна адреса	Закордонна прийнята
1	Лобанчикова Н.М.	02.02.2026	02.02.2026
2	Лобанчикова Н.М.	02.02.2026	02.02.2026
3	Лобанчикова Н.М.	02.02.2026	02.02.2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
2 лютого 2026 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студентка: Ніколаєнко Марина Вікторівна

Тема роботи: «Проект інтегрованої системи контролю та управління доступом медичного закладу».

затверджена Наказом університету від 2 лютого 2026 р. № 58/с.

Термін здачі студентом закінченої роботи 8 червня 2026 р.

Вихідні дані роботи :

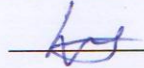
Процедури, що забезпечують контроль та управління доступом в медичному закладі, методи та інструменти для регулювання контролю та управління доступом.

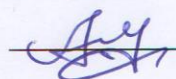
Обладнання та програмне забезпечення:

1. Мікроконтролери Wemos D1 та Arduino Nano
2. RFID-зчитувач та матрична клавіатура 4x4
3. Arduino IDE

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються.

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Лобанчикова Н.М.	02.02.2026	02.02.2026
2	Лобанчикова Н.М.	02.02.2026	02.02.2026
3	Лобанчикова Н.М.	02.02.2026	02.02.2026

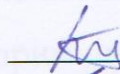
Студентка  Марина НІКОЛАЄНКО

Керівник  Олексій ШЕЛУХА

Календарний план

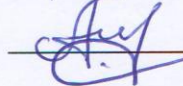
№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.02.2026	Виконано
2	Складання плану роботи	15.02.2026	Виконано
3	Аналіз літературних джерел	26.02.2026	Виконано
4	Підготовка необхідного обладнання	30.02.2026	Виконано
5	Встановлення ПЗ Arduino IDE та базове налаштування бібліотек	03.03.2026	Виконано
6	Тестування підключення зони 2 та 3 на макетній платі для прототипування	25.03.2026	Виконано
7	Монтування усіх компонентів на стенді та їх підключення	02.04.2026	Виконано
8	Написання кодової частини для Wemos D1 та Arduino Nano	04.04.2026	Виконано
9	Тестування роботи компонентів СКУД	11.04.2026	Виконано
10	Оформлення пояснювальної записки	05.05.2026	Виконано
11	Захист кваліфікаційної роботи		

Студентка



Марина НІКОЛАЄНКО

Керівник



Олексій ШЕЛУХА

ВКЖ.Б.Б.-125-10-ПЗ

ФІКТ.Гр.КБ-22-2

АНОТАЦІЯ

У кваліфікаційній роботі розроблено інтегровану систему контролю та управління доступом для медичного закладу на основі мікроконтролерів Arduino Nano та Wemos D1 mini. Визначено і проаналізовано сучасні системи безпеки, методи ідентифікації користувачів та особливості використання RFID-технологій у системах контролю та управління доступом.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаних джерел.

Текстова частина викладена на 56 сторінках друкованого тексту. Пояснювальна записка містить 2 додатки на 13 сторінках. Список використаних джерел містить 24 найменування і займає 3 сторінки. В роботі наведено 59 рисунків та 4 таблиці. Загальний обсяг роботи - 75 сторінок.

У першому розділі проаналізовано вимоги до безпеки медичних установ, методи автентифікації користувачів та особливості роботи мікроконтролерів і RFID-технологій.

В другому розділі розроблено структуру інтегрованої системи контролю доступу, виконано підбір апаратного та програмного забезпечення, а також налаштовано середовище Arduino IDE для програмування компонентів системи.

У третьому розділі описано процес підключення, налаштування та тестування компонентів стенду. Реалізовано вебінтерфейс для ІТ-відділу та двофакторну автентифікацію для доступу до приміщення, де зберігаються ліки та наркотичні речовини.

Результати виконання і тестування підтвердили стабільну та коректну роботу інтегрованої системи контролю та управління доступом.

Ключові слова: СКУД, RFID, ARDUINO NANO, WEMOS D1 MINI, МІКРОКОНТРОЛЕР, КОНТРОЛЬ ДОСТУПУ, ВЕБ-СЕРВЕР, АВТЕНТИФІКАЦІЯ, МЕДИЧНИЙ ЗАКЛАД.

					ККІК.КР.Б – 125 – 10 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект інтегрованої системи контролю та управління доступом медичного закладу	Літ.	Арк.	Аркуші
Розроб.		Ніколаєнко М.В.		08.06				
Керівник		Шелуха О.О.		08.06			4	75
Реценз.		Пірог О.В.		09.06				
Н. контр.		Шелуха О.О.		08.06				
Затверд.		Єфіменко А.А.		08.06				
						ФІКТ, Гр. КБ-22-2		

ANNOTATION

In the qualification work, an integrated access control and control system for a medical institution based on Arduino Nano and Wemos D1 mini microcontrollers was developed. Modern security systems, user identification methods and features of the use of RFID technologies in the ACS were determined and analyzed.

The qualification work consists of an introduction, three chapters, conclusions and a list of used sources.

The text part is presented on 56 pages of printed text. The explanatory note contains 2 appendices on 13 pages. The list of sources used contains 24 names and occupies 3 pages. The work contains 59 figures and 4 tables. The total volume of the work is 75 pages.

The first chapter analyzes the security requirements of medical institutions, user authentication methods, and the peculiarities of microcontrollers and RFID technologies.

In the second section, the structure of the integrated access control system was developed, the hardware and software were selected, and the Arduino IDE environment for programming system components was configured.

The third chapter describes the process of connecting, configuring and testing stand components. A website for the IT department and two-factor authentication for access to the premises where medicines and narcotic substances are stored have been implemented.

The results of execution and testing confirmed the stable and correct operation of the integrated access control and management system.

Keywords: ACS, RFID, ARDUINO NANO, WEMOS D1 MINI, MICROCONTROLLER, ACCESS CONTROL, WEB SERVER, AUTHENTICATION, MEDICAL FACILITY.

		Ніколаєнко М..В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ.....	10
1.1. Аналіз вимог до безпеки та принципів розмежування доступу в установах охорони здоров'я.....	10
1.2. Огляд характеристик мікроконтролерів та периферійних пристроїв для СКУД.....	13
1.3. Дослідження способів захисту даних та ідентифікації користувачів.....	16
1.4. Обґрунтування технічного завдання для розробки СКУД.....	19
РОЗДІЛ 2. РОЗРОБКА СТРУКТУРИ ТА ВИБІР ОБЛАДНАННЯ ДЛЯ ІНТЕГРОВАНОЇ СКУД.....	22
2.1. Аналіз загроз безпеки та побудова моделі порушника.....	22
2.2. Розробка структури інтегрованої системи контролю та управління доступом в медичному закладі.	24
2.3. Підбір апаратних засобів для створення демонстраційного стенду.	29
2.4. Базове налаштування програмного забезпечення для програмування апаратної бази стенду	35
РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ РОЗРОБЛЕНОЇ ІНТЕГРОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ТА КОНТРОЛЮ ДОСТУПУ.....	41
3.1. Налаштування на макетній платі захищеної зони СКУД.....	41
3.2. Налаштування на макетній платі зони посиленого контролю доступу.....	45
3.3. Тестування працездатності розробленого проекту інтегрованої СКУД....	50
ВИСНОВКИ.....	63
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	65
ДОДАТКИ.....	68

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

COM-порт - віртуальний порт для обміну даними з мікроконтролером

GDPR (General Data Protection Regulation) - Загальний регламент про захист даних

GPIO (General Purpose Input/Output) - входи та виходи мікроконтролера

HTML (HyperText Markup Language) - мова розмітки веб-сторінок

IDE (Integrated Development Environment) - інтегроване середовище розробки

IoT (Internet of Things) - технологія «Інтернет Речей»

NTP (Network Time Protocol) - мережевий протокол синхронізації часу

PIN-код - персональний ідентифікаційний код користувача

RFID(Radio Frequency Identification) - технологія радіочастотної ідентифікації

UDP (User Datagram Protocol) - протокол передачі даних у мережі

Wi-Fi - технологія бездротової передачі даних

БД – база даних

СКУД - система контролю та управління доступом

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасний час медичні заклади потребують хорошого рівня безпеки, оскільки саме в лікарнях зберігаються персональні дані пацієнтів, дороге обладнання, лікарські препарати та службова інформація. Через постійний потік працівників, пацієнтів і відвідувачів виникає потреба обмежувати та авторизувати їх доступ до контрольованих приміщень.

Саме тому системи контролю та управління доступом сьогодні є важливою частиною безпеки медичних установ. Використання RFID-карток, PIN-кодів, мікроконтролерів та персоналу з служби безпеки, дозволяє підвищити рівень захисту приміщень і вести журнал усіх подій у системі, за допомогою моніторингу через вебінтерфейс.

Метою кваліфікаційної роботи є розробка інтегрованої системи контролю та управління доступом медичного закладу на основі мікроконтролерів Arduino Nano та Wemos D1 mini з різними рівнями захищеності. Для досягнення поставленої мети було поставлено наступні завдання:

- провести аналіз вимог безпеки медичних закладів, та дослідити сучасні методи ідентифікації та автентифікації користувачів;
- провести аналіз та підбір апаратного та програмного забезпечення для побудови системи контролю та управління доступом;
- розробити структуру інтегрованої системи контролю та управління доступом медичного закладу;
- виконати розгортання та програмування макету системи контролю та управління доступом та провести тестування функціоналу усіх її елементів.

Об'єктом дослідження є процес функціонування інтегрованої системи контролю та управління доступом медичного закладу.

Предметом дослідження є методи та засоби проєктування, моделювання та тестування інтегрованої системи контролю та управління доступом.

В результаті виконання завдання було створено демонстраційний стенд системи контролю та управління доступом у медичному закладі. Цей стенд наочно

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

демонструє, як працює багаторівнева система безпеки приміщень, що передбачає різні методи ідентифікації користувачів.

Основою системи є мікроконтролери Wemos D1 та Arduino Nano, запрограмовані за допомогою Arduino IDE. Для наглядного прикладу двері були надруковані на 3D-принтері та встановлені разом з іншим обладнанням на дерев'яній основі. Апаратна частина включає IP-камеру, RFID-зчитувач та матричну клавіатуру.

Стенд включає чотири зони безпеки:

1. Реєстратура: Мінімальний рівень захисту, зона з камерою відеоспостереження.
2. Службове приміщення (кабінети лікарів): Середній рівень захисту, доступ за RFID-карткою.
3. Зберігання ліків: Найвищий рівень безпеки, що вимагає введення паролю та для входу підтвердження за допомогою прикладання магнітного ключа.
4. IT-відділ: Зона з інтегрованим вебінтерфейсом для моніторингу доступу в реальному часі та автоматичного ведення журналу подій.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

1.1. Аналіз вимог до безпеки та принципів розмежування доступу в установах охорони здоров'я.

Сучасні заклади охорони здоров'я являють собою об'єкти із підвищеними вимогами до організації безпеки. Це обумовлено необхідністю забезпечення збереження конфіденційної інформації, підтримання функціональності медичного обладнання та забезпечення стабільної роботи персоналу. У медичних установах щоденно спостерігається значна кількість працівників, пацієнтів та відвідувачів, що зумовлює потребу у впровадженні комплексних систем контролю та управління доступом (СКУД). Актуальність застосування зазначених систем підтверджується динамікою зростання випадків компрометації медичних даних, несанкціонованого доступу до інформаційних ресурсів та викрадення матеріальних цінностей у медичних установах. Міжнародні дослідження у сфері кібербезпеки свідчать про належність медичної галузі до числа найбільш вразливих об'єктів критичної інфраструктури.

Ключовим завданням цих систем є гарантування захисту персоналу, пацієнтів, матеріальних ресурсів та інформаційних систем від несанкціонованого доступу [1].

Особливого контролю вимагають приміщення, де розміщені наркотичні засоби, вакцини, біологічні зразки та серверне обладнання. Несанкціонований доступ до цих зон може спричинити не лише фінансові втрати, але й становити серйозну небезпеку для життя та здоров'я пацієнтів.

У сучасних умовах широко застосовуються RFID (Radio Frequency Identification), які дозволяють автоматизувати процес ідентифікації користувачів та організувати багаторівневий контроль доступу [2]. Система RFID складається з зчитувачів і електронних міток, які сприяють швидкому обміну інформацією через радіочастотний сигнал. Значною перевагою RFID-міток та карток є їх пасивна робота. Вони не є активними випромінювачами, а отримують енергію від

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

зчитувача, що робить їх абсолютно безпечними для використання у медичних закладах. Це гарантує відсутність негативного впливу на чутливе медичне обладнання та інші електронні системи.

Використання RFID у сфері охорони здоров'я дає змогу:

- контролювати доступ до службових приміщень;
- здійснювати ідентифікацію персоналу;
- фіксувати відвідування;
- забезпечувати моніторинг переміщень працівників та пацієнтів.

Крім цього, сучасні RFID-системи можуть інтегруватися із системами відеоспостереження, охоронної сигналізації та моніторингу температурних режимів. Це особливо важливо для приміщень зберігання медикаментів і вакцин, де необхідно підтримувати визначені умови зберігання препаратів.



Рисунок 1.1 - Принцип роботи RFID-системи контролю доступу

Однією з важливих вимог для розробки та впровадження сучасних СКУД є розмежування прав доступу між різними категоріями користувачів. У контексті медичних установ доступ має визначатися відповідно до посадових обов'язків працівників та рівня їх авторизації. Наприклад, адміністративний персонал може мати доступ до службових приміщень і робочих інформаційних систем, тоді як технічний персонал обмежується певними зонами обслуговування. Особливо

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

жорсткий контроль встановлюється для серверних приміщень та сховищ медикаментів, який дозволяється лише строго авторизованим співробітникам [3].

Розподіл рівнів доступу є основним елементом забезпечення інформаційної безпеки. Він базується на таких принципах, як:

- конфіденційність це запобігання несанкціонованому доступу до даних;
- цілісність це гарантія незмінності інформації;
- доступність це забезпечення оперативного отримання даних уповноваженими користувачами.

Особливу увагу приділяють на захисті персональних даних пацієнтів. У розвитку електронних систем охорони здоров'я використовуються багаторівневі механізми автентифікації, такі як двофакторний вхід, електронний цифровий підпис і моделі розподілу ролей користувачів. В Україні ці принципи реалізуються за допомогою системи eHealth, у якій доступ до медичної інформації можливий лише після проходження процесу авторизації та перевірки прав доступу.

В Україні питання захисту персональних даних регулюється Законом України «Про захист персональних даних». Цей нормативний акт визначає вимоги щодо збору, обробки, зберігання та захисту персональної інформації, а також встановлює обов'язок організацій забезпечувати належний рівень захисту даних від несанкціонованого доступу [4]. Проте, як у країнах Європейського Союзу основним нормативним документом у сфері захисту персональних даних є Загальний регламент про захист даних GDPR - General Data Protection Regulation. Він встановлює більш жорсткі вимоги до обробки персональної інформації, передбачає обов'язкове впровадження технічних і організаційних заходів безпеки, а також посилює відповідальність за порушення конфіденційності даних [5].

Окрім інформаційної безпеки, важливим є й фізичний контроль доступу до приміщень. Традиційні механічні ключі мають низку недоліків, пов'язаних із ризиком копіювання, втрати або несанкціонованого використання. У зв'язку з цим сучасні СКУД базуються на використанні RFID-карток, PIN-кодів, біометричних технологій або їх комбінованих варіантів.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Для забезпечення ефективного рівня захисту система контролю доступу повинна виконувати такі функції:

- ідентифікація користувача;
- автентифікація;
- авторизація доступу;
- ведення журналу подій;
- моніторинг спроб несанкціонованого проникнення;
- резервне збереження інформації;
- дистанційне адміністрування.

Також для сучасних СКУД важливим компонентом є ведення журналів подій та облік візитів. Ці функціональні можливості забезпечують фіксацію часу входу та виходу користувачів, сприяють контролю переміщень персоналу й створюють умови для ретельного аналізу інцидентів, пов'язаних із безпекою. Крім основних функцій, сучасні СКУД дозволяють керувати ними віддалено та швидко реагувати на аварії. Завдяки цьому можна оперативно блокувати доступ, відстежувати спроби вторгнення та спостерігати за роботою системи у реальному часі.

Однак важливою проблемою залишається забезпечення сталого функціонування системи безпеки при виникненні аварійних ситуацій або технічних збоїв обладнання. Для цього широко застосовуються резервні джерела електроживлення, резервні бази даних та процедури резервного копіювання, що знижують ризики втрати критичної інформації [7-8].

1.2. Огляд характеристик мікроконтролерів та периферійних пристроїв для СКУД.

Система контролю та управління доступом - це інтегрований комплекс технічних і програмних рішень, основною метою якого є ідентифікація користувачів, обмеження доступу до визначених зон і фіксація подій [16]. Центральна роль у функціонуванні таких систем належить мікроконтролерам та периферійним

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

пристроєм, які забезпечують взаємодію між користувачем та складною системою безпеки [9].

Мікроконтролер - інтегрований обчислювальний пристрій, який в своєму корпусі поєднує головний процесор, оперативну пам'ять і набір інтерфейсів для вводу та виводу даних. Завдяки низькому рівню енергоспоживання та можливості програмного управління різними компонентами, ці пристрої стали невід'ємною складовою сучасних автоматизованих систем [12].

Типовими прикладами мікроконтролерів є:

STM32 - високопродуктивний 32-бітний мікроконтролер із великою кількістю периферійних інтерфейсів та значним обсягом пам'яті. Перевагами STM32 є висока швидкодія, підтримка багатозадачності та можливість роботи зі складними алгоритмами шифрування і мережевими протоколами. Недоліком є складність програмування та необхідність використання спеціалізованих середовищ розробки. Такі контролери широко застосовуються у промислових СКУД та системах із підвищеними вимогами до надійності [17].

AVR - потужний 8-бітний чіп з високими характеристиками, що включають 256 КБ пам'яті Flash, 8 КБ SRAM і 54 цифрові контакти. Основними перевагами є простота програмування, доступність та низьке енергоспоживання. Недоліками є обмежена продуктивність і менший обсяг оперативної пам'яті у порівнянні з сучасними 32-бітними рішеннями [21].

ESP8266 - компактна і дуже швидка 32-бітна плата, що має великий об'єм пам'яті 4 МБ. Його головною перевагою є підтримка бездротового зв'язку та можливість реалізації віддаленого моніторингу системи. Недоліком є обмежена кількість GPIO-портів та підвищене енергоспоживання під час передачі даних через Wi-Fi [10].

Arduino Uno - класична, надійна і легка у використанні 8-бітна плата, ідеальна для навчання та створення макетів. Перевагами є простота програмування, велика кількість готових бібліотек і стабільна робота. До недоліків належать обмежена продуктивність і порівняно великі фізичні розміри плати [22].

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Arduino Nano - зменшена копія Arduino Uno, має такі ж самі характеристики.

Основною перевагою є малі габарити, що дозволяє використовувати плату у компактних пристроях. Недоліком є менша зручність підключення через обмежені розміри контактних груп [22].

Ці пристрої відрізняються один від одного не лише рівнем продуктивності та обсягом пам'яті, але й наявністю додаткових вбудованих функцій, зокрема модулів зв'язку. Завдяки цьому їхнє використання можливе в системах різного ступеня складності - від простих локальних СКУД до централізованих мережових систем безпеки.



Рисунок 1.2 - Типові приклади мікроконтролерів

Також мікроконтролери виконують важливі функції, а саме:

- обробка даних від пристроїв ідентифікації;
- управління виконавчими механізмами;
- організація інформаційного обміну з серверною частиною;
- реалізація алгоритмів авторизації та підтвердження доступу.

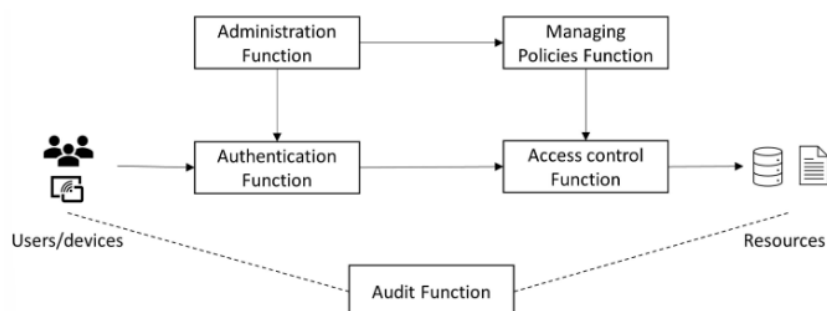


Рисунок 1.3 - Взаємодія мікроконтролера з периферійними пристроями СКУД

Завдяки інтеграції мікроконтролерів з підтримкою бездротових технологій, стає можливим створення централізованих систем управління. Це, у свою чергу, надає можливість дистанційного контролю за роботою обладнання, що суттєво підвищує загальну ефективність системи. Крім того, така конфігурація дозволяє оперативно реагувати на будь-які позаштатні ситуації чи спроби несанкціонованого втручання.

Важливою особливістю сучасних мікроконтролерів у СКУД є їхня здатність до інтеграції, що забезпечує спільну роботу з іншими підсистемами безпеки, включаючи відеоспостереження, пожежну сигналізацію та системи моніторингу стану приміщень.

1.3. Дослідження способів захисту даних та ідентифікації користувачів.

Для забезпечення безпеки та контролю доступу в організаціях застосовуються різноманітні методи перевірки особистості користувачів. Серед найпоширеніших виділяють:

- Безконтактні картки та електронні мітки (RFID): Ці пристрої містять унікальний ідентифікатор, який зчитується спеціальним пристроєм на відстані;
- Секретні коди та паролі: Користувачі вводять комбінацію цифр або символів для підтвердження своєї особи;
- Біометричні дані: Використовуються унікальні фізичні ознаки людини, такі як відбитки пальців, риси обличчя або візерунок райдужної оболонки ока;
- Багатофакторна автентифікація: Поєднання двох або більше вищезазначених методів для посилення безпеки.

Додатково варто враховувати, що ефективність систем контролю доступу безпосередньо залежить від рівня захисту каналів передачі даних та способу зберігання ідентифікаційної інформації [7]. Сучасні СКУД активно застосовують шифрування, унікальні ідентифікатори користувачів та алгоритми захисту від повторного використання сигналів, що дозволяє ефективно знижувати ризики несанкціонованого доступу [8].

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Кожен із зазначених методів має свої особливості, переваги та недоліки. Проведемо дослідження кожного методу окремо.

RFID-технологія: лідер серед сучасних рішень.

На сьогоднішній день RFID-технологія є одним із найпопулярніших рішень у систем контролю та управління доступом (СКУД) [2]. Кожна RFID-картка має свій неповторний код, який безконтактно зчитується спеціальним пристроєм. Після успішної верифікації даних система або надає доступ, або обмежує його [3]. Основні переваги RFID полягають у швидкості роботи, зручності для користувачів та можливості централізованого управління доступом [14]. З недоліків RFID виділяють можливість втрати або несанкціонованого копіювання карток. Для мінімізації таких ризиків часто використовують багатофакторну автентифікацію.

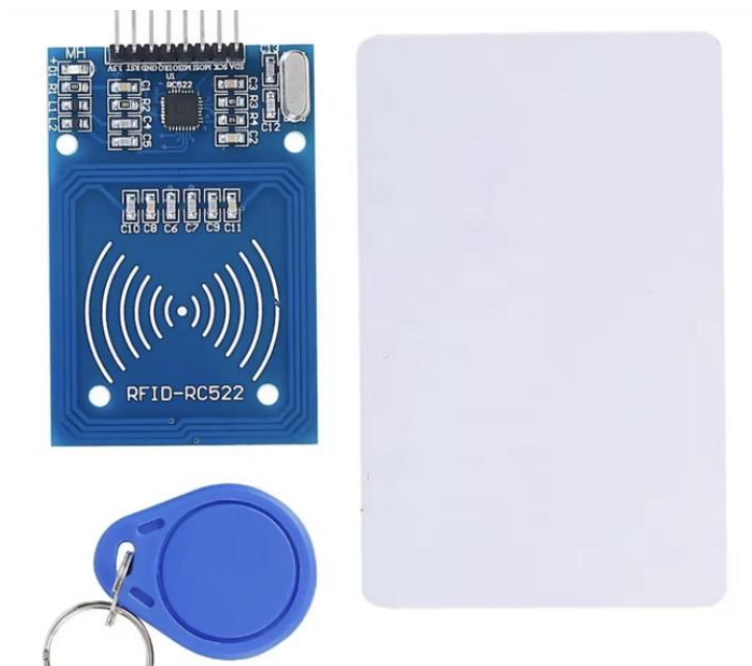


Рисунок 1.4 – Приклад RFID-технології

Простота та вразливість PIN-кодів і паролів.

PIN-коди та паролі є одним із найпростіших способів ідентифікації. Доступ надається після коректного введення встановленої комбінації. Головною перева-

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

гою цього методу є легкість його впровадження, проте суттєвим недоліком є ризик підбору пароля зловмисниками або його передачі третім особам. Щоб зробити PIN-код безпечнішим, їх часто використовують у поєднанні з додатковими захисними засобами. Це включає обмеження кількості спроб введення, тимчасове блокування та запис неудальних спроб [9]. Така комбінація допомагає запобігти підбору коду методом перебору.



Рисунок 1.5 – Приклад клавіатури для введення паролів

Біометрія: високий рівень захисту.

Біометричні методи автентифікації базуються на унікальних фізіологічних характеристиках кожної людини. Найчастіше використовуються такі методи, як сканування відбитків пальців, розпізнавання обличчя або аналіз райдужної оболонки ока. Ці системи забезпечують високий ступінь захисту і є ідеальним вибором для приміщень з підвищеними вимогами до безпеки. Штучний інтелект значно покращує точність сучасних біометричних систем, зменшуючи кількість помилок [1]. Проте, для їхньої стабільної роботи потрібні якісне обладнання та сприятливі умови, що впливає на ціну та складність встановлення.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.6 – Приклад: біометричний термінал ZKTeco

Багатофакторна автентифікація: максимальна безпека.

Багатофакторна автентифікація поєднує кілька методів перевірки особистості одночасно. Наприклад, для отримання доступу може знадобитися як прикласти RFID-картку, так і ввести PIN-код. У контексті сучасних систем контролю та управління доступом, багатофакторна автентифікація виступає як один із найдієвіших методів захисту. Це зумовлено тим, що комбінування кількох незалежних факторів для підтвердження особистості суттєво підвищує стійкість системи до несанкціонованого доступу, навіть якщо один із компонентів автентифікації буде скомпрометовано [7, 16].

Дослідження актуальних методів аутентифікації користувачів свідчить про перевагу комплексних, багатофакторних систем доступу. Ці системи, інтегруючи апаратні та програмні складові безпеки, забезпечують високий рівень захищеності.

1.4. Обґрунтування технічного завдання для розробки СКУД.

Розробка інтегрованої системи контролю та управління доступом для медичних закладів є актуальним і практично значущим завданням. Сучасні лікарні характеризуються інтенсивним потоком людей, зокрема медичного персоналу, пацієнтів і відвідувачів. Водночас у приміщеннях таких закладів зосереджені ва-

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

жливі ресурси: конфіденційні медичні дані, дороге обладнання й медикаменти.

Традиційні механічні замки недостатньо ефективні для забезпечення безпеки, адже вони вразливі до втрати, крадіжки чи копіювання ключів. Сучасні електронні системи на базі мікроконтролерів дозволяють інтегрувати додаткові рівні захисту: налаштовувати диференційований доступ, а також автоматично фіксувати всі події.

Метою роботи є розробка системи контролю та управління доступом у медичному закладі, реалізовану на демонстраційному стенді. Система повинна забезпечувати: багаторівневу перевірку користувачів, розмежування прав доступу, ведення журналу подій та можливість віддаленого моніторингу стану системи.

Для того, щоб виконати поставлену мету необхідно виконати такі завдання:

- Проаналізувати специфіку та стандарти безпеки, які застосовуються у медичних установах;
- Ознайомитися із сучасними методами ідентифікації користувачів;
- Дослідити потенційні моделі порушників для формування рівнів захисту;
- Вибрати відповідні мікроконтролери, датчики і програми;
- Розробити структуру майбутньої системи, враховуючи всі її компоненти;
- Написати програмний код для управління мікроконтролерами й налаштувати вебсервер для моніторингу системи;
- Протестувати кожен зону на макетних платах окремо, перевірити їх роботу;
- Зібрати усі компоненти на одному стенді.

Вихідні дані для виконання роботи - це вимоги до безпеки лікарень, правила розмежування доступу до приміщень різного рівня важливості, а також характеристики сучасних електронних компонентів.

Також треба обрати програмне забезпечення для програмування мікроконтролерів. Для виконання усіх необхідних завдань доцільно обрати ПЗ Arduino

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

IDE. Це інтегроване середовище розробки (IDE) надає функціонал для написання, компіляції та завантаження коду в мікроконтролери через USB-інтерфейс. Воно дозволить виконати усі поставлені завдання у повному обсязі.

Висновки до першого розділу: у цьому розділі я дослідила ключові аспекти безпеки медичних закладів, зосередившись на принципах побудови систем контролю доступу. З'ясувала, що лікарні та подібні установи вимагають особливої уваги до безпеки через зберігання чутливої інформації про пацієнтів, наявність дорогого медичного обладнання та постійний потік людей.

Розглянуто нормативно-правове забезпечення у сфері захисту інформації, зокрема Закон України «Про захист персональних даних» та регламент GDPR, що діє в країнах Європейського Союзу.

Були проаналізовані поширені методи автентифікації користувачів, включаючи використання RFID-карток, введення PIN-кодів та біометричних даних, а також їх комбіноване застосування. Встановлено, що максимальний рівень захисту досягається шляхом застосування кількох факторів ідентифікації одночасно.

Було досліджено види популярних мікроконтролерів, які широко використовуються, такі як Arduino Uno, Arduino Nano та ESP8266, вони дозволяють інтегрувати замки, зчитувачі та інші компоненти. Процес налаштування мікроконтролерів спрощується завдяки середовищу Arduino IDE.

Отже, сучасні системи контролю та управління доступом, побудовані на основі мікроконтролерів та багаторівневих методів ідентифікації, є ефективним рішенням для підвищення рівня безпеки медичних закладів та мінімізації ризиків несанкціонованого доступу.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. РОЗРОБКА СТРУКТУРИ ТА ВИБІР ОБЛАДНАННЯ ДЛЯ ІНТЕГРОВАНОЇ СКУД

2.1. Аналіз загроз безпеки та побудова моделі порушника.

У процесі розробки системи контролю й управління доступом доцільним є врахування потенційних сценаріїв порушення безпеки, які можуть виникати в умовах функціонування медичних закладів. Такий підхід є критично важливим для формування оптимальної архітектури системи, застосування відповідних методів ідентифікації користувачів, а також забезпечення дієвих механізмів захисту від несанкціонованого доступу[23].

Безпекова система має забезпечувати захист від зовнішніх і внутрішніх загроз, водночас враховуючи можливість помилок або недобросовісних дій з боку уповноважених осіб, таких як адміністратори. У межах цього можна виділити такі категорії порушників [24]:

1. Зовнішні порушники

Особа, яка не є працівником закладу й намагається потрапити на його територію без відповідного дозволу, становить очевидну загрозу для системи безпеки. Подібні інциденти потребують особливої уваги й швидкої реакції.

Для запобігання таким порушенням застосовуються як фізичні, так і технічні заходи контролю доступу. До них належать системи RFID-ідентифікації, відеоспостереження, а також автоматизовані механізми блокування входу у випадку відсутності дозволу. Крім того, кожна спроба несанкціонованого проникнення детально реєструється в журналі подій. Це забезпечує можливість ретельного аналізу інцидентів та прийняття заходів для посилення безпеки.

2. Внутрішній порушник

Це співробітник закладу, який має певні рівні доступу, але намагається отримати доступ до зон, що виходять за межі його повноважень. Подібні дії важче ідентифікувати, оскільки порушник вже володіє авторизованими обліковими даними. Для мінімізації подібних ризиків у системі запроваджується чітке

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

розмежування прав доступу. Журналювання подій зберігає всі записи про входи і виходи із приміщень, що забезпечує прозорий контроль переміщень персоналу.

3. Порущник з адміністративними привілеями

Цей тип порушника є найбільш небезпечним через доступ до ключових компонентів системи, включаючи конфігураційні налаштування, бази даних і журнали подій. Компрометація адміністративного доступу може повністю порушити функціональність всієї системи безпеки.

Для зниження таких загроз використовуються багатофакторна автентифікація, регулярне резервне копіювання журналів подій і дублювання критично важливої інформації на віддалених серверах. Крім того, будь-які дії адміністратора фіксуються у спеціальних логах для подальшої можливості перевірки внесених змін [23].

Усі три категорії порушників можна представити у вигляді схеми, яка наведена на рисунку 2.1.

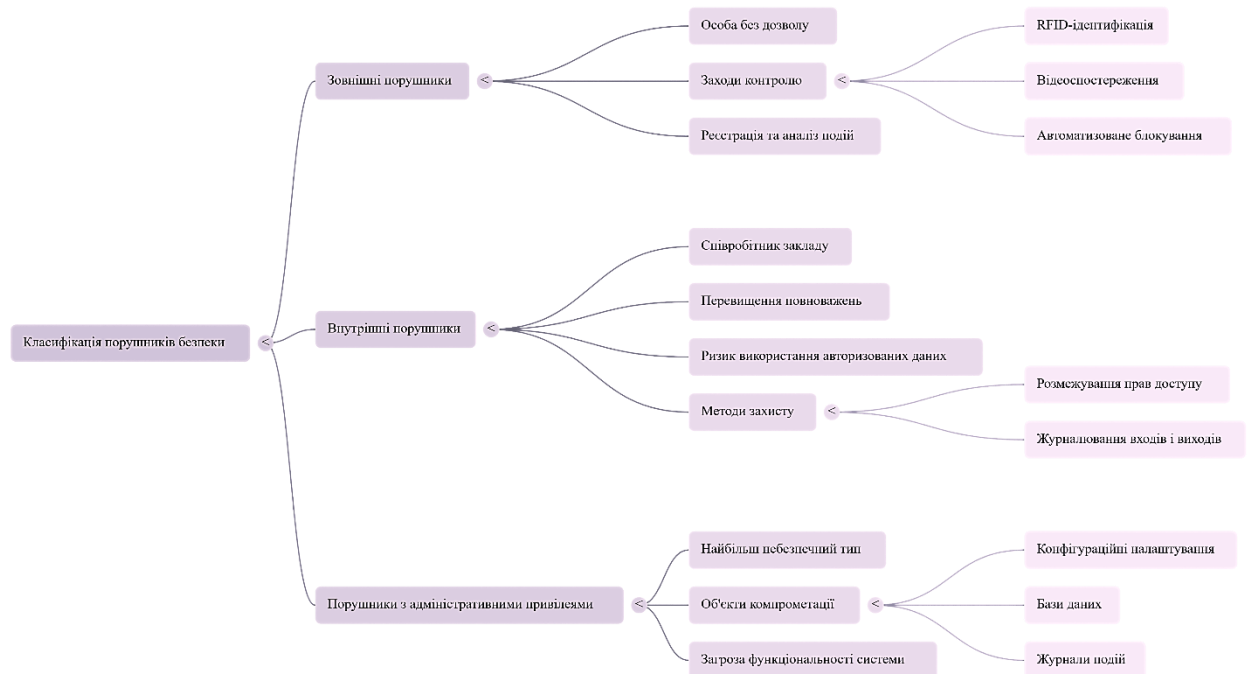


Рисунок 2.1 – Модель порушників

Проаналізована модель порушників показує різний рівень загроз залежно від доступу та можливостей впливу на систему. Зовнішні порушники становлять фізичну загрозу та ефективно контролюються технічними засобами доступу й спостереження. Внутрішні користувачі та адміністратори є більш критичними, оскільки мають легітимний доступ, тому потребують суворого розмежування прав і посиленого контролю дій.

2.2. Розробка структури інтегрованої системи контролю та управління доступом в медичному закладі.

2.2.1. Розмежування багаторівневого доступу в інтегрованій СКУД.

Для побудови демонстраційного стенду СКУД було розроблено структурну модель, яка імітує роботу реального медичного закладу. Система поділена на окремі функціональні зони, кожна з яких має свій рівень доступу та рівень безпеки.

Такий підхід дозволяє реалізувати багаторівневий захист об'єкта та наочно продемонструвати принцип роботи СКУД у різних умовах експлуатації.

Розроблена мною структура складається з чотирьох основних зон:

1. Перша зона відеоспостереження (реєстратура): Ця ділянка повністю відкрита для пацієнтів та відвідувачів, тому в цій зоні реалізований мінімальний захист. Основний акцент тут зроблено на відеоспостереженні у режимі реального часу. Для цього встановлено автономну відеокамеру, яка забезпечує загальний нагляд, фіксує рух людей та надає оперативну інформацію для служби безпеки з метою запобігання можливим правопорушенням.

2. Друга зона контрольованого доступу персоналу (кабінети лікарів та ординаторські): Ця зона призначена для обмеження сторонніх осіб до робочих приміщень медичного персоналу. Принцип роботи цієї частини ґрунтується на тому, що вхід відбувається до кабінету за допомогою персональних RFID-карток співробітників.

Також доцільно в цій зоні встановити камери відеоспостереження для забезпечення особистої безпеки персоналу при прийомі пацієнтів.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				24
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.2 – Приклад першої зони СКУД (реєстратура)



Рисунок 2.3 – Приклад другої зони СКУД (кабінет лікаря)

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

3. Третя зона підвищеного рівня безпеки (зберігання медикаментів): У цій зоні зберігаються лікарські засоби та наркотичні речовини, тому тут є вимога особливого рівня захисту. Я вирішила, що тут буде доцільно використати двофакторну автентифікацію, комбінуючи цифровий код та персональну RFID-картку. Враховуючи високий ризик цієї зони, потрібно щоб відбувався безперервний відеоконтроль. При цьому камера має фіксувати відкриття та закриття дверей, що дозволить при необхідності співставляти час реєстрації картки в системі з відеозаписом особи, яка входила.



Рисунок 2.4 – Приклад третьої зони СКУД (зберігання медикаментів)

4. Четверта зона управління та моніторингу (ІТ-відділ): Зона реалізована як локальний веб-ресурс, призначений для ІТ-відділу або служби безпеки. Для забезпечення безпеки самого сервера передбачено захист: доступ до сторінки надається лише після введення логіну та паролю адміністратора. На веб-сервері відображається поточний стан точок доступу та ведеться онлайн-журнал усіх подій із зазначенням точного часу та імен користувачів, які виконували вхід.

Відповідно у результаті, була розроблена система, яка заснована на зонуванні доступу за рівнями (рисунок 2.5).

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

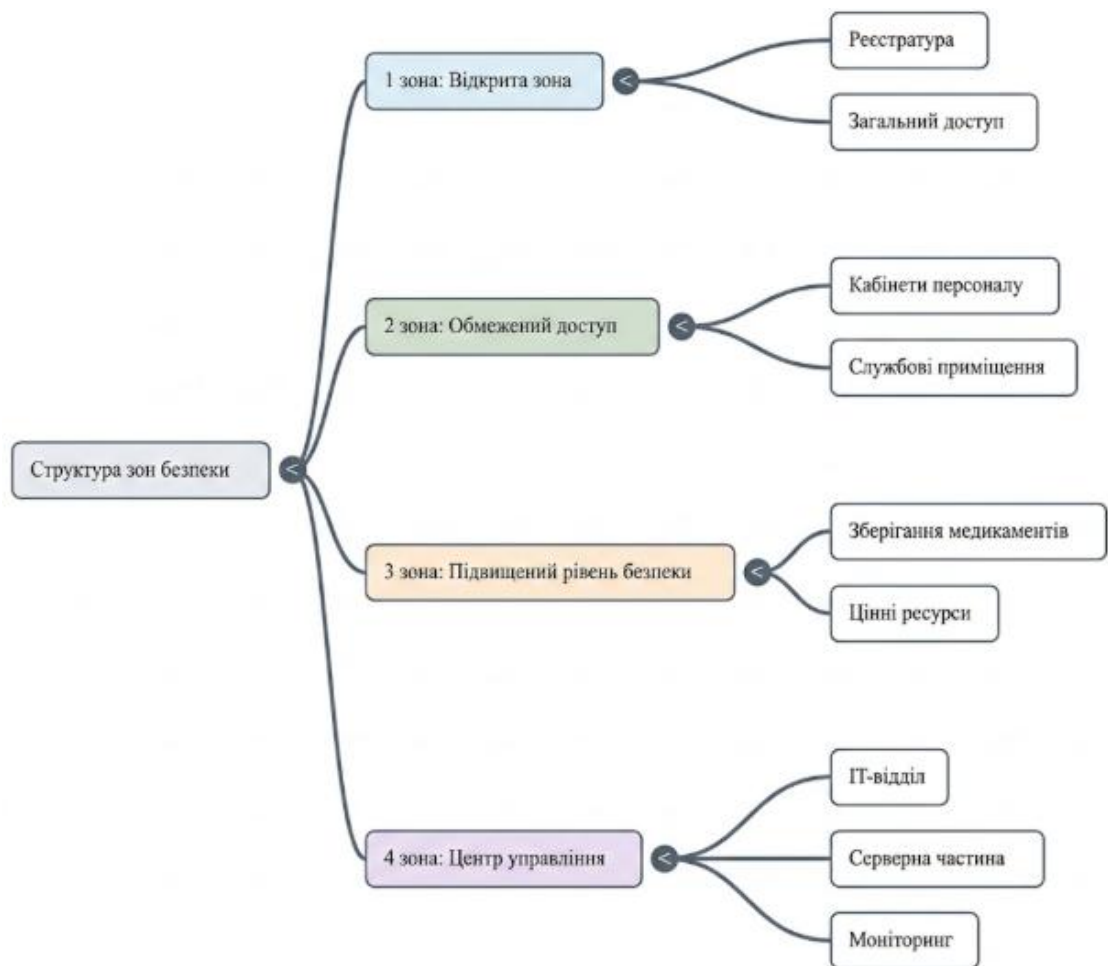


Рисунок 2.5 – Структура зонування

Використовуючи таку структуру розділення зон з різними рівнями доступу, від самого мінімального відеоспостереження до двофакторної автентифікації підвищує рівень безпеки для системи контролю доступом в медичному закладі [5].

2.2.2. Реєстрація, блокування та політика безпеки системи контролю та управління доступом.

У реальних умовах більшість СКУД працюють за принципом «клієнт-сервер». Тобто усі пристрої підключені до одного головного сервера в ІТ-відділі, де є база даних усіх працівників. Завдяки такій роботі усі проблеми, які виникають вирішуються через сервер адміністратором системи.

При реалізації інтегрованої системи контролю та управління доступом у медичному закладі можна виділити три основні адміністративні процедури: реєстрація користувачів, реагування на втрату чи викрадення картки та відновлення чи зміна паролю.

Розберемо процедуру реєстрації користувачів та видача картки:

1. Внесення особистих даних: Адміністратор вносить в базу даних ПІБ нового користувача та його посаду.
2. Налаштування прав доступу: Надання прав доступу до кабінетів та зон, в які може входити користувач.
3. Внесення картки: Реєстрація нової картки через зчитувач. Автоматичний запис на сервер унікального коду картки.
4. Активація картки: Зчитаний код закріплюється за доданим користувачем у БД. Картка активна і готова до роботи.

Окрему увагу слід приділити питанню, що робити при втраті та викраденні карток, а також при забутті паролю.

Окремо розглянемо процедуру втрати чи викрадення картки, виконується миттєво:

1. Повідомлення про інцидент: Лікар повідомляє службу безпеки чи ІТ-відділ про втрату або викрадення картки.
2. Блокування: Адміністратор знаходить у БД профіль користувача та заблоковує картку. Сервер автоматично зобороняє доступ.
3. Захист від крадіїв: При спробі прикласти заблоковану картку доступ буде заборонено, і відправиться сповіщення про проникнення службі охорони.
4. Зміна картки: Після всіх дій адміністратор вносить нову картку в БД і видає її користувачу.

Останнім важливим етапом є процедура відновлення та планової зміни пароля для двофакторної автентифікації. Тому варто дотримуватися таких кроків:

1. Дотримання політики безпеки: Для зон з підвищеним рівнем ризику, цифровий пароль повинен автоматично оновлюватися кожні 3 місяці для запобігання його підгляданню чи підбору сторонніми особами.

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

2. Скидання паролю: Якщо користувач забув пароль, він повинен звернутися до ІТ-відділу. Далі адміністратор системи вирішує проблему і користувачу надається новий тимчасовий пароль, з яким він може увійти у потрібну йому зону.

3. Оновлення пароля: Коли доступ відновлено користувач зобов'язаний встановити новий секретний пароль. Після введення нового паролю, він зберігається в БД у зашифрованому вигляді, тимчасовий видаляється.

2.3. Підбір апаратних засобів для створення демонстраційного стенду.

Для побудови та реалізації демонстраційного стенду мені потрібні, доступні, надійні та сумісні між собою апаратні компоненти. Вибір апаратних засобів забезпечує повну функціональність системи контролю та управління доступом, охоплюючи весь цикл роботи: від зчитування ідентифікаційних даних до управління виконавчими пристроями та реєстрації подій. Виходячи з цього, мій вибір технічних засобів зупинився на наступних компонентах:

1. ІР-камера відеоспостереження:

Для відеомоніторингу використовується ІР-камера з підтримкою передачі даних через Ethernet або Wi-Fi.

Основні характеристики:

- роздільна здатність від 720p до 1080p;
- кут огляду близько 90-120°;
- підтримка потокового відео;
- можливість нічного бачення;
- живлення здійснюється через 5-12 В.

Камера забезпечує безперервну передачу відеопотоку для контролю доступу в режимі реального часу. Це дає змогу відстежувати вхід користувачів та реєструвати потенційні порушення, що є ключовим для безпеки медичних закладів.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				29
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.6 – IP відеокамера

2. Мікроконтролери:

Плата Wemos D1 mini - це енергоефективний мікроконтролер із вбудованим модулем Wi-Fi, призначений для створення пристроїв IoT, а також для організації бездротової передачі даних.

Основні характеристики:

- 32-бітний процесор;
- Wi-Fi модуль;
- пам'ять 4 МБ;
- GPIO - обмежена кількість цифрових виходів;
- живлення 3.3 В.

Ця плата виконує функцію центрального вузла мережевої взаємодії 2 зони. Її основна перевага полягає у вбудованому модулі Wi-Fi, який забезпечує можливість віддаленого доступу до системи та передачі подій на сервер. Це має критичне значення для СКУД у медичних установах, де потрібен безперервний моніторинг подій, що відбуваються.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

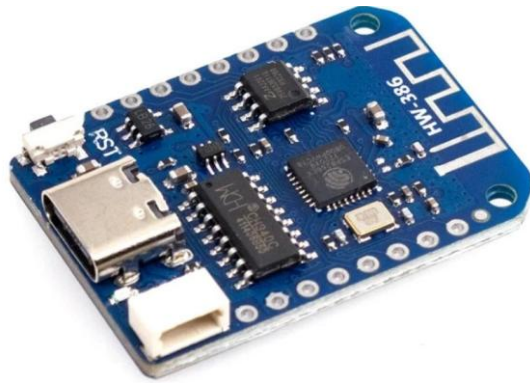


Рисунок 2.7 – Мікроконтролер Wemos D1 mini

Плата Arduino Nano - це компактний модуль на базі ATmega328 призначений для прототипування та керування периферійними пристроями.

Основні характеристики:

- пам'ять 32 КБ;
- SRAM 2 КБ;
- цифрові входи/виходи 14;
- аналогові входи 8;
- живлення 5 В.

Переваги, малий розмір, велика кількість цифрових та аналогових контактів, простий у програмуванні. Недоліки, відсутність Wi-Fi модуля та Bluetooth, а також має обмежену пам'ять [7].

Arduino Nano функціонує як центральний вузол для керування периферійними компонентами 3 зони. Завдяки його перевагам це оптимальний варіант для інтеграції з RFID-зчитувачами, клавіатурами та виконавчими механізмами у процесі виконання стенду.

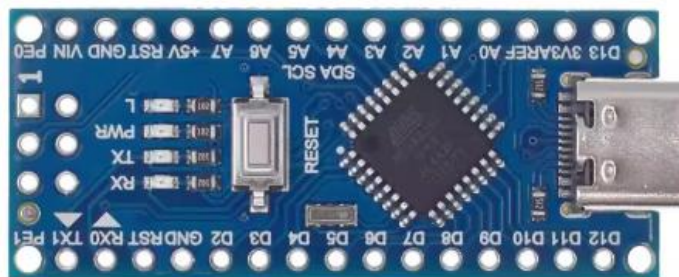


Рисунок 2.8 – Мікроконтролер Arduino Nano

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

3. Пристрої розпізнавання та введення даних:

RFID-зчитувач RC522 - радіочастотний модуль.

Основні характеристики:

- частота 13.56 МГц;
- інтерфейс SPI;
- робоча напруга 3.3 В;
- дальність зчитування 2-5 см.

RC522 дозволяє легко та швидко визначати, хто є хто, використовуючи безконтактні картки. Це основна частина системи контролю доступу, яка перевіряє, чи має людина право на вхід. Оскільки він недорогий і добре працює з Arduino, це чудовий варіант для виконання завдань.



Рисунок 2.9 - RFID-зчитувач RC522 та картка і мітка

Матрична клавіатура 4x4 – Має 16 кнопок, організованих у матрицю 4x4. Працює без додаткового контролера, підключається напряму до GPIO-пінів мікроконтролера.

Основні характеристики:

- живлення 3.3-5 В;
- підключення через GPIO;
- матрична схема зчитування.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

Клавіатура потрібна для введення секретного коду, що додає ще один рівень захисту. Разом з RFID-картою це створює надійну систему перевірки (двофакторну автентифікацію). Оскільки клавіатуру легко підключити та налаштувати програмно, вона чудово підходить для роботи.



Рисунок 2.10 – Матрична клавіатура 4x4

Для реалізації відчинення дверей та індикації дозволу на вхід було використано:

Сервопривідний моторчик SG90 – це виконавчий механізм. Який повертається на заданий кут від 0 до 180 градусів. З переваг дуже дешевий, має маленьку вагу та просте керування, з недоліків через пластиковий корпус не дуже міцний та швидко зношується.

Світлодіоди (червоний та зелений) – вони максимально просто підключаються та миттєво реагують, дуже енергоекономічні. Робоча напруга 1.8-2.2 В (червоний) і 2.0-3.2 В (зелений). Струм споживання - 10-20 мА. Використовуються для індикації стану доступу (дозвіл/заборона). Мають з мінусів тільки те, що вони дуже примітивні у виконанні, тобто мають два стани увімкнено/вимкнено.

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

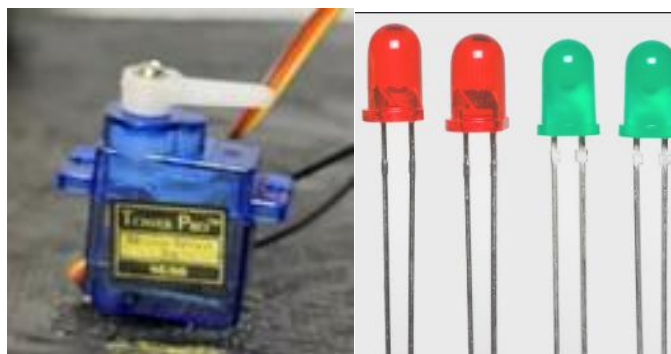


Рисунок 2.11 – Сервомоторик та світлодіоди

І на останок для коректної та безперебійної роботи усіх компонентів, слід обрати систему живлення та модуль для стабілізації роботи пристроїв. У межах цього було обрано такі пристрої, як блок живлення 90 Вт. та понижувальний перетворювач напруги LM2596.

Блок живлення перетворює напругу на постійний струм, а понижувач напруги стабілізує до безпечного рівня напругу, за рахунок чого всі компоненти працюють без проблем та немає ризику того, що щось згорить.



а

б

Рисунок 2.12 – Понижувач напруги (а) та блок живлення (б)

Обраний комплекс апаратних засобів задовольняє критерії технічної сумісності, економічної доцільності та функціональної повноти, необхідних для макетування інтегрованої СКУД медичного закладу.

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4. Базове налаштування програмного забезпечення для програмування апаратної бази стенду

Для практичної реалізації та програмування мікроконтролерів було обрано середовище Arduino IDE – це безкоштовне інтегроване середовище для розробки, написання, компіляції та завантаження програмного коду на плати.



Рисунок 2.13 – Програмне забезпечення Arduino IDE

Arduino IDE забезпечує зручний інтерфейс та спрощує процес програмування, дозволяючи зосередитись на роботі системи. Важливою перевагою Arduino IDE є наявність великої кількості бібліотек. Це дозволяє швидко інтегрувати функціональність різних периферійних пристроїв. Arduino IDE також надає потужні інструменти для налагодження та тестування. Функція Serial Monitor дозволяє здійснювати моніторинг обміну даними між мікроконтролером та підключеними пристроями. Це є критично важливим для діагностики проблем, пов'язаних з читанням RFID-карток, коректністю введення PIN-кодів, а також для перевірки роботи сервомоторів.

Після завершення написання програмного коду, Arduino IDE виконує його компіляцію, перетворюючи вихідний код на машинний код, який може бути виконаний мікроконтролером. Потім скомпільований бінарний файл завантажується в пам'ять плати, що забезпечує автономну роботу без необхідності постійного підключення до комп'ютера.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

Врахувавши усі можливості програми, можна з впевненістю її обирати для реалізації поставлених завдань.

Почнемо з базового налаштування програми.

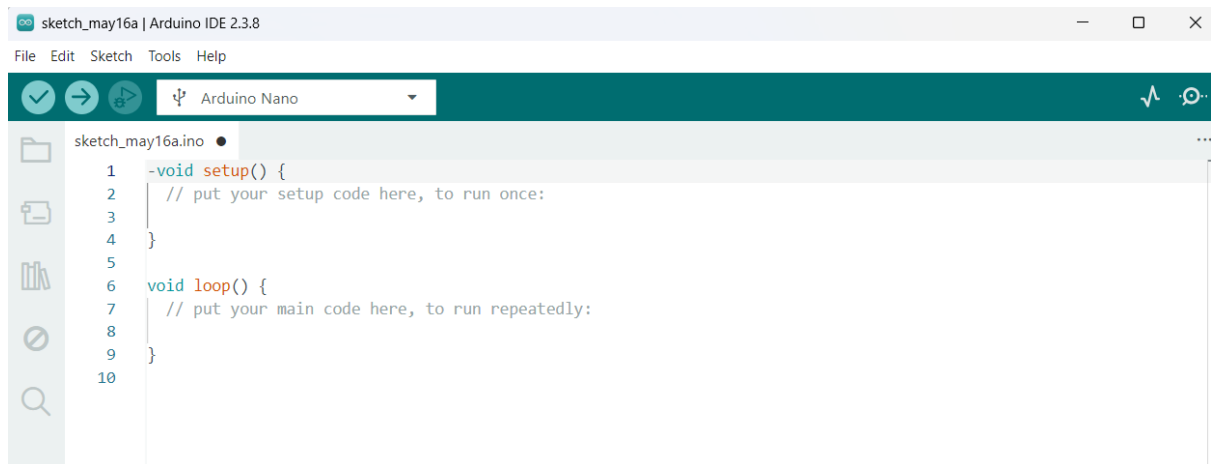


Рисунок 2.14 – Інтерфейс програмного середовища Arduino IDE

Налаштування ПЗ складалося з трох етапів:

1. Перший встановлення Arduino IDE: на ПК було завантажено та встановлено офіційну версію програми. Також в процесі встановлення та читання рекомендацій мені потрібно було ще встановити драйвер USB-SERIAL CH340 [4]. Це дозволило програмі розпізнавати підключення через USB-порт та створити віртуальні COM-порти для подальшого прошивання плат.

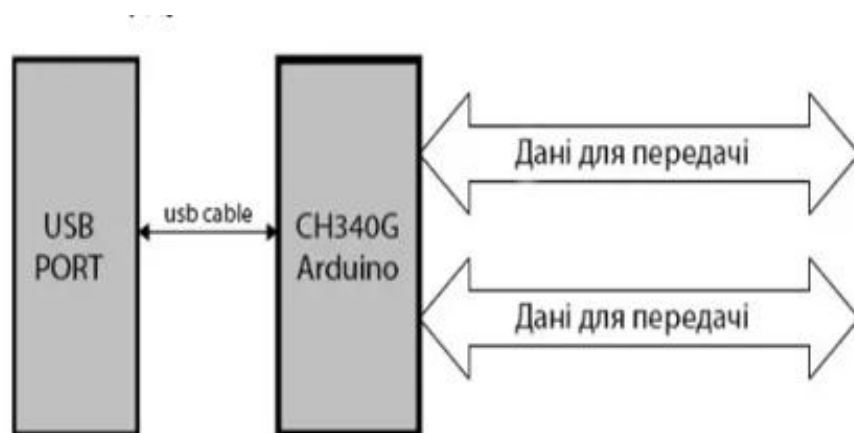


Рисунок 2.15 – Принцип роботи через порт

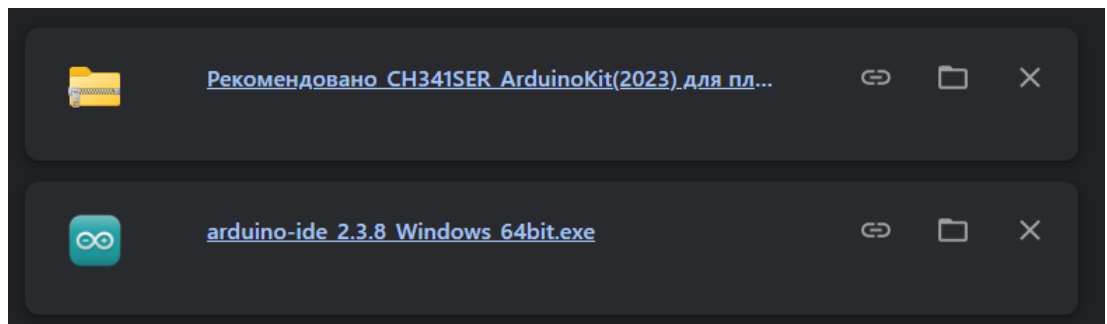


Рисунок 2.16 – Завантаження ПЗ та драйверу

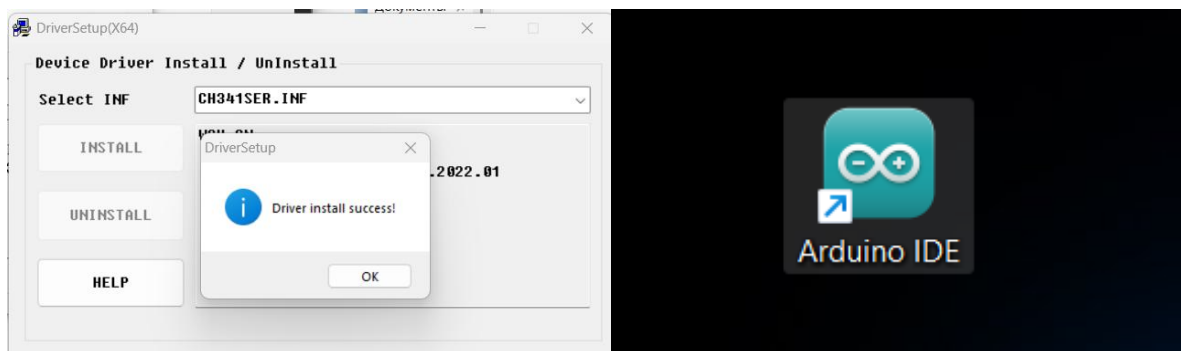


Рисунок 2.17 – Успішне встановлення ПЗ та драйверу

2. Другий встановлення розширення: так як за замовчуванням Arduino IDE підтримує тільки стандартні плати, наприклад як Arduino Nano, то потрібно було додати плату, яка функціонує у 2 зоні Wemos D1 mini. Для цього було додано офіційне посилання на репозиторій у менеджері плат. Цей етап забезпечив можливість використання Wi-Fi функціоналу, що є важливим для реалізації мережевої частини системи.

```
Processing esp8266:3.1.1: Replacing platform esp8266:esp8266@3.1.2 with esp8266:esp8266@3.1.1
```

Рисунок 2.18 – Процес встановлення розширення для esp8266

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

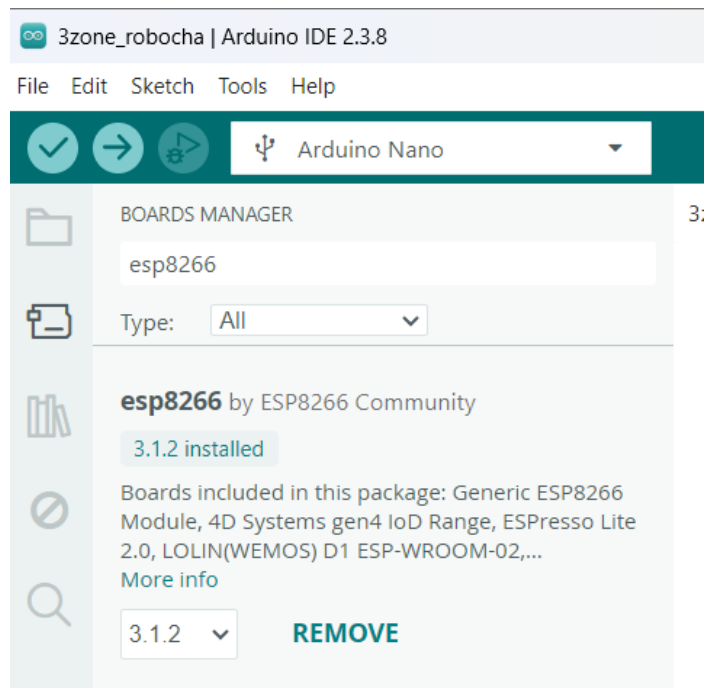


Рисунок 2.19 – Встановлення розширення

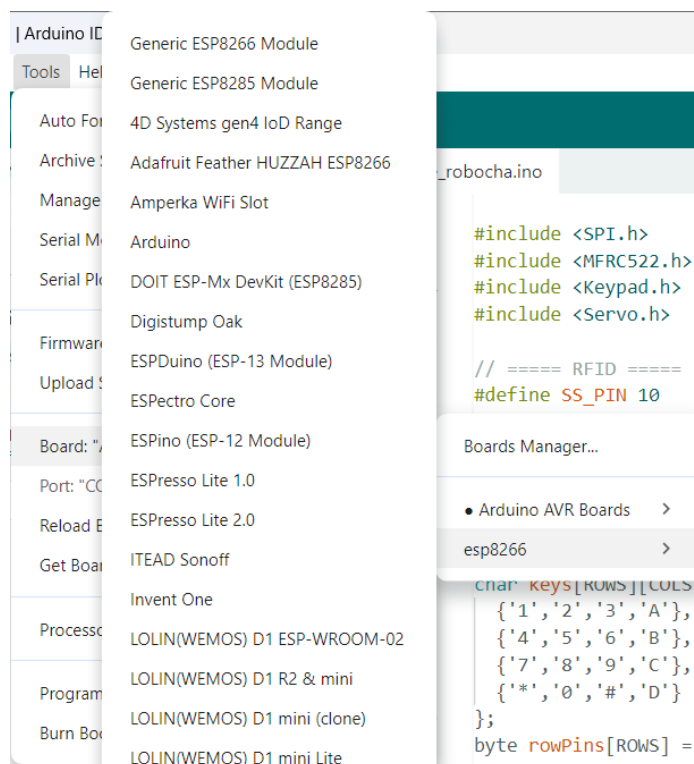


Рисунок 2.20 – Перевірка встановленого розширення

3. Третій підключення бібліотек: для коректної роботи програмного коду та уникнення помилок при програмуванні мікроконтролерів, через менеджер бібліотек було встановлено необхідні модулі, а саме:

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

- MFRC522.h - для взаємодії з RFID-зчитувачами;
- Keypad.h - управління матричною клавіатурою;
- Servo.h – встановлення необхідних кутів повороту сервомотору.

Встановлення бібліотек дозволило значно спростити розробку програмної частини та забезпечити стабільну роботу апаратних модулів.

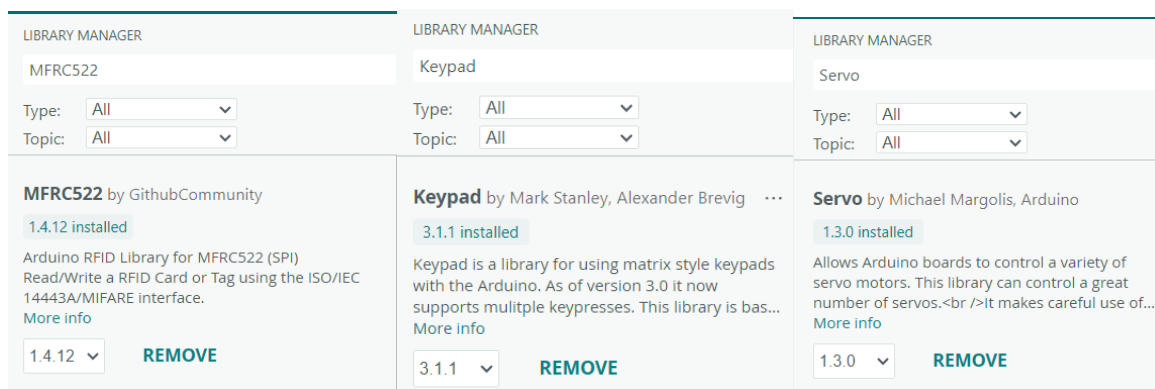


Рисунок 2.21 – Встановленні необхідні бібліотеки

Після успішного виконання всіх трьох етапів, програмне середовище цілком готове до коректної роботи та програмування усіх компонентів СКУД.

Висновки до другого розділу: у другому розділі мною було розроблено структуру побудови стенду та підібрано необхідне апаратне та програмне забезпечення для його реалізації. Систему розділено на чотири різні зони, кожна з яких відповідає за свій рівень безпеки в лікарні. Перша зона, реєстратура з самим мінімальним захистом - відеоспостереження, для кабінетів лікарів, друга зона доступ здійснювався за допомогою магнітних карток, а для третьої зони, де зберігаються ліки та наркотичні речовини, встановлено особливий контроль, двофакторна автентифікація - вхід лише за картокою та цифровим кодом одночасно. Ну и четвертою зоною було представлено, як приклад, веб-сторінка ІТ-відділу, де вхід здійснюється через введення логіну та паролю. На веб-сторінці ведеться журналювання подій у реальному часі.

Додатково було побудовано модель можливих порушників, яка дозволила проаналізувати потенційні загрози для системи та врахувати їх під час проєктування архітектури стенда. Це сприяло більш обґрунтованому вибору методів захисту та рівнів доступу для кожної зони.

Для реалізації стенду, я підбрала надійні та недорогі компоненти, які добре поєднуються між собою. Головними платами системи, я вирішила обрати Arduino Nano та Wemos D1 mini, вони підходили по усім параметрам для мого завдання. Також додатковими елементами стали: RFID-зчитувач RC522, матрична клавіатура 4x4, сервопривід SG90 та світлодіоди, які показують чи доступ дозволено чи заборонено. Для стабільної роботи усіх складових, я додала блок живлення та понижувальний перетворювач LM2596, щоб нічого не згоріло.

В кінці мною було налаштовано та підготовлено програмне середовище Arduino IDE на комп'ютері. Я встановила потрібні драйвери, додала плату Wemos та завантажила спеціальні бібліотеки для керування клавіатурою, картками й моторчиками, які в подальшому будуть написані в коді програми. Тепер усе обладнання готове до програмування та перевірка працездатності усіх компонентів.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ РОЗРОБЛЕНОЇ ІНТЕГРОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ТА КОНТРОЛЮ ДОСТУПУ

3.1. Налаштування на макетній платі захищеної зони СКУД.

Перед тим, як збирати стенд, потрібно перевірити працездатність усіх підключених компонентів на макетній платі. Спочатку я тестувала роботу другої зони, яку представлено на рисунку 3.1.

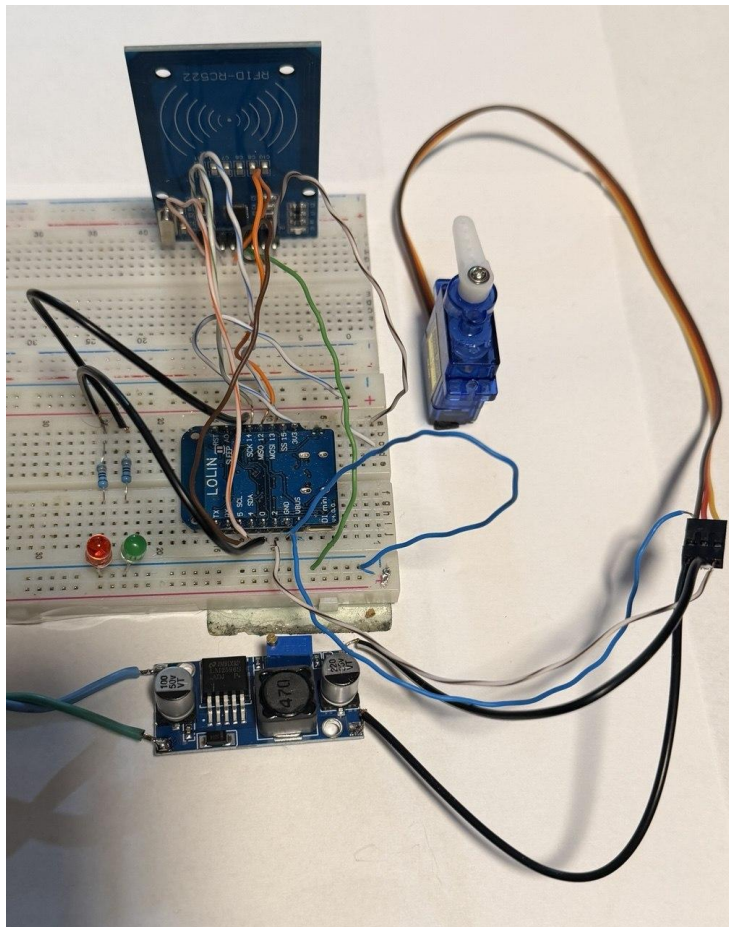


Рисунок 3.1 – Перевірка роботи другої зони, кабінет лікаря

Головну роль обчислювального пристрою виконує плата Wemos D1 mini. Для розпізнавання користувачів підключено зчитувач карток RFID RC522, а виконує дію відкриття та закриття дверей сервопривід SG90. Для наглядності, що двері відкриті чи закриті, було підключено світлодіоди червоного та зеленого кольорів.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Для того, щоб не відбувалося конфліктів та перенавантаження системи, я також інтегрувала понижувальний перетворювач напруги

Також для правильного з'єднання компонентів зони 2, було розроблено схему розподілу пінів. Опис підключення компоненту RFID RC522 наведено у таблиці 3.1.

Таблиця 3.1.

Підключення компоненту RFID RC522

Пристрій	Пін модуля	Пін Wemos D1	GPIO
RFID RC522	SDA/SS	D2	4
	RST	D1	5
	SCK	D5	14
	MISO	D6	12
	MOSI	D7	13
	3.3V	3.3V	
	GND	GND	

Для допоміжних компонентів, було розроблено окрему таблицю підключень, яка представлена у таблиці 3.2.

Таблиця 3.2.

Підключення допоміжних компонентів 2 зони

Пристрій	Пін модуля	Пін Wemos D1	GPIO
Сервомотор SG90	PWM	D4	2
Зелений світлодіод	Анод	D0	12
	Катод		
Червоний світлодіод	Анод	D3	0
	Катод		

Після підключення фізичних компонентів, для наглядного приклада роботи системи я вирішила в цій зоні реалізувати четвертий сектор – вебінтерфейс

ІТ-відділу. Так, як саме плата Wemos D1 mini має вбудований Wi-Fi модуль та Bluetooth, отже доречно вебінтерфейс розробити в 2 зоні.

Програмна логіка роботи виглядає так:

1. Плата підключається до Wi-Fi роутера, в моєму випадку це Xiaomi_961C, а потім через UDP-протокол звертається до NTP-сервера. Це потрібно для того, щоб час було вказано правильно та щоб журнал подій формувався коректно. Реалізація в коді на рисунку 3.2.

```
11 // ===== НАЛАШТУВАННЯ WIFI =====  
12 const char* wifiSSID = "Xiaomi_961C";  
13 const char* wifiPassword = "00000000";  
14
```

Рисунок 3.2 – Підключення плати до Wi-Fi роутера

2. Другим етапом створюється власна закрита точка доступу SECURITY_SERVER_HUB, яка реалізована за стандартним безпеки WPA2-PSK. Також вбудовано DNS-сервер для автономного підключення адміністратора. Після відкриття дверей система автоматично закриває замок через 10 секунд. Реалізація в коді на рисунку 3.3.

```
const char* apSSID = "SECURITY_SERVER_HUB";  
const char* apPassword = "12345678";  
  
✓ void closeDoor() {  
    digitalWrite(GREEN_LED, LOW);  
    digitalWrite(RED_LED, HIGH);  
    doorServo.write(0);  
    doorStatus = "Заблоковано";  
    addLog(lastUID, "Двері закриті", "#9ca3af");  
    lastUID = "ID";  
    lastUser = "Чекає...";  
    doorCloseTime = 10;  
}
```

Рисунок 3.3 – Створення точки доступу та автоматичне закриття дверей

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

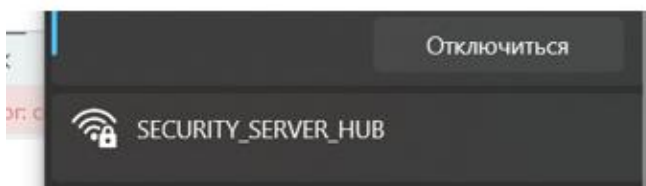


Рисунок 3.4 – Перевірка створеної точки доступу

3. Далі за допомогою функції `makePage()` у пам'ять мікроконтролера записується зформована HTML-сторінка. В коді прописана умова оновлення сторінки кожні 3 секунди та вона повинна відображати такі відомості:

- Поточний стан дверей – відчинено чи заблоковано;
- Останій співробітник який здійснив вхід;
- UID-код останньої зчитаної картки;
- Онлайн-журнал подій із мітками часу;

Вигляд HTML-сторінки на рисунку 3.5.

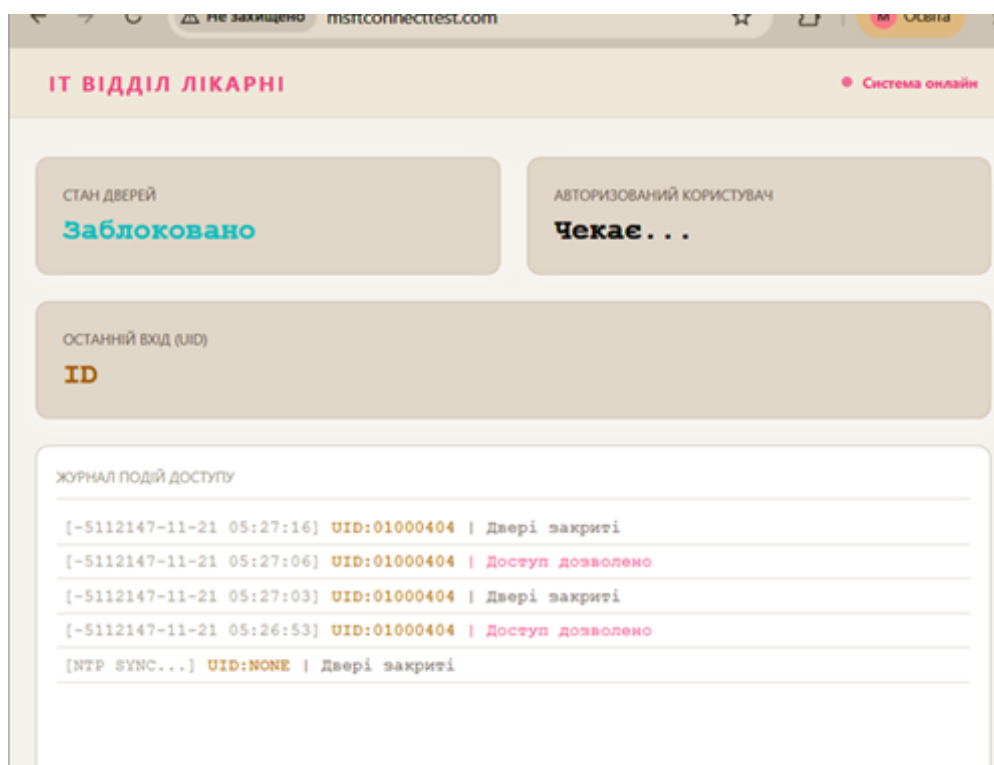


Рисунок 3.5 – Сформована веб-сторінка ІТ-відділу

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Захист даних та доступу до сторінки обмежених. Вхід здійснюється при вимаганні ввести логін та пароль для авторизації, як це виглядає на рисунку 3.6.

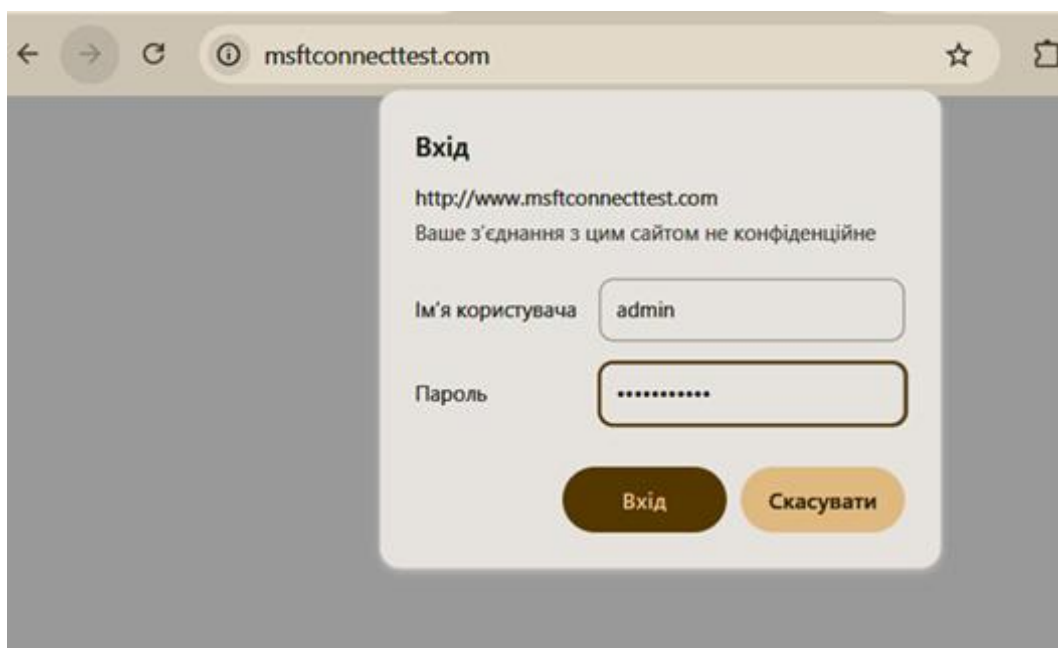


Рисунок 3.6 – Вхід в систему

Протестувавши 2 зону на макетній платі, а також перевіривши коректну роботу вебінтерфейсу для 4 зони, дана частина системи готова до кріплення на основний стенд СКУД.

3.2. Налаштування на макетній платі зони посиленого контролю доступу.

Наступним кроком у тестуванні стало складання 3 зони на макетній платі, для перевірки працездатності. Так, як ця зона у мене має підвищений рівень безпеки, треба дотримуватися алгоритму двофакторної автентифікації.

Для цієї зони я обрала головною платою Arduino Nano на базі мікросхеми ATmega328. Вибір було зумовлено тим, що плата має досить велику кількість цифрових і аналогових пінів, які знадобляться для підключення матричної клавіатури, зчитувача карток та допоміжних компонентів таких, як сервомоточик і стабілізатор напруги.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

Оскільки для підключення матричної клавіатури 4x4 потрібно 8 цифрових ліній, а для підключення зчитувача картки 5 ліній, треба чітко розділити схему комутації для уникнення конфліктів між пристроями. Отже, врахувавши усі умови, розподілення пінів представлено в таблиці 3.3.

Таблиця 3.3.

Підключення апаратних компонентів 3 зони

Пристрій	Пін модуля	Пін на платі Arduino Nano
RFID-зчитувач MFRC522	SDA/SS	D10
	RST	D0
	SCK	D13
	MISO	D12
	MOSI	D11
	3.3V	3.3V
	GND	GND
Матрична клавіатура 4x4	Рядки: R1, R2, R3, R4	D2, D3, D4, D5
	Стовпці: C1, C2, C3, C4	D6, D7, D8, D9
Сервомотор SG90	PWM	A2
	VCC	5V
	GND	GND

Тепер знаючи правильне підключення пінів можна збирати 3 зону на макетній платі. Фізичне збирання представлена на рисунку 3.7.

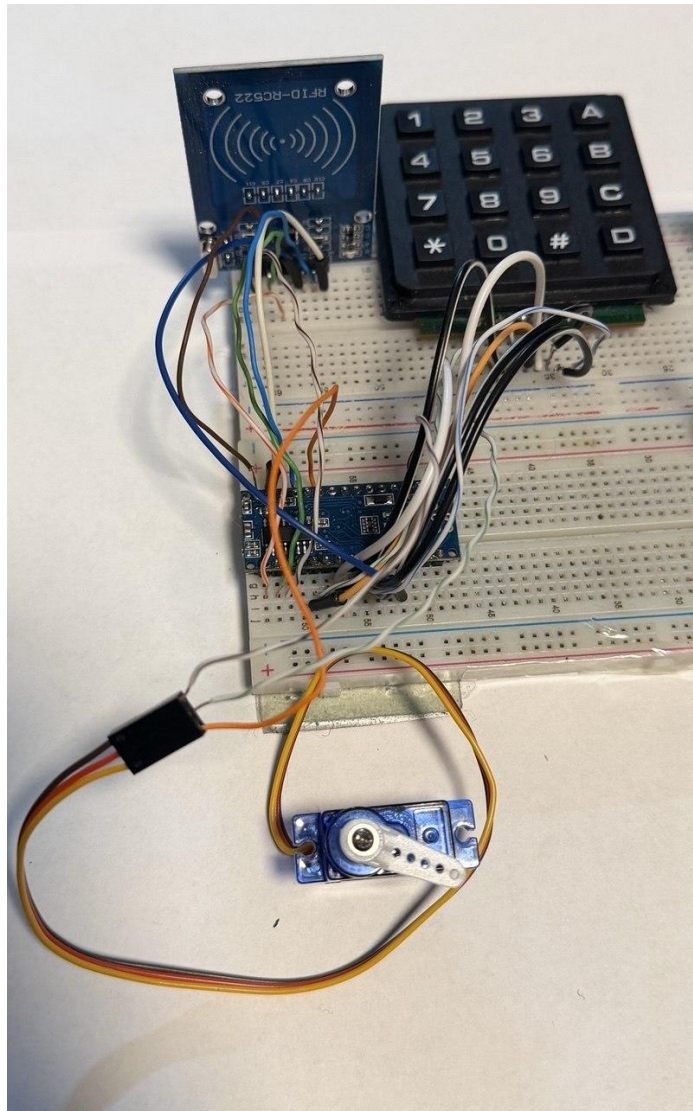


Рисунок 3.7 – Фізичне підключення компонентів 3 зони

Наступний крок це процес налагодження та програмування усіх апаратних складових. Щоб усе працювало коректно, слід враховувати умову виконання двофакторного доступу до системи. Для того щоб досягнути бажаного результату, потрібно прописати в коді необхідні функції для мікроконтролерів.

Почнемо зі стану спокою, сервомотор повинен бути запрограмований на 0 градусів, двері де зберігаються ліки закриті. Це реалізована за допомогою кодової частини на рисунку 3.8.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

```
// ===== Стан доступу =====
bool codeAccepted = false;
bool rfidAccepted = false;
```

Рисунок 3.8 – Двері закриті

Наступний етап верифікація, перша перевірка яка потребує введення PIN-коду. Спочатку система чекає, поки я введу пароль. У коді я задала комбінацію 3321AD. Щоб бачити, що кнопки натискаються, я налаштувала вивід паролю зірочками (*), для того щоб пароль залишався прихованим. Коли код введено, треба натиснути решітку (#). Якщо все було введено правильно, то програма це запам'ятовує і дозволяє перейти до наступного кроку - підтвердження за допомогою картки. А якщо випадково натиснути не ту кнопку, можна скинути введення використовуючи зірочкою (*) і почати все спочатку. Весь описаний алгоритм та кодова реалізація наведено на рисунках 3.9. та 3.10.

```
72 // ===== Функція зчитування клавіатури =====
73 void readKeypad() {
74     char key = keypad.getKey();
75     if (!key) return;
76
77     if (!codeAccepted) { // ще не пройдено пароль
78         if (key == '#') { // підтвердити код
79             Serial.println();
80             if (inputCode == correctCode) {
81                 Serial.println("Пароль правильний! Прикладіть карту.");
82                 codeAccepted = true;
83             } else {
84                 Serial.println("Невірний пароль! Спробуйте ще раз.");
85             }
86             inputCode = "";
87         }
88         else if (key == '*') { // скидання вводу
89             inputCode = "";
90             Serial.println("\nВведення скинуто. Введіть пароль заново.");
91         }
92         else {
93             inputCode += key;
94             Serial.print("*");
95         }
96     }
97 }
```

Рисунок 3.9 – Ралізація кодової частини

```
Message (Enter to send message to 'Arduino Nano')
*****
Пароль правильний! Прикладіть карту.
```

Рисунок 3.10 – Успішна верифікація

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі після введення правильно паролю система надає дозвіл на прикладання картки. Програма аналізує команду з зчитувача картки та чекає на кодову мітку. При піднесені картки, мікроконтролер перетворює унікальний номер у текстовий формат, а потім порівнює його з дозволеним номером у коді. Зчитування та співставлення номеру з кодом на рисунку 3.11.

```
// ===== ДОЗВОЛЕНИЙ UID ТА ПАРОЛЬ =====
String allowedUID = "79CCC801";
String correctCode = "3321AD";
String inputCode = "";

// ===== Функція зчитування RFID =====
void readRFID() {
  if (mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial()) {
    String uid = uidToString(mfrc522.uid);
    Serial.print("Зчитано UID: ");
    Serial.println(uid);

    if (uid == allowedUID) {
      Serial.println("Картка дозволена! Доступ дозволено!");
      openDoor();
    } else {
      Serial.println("Картка не дозволена! Доступ заборонено.");
    }
  }

  // після перевірки карта скидається
  codeAccepted = false;
  mfrc522.PICC_HaltA();
  mfrc522.PCD_StopCrypto1();
}

*****
Пароль правильний! Прикладіть карту.
Зчитано UID: 79CCC801
```

Рисунок 3.11 – Порівняння номеру дозволеної картки

І останнім етапом є відкриття дверей. Якщо і код, і картка правильні, то відбувається відкриття дверей та доступ дозволено. Потім через 10 секунд двері автоматично зачиняються, а система скидає усі дозволи та чекає на повторний вхід.

Результати виконання процесу на рисунку 3.12.

```
Картка дозволена! Доступ дозволено!
Відкриваємо двері...
ДВЕРІ ВІДЧИНЕНО
Закриваємо двері...
ДВЕРІ ЗАЧИНЕНО
```

Рисунок 3.12 – Завершення роботи системи

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Попереднє підключення та налаштування 3 зони показало повну сумісність плати з допоміжними компонентами системи. Успішне тестування показує готовність цієї зони до кріплення на основний стенд СКУД.

3.3. Тестування працездатності розробленого проєкту інтегрованої СКУД.

Після успішної перевірки зони 2 та 3 на макетній платі, можна усі апаратні та виконавчі механізми вбудовувати на остаточний стенд. Самим першим, що слід було прикріпити, це камера відеоспостереження, яка відповідає за 1 зону, реєстрація, мінімальний захист. Встановлення камери дуже просте та зайняло найменше часу. Ось приклад готової зони, який представлено на рисунку 3.13.



Рисунок 3.13 – Готова 1 зона

Коли камеру встановлено, я підключила її за допомогою спеціального програмного забезпечення 360 EyeS (рисунок 3.14.), яке призначене спеціально для хмарного моніторингу в реальному часі. В програмі я виконала налаштування базових потреб, таких як:

- Синхронізація з пристроєм;
- Максимальна якість відео;

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

- Фіксування руху;
- Безперервний запис та зберігання даних;
- Нічний режим.

Налаштування дозволило камері працювати стабільно та безперебійно, що можна побачити на рисунку 3.15.

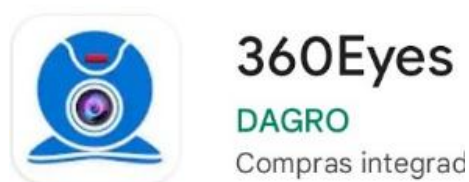


Рисунок 3.14 – ПЗ 360 EyeS



Рисунок 3.15 – Готовність камери спостереження до роботи

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі я прикріпила 2 та 3 зони на стенд. Для прикріплення зчитувачів карток та матричної клавіатури, я вирішила використати вирізані дощечки на які кріпила усі компоненти системи. Також, було надруковано двері на 3D принтері, для кращого вигляду. В завершенні все необхідне обладнання було зафіксоване на стенді (рисунки 3.16 та 3.17, 3.18 та 3.19, 3.20).



Рисунок 3.16 – Підготовлений варіант стенду



Рисунок 3.17 – Повністю готова 2 зона

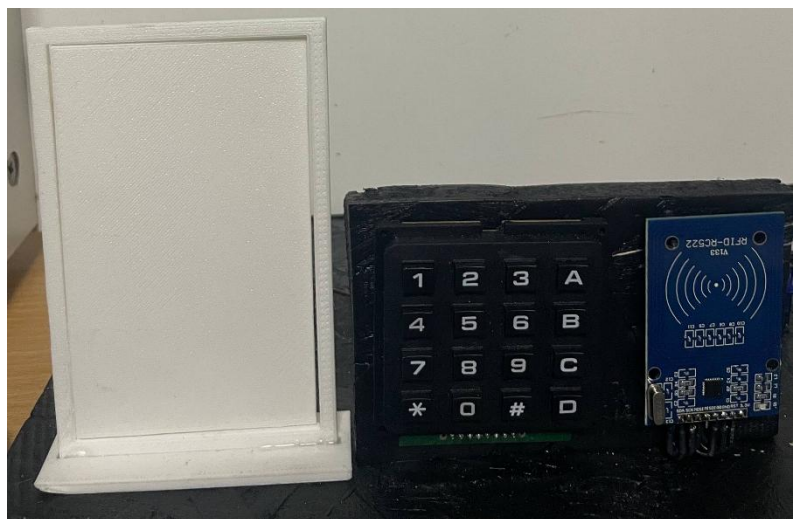


Рисунок 3.18 - Повністю готова 3 зона



Рисунок 3.19 – Готова інтегрована система управління контролем

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				53
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.20 - Готова інтегрована система управління зверху

Перейдемо до тестування інтегрованої системи контролю доступом.

Спочатку перевіримо роботу системи безпеки з середнім захистом, а саме вхід до кабінету лікаря. Тут буде представлень функціонал роботи відкриття та закриття дверей, а також одразу показано як ці данні передаються до 4 зони. Так званого ІТ-відділу.

Початкове підключення системи на рисунках 3.21. та 3.22.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

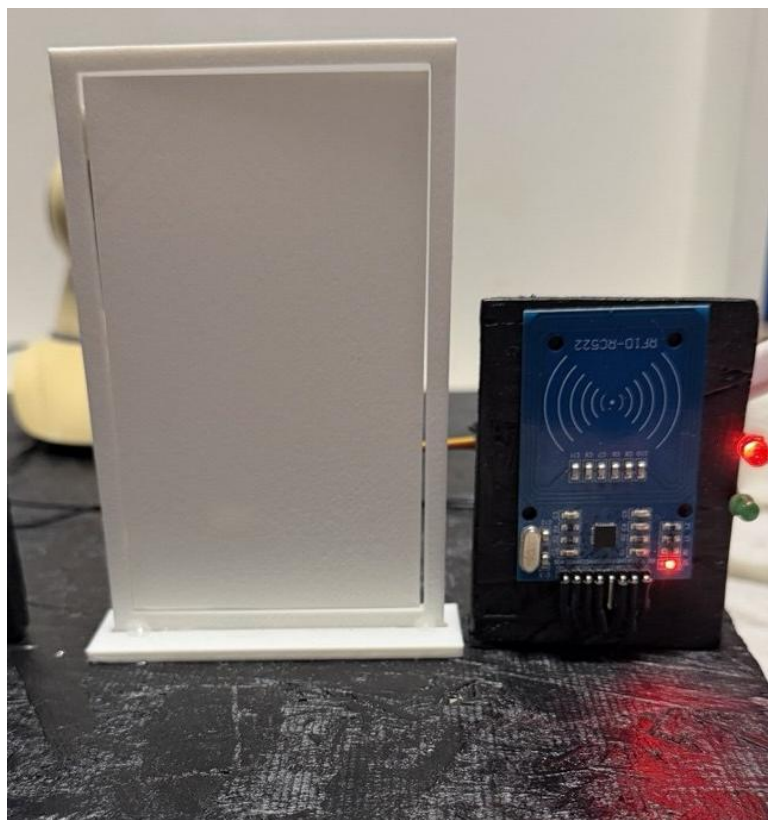


Рисунок 3.21 – Система готова до роботи

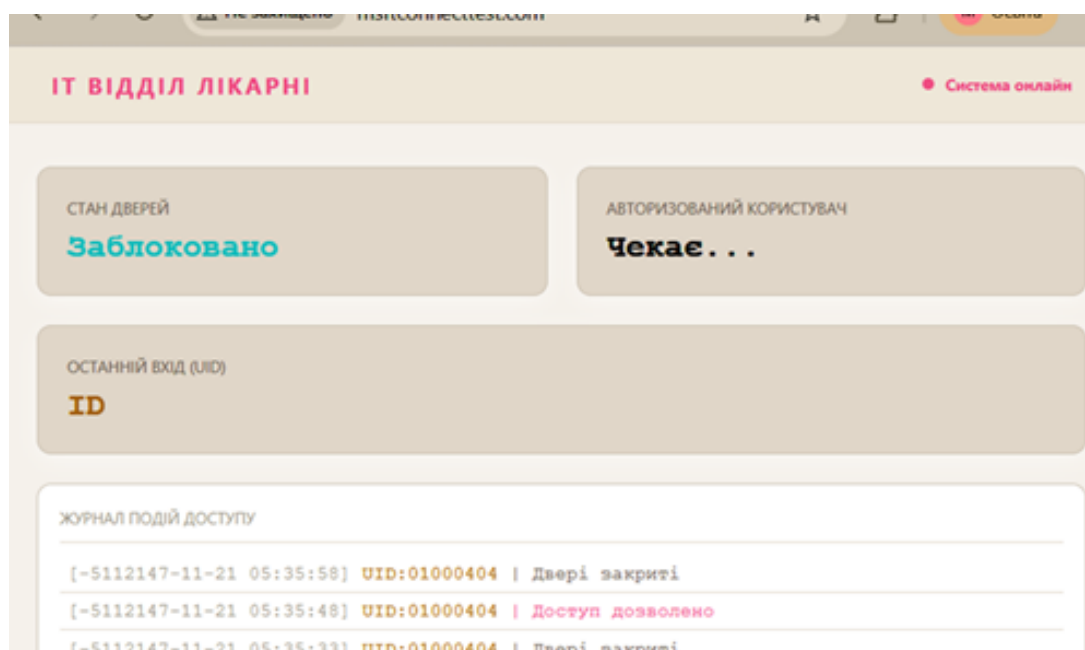


Рисунок 3.22 – Інформація на вебінтерфейсі

Наступний тест це піднесення картки до зчитувача та відображення інформації про дію у вебінтерфейсі системи, рисунки 3.23. та 3.24.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				55
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.23 – Прикладання картки

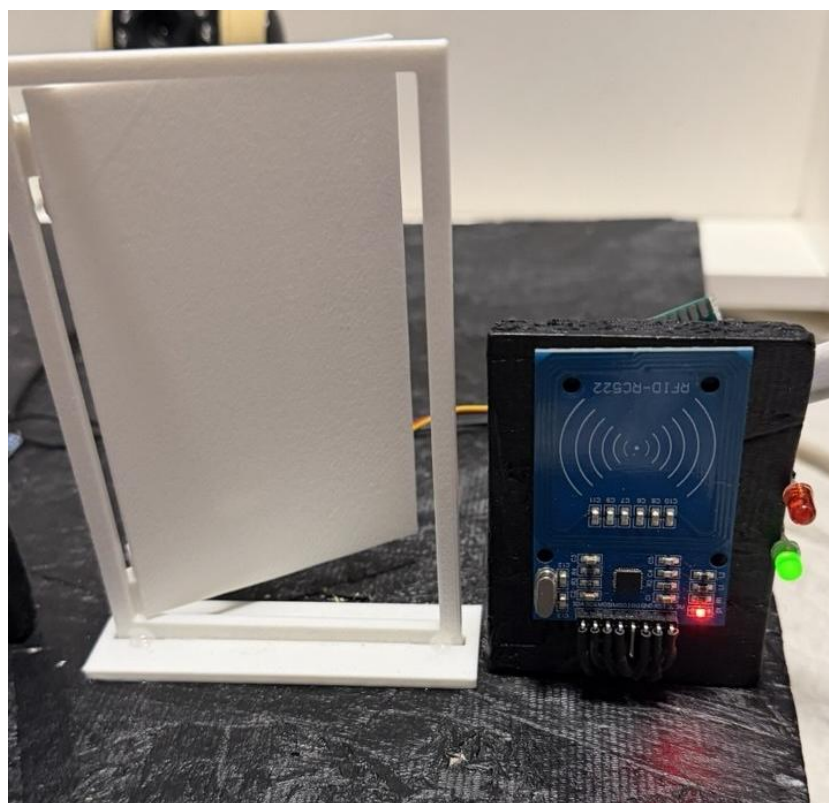


Рисунок 3.24 – Відкриття дверей

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

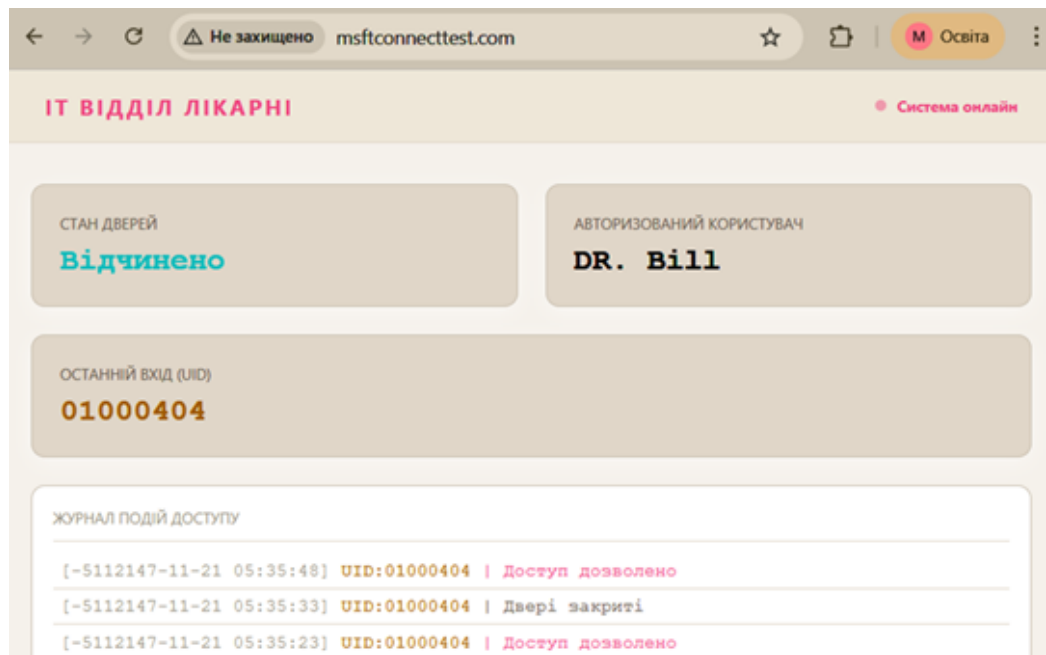


Рисунок 3.25 – Відображення у вебінтерфейсі, доступ дозволено

Після тестування роботи системи можна зробити висновки, що 2 зона , а також інтегрований вебінтерфейс 4 зони працюють відповідно до поставлених вимог та без дефектів. Усі входи та виходи автоматично записуються у журналі подій, що допоможе при необхідності звірити записи входів співробітників з камерами відеоспостереження, у реальному часі.

Тепер почнемо тестувати 3 зону, в якій зберігаються ліки та наркотичні речовини. Тут, як раніше було зазначено функціоніє двоетапна перевірка, спочатку потрібно ввести секретний код, а потім для завершення перевірки підтвердити вхід за допомогою магнітної мітки. (рисунок 3.26.)

Перевірка працездатності була здійснена за допомогою вбудованого Serial Monitor програмного забезпечення Arduino IDE (рисунок 3.27.).

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				57
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.26 – Готовність 3 зони

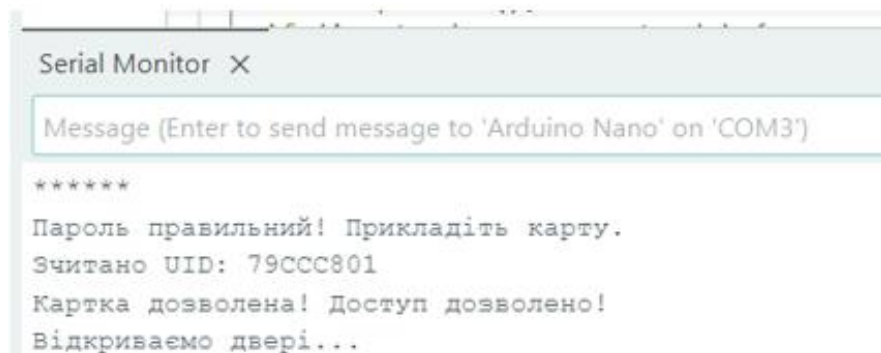


Рисунок 3.27 - Відображення введеної інформації

Коли система розуміє, що пароль та магнітна мітка правильні на екрані пишеться картка правильна, доступ дозволено і двері відчиняються (рисунок 3.28.)

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				58
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.28 – Особу підтверджено, двері відчинено

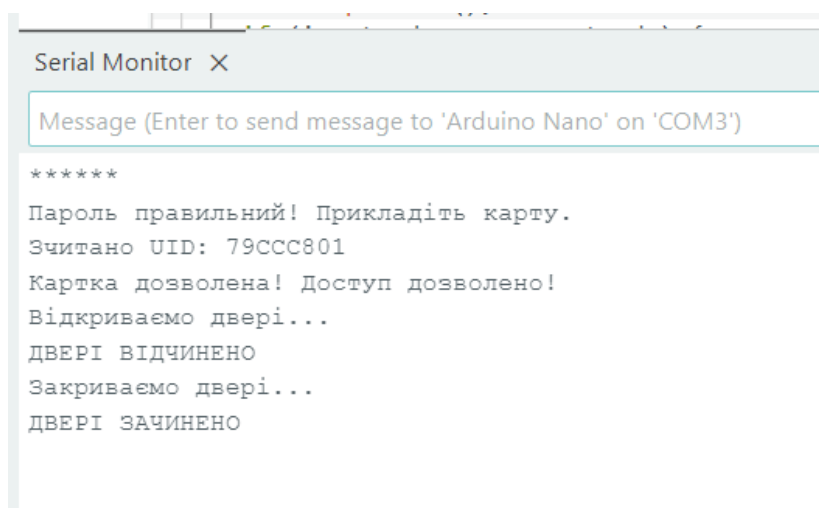


Рисунок 3.29 – Фінальний результат виведення інформації

Тестування системи в режимі виявлення несанкціонованого доступу.

Також, в 2 та 3 зонах, проведено перевірку несанкціонованого доступу до системи. Було використано підроблені та незареєстровані у базі картки, та введення помилкових паролів.

При спробі зайти в 2 зоні за рахунок іншої картки, яка належить персоналу з іншого відділення, система видавала повідомлення, що доступ заборонено, все це повинно буде автоматично повідомлятися співробітникам ІТ-відділу, які далі приймають необхідні заходи безпеки (рисунок 3.30).

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

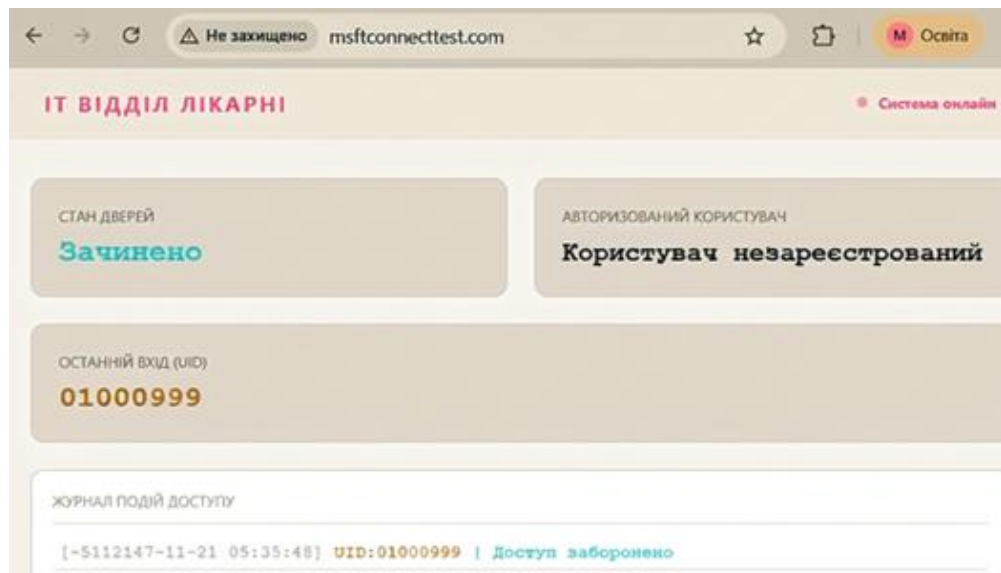


Рисунок 3.30 - Спроба несанкціонованого доступу до 2-ї зони

Під час тестування 3 зони, яка має найвищий пріоритет секретності в медичному закладі, було проведено комплексну перевірку двофакторної автентифікації. Спочатку було змодельовано ситуацію, коли зломисник намагався підібрати пароль на кодовій клавіатурі. Оскільки комбінація виявилася невірною, система заблокувала подальший розпізнавальний цикл і навіть не дозволила зчитувати картку. Також виконано перевірку системи коли пароль вірний, а картка ні, доступ було заборонено і вся інформація занесена до журналу подій. Результати тестування наведенно на рисунках 3.31 та 3.32.

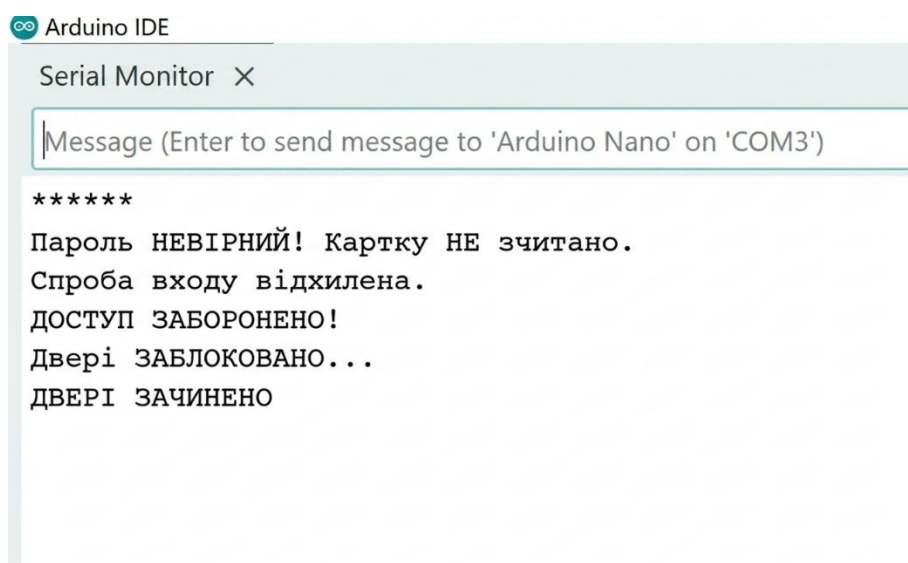


Рисунок 3.31 – Спроба введення неправильного паролю

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

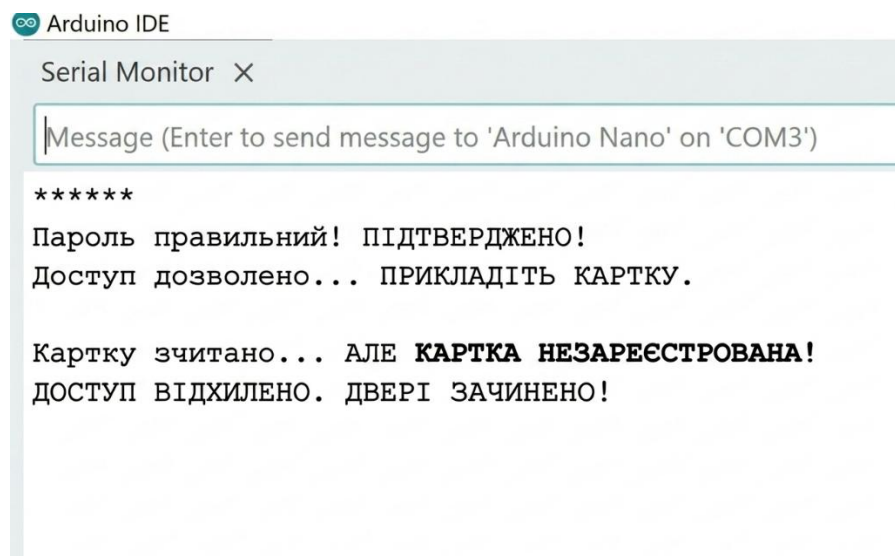


Рисунок 3.32 – Введення правильного паролю та картки з іншого відділу

Отже, результати комплексного тестування підтвердили, що інтегрована СКУД відповідає поставленим вимогам технічного завдання. Система забезпечує розмежування прав доступу, а також гарантує прозорий дистанційний контроль за станом безпеки медичного закладу в режимі реального часу.

Висновки до третього розділу: у третьому розділі проведено повне налаштування, прикріплення та тестування усіх компонентів системи управління доступом.

На початковому етапі було проведено тестування другої та третьої зон на макетній платі. Це дозволило переконатися у коректній роботі мікроконтролерів, з допоміжними елементами системи та налагодити їх функціонування за допомогою розроблення програмного коду.

У процесі виконання, успішно реалізовано функціонал вебінтерфейсу для IT-відділу, який надає інформацію про стан дверей та журнал подій. Крім того, налагоджено надійний механізм двофакторного доступу до місця зберігання ліків, що вимагає введення PIN-коду та прикладання картки для активації сервомотора, який відчиняє двері.

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

Після всіх необхідних перевірок роботи компонентів, було виконано їх прикріплення на основний стенд. В першій зоні підключено камеру відеоспостереження та налаштовану на постійну роботу з датчиком руху та високою якістю зображення через додаток 360 EyeS. Решту зон було перенесено з макетних плат на інтегрований стенд, а також для візуальної демонстрації роздруковано за допомогою 3D принтера двері.

Комплексне тестування готового стенду показало, що всі компоненти СКУД працюють злагоджено, як і повинно бути. Система забезпечує передачу даних про вхід співробітників на вебінтерфейс, стабільну роботу сервомоторів та блокування при фіксації спроб несанкціонованого доступу. Розроблений демонстраційний стенд повністю готовий до захисту приміщень медичного закладу.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

Під час виконання кваліфікаційної роботи проведено детальний аналіз вимог до безпеки медичних закладів, принципів розмежування доступу, а також сучасних методів ідентифікації користувачів у системах контролю та управління доступом. Досліджено характеристики мікроконтролерів і периферійного обладнання, які можуть бути залучені для створення інтегрованих безпекових систем.

Під час виконання роботи обґрунтовано технічне завдання та спроектовано структуру інтегрованої системи контролю та управління доступом для медичного закладу. Система поділена на кілька зон безпеки з відповідними рівнями захисту та методами автентифікації. Для кожної зони визначено специфічний спосіб контролю доступу, враховуючи важливість приміщень.

Окрім цього, побудовано та проаналізовано модель можливих загроз для системи. Розглянуто різні типи потенційних порушників, зокрема зовнішніх осіб, внутрішніх користувачів та осіб із адміністративними привілеями. Це дозволило ідентифікувати потенційні ризики та врахувати їх при проектуванні системи та виборі засобів захисту.

Основою демонстраційного стенду стали мікроконтролери Arduino Nano та Wemos D1 mini, на базі яких реалізовано роботу всієї системи. Також було застосовано і додаткові елементи: зчитувачі карток, матрична клавіатура, сервопривід та світлодіодні індикатори для наглядності. Програмні забезпеченням обрано середовище Arduino IDE із застосуванням спеціалізованих бібліотек для інтеграції апаратних компонентів. Для функціоналу віддаленого моніторингу реалізовано web-сервер із можливістю ведення журналу подій.

У ході виконання проекту створено демонстраційний стенд системи, налаштовано програмне забезпечення, написано код для мікроконтролерів і проведено тестування на рівні кожної окремої зони. Після успішного тестування весь комплексний підхід був перевірений і підтверджений у режимі інтегрованої роботи.

Результатом виконаної роботи стало створення демонстраційного стенду інтегрованої системи контролю та управління доступом для медичних закладів

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

на основі мікроконтролерів Arduino Nano та Wemos D1 mini. Експериментальне тестування показало її повну функціональність і готовність до практичного використання.

Підсумовуючи, у результаті виконання поставленого завдання на кваліфікаційну роботу, створено працездатний демонстраційний стенд інтегрованої системи контролю та управління доступом до медичного закладу. Розроблена система забезпечує багаторівневий захист приміщень, контроль доступу персоналу, а також журналювання подій відповідно до різних рівнів безпеки. Усі поставлені завдання виконано, а створений стенд має можливість для подальшого вдосконалення та інтеграції нових технологій у майбутньому.

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Біометрична система контролю доступу для закладів охорони здоров'я. *Suprema Україна*. Режим доступу: <https://supremainc.com.ua/galuzevi-rishennja-suprema/biometrychna-systema-kontrolju-dostupu-dlja-zakladiv-ohorony-zdorovja/>
2. Radio Frequency Identification (RFID) in Medical Devices. *U.S. Food and Drug Administration (FDA)*. Режим доступу: <https://www.fda.gov/radiation-emitting-products/electromagnetic-compatibility-emc/radio-frequency-identification-rfid>
3. RFID Medical Access Control Application. *Pongee Industries Co., Ltd.* Режим доступу: <https://www.pongee.com.tw/en/news-detail/rfid-medical-access-control-application/>
4. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 р. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR). Режим доступу: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
6. Встановлення драйверу CH340 для плат Arduino. *ArduinoKit*. Режим доступу: <https://arduinokit.com.ua/ua/a462945-ustanovka-drajvera-ch340.html>
7. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист приватності. Системи управління інформаційною безпекою. Режим доступу: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf
8. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection –Information Security Controls. Режим доступу: <https://www.nsai.ie/certification/management-systems/iso-iec-27001-information-security-management-system/iso-iec-270022022/>
9. Системи тривожної сигналізації та електронні системи безпеки. Частина 11-1. Електронні системи контролю доступу. Вимоги до компонентів та систем. Київ. ДП «УкрНДНЦ», 2017. 48 с. Режим доступу: https://online.budstandart.com/ua/catalog/doc-page?id_doc=68249

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

10. WEMOS D1 mini — ESP8266 Board. Official Documentation and Hardware Specification. *WEMOS Electronics*. Режим доступу: https://www.wemos.cc/en/latest/d1/d1_mini.html
11. MFRC522 Standard Performance MIFARE and NTAG Frontend. Product Data Sheet. Rev. 3.9. *NXP Semiconductors*, 2016. 95 p. Режим доступу: <https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf>
12. Arduino IDE 2.x Documentation. Getting Started with Arduino Software. *Arduino CC*. Режим доступу: <https://docs.arduino.cc/software/ide-v2>
13. MFRC522 Library for Arduino. GitHub Repository. *Miguel Balboa*. Режим доступу: <https://github.com/miguelbalboa/rfid>
14. RAIN RFID, UHF RFID, EPC RFID, ... – Confused by the Different Names? *Voyantic*. Режим доступу: <https://voyantic.com/blog/posts/rfid-rain-rfid-uhf-rfid-epc-rfid-confused/>
15. Arduino Keypad Library Tutorial. *Arduino CC*. Режим доступу: <https://docs.arduino.cc/built-in-examples/unused/Keypad/>
16. Access Control Systems and Video Integration Solutions. *Bosch Security and Safety Systems*. Режим доступу: <https://www.boschsecurity.com/xc/en/solutions/access-control-systems/>
17. STM32 Microcontrollers. *STMicroelectronics*. Режим доступу: <https://www.st.com/en/microcontrollers-microprocessors/stm32-32-bit-arm-cortex-mcus.html>
18. LM2596 SIMPLE SWITCHER Power Converter Series 150-kHz 3-A Step-Down Voltage Regulator. Datasheet. *Texas Instruments Incorporated*, 2020. 33 p. Режим доступу: <https://www.ti.com/lit/ds/symlink/lm2596.pdf>
19. Using Servos with Arduino Microcontrollers. *Adafruit Learning System*. Режим доступу: <https://learn.adafruit.com/adafruit-motor-shield-v2-for-arduino/using-rc-servos>
20. ESP8266 WiFi Wi-Fi library for Arduino. ESP8266 Arduino Core Documentation. Режим доступу: <https://arduino-esp8266.readthedocs.io/en/latest/esp8266wifi/readme.html>

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				66
Змн.	Арк.	№ док.м.	Підпис	Дата		

21. ATmega640/1280/1281/2560/2561 Режим доступу: https://theswissbay.ch/pdf/Datasheets/Atmel/Atmel-2549-8-bit-AVR-Microcontroller-ATmega640-1280-1281-2560-2561_Summary.pdf
22. Інструкції та посібники користувача з Arduino Manuals+. Режим доступу: <https://uk.manuals.plus/category/arduino>
23. Управління ризиками під час впровадження інформаційних систем та технологій. Режим доступу: <https://moz.gov.ua/uk/upravlinnya-rizikami-pid-chas-vprovadzhennya-informacijnih-sistem-ta-tehnologij>
24. Моделі загроз та моделі порушників. Режим доступу: https://e-tk.lntu.edu.ua/pluginfile.php/25376/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2017.pdf

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Лістинг програмної реалізації 2 зона

```

#include <SPI.h>
#include <MFRC522.h>
#include <ESP8266WiFi.h>
#include <ESP8266WebServer.h>
#include <DNSServer.h>
#include <NTPClient.h>
#include <WiFiUdp.h>
#include <Servo.h>
#include <time.h>

// ===== НАЛАШТУВАННЯ WIFI =====
const char* wifiSSID = "Xiaomi_961C";
const char* wifiPassword = "00000000";

const char* apSSID = "SECURITY_SERVER_HUB";
const char* apPassword = "12345678";

// ===== НАЛАШТУВАННЯ ДОСТУПУ ДО САЙТУ =====
const char* webUser = "admin";
const char* webPassword = "hospital123";

// ===== ПЕРИФЕРІЯ =====
#define SS_PIN 4
#define RST_PIN 5
#define SERVO_PIN 2
#define RED_LED 0
#define GREEN_LED 16

MFRC522 mfrc522(SS_PIN, RST_PIN);
Servo doorServo;
WiFiUDP ntpUDP;
NTPClient timeClient(ntpUDP, "pool.ntp.org", 2 * 3600, 60000);
ESP8266WebServer server(80);
DNSServer dnsServer;

// ===== ДАНІ ТА СТАН =====
byte allowedUID[] = {0x01, 0x00, 0x04, 0x04};
String lastUID = "NONE";
String lastUser = "WAITING...";
String doorStatus = "LOCKED";
String logEntries = "";

unsigned long doorCloseTime = 0;
const unsigned long doorOpenDuration = 10000;

bool errorState = false;
unsigned long errorStart = 0;
int errorCount = 0;
const int errorMax = 2;
const unsigned long errorInterval = 200;

// ===== ФУНКЦІЯ ОТРИМАННЯ ЧАСУ =====
String getDateTime() {
    // Оновлюємо клієнт
    timeClient.update();
    unsigned long epochTime =
        timeClient.getEpochTime();

    if (epochTime < 100000) {
        return "NTP SYNC...";
    }

    struct tm *ptm = gmtime((time_t *)&epochTime);

    int year = ptm->tm_year + 1900;
    int month = ptm->tm_mon + 1;
    int day = ptm->tm_mday;
    int hour = ptm->tm_hour;
    int minute = ptm->tm_min;
    int second = ptm->tm_sec;

    char buffer[25];
    sprintf(buffer, "%04d-%02d-%02d %02d:%02d:%02d",
        year, month, day, hour, minute, second);

    return String(buffer);
}

// ===== ЛОГУВАННЯ ПОДІЙ =====
void addLog(String uid, String userStatus, String color = "#10b981") {
    String entry = "<div style='font-family: \"Courier New\", monospace; font-size: 13px; padding: 5px; border-bottom: 1px solid #1f2937;'>";
    entry += "<span style='color: #6b7280;'>[" + getDateTime() + "]</span> ";
    entry += "<span style='color: #60a5fa;'>UID: " + uid + "</span> ";
    entry += "<span style='color: " + color + ";'> | " + userStatus + "</span>";
    entry += "</div>";
    logEntries = entry + logEntries;
}

// ===== ГЕНЕРАЦІЯ САЙТУ =====
String makePage() {
    String statusColor = (doorStatus == "Відкрито") ? "#10b981" : "#ef4444";

    String page = "<!DOCTYPE html><html lang='uk'><head><meta charset='UTF-8'>";
    page += "<meta http-equiv='refresh' content='3'>";
    page += "<meta name='viewport' content='width=device-width, initial-scale=1.0'>";
    page += "<title>Обласна лікарня</title>";
    page += "<style>";
    page += "body { font-family: 'Segoe UI', sans-serif; background: #0a0e14; color: #d1d5db; margin: 0; }";
    page += "header { background: #111827; padding: 15px 30px; display: flex; justify-content: space-between; align-items: center; border-bottom: 1px solid #1f2937; }";
    page += "h1 { font-size: 16px; color: #10b981; margin: 0; text-transform: uppercase; letter-spacing: 2px; }";
    page += ".live { display: flex; align-items: center; font-size: 11px; color: #10b981; font-weight: bold; }";

```

		Ніколаєнко М.В.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

    page += ".dot { height:8px; width:8px;
background:#10b981; border-radius:50%; margin-
right:8px; animation: blink 1.2s infinite; }";
    page += "@keyframes blink { 0%, 100% { opacity:1;
} 50% { opacity:0.3; } }";
    page += ".container { max-width: 800px; margin: 30px
auto; padding: 0 20px; }";
    page += ".grid { display: grid; grid-template-columns:
1fr 1fr; gap: 20px; margin-bottom: 20px; }";
    page += ".card { background:#1f2937; padding:20px;
border-radius:10px; border:1px solid #374151; box-
shadow: 0 4px 15px rgba(0,0,0,0.5); }";
    page += ".card-title { font-size:11px; color:#9ca3af;
text-transform:uppercase; margin-bottom:8px; }";
    page += ".value { font-family: 'Courier New',
monospace; font-size:22px; color:#fff; font-
weight:bold; }";
    page += ".log-container { background:#000;
border:1px solid #374151; border-radius:10px;
padding:15px; height:350px; overflow-y:auto; }";
    page += "::-webkit-scrollbar { width:6px; } ::-webkit-
scrollbar-thumb { background:#374151; border-
radius:10px; }";
    page += "</style></head><body>";

    // Шапка сайту
    page += "<header><h1>ІТ відділ лікарні</h1>";
    page += "<div class='live'><span
class='dot'></span>Система онлайн</div></header>";

    page += "<div class='container'>";

    // Сітка з картками
    page += "<div class='grid'>";
    page += "<div class='card'><div class='card-
title'>Стан дверей</div><div class='value'
style='color:" + statusColor + ">" + doorStatus +
"</div></div>";
    page += "<div class='card'><div class='card-title'>Ав-
торизований користувач</div><div class='value'>" +
lastUser + "</div></div>";
    page += "</div>";

    // Картка останнього сканування
    page += "<div class='card' style='margin-
bottom:20px;'><div class='card-title'>Останній вхід
(Uid)</div><div class='value' style='color:#60a5fa;'>"
+ lastUID + "</div></div>";

    // Журнал подій
    page += "<div class='log-container'><div class='card-
title' style='color:#6b7280; border-bottom:1px solid
#1f2937; padding-bottom:10px;'>Журнал подій дос-
тупу</div>";
    page += logEntries;
    page += "</div>";

    // Підвал
    page += "<p style='text-align:center; font-size:11px;
color:#4b5563; margin-top:20px;'>Дата сервера: " +
getDate() + " | Версія 2.4.1</p>";
    page += "</div></body></html>";

```

```

    return page;
}

// ===== ЛОГІКА ДВЕРЕЙ =====
void openDoor(String uid) {
    digitalWrite(REDD_LED, LOW);
    digitalWrite(GREEN_LED, HIGH);
    doorServo.write(180);
    doorStatus = "Відчинено";
    lastUID = uid;
    lastUser = "DR. Bill";
    addLog(uid, "Доступ дозволено", "#10b981");
    doorCloseTime = millis() + doorOpenDuration;
}

void closeDoor() {
    digitalWrite(GREEN_LED, LOW);
    digitalWrite(REDD_LED, HIGH);
    doorServo.write(0);
    doorStatus = "Заблоковано";
    addLog(lastUID, "Двері закриті", "#9ca3af");
    lastUID = "ID";
    lastUser = "Чекає...";
    doorCloseTime = 10;
}

void setup() {
    Serial.begin(115200);
    SPI.begin();
    mfrc522.PCD_Init();
    pinMode(REDD_LED, OUTPUT);
    pinMode(GREEN_LED, OUTPUT);
    doorServo.attach(SERVO_PIN);
    closeDoor();

    WiFi.mode(WIFI_AP_STA);
    WiFi.begin(wifiSSID, wifiPassword);
    while (WiFi.status() != WL_CONNECTED) {
        delay(500); Serial.print(".");
    }

    timeClient.begin();
    WiFi.softAP(apSSID, apPassword);
    dnsServer.start(53, "*", WiFi.softAPIP());

    server.on("/", []() {
        if (!server.authenticate(webUser, webPassword))
            return server.requestAuthentication();
        server.send(200, "text/html", makePage());
    });

    server.onNotFound([]() {
        server.sendHeader("Location", "/", true);
        server.send(302, "text/plain", "");
    });

    server.begin();
    Serial.println("\nSystem Ready");
}

void loop() {
    dnsServer.processNextRequest();
    server.handleClient();
}

```

		Ніколаєнко М..В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```

        if (mfrc522.PICC_IsNewCardPresent() &&
mfrc522.PICC_ReadCardSerial()) {
            String uid = "";
            for (byte i = 0; i < mfrc522.uid.size; i++) {
                uid += (mfrc522.uid.uidByte[i] < 0x10 ? "0" : "") +
String(mfrc522.uid.uidByte[i], HEX);
            }
            uid.toUpperCase();

            bool allowed = true;
            for (byte i = 0; i < 4; i++) { if (mfrc522.uid.uidByte[i]
!= allowedUID[i]) allowed = false; }

            if (allowed) {
                openDoor(uid);
            } else {
                lastUser = "Неавторизований";
                lastUID = uid;
                addLog(uid, "Доступ заборонено", "#ef4444");
                errorState = true;
                errorStart = millis();
                errorCount = 0;
            }
            mfrc522.PICC_HaltA();
        }

        if (doorCloseTime > 0 && millis() > doorCloseTime)
closeDoor();

        if (errorState && millis() - errorStart >= errorInterval)
        {
            digitalWrite(RED_LED, !digitalRead(RED_LED));
            errorStart = millis();
            if (++errorCount >= 6) { digitalWrite(RED_LED,
HIGH); errorState = false; }
        }
    }
}

```

Лістинг програмної реалізації 3 зона

```

#include <SPI.h>
#include <MFRC522.h>
#include <Keypad.h>
#include <Servo.h>

// ===== RFID =====
#define SS_PIN 10
#define RST_PIN 0
MFRC522 mfrc522(SS_PIN, RST_PIN);

// ===== КЛАВІАТУРА 4x4 =====
const byte ROWS = 4;
const byte COLS = 4;
char keys[ROWS][COLS] = {
    {'1','2','3','A'},
    {'4','5','6','B'},
    {'7','8','9','C'},
    {'*','0','#','D'}
};
byte rowPins[ROWS] = {2,3,4,5};
byte colPins[COLS] = {6,7,8,9};
Keypad keypad = Keypad(makeKeymap(keys),
rowPins, colPins, ROWS, COLS);

```

```

// ===== Сервопривід =====
#define SERVO_PIN A2
Servo doorServo;

// ===== ДОЗВОЛЕНИЙ UID ТА ПАРОЛЬ =====
String allowedUID = "79CCC801";
String correctCode = "3321AD";
String inputCode = "";

// ===== Стан доступу =====
bool codeAccepted = false;
bool rfidAccepted = false;

// ===== Таймер для дверей =====
unsigned long doorEndTime = 0;
const unsigned long doorDuration = 10000; // 10 се-
кунд

void setup() {
    Serial.begin(115200);
    SPI.begin();
    mfrc522.PCD_Init();
    Serial.println("Система доступу готова. Введіть код
на клавіатурі.");

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

String uidToString(MFRC522::Uid uid) {
    String s = "";
    for (byte i = 0; i < uid.size; i++) {
        if (uid.uidByte[i] < 0x10) s += "0";
        s += String(uid.uidByte[i], HEX);
    }
    s.toUpperCase();
    return s;
}

```

```

void loop() {
    readKeypad(); // обробка клавіатури
    if (codeAccepted) readRFID();

    // Таймер для закриття дверей
    if (doorEndTime != 0 && millis() > doorEndTime) {
        closeDoor();
    }

    // ===== Функція зчитування клавіатури =====
    void readKeypad() {
        char key = keypad.getKey();
        if (!key) return;

        if (!codeAccepted) { // ще не пройдено пароль
            if (key == '#') { // підтвердити код
                Serial.println();
                if (inputCode == correctCode) {
                    Serial.println("Пароль правильний! Прикладіть
карту.");
                    codeAccepted = true;
                } else {

```

		Ніколаєнко М..В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```

        Serial.println("Невірний пароль! Спробуйте ще
раз.");
    }
    inputCode = "";
}
else if (key == '*') { // скидання вводу
    inputCode = "";
    Serial.println("\nВведення скинуто. Введіть па-
роль заново:");
}
else {
    inputCode += key;
    Serial.print("*");
}
}
}

// ===== Функція зчитування RFID =====
void readRFID() {
    if (mfrc522.PICC_IsNewCardPresent() &&
mfrc522.PICC_ReadCardSerial()) {
        String uid = uidToString(mfrc522.uid);
        Serial.print("Зчитано UID: ");
        Serial.println(uid);

        if (uid == allowedUID) {
            Serial.println("Картка дозволена! Доступ дозво-
лено!");
            openDoor();
        } else {
        }
    }
}

```

```

        Serial.println("Картка не дозволена! Доступ за-
боронено.");
    }

    // після перевірки карта скидається
    codeAccepted = false;
    mfrc522.PICC_HaltA();
    mfrc522.PCD_StopCrypto1();
}

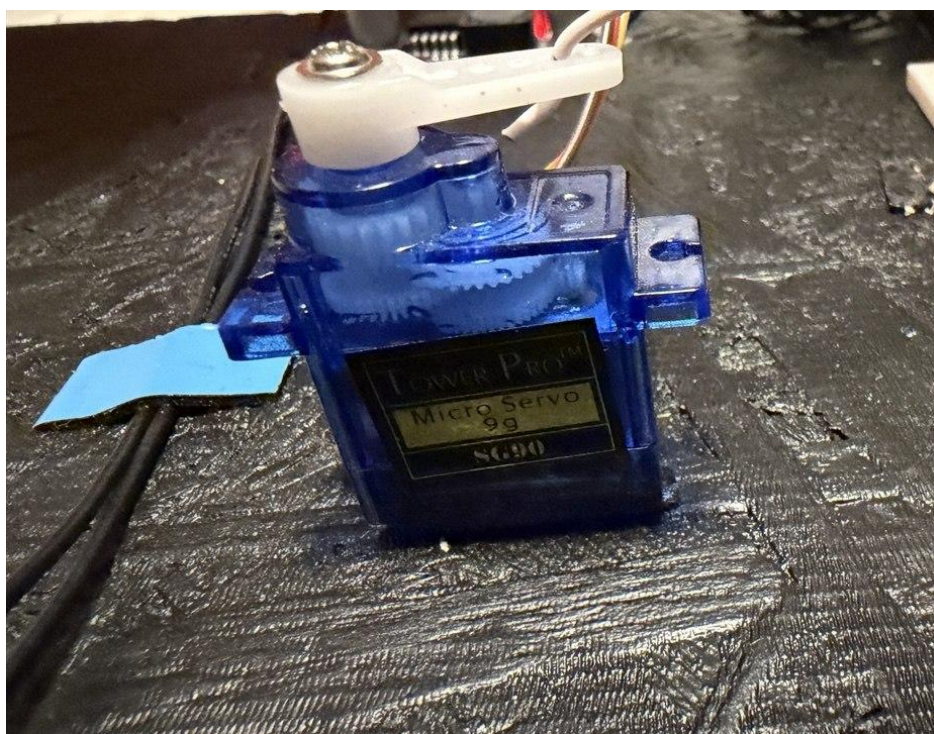
// ===== Функції відкриття/закриття дверей =====
void openDoor() {
    Serial.println("Відкриваємо двері...");
    for (int pos = 0; pos <= 90; pos += 5) {
        doorServo.write(pos);
        delay(20);
    }
    Serial.println("ДВЕРІ ВІДЧИНЕНО");
    doorEndTime = millis() + doorDuration;
}

void closeDoor() {
    Serial.println("Закриваємо двері...");
    for (int pos = 90; pos >= 0; pos -= 5) {
        doorServo.write(pos);
        delay(20);
    }
    Serial.println("ДВЕРІ ЗАЧИНЕНО");
    doorEndTime = 0;
}

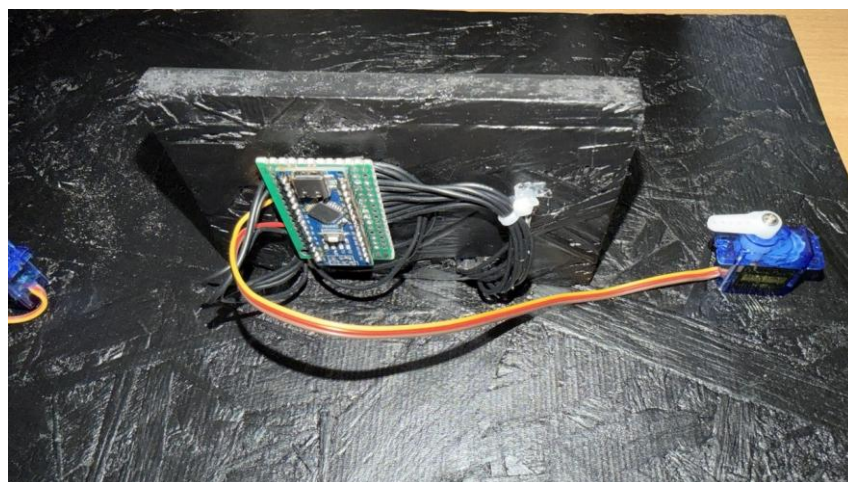
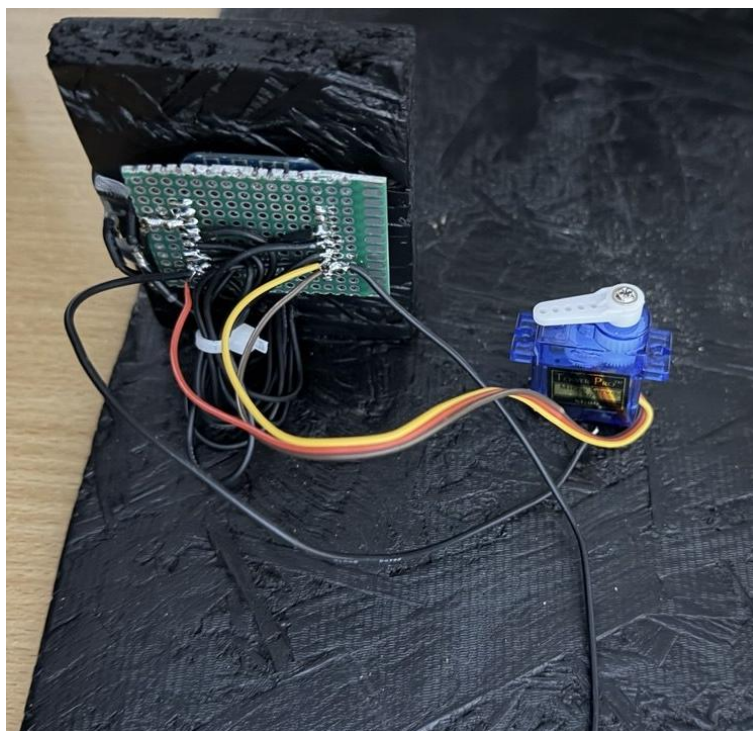
```

		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

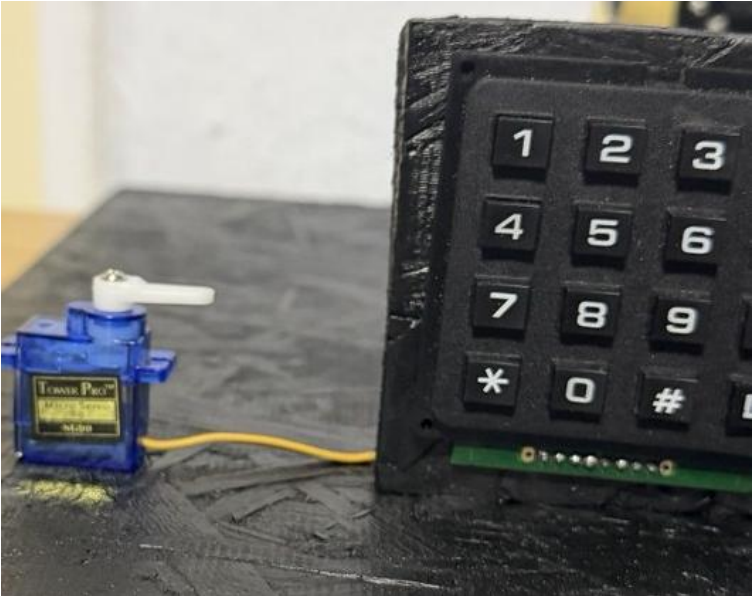
Проміжні етапи розробки стенду



		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				73
Змн.	Арк.	№ докум.	Підпис	Дата		



		Ніколаєнко М., В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				74
Змн.	Арк.	№ докум.	Підпис	Дата		



		Ніколаєнко М.,В			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Шелуха О.О.				75
Змн.	Арк.	№ докум.	Підпис	Дата		