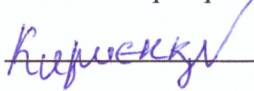


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи контролю та управління дос-
тупом на основі технології RFID»

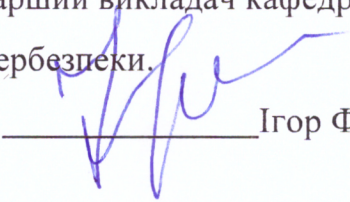
Виконав: студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кіберберзпека»

 Євгеній КИРИЄНКО

Керівник: доцент кафедри комп'ютерної інженерії та кі-
бербезпеки, кандидат технічних наук.

 Олексій ШЕЛУХА

Рецензент: старший викладач кафедри комп'ютерної ін-
женерії та кібербезпеки.

 Ігор ФАЛЬКОВСЬКИЙ

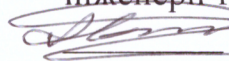
Житомир – 2024

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
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Кириєнко Євгеній Володимирович

Тема роботи: «Проект системи контролю та управління доступом на основі технології RFID»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

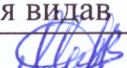
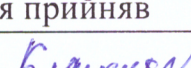
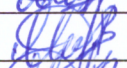
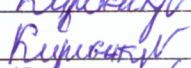
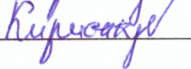
Вихідні дані роботи:

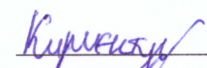
- дослідження та аналіз процесу функціонування систем контролю та управління доступом;
- розробка системи контролю та управління доступом за допомогою технології RFID, та технологія RFID в цілому;

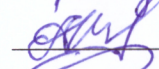
Обладнання та програмне забезпечення:

1. Arduino
2. Модуль RFID RC522

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

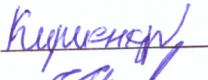
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Маєвський О.В.	11.03.2024 	11.03.2024 
2	Маєвський О.В.	03.04.2024 	03.04.2024 
3	Маєвський О.В.	16.05.2024 	16.05.2024 

Студент  Євгеній КИРИЄНКО

Керівник  Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	07.03.2024	Виконано
2	Аналіз об'єкта дослідження	14.03.2024	Виконано
3	Постановка задачі дослідження	21.03.2024	Виконано
4	Опрацювання літературних джерел	21.04.2024	Виконано
5	Розробка теоретичного макету	28.04.2024	Виконано
6	Пошук та аналіз комплектуючих	10.05.2024	Виконано
7	Вибір набору складових для складання схеми	14.05.2024	Виконано
8	Складання схеми	20.05.2024	Виконано
9	Написання програмного коду	24.05.2024	Виконано
10	Тестування готової системи	27.05.2024	Виконано
11	Оформлення пояснювальної записки	06.06.2024	Виконано
12	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	12.06.2024	Виконано
13	Захист	26.06.2024	Виконано

Студент  Євгеній КИРИЄНКО
 Керівник  Олексій ШЕЛУХА

АНОТАЦІЯ

У кваліфікаційній роботі розглянуто процес побудови та функціонування систем контролю та управління доступом. Проведено аналіз основних складових таких систем, визначено роль та функціональні можливості технології радіочастотної ідентифікації (RFID). Проведено дослідження методів ефективного застосування розглянутих технологій для захисту об'єкта критичної інфраструктури.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків та списку використаної літератури.

Текстова частина кваліфікаційної роботи включає 55 сторінок друкованого тексту. Список використаних джерел складається з 20 найменувань та займає 2 сторінки. У роботі представлено 38 рисунків.

Кваліфікаційна робота містить три розділи. У першому розділі розглянуто основні відомості про технологію RFID її типи та перспективи майбутнього розвитку, проаналізовано вартість та ефективність таких систем. У другому розділі розглянуто технічну та безпекову складову RFID систем, а саме архітектура системи контролю та управління доступом RFID, програмне забезпечення що використовується і також розглянуто безпекову складову в RFID системах. У третьому розділі описано основні моменти практичної розробки проекту, та наведено результати роботи системи в цілому.

Висновок містить в собі результат проведеної роботи, висновки після кожного розділу підсумовують що було проаналізовано в конкретному розділі.

Ключові слова: СКУД, RFID, мітка, зчитувач, контроль доступу, безконтактна ідентифікація, системна контролю та управлінням доступу, радіочастотна ідентифікація, RFID-мітка, RFID-зчитувач, Arduino, ESP8266, релейний модуль Songle, система обміну повідомленнями Telegram.

					KKIKB.KP.B – 125 – 09 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект системи контролю та управління доступом на основі технології RFID	Літ.	Арк.	Аркушів
Розроб.		Кириченко Є. В.		24.06				
Керівник		Шелуха О. О.		24.06			4	61
Реценз.		Фальковський І.		24.06				
Н. контр.		Шелуха О. О.		24.06				
Затверд.		Сфіменко А. А.		24.06		ФІКТ, Гр. КБ-20-2		

ANNOTATION

The qualification work considers the process of building and operating access control and management systems. The main components of such systems are analyzed, the role and functionality of radio frequency identification (RFID) technology are determined. The methods of effective application of the considered technologies for the protection of critical infrastructure are studied.

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

The text part of the qualification work includes 55 pages of printed text. The list of references consists of 20 titles and occupies 2 pages. The work contains 38 figures.

The qualification paper contains three sections. The first chapter discusses the basic information about RFID technology, its types and prospects for future development, analyzes the cost and efficiency of such systems. The second section discusses the technical and security components of RFID systems, namely the architecture of the RFID access control system, the software used, and also considers the security component in RFID systems. The third section describes the main points of the practical development of the project, and presents the results of the system as a whole.

The conclusion contains the result of the work done, and the conclusions after each section summarize what was analyzed in a particular section.

Keywords: ACS, RFID, tag, reader, access control, contactless identification, access control system, radio frequency identification, RFID tag, RFID reader, Arduino, ESP8266, SONGLE relay module, Telegram messaging system.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ОСНОВИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ RFID	10
1.1 Загальні відомості про технологію RFID.....	10
1.2 Принцип роботи RFID-систем.....	12
1.3 Компоненти системи RFID	13
1.4 Типи RFID - міток	14
1.5 Аналіз вартості та ефективності	17
1.6 Майбутнє розвитку RFID	18
РОЗДІЛ 2. СТРУКТУРА ТА БЕЗПЕКА СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПУ НА ОСНОВІ RFID.....	22
2.1 Архітектура системи контролю та управління доступу RFID	22
2.2 Програмне забезпечення у СКУД на основі RFID	24
2.3 Безпека в системах RFID	25
2.4 Загальні відомості про СКУД.....	27
2.5 Порівняння механічних та електронних СКУД.....	30
РОЗДІЛ 3. ПІДБІР ТА АНАЛІЗ КОМПОНЕНТІВ ДЛЯ ПОБУДОВИ, ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА БАЗІ ARDUINO КОМПОНЕНТІВ.....	36
3.1 Підбір та аналіз компонентів для побудови.....	36
3.2 Підключення компонентів та написання коду реалізації системи керування доступом.	43
3.3 Перевірка роботи реалізованої СКУД системи	49
3.4 Пропозиції для подальшого розвитку.....	53
ВИСНОВКИ	55
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	56
ДОДАТКИ	58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СКУД – Система контролю і управління доступом

RFID – Radio frequency identification - радіочастотна ідентифікація

IoT - Internet of Things - Інтернет речей

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

У контексті стрімкої цифровізації сучасного світу, системи контролю та управління доступом набувають все більшої важливості у забезпеченні безпеки та ефективності в широкому спектрі галузей, від офісних просторів до промислових об'єктів. Однією з ключових технологій, яка змінює підходи до контролю доступу, є технологія радіочастотної ідентифікації (RFID). Ця технологія, застосовуючи електронні мітки для збору даних без використання прямого візуального або фізичного контакту, відкриває нові можливості для автоматизації та підвищення безпеки систем контролю доступу.

RFID системи виявились особливо ефективними в управлінні доступом, де необхідна швидкість, точність і гнучкість. Від традиційних ключів та магнітних карт до сучасних RFID рішень, еволюція у цій сфері відображає зростаючу потребу в забезпеченні безпеки та ефективності. RFID технологія, завдяки своїй відносно невисокій вартості, високій надійності та легкості інтеграції з іншими системами, вже знайшла широке застосування в різних секторах.

Метою кваліфікаційної роботи є глибоке дослідження, аналіз та створення систем контролю та управління доступом, заснованих на технології RFID. Це включає в себе розуміння технічних аспектів RFID, вивчення різних типів RFID-систем, аналіз їхньої ефективності, безпеки, та можливих застосувань. Також мета проекту полягає у визначенні спектру використання таких систем, пов'язаних з впровадженням цих систем, а також оцінці їх впливу на безпеку.

Для виконання поставленої мети було сформовано наступні завдання:

1. Провести аналіз існуючих систем та визначити ідеальну для наших цілей.
2. Розробити схему системи контролю та управління доступом.
3. Побудувати програмно-апаратний комплекс системи контролю та управління доступом
4. Провести тестування розробленої системи.

Об'єктом дослідження є процес функціонування систем контролю і управління доступом, що включає в себе фізичні та програмні компоненти, які

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

використовуються для ідентифікації, авторизації, моніторингу та управління доступом до різних об'єктів або просторів.

Предметом дослідження є методи, засоби та технології що використовуються при розробці та при контролі функціонування систем контролю та управління доступом, зокрема технологія RFID.

У процесі виконання кваліфікаційної роботи було розроблено проєкт системи контролю та управління доступом на основі технології RFID.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ОСНОВИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ RFID

1.1 Загальні відомості про технологію RFID

RFID — це технологія автоматичної ідентифікації, яка використовує радіочастотні хвилі для зчитування та передачі даних. Це включає використання транспондерів або міток RFID, які можуть бути вбудовані або прикріплені до предметів для ідентифікації [1].

Технологія RFID (Radio Frequency Identification) знаходить широке застосування в повсякденному житті, часто в місцях та ситуаціях, які ми можемо і не вважати застосуванням цієї технології.

Це може бути пасивний RFID – ключ у вигляді картки:



Рисунок 1.1 – Пасивний RFID – ключ

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

RFID може використовувати у роздрібній торгівлі, це так звані RFID-мітки, що використовуються для відстеження товарів на складі та в магазинах.

Ось так приблизно вона буде виглядати:

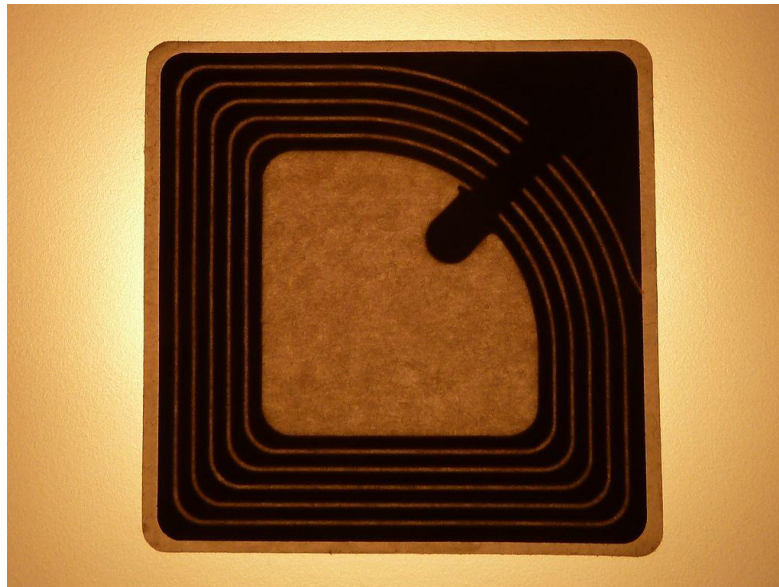


Рисунок 1.2 – Радіомітка на товарах роздрібної торгівлі

Або ось такі браслети, що надають доступ до спортивного залу або басейну:



Рисунок 1.3 – Електронний ключ доступу

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Або це може бути усім нам дуже добре відомий ключ від домофону:



Рисунок 1.4 – RFID-ключ від домофону

Ці приклади показують, що технологія RFID є життєво важливою для багатьох сфер нашого повсякденного життя, часто непомітно покращуючи та спрощуючи процеси та послуги.

1.2 Принцип роботи RFID-систем

Загальний принцип роботи дуже простий у користувача є електронний ключ, може бути у вигляді картки, брелка, тощо. У будівлі куди користувач хоче отримати доступ буде встановлено зчитувач до якого потрібно піднести електронний ключ, після чого буде надано доступ якщо записана ключ ідентифіковано, приклад використання на рисунку нижче [7]:



Рисунок 1.5 – Приклад використання RFID-ключа

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Коли людина наближається до замка з RFID-міткою або карткою, зчитувач RFID створює низькоенергетичне радіочастотне поле. після того, як ви підносите ключ до поля зчитування.[13]

Це поле запускає RFID-мітку. Радіохвилі зчитувача забезпечують енергію для відповіді на пасивну мітку. Активна мітка генерує відповідь самостійно.

RFID-мітка використовує радіохвилі, щоб передати дані (унікальний ідентифікатор) зчитувача.

Зчитувач RFID приймає дані та порівнює їх зі списком дозволених ідентифікаторів, який зберігається в пам'яті замка.

Якщо ідентифікатор, отриманий, відповідає одному з дозволених, замок запустить механізм відкривання.

Коли RFID-мітка або картка отримає дозвіл, електронний механізм замка відкриває замок. Залежно від налаштувань замка він може автоматично закритися після певного періоду часу або коли двері зачинені.

Управління доступом через RFID-замки часто включає можливість дистанційного оновлення списку дозволених ідентифікаторів, забезпечуючи гнучке керування доступом та безпекою.

1.3 Компоненти системи RFID

Система RFID (радіочастотна ідентифікація) складається з декількох ключових компонентів [6].

Ось основні з них:

1. RFID – мітка (тег)

- Мікрочіп: У ньому міститься інформація, включаючи унікальний ідентифікаційний номер. Крім того, цей чіп може мати пам'ять для зберігання додаткових даних.

- Антена: обробляє та передає радіохвилі. Форма та розмір антени залежать від призначення мітки та відстані, на яку має передаватися сигнал.

- Підложка: Матеріал, на якому розміщені мікрочіп та антена.

- Корпус (опціонально): Захищає електронні частини мітки, особливо в умовах, де її можуть фізично пошкодити або агресивне середовище.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

2. RFID-Зчитувач

- Трансівер (Передавач-Приймач): Генерує радіочастотне поле та приймає сигнали від RFID-міток.
- Антена: Використовується для створення радіочастотного поля і для прийому даних від міток.
- Процесор: Обробляє отримані дані, забезпечує управління зчитувачем та комунікацію з зовнішніми системами.
- Інтерфейси зв'язку: Забезпечують з'єднання з іншими системами, такими як комп'ютерні мережі або системи контролю доступу.

3. Програмне Забезпечення

- Програми для обробки даних: Збирають, обробляють та аналізують дані, отримані від RFID-зчитувачів.
- Інтерфейс користувача: Дозволяє користувачам взаємодіяти з системою, налаштовувати параметри, переглядати інформацію тощо.
- Інтеграційні інструменти: Забезпечують інтеграцію з іншими інформаційними системами, наприклад, з системами управління запасами або ERP-системами.

4. Комунікаційна Інфраструктура

- Мережеве обладнання: Забезпечує зв'язок між RFID-зчитувачем та центральною обробкою даних.
- Бездротові та дротові мережі: Забезпечують передачу даних між зчитувачами та серверами або хмарними сервісами.

1.4 Типи RFID - міток

RFID-мітки бувають активними та пасивними. Пасивна мітка RFID отримує енергію від зчитувача, а активна мітка RFID використовує власне живлення. Існують також напівпасивні RFID-мітки, у яких інтегральну схему живить батарея, а зв'язок робить зчитувач.

RFID-мітки зазвичай містять менше 2000 КБ даних, включаючи унікальний ідентифікатор/серійний номер.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Теги доступні тільки для читання або читання/запису, коли зчитувач може додати дані.

RFID-мітки мають різний діапазон зчитування. Ці фактори включають тип тега, тип зчитувача, частоту RFID, перешкоди в навколишньому середовищі та інші RFID-мітки та зчитувачі. Взагалі кажучи, активні та пасивні мітки RFID мають більші відстані зчитування.

RFID-мітки (теги) можна класифікувати за різними критеріями, такими як застосування, тип живлення, частота роботи та пам'ять. Основні види RFID-міток описані нижче [5].

За типом живлення:

- Пасивні - роздрібна торгівля та бібліотеки часто використовують пасивні мітки RFID для відстеження товарів, управління запасами та автоматизації видачі та повернення книг.

Таблиця 1.1

Описова таблиця мітки

Живлення	Не мають власного джерела енергії. отримують енергію від створеного RFID-зчитувачем електромагнітного поля.
Дальність	Обмежена (зазвичай до кількох метрів).
Вартість	Низька, оскільки вони простіші за конструкцією.
Застосування	Широко використовуються в роздрібній торгівлі, управлінні запасами, відстеженні активів тощо.

- Активні мітки застосовуються для відстеження великих активів, таких як транспортні засоби в логістиці та медичне обладнання в лікарнях, яке потребує тривалого зберігання.

Таблиця 1.2

Описова таблиця мітки

Живлення	Мають вбудоване джерело живлення (наприклад, батарею).
Дальність	Більша дальність дії (може сягати сотень метрів).
Вартість	Вища порівняно з пасивними мітками.

Продовження табл. 1.2 – Описова таблиця мітки

Застосування	використовуються для моніторингу великих активів, охорони здоров'я, умов навколишнього середовища та інших цілей.
--------------	---

- Напівпасивні маркування використовуються в ситуаціях, коли потрібна висока точність зчитування, наприклад, для збереження чутливих товарів.

Таблиця 1.3

Описова таблиця мітки

Живлення	Мають власну батарею, але використовують енергію від зчитувача для передачі даних.
Дальність	Покращена дальність і надійність у порівнянні з пасивними мітками.
Вартість	Вища порівняно за рахунок наявності батареї
Застосування	Часто використовуються в ситуаціях, де потрібна висока надійність зчитування, але не потрібна велика дальність, як у активних міток.

За частотою роботи:

Низькочастотні (LF) Мітки (125 - 134 кГц), що працюють на низьких частотах, ідеально підходять для контролю доступу та ідентифікації тварин, оскільки вони добре проникають крізь рідини та органічні матеріали [8]:

- Переваги: Добра проникаюча здатність через рідини і метал.
- Недоліки: Обмежена швидкість передачі даних, менша дальність читання.
- Застосування: Контроль доступу, ідентифікація тварин.

Високочастотні (HF) Мітки (13.56 МГц) часто використовуються в системах безконтактних платежів і бібліотечних системах через їхню здатність до швидкої передачі даних на короткій відстані [4]:

- Переваги: Краща швидкість передачі даних у порівнянні з LF.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Недоліки: Менша проникаюча здатність через метал і рідини.
- Застосування: Бібліотечні книги, бейджі, платіжні системи.

Ультрависокочастотні (UHF) Мітки (865 - 928 МГц) ідеальні для управління запасами і логістики, забезпечуючи швидке зчитування багатьох об'єктів на великій відстані:

- Переваги: Довга дальність читання, висока швидкість передачі даних.
- Недоліки: Низька проникаюча здатність через рідини та метали.
- Застосування: Відстеження запасів, логістика, управління активами.

Мікрохвильові Мітки (2.45 ГГц) використовуються для відстеження транспортних засобів та інших високошвидкісних застосувань завдяки їхній високій швидкості передачі даних і дальності [8]:

- Переваги: Дуже висока швидкість передачі даних, велика дальність.
- Недоліки: Відносно високі витрати, погана проникаюча здатність.
- Застосування: Відстеження транспортних засобів, високошвидкісні додатки.

За типом пам'яті:

Тільки для Читання (Read-Only), зазвичай використовуються для основних ідентифікаційних застосувань, де дані на мітці не потрібно змінювати, як-от в ідентифікаційних бейджах [8]:

- Характеристики: Пам'ять запрограмована на заводі, не може бути змінена.
- Застосування: Ідентифікаційні додатки, де не потрібно змінювати дані.

Читання/Запис (Read/Write) такі підходять для додатків, де інформація на мітці може змінюватися або оновлюватися, як наприклад, у відстеженні активів, що потребують обліку стану або місцезнаходження:

- Характеристики: Дозволяє не тільки читати дані, але й записувати нові дані на мітку.
- Застосування: Застосування, де дані на мітці потребують оновлення або зміни.

1.5 Аналіз вартості та ефективності

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Аналіз вартості та ефективності RFID систем залежить від багатьох факторів, включаючи тип використовуваних міток, обсяг застосування, інфраструктуру та специфіку галузі.

Оскільки вони прості у виробництві та не потребують внутрішніх джерел живлення, пасивні мітки є найдешевшим варіантом. Це робить їх чудовими для масового відстеження товарів, особливо в роздрібній торгівлі, де вони можуть покращити управління запасами та значно зменшити втрати від крадіжок.

Через наявність складнішої електроніки та внутрішнього джерела живлення активні мітки значно дорожчі. Тим не менш, їхня вища ціна виправдана в сферах, де потрібна висока дальність зчитування та підвищена надійність, наприклад, у логістиці великих активів.[15]

Установка та підтримка RFID-систем вимагає придбання зчитувачів, антен, програмного забезпечення та інтеграції до існуючих інформаційних систем. Ці витрати можуть бути значними, але вони часто швидко окупаються завдяки покращенню ефективності, зниженню витрат на працю та покращенню точності управління активами та запасами.

Здатність автоматично збирати великі кількості даних без необхідності ручного сканування є однією з основних характеристик ефективності RFID. Це значно економить час і ресурси в логістиці та складському господарстві. RFID-системи збільшують точність даних, що підвищує загальну ефективність операцій. Це дозволяє компаніям знижувати втрати від помилок у відстеженні активів і управлінні ними.

Однак системи RFID також можуть працювати погано через навколишнє середовище. Це включає перешкоди металу або води, особливо для ультрависокочастотних міток.

Таким чином, системи RFID в значній мірі залежать від умов застосування та їх вартості. Інвестування в RFID-технології дає багато переваг багатьом компаніям через підвищення ефективності, точності та здатності масштабувати операції.

1.6 Майбутнє розвитку RFID

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Майбутнє розвитку RFID технологій передбачається як надзвичайно перспективне та інноваційне. Декілька ключових напрямків, які, як очікується, визначатимуть розвиток цієї технології наведено нижче[10]:

- Зменшення Ціни та Розміру Міток: Якщо ціни та розміри RFID-міток продовжуватимуть знижуватися, вони стануть ще більш доступними та корисними для багатьох цілей, таких як використання в одноразових або невеликих упаковках.
- Покращення дальності та надійності: Технологічні розробки можуть підвищити надійність і дальність читання міток, особливо в складних умовах, як-от у присутності рідин або металів.[16]
- Інтеграція з іншими технологіями: Коли RFID інтегрується з технологіями, такими як Інтернет речей (IoT), штучний інтелект (AI) і хмарні обчислення, ви зможете отримати нові можливості для автоматизації та аналітики в реальному часі.
- Безпека та приватність: Очікується розробка більш надійних методів шифрування та аутентифікації для RFID-міток і систем через зростаючі проблеми конфіденційності та безпеки. Розробка Спеціалізованих Міток: Створення спеціалізованих міток для конкретних галузей, наприклад, міток з датчиками для моніторингу умов зберігання, або міток, оптимізованих для використання в медицині чи агропромисловості.
- Розвиток Стандартів: Уніфікація та розвиток міжнародних стандартів для RFID технологій сприятиме їх ширшому впровадженню та спрощенню міжнародної торгівлі.
- Екологічні Рішення: Розробка екологічно безпечних, біорозкладних або перероблюваних міток, з огляду на зростаючу увагу до екологічних питань.
- Пасивні Мітки з Додатковими Функціями: Розвиток пасивних міток, які можуть виконувати додаткові функції, як-от вимірювання температури або вологості, без потреби в активному джерелі живлення.[18]

У результаті цих змін з'являються нові можливості для оптимізації бізнес-процесів, підвищення ефективності управління активами та забезпечення вищого рівня автоматизації в різних секторах економіки. Підвищення загальної

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

ефективності та зниження витрат, а також нові можливості для створення розумних і інтерактивних товарів і послуг є результатом цих інновацій.

Для створення системи контролю та управління доступом, яка використовує технологію RFID, необхідно виконати низку важливих завдань.

Насамперед система повинна бути ретельно оцінена, враховуючи як функціональні, так і нефункціональні компоненти, а також стандарти безпеки. Далі потрібно розробити план проєкту, який включатиме всі етапи, терміни та осіб, які відповідають за їх виконання.

Зібрані вимоги повинні бути враховані під час проектування архітектури системи, яка включатиме апаратну та програмну складові. визначте необхідне обладнання, таке як сканери RFID, контролери доступу, карти або мітки, а також створіть базу даних, яка зберігатиме важливі дані. Після цього потрібно розробити програмне забезпечення, яке буде керувати доступом і взаємодіяти з RFID-обладнанням. Програма повинна мати можливість записувати події, які були доступні.

Наступним кроком є впровадження апаратного та програмного забезпечення, а також тестування системи на коректність і сумісність. Після інтеграції система повинна бути ретельно протестована в різних режимах роботи, щоб знайти можливі помилки та несправності та виправити їх, щоб зробити роботу ефективнішою.

Завдяки виконанню цих завдань має бути створена система управління та контролю доступу на основі RFID, яка відповідатиме визначеним вимогам.

Висновки до першого розділу: у даному розділі було проведено глибокий аналіз RFID технології, її ключових компонентів, різновидів міток, а також потенціалу їх застосування в різних сферах. Було розглянуто основні типи RFID-міток — пасивні, активні та напівпасивні — та окреслено сфери, де кожен з цих типів міток є найбільш ефективним. Зокрема, пасивні мітки виявилися ідеальними для масового відстеження товарів у роздрібній торгівлі, тоді як активні мітки більше підходять для управління великогабаритними активами на значних відстанях.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Також було висвітлено питання вартості та ефективності RFID систем, розглянуто первинні інвестиції, пов'язані з установкою та обслуговуванням обладнання, та їх вплив на загальну рентабельність інвестицій. У цьому контексті, було підкреслено, що хоча первинні витрати можуть бути значними, покращення в ефективності операцій та управлінні запасами часто швидко окупають ці витрати.

У розділі також обговорювалися перспективи майбутнього розвитку RFID технології, включаючи інтеграцію з Інтернетом речей (IoT) та іншими сучасними технологіями, що відкриває нові можливості для автоматизації, підвищення ефективності та інновацій у різних галузях. Також було вказано на важливість розвитку безпечних та екологічно чистих рішень, які б відповідали сучасним вимогам приватності та сталого розвитку.

Загалом, цей розділ надає цілісне уявлення про RFID технологію, відкриваючи її потенціал та місце в сучасному технологічному ландшафті, а також підкреслює важливість подальших досліджень та розвитку в цій області.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

РОЗДІЛ 2. СТРУКТУРА ТА БЕЗПЕКА СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПУ НА ОСНОВІ RFID

2.1 Архітектура системи контролю та управління доступу RFID

Система контролю та управління доступом на основі RFID, інтегрована з домофонною системою, як наприклад VIZIT, може мати складну архітектуру, яка включає кілька ключових компонентів та етапів взаємодії.



Рисунок 2.1 – Приклад системи контролю та управління доступом на основі RFID

Компоненти системи:

- RFID-мітки - носії ідентифікаційної інформації, які видаються мешканцям або відвідувачам. Мітки можуть бути у формі карток, брелків або інших малогабаритних предметів.



Рисунок 2.2 – Приклад RFID-мітки

- RFID-зчитувачі - встановлені на вході або в інших контрольних точках. Зчитувачі сканують RFID-мітки для отримання ідентифікаційної інформації.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22



Рисунок 2.3 – RFID-зчитувач

- Контролер доступу основний пристрій, який управляє доступом на основі даних, отриманих від RFID-зчитувачів. Контролер може бути інтегрований з домофонною системою Vizit.



Рисунок 2.4 – Контролер доступу

- Механізм блокування - якщо доступ дозволений, контролер активує механізм відкривання дверей. У випадку відмови в доступі, двері залишаються заблокованими.



Рисунок 2.5 – Механізм блокування

Ця інтегрована система забезпечує зручний та безпечний контроль доступу, здатний адаптуватися до різних потреб житлових комплексів або комерційних

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

будівель. Вона також забезпечує додатковий рівень безпеки та комфорту для мешканців та відвідувачів.

2.2 Програмне забезпечення у СКУД на основі RFID

Програмне забезпечення в системах контролю доступу (СКУД) на основі RFID відіграє критичну роль, оскільки воно є містком між фізичними компонентами системи (такими як RFID-зчитувачі та мітки) та кінцевими користувачами, які управляють системою. Далі розглянемо основні функції та характеристики.

Функції СКУД на основі RFID:

- Ідентифікація та Аутентифікація

Програмне забезпечення для систем контролю доступу на основі RFID виконує багато важливих завдань і має важливі характеристики, які гарантують ефективність і безпеку системи. Воно використовує дані, отримані від RFID-зчитувачів, для ідентифікації та аутентифікації користувачів, перевіряючи їх право на доступ до певних зон.

- Управління доступом

Крім того, це програмне забезпечення відповідає за управління доступом, дозволяючи налаштовувати різні правила доступу для різних користувачів і груп, а також встановлювати часові та просторові обмеження.

- Моніторинг та звітність

Ще однією важливою функцією є моніторинг і звітність, яка включає ведення записів про всі події доступу, що дозволяє відстежувати та аналізувати активність користувачів. Це має вирішальне значення для безпеки, оскільки дозволяє виявити спроби несанкціонованого доступу та вжити відповідних заходів.

- Інтеграція з іншими системами

Програмне забезпечення також можна інтегрувати з іншими системами безпеки, такими як протипожежні системи та відеонагляд. Це створює єдину систему управління безпекою. Це забезпечує комплексний підхід до безпеки та реагування на надзвичайні ситуації.

Характеристики RFID систем:

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

- Користувацький інтерфейс

Інтуїтивно зрозумілий і простий у використанні інтерфейс дозволяє швидко налаштувати правила доступу, переглядати події та керувати користувачами.

- Масштабованість

адаптація до зростаючих потреб організації, таких як здатність керувати великою кількістю користувачів і точок доступу, а також обробляти великі кількості даних.

- Безпека

Сучасні методи шифрування та безпечне зберігання забезпечують захист конфіденційності даних користувачів і інформації про доступ. Виявлення та попередження потенційних порушень безпеки за допомогою процедур моніторингу та аудиту.

- Модульність та Інтеграція

Гнучкість дозволяє створювати комплексні рішення безпеки, адаптовані до конкретних потреб, додаючи нові функції або інтегруючи з іншими системами.

- Дистанційне управління

Можливість дистанційно керувати системою, моніторити події та контролювати доступ через веб-інтерфейси або мобільні програми.

Таким чином, програмне забезпечення в системах контролю доступу на основі RFID є важливим для забезпечення гнучкості, безпеки та ефективності управління доступом.

2.3 Безпека в системах RFID

Оскільки системи RFID широко застосовуються для ідентифікації, відстеження та управління доступом до різних об'єктів і ресурсів, безпека цих систем є важливим питанням. Захист цих систем від несанкціонованого доступу, злому, підслуховування даних та інших потенційних загроз є важливими для забезпечення безпеки цих систем.

Основні аспекти безпеки в системах RFID:

- Шифрування Даних: Дані, які передаються між зчитувачем і міткою, повинні бути добре зашифровані, щоб запобігти підслуховуванню та

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

несанкціонованому доступу до інформації.

- Безпечні Протоколи Аутентифікації: Для запобігання атакам повторного відтворення (cloning) та іншим типам злому необхідно створити та запровадити протоколи, які гарантують валідність і достовірність комунікації між мітками та зчитувачем.

- Фізичний Захист Міток та Зчитувачів: Захистити мітки від пошкодження або несанкціонованого доступу, а також захистити зчитувачі від пошкоджень і крадіжок.

- Менеджмент Ключів та Доступу: Ефективне управління ключами шифрування та доступом до системи контролю, включаючи регулярну зміну ключів і відстеження доступу до системи.

- Захист від Деніал-оф-Сервіс (DoS) Атак: Запобігання атакам, які можуть блокувати або зривати роботу системи RFID, наприклад через радіоперешкоди або шкідливе програмне забезпечення.

- Політика Конфіденційності та Згода Користувача: Важливо переконатися, що використання RFID-систем відповідає правилам конфіденційності, особливо коли вони використовуються для відстеження рухів людей.

- Регулярні Аудити та Оновлення Безпеки: Проведення аудитів безпеки та регулярне оновлення програмного забезпечення допомагає виявляти та усувати потенційні вразливості в системі.

- Обмеження Функціональності Міток: У деяких випадках, може бути доцільно обмежити функціональність міток, наприклад, забезпечивши можливість читання даних лише з певної відстані.

Забезпечення безпеки систем RFID вимагає комплексного підходу, який включає як технічні, так і організаційні заходи, а також постійний моніторинг і адаптацію до змінних обставин і загроз. Крім того, варто подумати про атаки, які можуть бути використані проти RFID-систем; ці атаки спрямовані на отримання несанкціонованого доступу або на унеможливлення роботи RFID-системи..

Основні атаки, що можуть бути успішно використані проти RFID-систем:

- Атака Евесдропінг (Підслуховування) - атакуючий може перехоплювати

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

комунікацію між RFID-міткою та зчитувачем для витоку конфіденційної інформації. Це можливо, оскільки радіохвилі можуть бути перехоплені на відстані.

- Атака Відтворення - атака полягає у копіюванні інформації з легітимної RFID-мітки для створення копії, яка може бути використана для обману системи.

- Ретрансляційні атаки - в цьому випадку атакуючий перехоплює сигнал з мітки і передає його на більшу відстань, щоб змусити систему думати, що мітка знаходиться ближче, ніж вона є насправді.

- Фізичні атаки на мітки - це може включати фізичне знищення міток або їх блокування за допомогою матеріалів, що перешкоджають радіосигналам.

- Атаки на конфіденційність - оскільки RFID-мітки часто використовуються для відстеження руху товарів або осіб, існує ризик незаконного відстеження та збору даних про осіб або об'єкти.

- Атака, спрямована на зрив роботи RFID-системи, шляхом затоплення зчитувача великою кількістю запитів або використанням радіоперешкод, що унеможлиблює читання міток.

2.4 Загальні відомості про СКУД

Системи контролю та управління доступом (СКУД) відіграють важливу роль у забезпеченні безпеки об'єктів та регулюванні доступу осіб до певних зон чи приміщень.

Призначення та функції СКУД:

- Регулювання Доступу: СКУД дозволяють контролювати, хто, коли та куди може потрапити, обмежуючи доступ до визначених зон.

- Моніторинг та Звітність: Збір та аналіз даних про входи та виходи, включаючи ведення записів та генерацію звітів для аудиту.

- Інтеграція з Іншими Системами Безпеки: Часто інтегруються з системами відеоспостереження, протипожежними системами та іншими заходами безпеки.

- Компоненти СКУД:

- Автономні Системи: Прості системи для одного входу/дверей.

- Мережеві Системи: Підключені до мережі, керуються центрально, ідеальні для великих будівель чи комплексів.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

- Інтегровані Системи: Комбінують контроль доступу з іншими системами безпеки.

Системи контролю та управління доступом (СКУД) використовуються в багатьох сферах, включаючи офісні та комерційні будівлі, промислові об'єкти, заклади освіти, готелі та лікарні. Вони дозволяють контролювати доступ до певних місць, відстежувати вхід і вихід працівників, відвідувачів та інших людей. Це не тільки охороняє співробітників і гостей, але й захищає важливі активи та конфіденційні дані від несанкціонованого доступу.

З метою захисту та безпеки СКУД включають низку заходів для захисту даних і інформації про доступ. Щоб запобігти несанкціонованому доступу та злому системи, важливо використовувати шифрування даних і безпечні протоколи обміну інформацією. Окрім технічних заходів безпеки, політики конфіденційності є життєво важливими, щоб переконатися, що інформація про доступ осіб обробляється відповідно до законів і моральних стандартів.

Крім того, СКУД можна використовувати разом з іншими системами безпеки, такими як відеоспостереження та протипожежні системи, щоб створити комплексний підхід до управління безпекою. Ця інтеграція покращує огляд безпеки та дозволяє швидко реагувати на будь-які інциденти або надзвичайні ситуації.

Сучасні системи безпеки вимагають використання СКУД, які підвищують продуктивність операційних процесів і забезпечують безпеку та захист багатьох об'єктів і установ..

Типовими представниками реалізованої системи контролю та управління доступом є:

- Шлагбауми — це пристрої, які обмежують доступ транспортних засобів на або з території. Це механічний бар'єр, який зазвичай складається з горизонтальної балки або стрижні, яка піднімається або опускається, щоб дозволити або перешкоджати проїзду автомобілів.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		28



Рисунок 2.6 – Шлагбаум

- Турнікет - це пристрій, який використовується в різних громадських і приватних об'єктах для контролю доступу людей. Одна людина може проходити через цей обертовий бар'єр, за раз, що дозволяє керувати потоком людей.



Рисунок 2.7 – Турнікет

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

- Домофони служать для контролю доступу та зв'язку між вхідними дверима будівлі (наприклад, офісу, квартири чи приватного будинку) та внутрішніми приміщеннями будівлі. Ця система дозволяє мешканцям або співробітникам бачити, хто прибув, і контролювати доступ до будівлі без фізичного доступу.



Рисунок 2.8 – Домофон

2.5 Порівняння механічних та електронних СКУД

Найвідомішим представником механічного обмежувача доступу, є механічний кодовий замок, найчастіше такі можна зустріти на дверях під'їздів багатоповерхівок або на вхідних дверях на територію в приватному секторі, виглядають такі замки приблизно так:

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		30



Рисунок 2.9. – Загальний вигляд кодового замка

Механізм кодування відбувається перед встановленням, тип кодування кодонабірний, тобто код можна встановити власноруч, для цього потрібно зняти внутрішню панель та перемісти сульвади які є учасниками кодування скосом у напрямку замка, не кодовані кнопки ж навпаки скосом у напрямку від осі замка.

Переваги:

- Відсутність ключів
- Простота монтажу та використання
- Легкість заміни коду доступу

Недоліки:

- Не стійкі до погодних умов
- У разі зміни коду потрібно сповіщувати усіх особисто
- Можливість підбору коду

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Ще одним типовим представником обмеження безперешкодного отримання доступу до певної території є замок з ключем, зображений на (Рисунок 2.10):

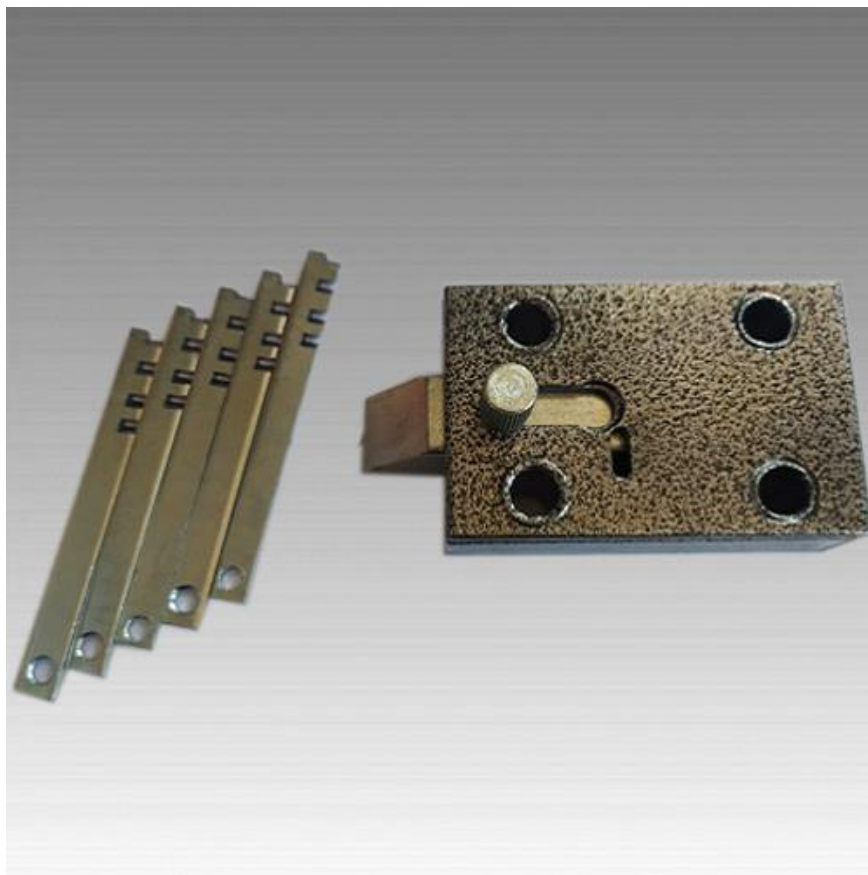


Рисунок 2.10. – Загальний вигляд замка з ключем

Такі види замків теж надзвичайно часто зустрічаються в під'їздах багатоповерхівок, але вони не є такими надійними як кодові замки, оскільки для відкриття не завжди потрібно використовувати саме підходящий ключ, можна скористатись іншим ключем або спеціальними інструментами по типу ломика або кусачок.

Переваги:

- Портативність
- Простота використання
- Стійкість до використання на вулиці

Недоліки:

- Ризик втрати ключа
- Вразливість до злому
- Залежність від погодних умов

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Загалом навісні замки є хорошим способом контролювати та надавати доступ до території чи майна. Однак у них є один недолік — вони не такі міцні, як інші види замків і можуть взламуватися через погодні умови.

Найкращим і найнадійнішим варіантом є домофон на основі технології RFID. Це пристрій, який дозволяє отримати доступ до квартири за допомогою теги або дзвінка, а потім відкриває двері за допомогою кнопки, яка знімає напругу з магніта. Ці системи легкі у використанні, стійкі до погоди та злому:



Рисунок 2.11 – Загальний вигляд домофону на основі RFID

Переваги:

- Стійкість до злому
- Контроль доступу
- Зручність

Недоліки:

- Технічне обслуговування
- Вартість
- Вандалізм

У результаті аналізу переваг і недоліків СКУД на основі RFID технології було виявлено, що він є найкращим варіантом серед розглянутих.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

З цієї причини при моделюванні власного проекту пріоритет буде надаватися саме цьому типу СКУД.

Для повного узагальнення схеми роботи майбутньої системи створимо блок-схему за якою буде написано програмний код і за якою в майбутньому буде працювати сама СКУД-система.

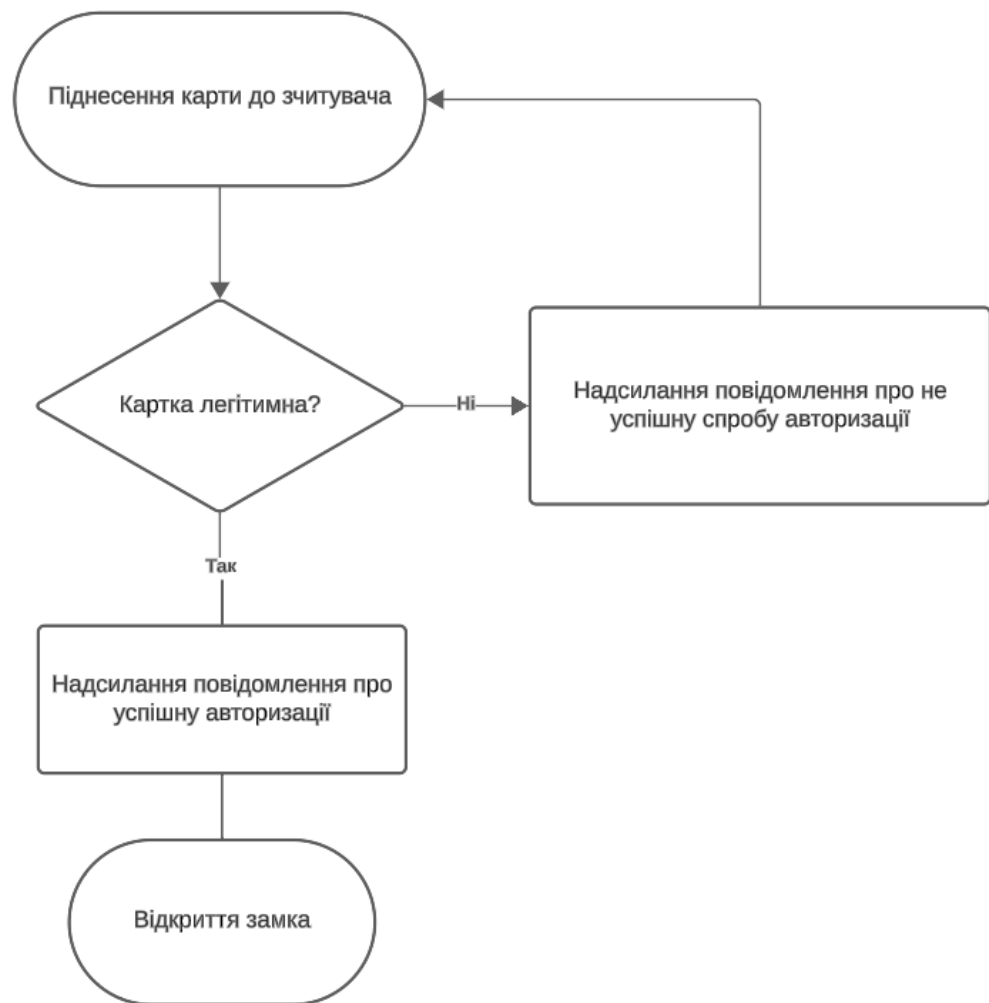


Рисунок 2.12 – Загальна схема роботи СКУД-системи

У відповідності до розробленої схеми система має працювати наступним чином. Зчитувач карток активний за замовчуванням, користувач наближає картку, після цього система переходить до перевірки коду картки і у разі відсутності реєстрації картки в системі, програмний код буде виконувати відправку повідомлення про не успішну авторизацію в системі, та поверне користувача на етап зчитування картки.

У разі якщо авторизацію пройдено успішно, система надішле повідомлення з результатом вдалої авторизації та надасть доступ, відкривши замок.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Висновок до другого розділу: у цьому розділі ми розглянули ключові аспекти архітектури систем контролю та управління доступом (СКУД) на основі RFID, їх програмного забезпечення, порівняли загально відомі системи контролю доступу та визначили на яку із них орієнтуватись, а також розглянули питання безпеки, що є важливими для розуміння цілісності та функціональності таких систем.

Архітектура СКУД на основі RFID включає в себе інтеграцію RFID-міток, зчитувачів, контролерів доступу та інтерфейсних систем. Це створює комплексну систему, здатну точно ідентифікувати осіб або об'єкти та управляти доступом до різних зон безпеки.

Програмне забезпечення в СКУД на основі RFID грає ключову роль у забезпеченні гнучкості та ефективності системи. Воно включає функціонал для ідентифікації, аутентифікації, моніторингу доступу, інтеграції з іншими системами безпеки та забезпечення звітності.

Питання безпеки в системах RFID охоплюють заходи для захисту від несанкціонованого доступу, злому, перехоплення даних та інших потенційних загроз. Застосування шифрування, безпечних протоколів аутентифікації, фізичного захисту обладнання та політик конфіденційності є важливими для забезпечення цілісності та безпеки даних у СКУД.

В загальному огляді СКУД відмічено, що ці системи є невід'ємною частиною сучасних заходів безпеки, забезпечуючи контроль та управління доступом у різноманітних об'єктах, від приватних територій до комерційних і освітніх установ.

Таким чином, розгляд архітектури, програмного забезпечення, аспектів безпеки та загальних характеристик СКУД на основі RFID дозволяє глибше зрозуміти їх важливість, складність та значення для створення ефективних та безпечних систем контролю доступу.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

РОЗДІЛ 3. ПІДБІР ТА АНАЛІЗ КОМПОНЕНТІВ ДЛЯ ПОБУДОВИ, ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА БАЗІ ARDUINO КОМПОНЕНТІВ.

3.1 Підбір та аналіз компонентів для побудови

У процесі вибору контролера для вашого проекту були розглянуті два популярних варіанти: Arduino ESP8266 та Arduino UNO. Даваймо розглянемо їх переваги та недоліки для кращого розуміння.

Плюси Arduino ESP8266:

- Вбудований Wi-Fi: Однією з найбільших переваг ESP8266 є вбудований Wi-Fi, що робить його ідеальним для проектів IoT та бездротового зв'язку.
- Низька вартість: ESP8266 доступний за досить низьку ціну, що робить його доступним для широкого кола розробників та проектів з обмеженим бюджетом.
- Легкість використання: Завдяки широкій підтримці та документації, ESP8266 легко використовувати, особливо для початківців у світі мікроконтролерів та IoT.
- Мінуси Arduino ESP8266:
 - Обмежені ресурси: ESP8266 має обмежені ресурси в порівнянні з деякими іншими контролерами, що може призвести до обмежень в розмірі програми та обробці деяких завдань.
 - Менша кількість виводів: У порівнянні з деякими іншими контролерами, ESP8266 має меншу кількість виводів, що може обмежувати кількість підключених пристроїв або сенсорів.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

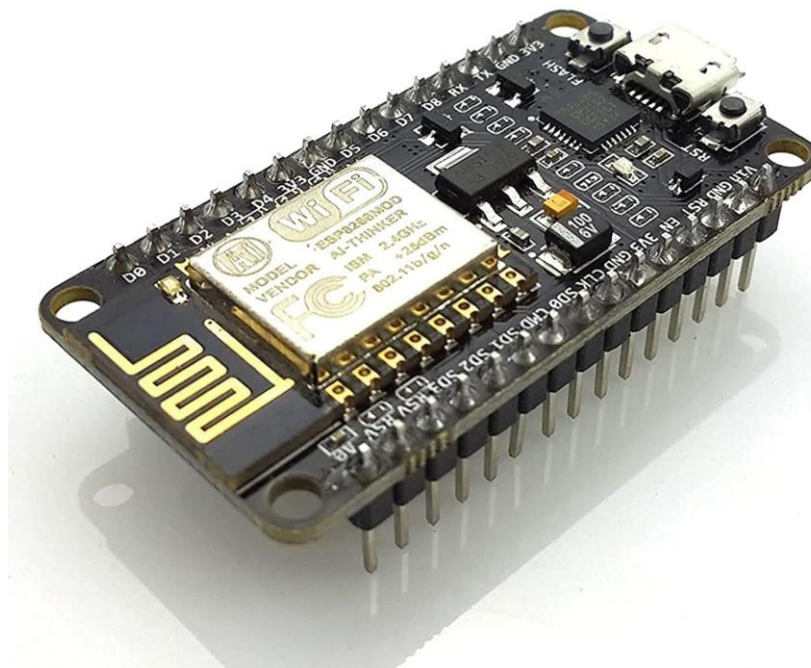


Рисунок 3.1 – Загальний вигляд плати Arduino ESP8266

Arduino UNO є одним з найпопулярніших та найрозповсюдженіших мікроконтролерів серії Arduino. Він базується на мікроконтролері ATmega328P від Microchip (раніше Atmel).

Плюси Arduino UNO:

- Широка підтримка: Arduino UNO має широку спільноту користувачів та багато бібліотек, що робить його відмінним вибором для широкого кола проєктів.
- Більша кількість виводів: У порівнянні з ESP8266, Arduino UNO має більшу кількість виводів, що дозволяє підключити більше пристроїв без розширювачів портів.

• Мінуси Arduino UNO:

- Відсутність вбудованого Wi-Fi: Arduino UNO не має вбудованого Wi-Fi, що може бути недоліком для проєктів, які потребують бездротового з'єднання.
- Вища вартість модулів Wi-Fi: Якщо вам потрібне бездротове з'єднання з Arduino UNO, ви мусите придбати додатковий модуль Wi-Fi, що може підвищити вартість проєкту.

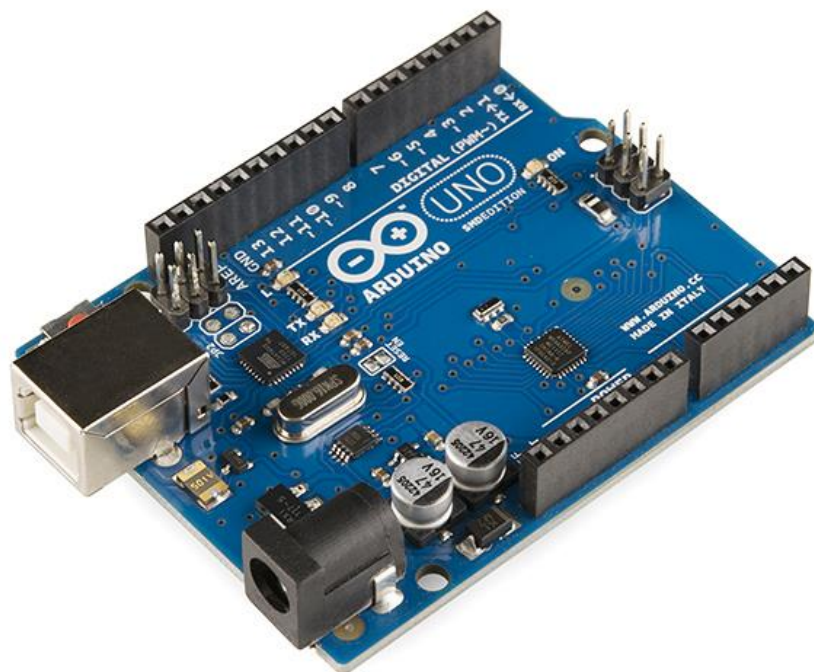


Рисунок 3.2 – Загальний вигляд Arduino UNO

Враховуючи вищенаведене, ESP8266 може бути кращим вибором для проєктів, які потребують бездротового з'єднання та мають обмежений бюджет, в той час як Arduino UNO може бути кращим вибором для проєктів, які потребують більшої кількості виводів або не потребують бездротового з'єднання.

Ще одним ключовим компонентом у нашому проєкті є зчитувач RFID через який безпосередньо і буде виконуватись перевірка користувачів. У даному курсовому проєкті було використано компонент RC522.

Модуль RC522 - це низькочастотний RFID-зчитувач, який широко використовується для зчитування RFID-міток і карток. Він базується на чіпі MFRC522 від NXP Semiconductors і має можливість зчитувати та записувати дані на RFID-мітках за допомогою радіочастотної ідентифікації.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

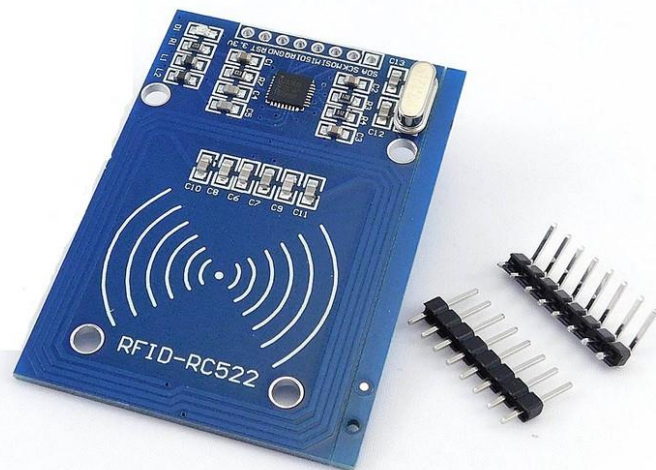


Рисунок 3.3 – Загальний вигляд модуля Arduino RC522

Основні характеристики включають:

- Підтримка протоколів зв'язку: модуль RC522 підтримує різні стандарти зв'язку, такі як ISO/IEC 14443A.
- Інтерфейс зв'язку: модуль може бути підключений до мікроконтролерів або інших пристроїв за допомогою інтерфейсу SPI.
- Висока швидкість передачі даних: зчитування та запис даних на RFID-мітках відбувається досить швидко, що робить модуль ефективним у використанні.
- Легка інтеграція: модуль має компактний розмір та простий інтерфейс, що робить його легким у використанні та інтеграції в різноманітні проекти.

Оскільки Arduino RC522 модуль найбільше підходить для проєктів де потрібно ідентифікувати об'єкти за допомогою RFID-технологій, тому вибір впав саме на цей модуль.

Одним із складових компонентів є електромагнітний замок. Цей тип замків використовує електромагніт для утримання дверей у замкненому стані.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

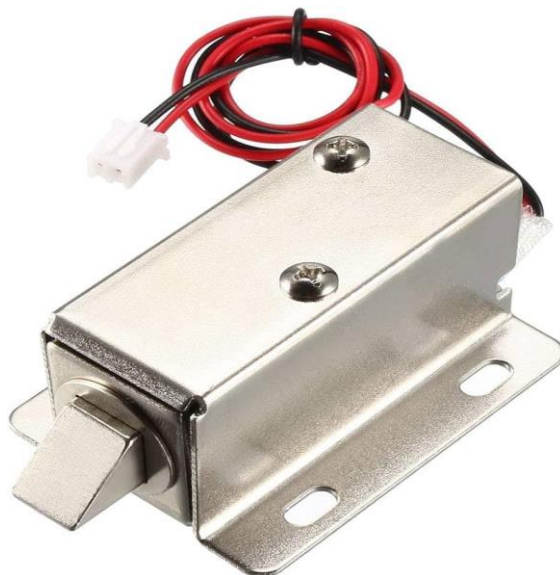


Рисунок 3.4 – Загальний вигляд модуля електромагнітного замка

Електромагнітний замок складається з двох основних компонентів: електромагніту та арматури. Електромагніт - це котушка дроту, яка при подачі напруги створює магнітне поле. Арматура - це шматок феромагнітного матеріалу, який притягується до електромагніту.

Коли на електромагніт подається напруга, він створює магнітне поле, яке притягує арматуру. Це утримує двері в зачиненому стані. Коли напруга знімається з електромагніту, магнітне поле зникає, і арматура звільняється. Це дозволяє відкрити двері.

Електромагнітні замки часто використовуються в системах контролю доступу. Їх можна використовувати для віддаленого відкривання та закривання дверей, а також їх можна інтегрувати з іншими системами безпеки, такими як сигналізація та відеоспостереження.

Електромагнітні замки мають кілька переваг перед традиційними механічними замками. Вони тихі, безпечні та їх легко встановити. Їх також можна використовувати з різними типами дверей, включаючи дерев'яні, металеві та скляні.

Однак електромагнітні замки також мають деякі недоліки. Вони залежать від електроенергії, тому не працюватимуть у разі відключення електроенергії. Їх також можна зламати за допомогою сильного магніту.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Загалом, електромагнітні замки є надійним та універсальним рішенням для контролю доступу. Вони підходять для різних застосувань, включаючи житлові, комерційні та урядові будівлі.

Релейний модуль Songle - це електронний пристрій, який використовується для керування електричними струмами за допомогою сигналу з низькою потужністю. Його можна використовувати для керування різними пристроями, включаючи лампи, двигуни та електромагнітні клапани.

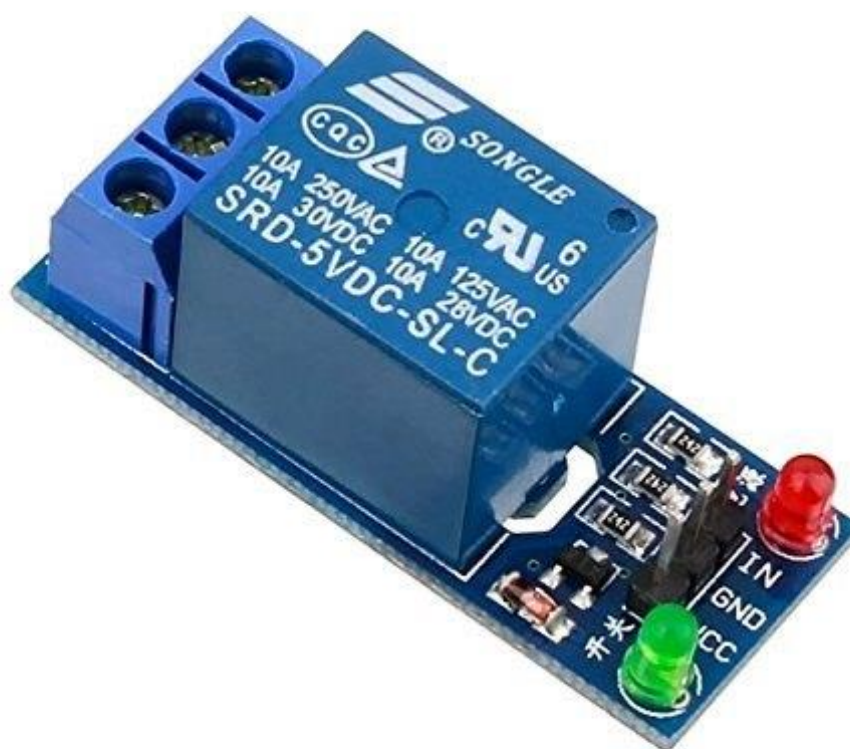


Рисунок 3.5 – Загальний вигляд релейного модуля Songle

Релейні модулі Songle використовуються в проектах електроніки та автоматизації. Їх можна використовувати для керування різними пристроями, включаючи:

- Лампи: релейний модуль можна використовувати для керування увімкненням і вимкненням ламп. Це можна використовувати для створення простих світлових шоу або для керування освітленням у будинку чи офісі.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

- Двигуни: релейний модуль можна використовувати для керування вмиканням і вимкненням двигунів. Це можна використовувати для керування роботою верстатів або для керування рухом роботів.
- Електромагнітні клапани: релейний модуль можна використовувати для керування відкриттям і закриттям електромагнітних клапанів. Це можна використовувати для керування потоком рідини або газу в системі.

Релейні модулі Songle - це універсальні та недорогі пристрої, які можна використовувати для різних цілей. Вони є цінним доповненням до будь-якого набору електроніки або автоматизації.

Додатковим живленням для електромагнітного замка буде виступати набір із трьох літій-іонних акумуляторів 18650.



Рисунок 3.6 – Загальний вигляд акумулятора 18650

Акумулятор 18650 - це акумулятор циліндричної форми, який широко використовується в електронних пристроях. Він має номінальну напругу 3,7 вольтів і ємність від 2200 до 3500 міліампер-годин (мАч).

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

3.2 Підключення компонентів та написання коду реалізації системи керування доступом.

Визначившись з компонентами та контролером, можемо перейти до підключення на налаштування нашої схеми:

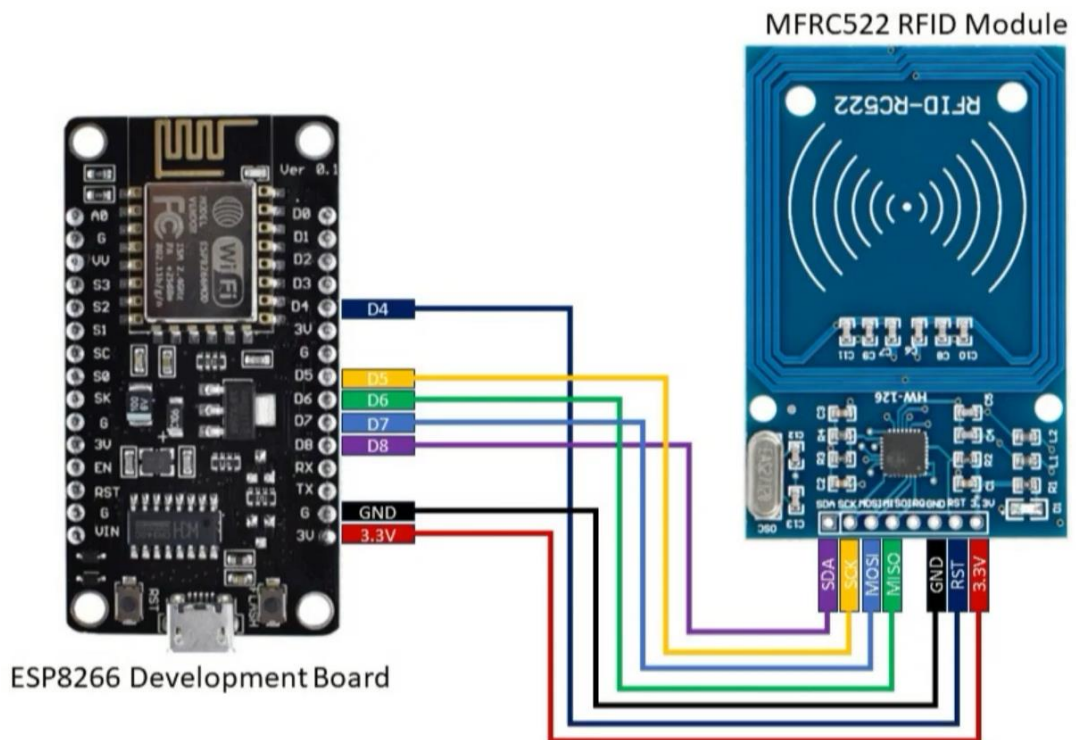


Рисунок 3.7 – Схема підключення контролера ESP8266 та модуля RC522

Детальна схема підключення:

1. Контакт RST RFID-модуля до контакту D4 плати розробки ESP8266.
2. Контакт SDA RFID-модуля до контакту D2 плати розробки ESP8266.
3. Контакт SCK RFID-модуля до контакту D5 плати розробки ESP8266.
4. Контакт MISO RFID-модуля до контакту D3 плати розробки ESP8266.
5. Контакт MOSI RFID-модуля до контакту D6 плати розробки ESP8266.
6. Контакт GND RFID-модуля до контакту GND плати розробки ESP8266.
7. Контакт 3.3V RFID-модуля до контакту 3.3V плати розробки ESP8266.
8. Контакт 12V RFID-модуля до джерела живлення 12V.

Після підключення RFID-сенсора, маємо підключити релейні модуль Songle, додаткове живлення та сам електромагнітний замок, для цього спочатку складемо схему, та будемо керуватись нею під час практичного налаштування. Загальна схема підключення враховуючі усі компоненти буде виглядати ось так [3]:

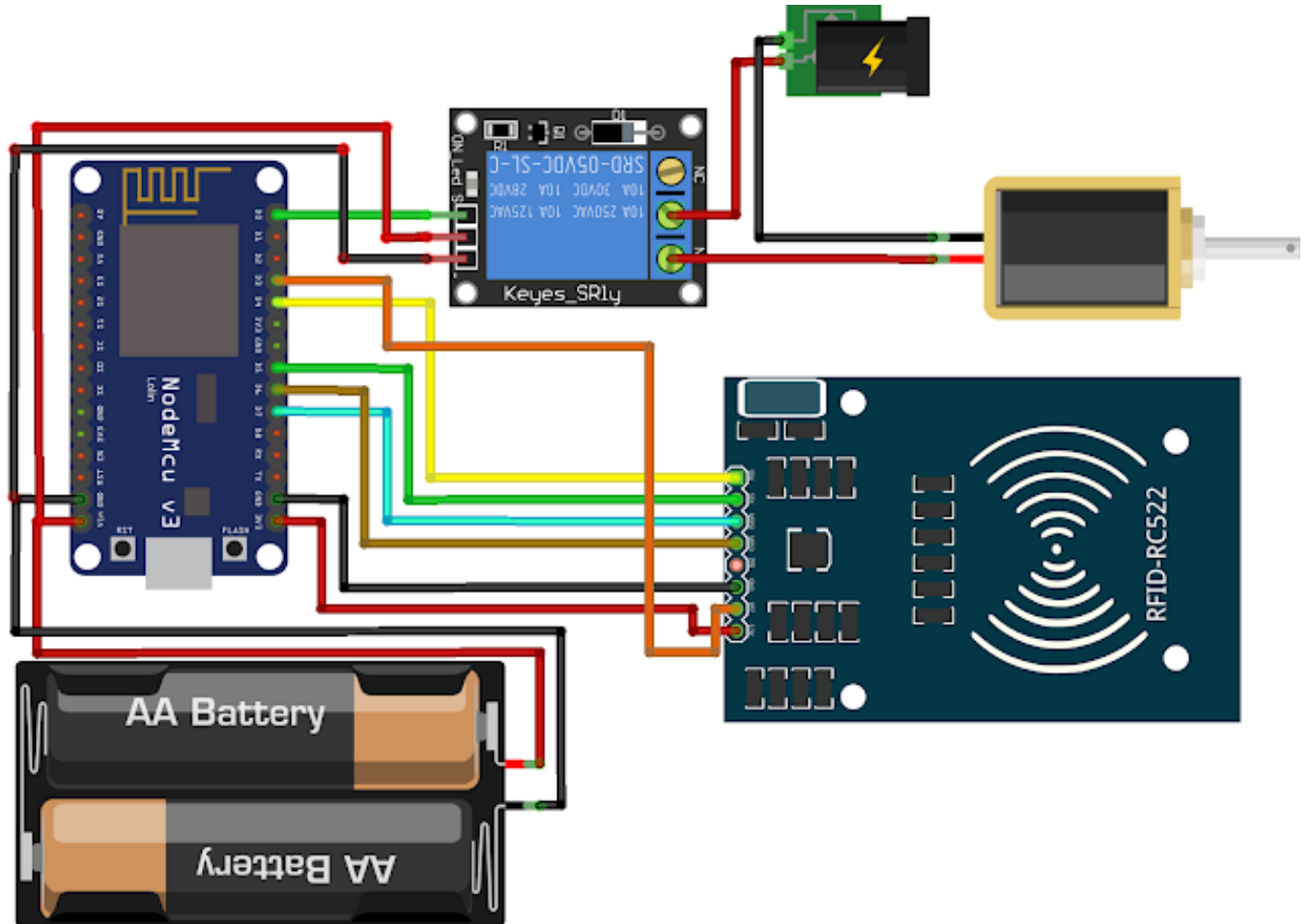


Рисунок 3.8 – Загальний вигляд спроектованої схеми підключення

Після виконання усіх теоретичних етапів підготовки, можемо переходити до практичного збирання та налаштування схеми системи контролю доступу.

Керуючись рисунком номер 3.7 підключимо RFID-сенсор, який буде реагувати на піднесення міток:

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

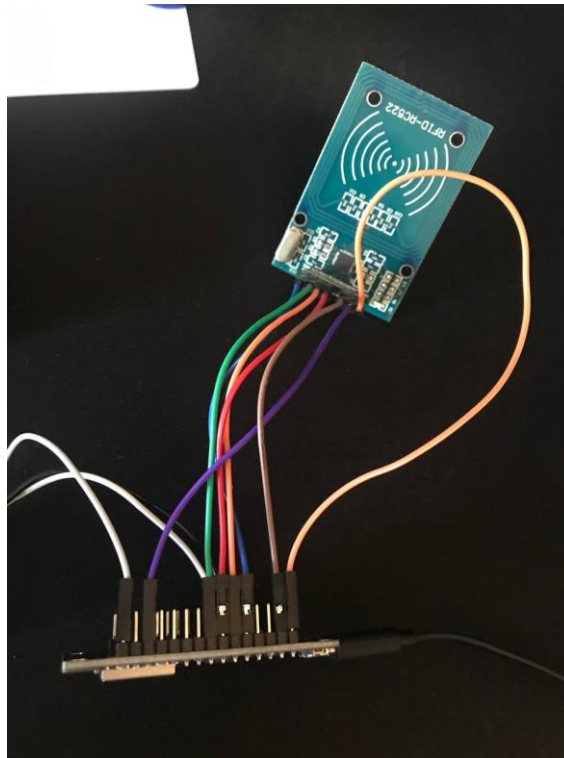


Рисунок 3.9 – Підключення RFID-сенсора до плати ESP8266

Наступним кроком буде підключення релейного модуля Songle, який має всього три піна, один з яких живлення, його потрібно підключити до піна живлення на платі, другий пін відповідає за заземлення і для керування використовується лише один пін, який ми підключаємо до довільного піна на платі, керування буде виконуватись, подачею напруги на вибраний пін.

Загальний вигляд підключення:

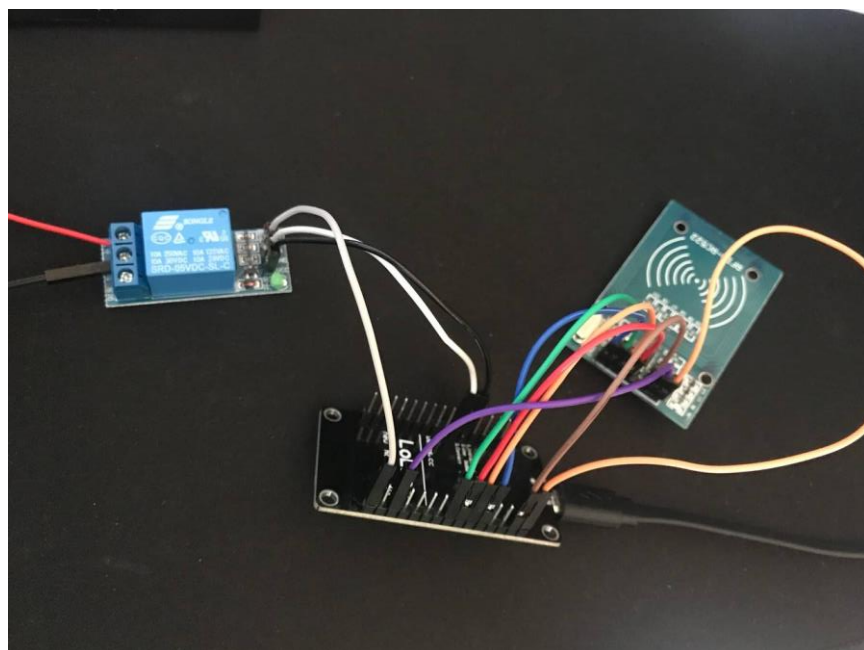


Рисунок 3.10 – Підключення релейного модуля Songle

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Наступним елементом для підключення буде додаткове живлення для електромагнітного замка, складається воно із 3 акумуляторів 18650 та боксу для їх підключення.

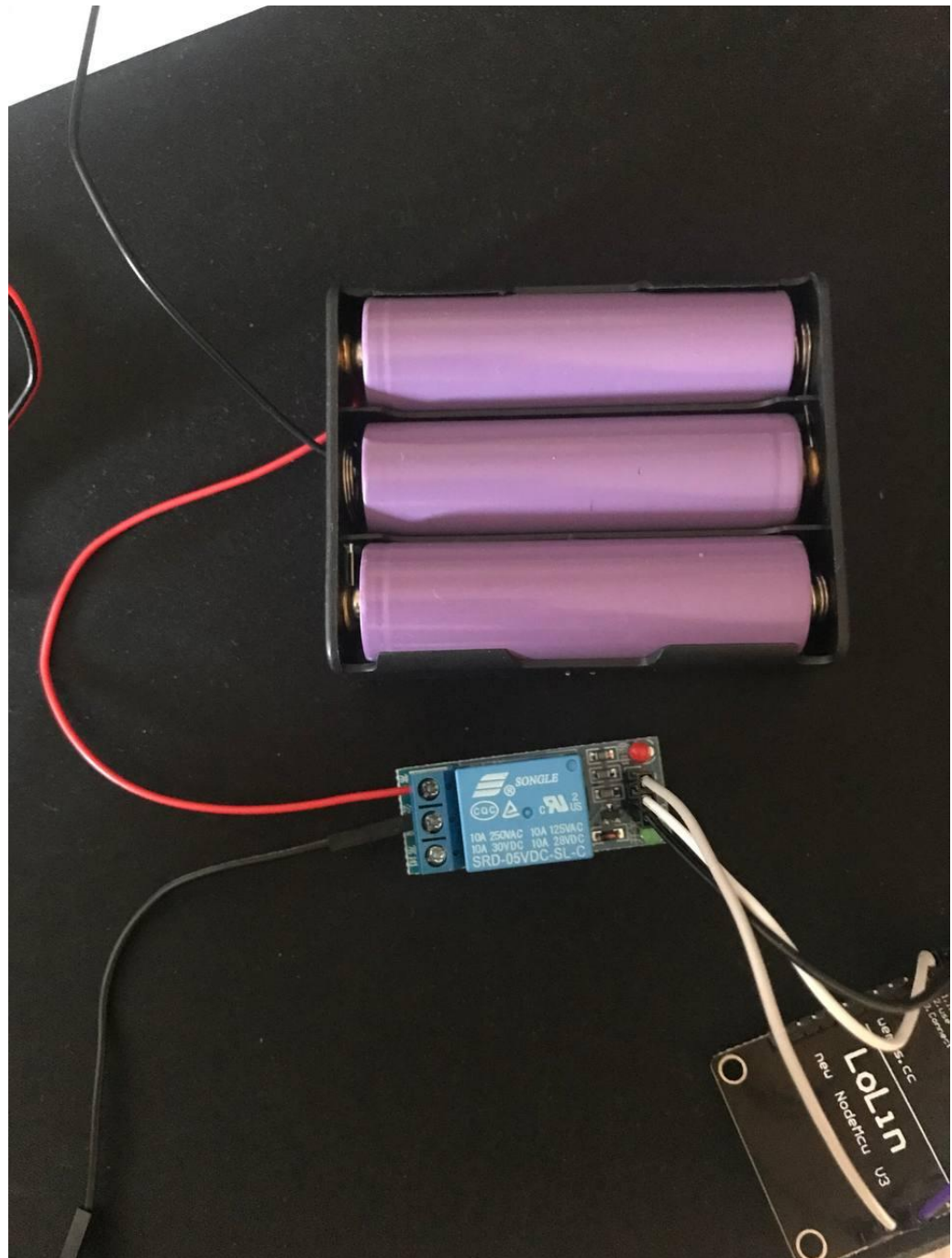


Рисунок 3.11 – Підключення додаткового живлення до реле

В боксі з додатковим живленням є позитивний та негативний виходи, позитивний вихід підключаємо до реле, а негативний вихід потрібно з'єднати з негативною жилою електромагнітного замка, після чого підключаємо позитивний вихід електромагнітного замка з центральним пазом реле, як на рисунку нижче.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

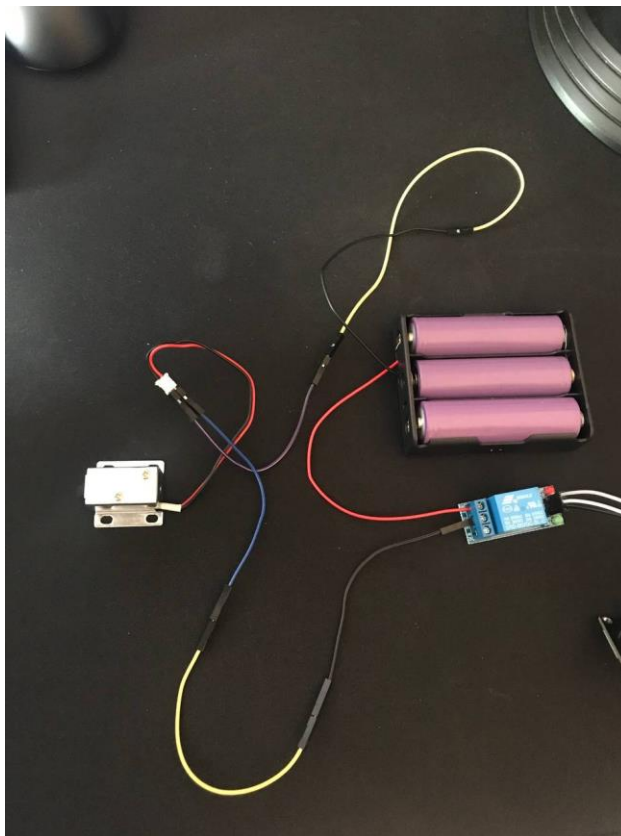


Рисунок 3.12 – Підключення електромагнітного замка до реле та додаткового живлення

Для налаштування телеграм бота, в якому ми будемо відслідковувати успішні та не успішні авторизації користувачів, нам потрібно зареєструвати за допомогою внутрішнього боту телеграм, який називається BotFather:

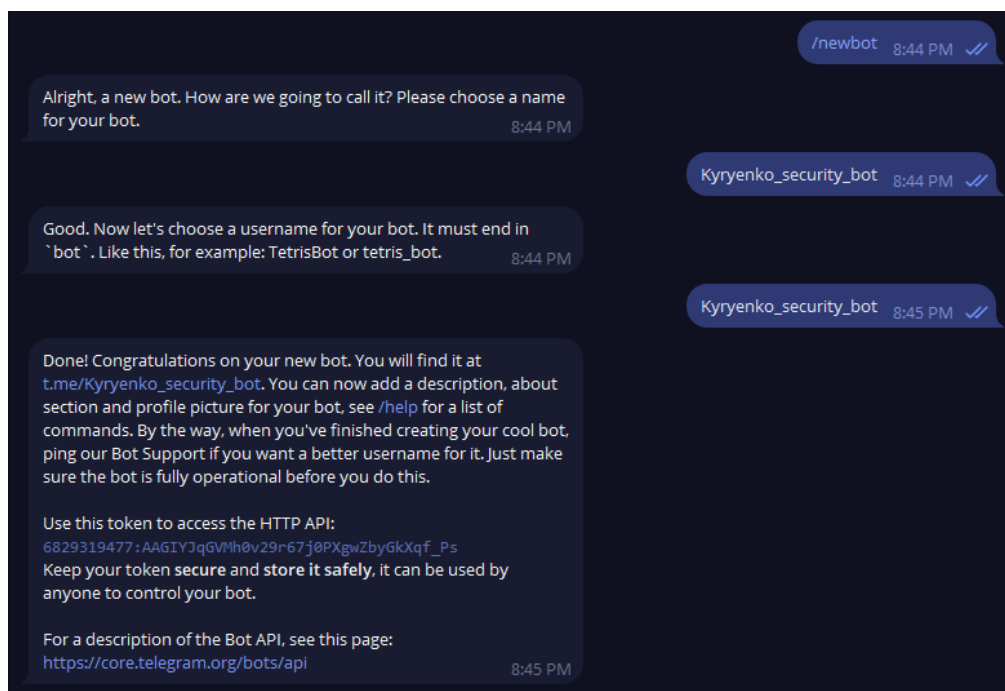


Рисунок 3.13 – Реєстрація телеграм бота

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

В результаті успішної реєстрації телеграм бота, маємо токен доступу, який вкажемо в програмному коді, це гарантує нам доступ до керування ботом, а саме надсиланням повідомлень.

Також потрібно визначити ідентифікатор чату відправивши GET-запит за токеном боту, в нашому випадку він виглядає так:



```
CHAT_ID "431918835"
```

Рисунок 3.14 – Визначення ідентифікатора боту

Таким чином ми розробили RFID-систему доступу, використовуючи Arduino ESP8266 та RFID-ридер, релейний модуль Songle та електромагнітний замок, інтегровані з месенджером Telegram для управління доступом до приміщень. Ця система дозволяє ідентифікувати користувачів за допомогою унікальних RFID-міток, забезпечуючи контроль над тим, хто відкриває двері. Коли користувач наближає мітку до зчитувача, система передає унікальний номер мітки, дозволяючи ідентифікувати особу та надати їй доступ.

Центральна ідея полягає в тому, що кожен користувач володіє індивідуальною RFID-міткою для доступу до певних приміщень. Ми відстежуємо використання цих міток, фіксуючи час та особу, що отримала доступ.

Завдяки інтеграції з Telegram, кожен раз, коли мітка наближається до зчитувача, відповідальний за безпеку менеджер отримує сповіщення із детальною інформацією про мітку. Це дозволяє не лише контролювати доступ, але й оперативно реагувати на спроби недозволеного доступу, оскільки система надсилає сповіщення про будь-яке сканування мітки, яка не входить до списку дозволених.

Також для експеременту визначимо картку, що є легітимною та картку, що не зареєстрована у системі безпеки.

Зареєстрована картка: 33 E7 3E B7

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		48



Рисунок 3.15 – Зареєстрована картка

Не зареєстрована картка: F8 08 89 0D



Рисунок 3.16 – Не зареєстрована картка

3.3 Перевірка роботи реалізованої СКУД системи

Для тестування функціональності нашої системи, спершу слід пред'явити зчитувачу заздалегідь зареєстровану RFID-картку, а після цього – картку, яка не була внесена до системи. Це дозволить нам оцінити ефективність системи у відповіді на визначення авторизованих та неавторизованих спроб доступу. Після пред'явлення кожної картки ми зможемо спостерігати відповідні сповіщення в месенджері Telegram, які вказуватимуть на те, чи була спроба доступу успішною або заблокованою.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Такий підхід допоможе нам переконатися у надійності та точності системи контролю доступу.

Стан системи у стані спокою:

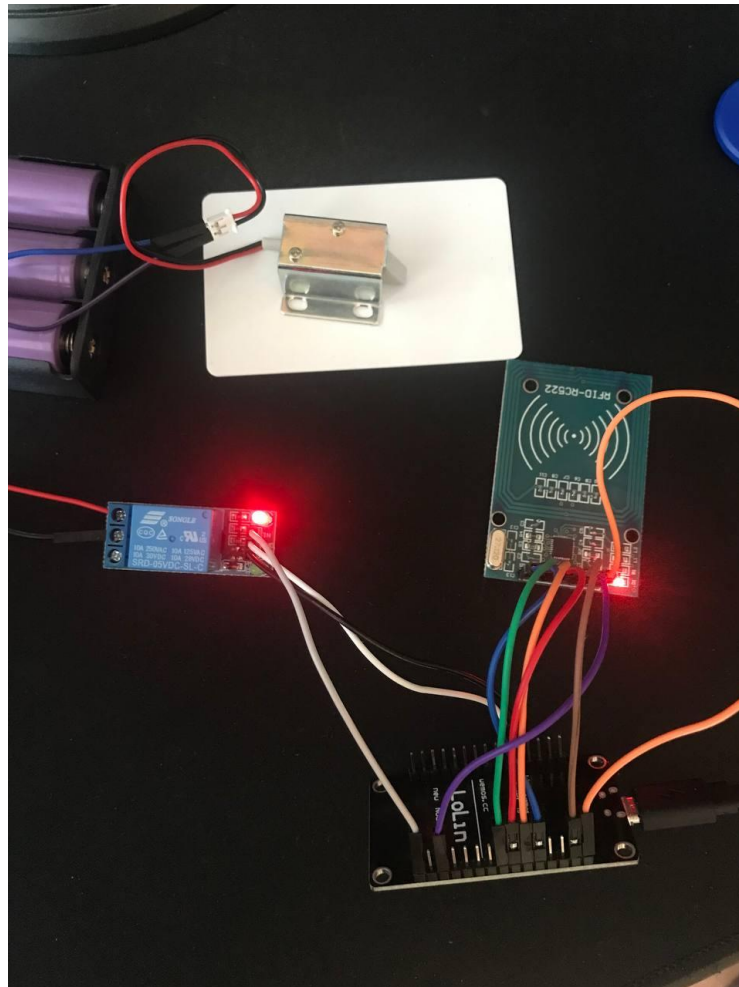


Рисунок 3.17 – Стан системи у стані спокою

Звідси бачимо, що замок закритий індикатори горять червоним кольором і сигналізують про замкнутість.

Спроба піднесення легітимної картки:

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

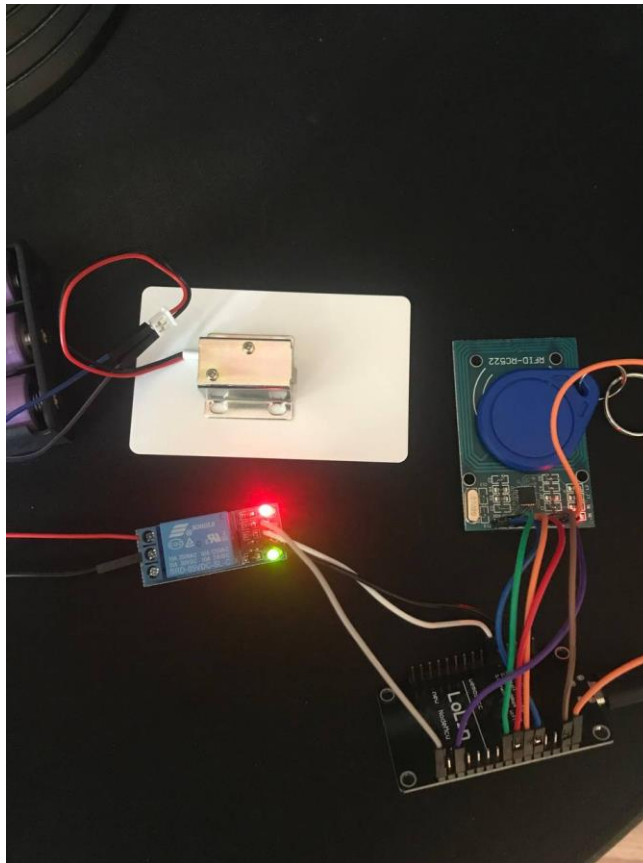


Рисунок 3.18 – Піднесення зареєстрованої картки

У разі якщо картка зареєстрована замок відчиняється, а зелений діод сигналізує про успішну авторизацію картки.

Час на який замок відкривається визначений як 5 секунд, але у разі потреби його можна змінити відносно до того, що за приміщення обслуговує даний замок.

У системі усі картки зареєстровані та для кожного тега маємо відповідні дані користувача, отже при піднесенні тега до ридера, в телеграмі будемо бачити детальну інформацію про людину, яка застосовує картку чи тег.

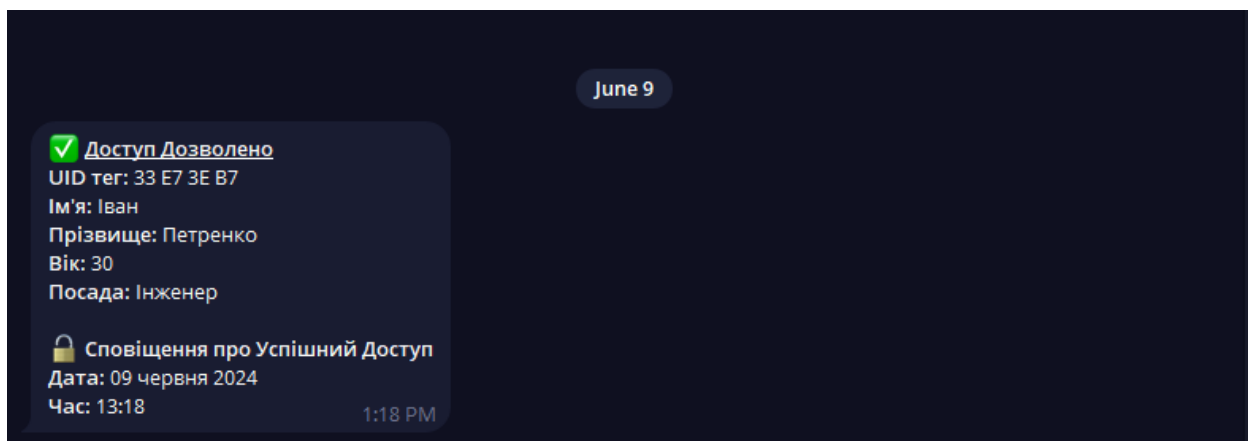


Рисунок 3.19 – Результат реакції на картку в телеграмі

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Спроба піднесення не легітимної картки:

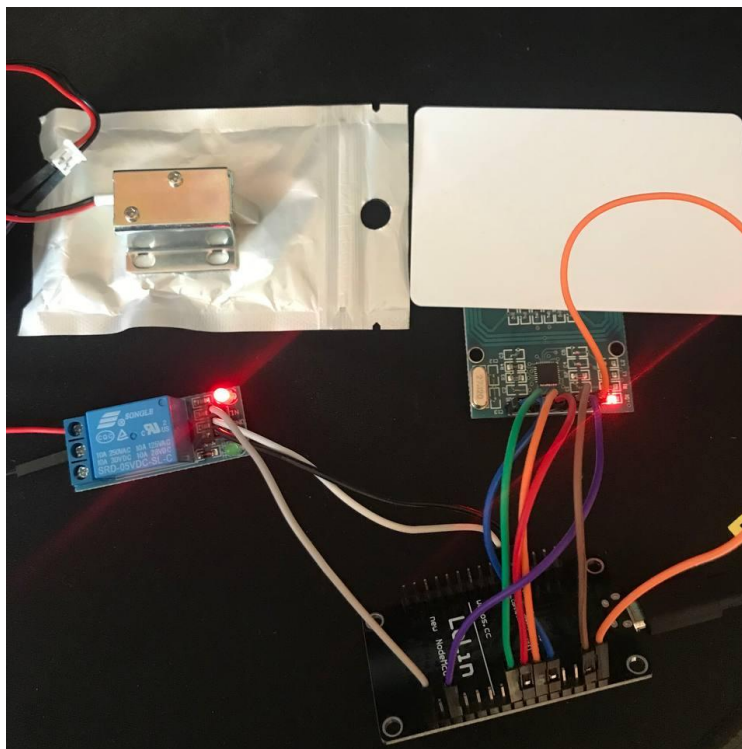


Рисунок 3.20 – Піднесення не зареєстрованої картки

У ситуації коли до RFID-ридера буде піднесено не зареєстровану у системі картку, ніяких дій від системи не послідує, діоди залишаться горіти червоними.

Менеджер який слідкує за периметром буде повідомлений, що було здійснено спробу піднесення не легітимної картки та бачити її тег.

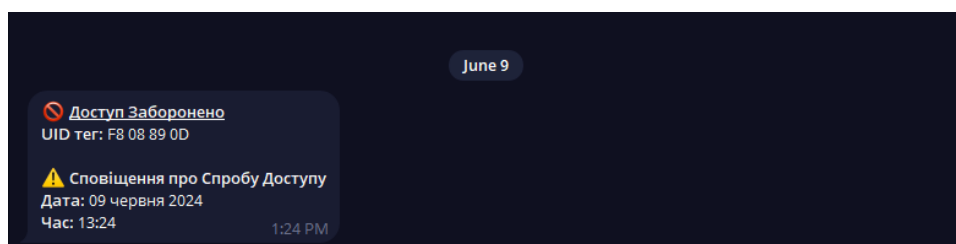


Рисунок 3.21 – Реакція на піднесення не зареєстрованої картки

На основі проведених тестів нашої RFID-системи контролю доступу, яка інтегрована з Telegram, можна зробити кілька ключових висновків.

По-перше, система ефективно розрізняє зареєстровані та незареєстровані картки, демонструючи високий рівень точності в ідентифікації користувачів.

По-друге, інтеграція з Telegram забезпечує оперативне сповіщення про всі спроби доступу, що підвищує рівень безпеки та контролю.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Таким чином, система не тільки забезпечує ефективний контроль доступу, але й дозволяє швидко реагувати на неавторизовані спроби входу, що є критично важливим для забезпечення безпеки об'єкта.

3.4 Пропозиції для подальшого розвитку

Розроблена система контролю та управління доступом на основі технології RFID з використанням Arduino та інтеграцією з Telegram має значний потенціал для подальшого вдосконалення та розширення функціональності. Загалом для подальшого розвитку можна виділити декілька векторів за якими варто рухатись:

Впровадження хмарної бази даних для зберігання інформації про користувачів, їх права доступу та історію входів, це дозволить ефективніше керувати великою кількістю користувачів та полегшить аналіз даних.

Розробка системи віддаленого оновлення прошивки Arduino через інтернет, це забезпечить можливість швидко виправляти помилки та додавати нові функції без фізичного доступу до пристрою.

Створення мобільного додатку для адміністраторів системи, який дозволить керувати правами доступу та переглядати логи в режимі реального часу;

Додавання додаткового рівня безпеки шляхом інтеграції біометричних сенсорів, таких як сканер відбитків пальців або розпізнавання обличчя;

Додавання можливостей керування системою через команди в Telegram боті, такі як додавання або видалення користувачів, блокування доступу на певний період часу, додавання або видалення ключа доступу;

Розробка механізму автоматичного резервного копіювання даних та можливості швидкого відновлення системи у разі технічних збоїв або аварій.

Наведені вище вектори розвитку розширяють функціональну та стабілізаційну складові систему контролю та управління доступом, в результаті зробивши її більш надійною та зручнішою у використанні як досвідченим користувачам так і новачкам.

Висновок до третього розділу: у процесі реалізації RFID системи було успішно впроваджено низку ключових компонентів, включаючи інтеграцію з Arduino ESP8266 та RFID-ридером, а також забезпечено зв'язок із месенджером

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Telegram для контролю доступу. Важливо відзначити, що система була ретельно спланована та виконана з урахуванням надійності та ефективності. Завдяки цьому, RFID система відзначається високою точністю ідентифікації, а також здатністю до швидкої обробки даних, що є критично важливим для безпеки та ефективності контролю доступу.

Під час тестування СКУД системи було виявлено, що система надійно відрізняє зареєстровані та незареєстровані RFID-мітки, що свідчить про високу точність та надійність роботи системи. Інтеграція з Telegram додатково забезпечила оперативне сповіщення про кожну спробу доступу, що є важливим для моніторингу безпеки об'єкта та відстеження діяльності користувачів. Висновок з цих тестів підтверджує, що СКУД система ефективно виконує свої функції та може бути надійним інструментом у системах контролю доступу.

Загалом, з урахуванням практичної реалізації та результатів тестування, можна вважати цю RFID-систему ефективною та надійною. Вона демонструє солідні переваги в контексті безпеки та контролю доступу, забезпечуючи високий рівень надійності та гнучкості у використанні.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

ВИСНОВКИ

У цій роботі ми детально розглянули основи, перспективи розвитку та технології RFID. У першому розділі ми зосередились на загальних відомостях про технологію RFID, розглянули принципи роботи RFID-систем, компоненти системи, типи RFID-міток, а також аналізували вартість і ефективність цих систем. Також ми оцінили майбутнє розвитку технології RFID.

У другому розділі була вивчена структура та безпека систем контролю та управління доступом на основі RFID. Ми розглянули архітектуру системи контролю та управління доступом RFID, програмне забезпечення у цих системах та ключові аспекти безпеки.

Нарешті, у третьому розділі ми перейшли до практичного застосування, де була представлена практична реалізація RFID системи та проведена перевірка роботи реалізованої системи контролю доступу.

В цілому, дана робота демонструє важливість та широкі можливості застосування RFID у різноманітних сферах, від покращення систем безпеки до ефективного управління ланцюжками поставок. Вона також підкреслює важливість уваги до аспектів безпеки і приватності при впровадженні цих технологій.

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. RFID TECHNOLOGY NAMES EXPLAINED [Електронний ресурс] – Режим доступу до ресурсу <https://voyantic.com/blog/posts/rfid-rain-rfid-uhf-rfid-epc-rfid-confused/>
2. Arduino RFID Solenoid Lock [Електронний ресурс] – Режим доступу до ресурсу - https://www.youtube.com/watch?v=nAcTO1LELN0&ab_channel=ViralScience-ThehomeofCreativity
3. RFID ідентифікація в логістиці [Електронний ресурс] – Режим доступу до ресурсу - <https://systemgroup.com.ua/uk/rfid-identyfikaciya-v-logistyci>
4. RFID-ключ [Електронний ресурс] – Режим доступу до ресурсу - <https://idcard.com.ua/ua/blog/rfid-klyuch-cto-eto-takoe-kak-rabotaet-i-kakie-vidy-byvayut/>
5. What is RFID and how it works? [Електронний ресурс] – Режим доступу до ресурсу - <https://www.techtarget.com/iotagenda/definition/RFID-radio-frequency-identification>
6. RFID reader [Електронний ресурс] – Режим доступу до ресурсу - <https://www.gartner.com/en/information-technology/glossary/rfid-reader>
7. What are RFID tags? – [Електронний ресурс] – Режим доступу до ресурсу – <https://www.camcode.com/blog/what-are-rfid-tags/>
8. Everything You Need to Know About RFID Tags – [Електронний ресурс] – Режим доступу до ресурсу – <https://blogs.bu.edu/llisa/everything-you-need-to-know-about-rfid-tags/>
9. What is a RFID? - [Електронний ресурс] – Режим доступу до ресурсу – <https://www.atlasrfidstore.com/rfid-resources/rfid-beginners-guide/>
10. RFID - [Електронний ресурс] – Режим доступу до ресурсу - https://www.pepperl-fuchs.com/global/en/classid_1542.htm
11. Design and Implementation of RFID Access Control System - [Електронний ресурс] – Режим доступу до ресурсу - <https://ieeexplore.ieee.org/document/9674127>

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

- 12.The Role of RFID in Access Control and Security Systems - [Електронний ресурс] – Режим доступу до ресурсу - <https://fastercapital.com/content/The-Role-of-RFID-in-Access-Control-and-Security-Systems.html>
- 13.Complete Guide To Rfid Access Control Door Lock And Entry Systems - [Електронний ресурс] – Режим доступу до ресурсу - <https://www.avigilon.com/blog/rfid-readers>
- 14.A Review of RFID in Supply Chain Management - [Електронний ресурс] – Режим доступу до ресурсу - https://ideas.repec.org/a/spr/gjofsm/v17y2016i2d10.1007_s40171-016-0136-2.html
- 15.Emerging RFID technology in structural engineering - [Електронний ресурс] – Режим доступу до ресурсу - <https://www.sciencedirect.com/science/article/abs/pii/S2352012420305968>
- 16.Evolution of Libraries: RFID and IoT Revolutionizing Access and Security- [Електронний ресурс] – Режим доступу до ресурсу - <https://medium.com/@contactrfid1/evolution-of-libraries-rfid-and-iot-revolutionizing-access-and-security-b1d99fc4f01b>
- 17.How to make rfid door lock using arduino - [Електронний ресурс] – Режим доступу до ресурсу - https://www.youtube.com/watch?v=XAxk_uQREiU&t=2s&ab_channel=SkynetRobotics
- 18.Access Control Systems [Features, Benefits & Challenges] - [Електронний ресурс] – Режим доступу до ресурсу - <https://webbylab.com/blog/10-top-features-of-modern-access-control-systems/>
- 19.RFID Door Lock - [Електронний ресурс] – Режим доступу до ресурсу - <https://projecthub.arduino.cc/mehmetefepekerr/rfid-door-lock-264c1e>
- 20.How to make a RFID door lock with Arduino - [Електронний ресурс] – Режим доступу до ресурсу - <https://srituhobby.com/how-to-make-a-rfid-door-lock-with-arduino/>

ДОДАТКИ

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Лістинг програмного коду

```

#define SS_PIN 15 // D3
#define RST_PIN 4 // D4
#include <SPI.h>
#include <MFRC522.h>
MFRC522 mfrc522(SS_PIN, RST_PIN);

#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>
#include <ESPDateTime.h>

const char* ssid = "TP-Link_35BC";
const char* password = "91604231";

#define CHAT_ID "431910835"
#define BOTtoken "6829319477:AAGIYJqGVMh0v29r67j0PXgwZbyGkXqf_Ps"
X509List cert(TELEGRAM_CERTIFICATE_ROOT);
WiFiClientSecure client;
UniversalTelegramBot bot(BOTtoken, client);

int relayPin = 16;
unsigned long lastTimeBotRan;

void setup() {
    Serial.begin(115200);
    SPI.begin();
    mfrc522.PCD_Init();
    pinMode(relayPin, OUTPUT);
    digitalWrite(relayPin, HIGH);
    Serial.println();
    Serial.println("Read UID tag on a MIFARE PICC:");

    configTime(2 * 3600, 3600, "pool.ntp.org", "time.nist.gov");
    setenv("TZ", "EET-2EEST,M3.5.0/3,M10.5.0/4", 1);
    tzset();

    client.setTrustAnchors(&cert);
    WiFi.mode(WIFI_STA);
    WiFi.begin(ssid, password);
    while (WiFi.status() != WL_CONNECTED) {
        delay(1000);
        Serial.println("Connecting to WiFi...");
    }
}

void loop() {
    if (!mfrc522.PICC_IsNewCardPresent()) {
        return;
    }
}

```

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

}

if (!mfr522.PICC_ReadCardSerial()) {
    return;
}

Serial.println();
Serial.print("UID tag :");
String content = "";

for (byte i = 0; i < mfr522.uid.size; i++) {
    Serial.print(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(mfr522.uid.uidByte[i], HEX);
    content.concat(String(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " "));
    content.concat(String(mfr522.uid.uidByte[i], HEX));
}
content.toUpperCase();
Serial.println();
String RFID_code = content.substring(1);
Serial.println(RFID_code);

String months[] = {"січня", "лютого", "березня", "квітня", "травня", "червня",
"липня", "серпня", "вересня", "жовтня", "листопада", "грудня"};

struct Person {
    String name;
    String surname;
    int age;
    String position;
    String uuid;
};

Person persons[] = {
    {"Іван", "Петренко", 30, "Інженер", "33 E7 3E B7"},
    {"Марія", "Іванова", 25, "Менеджер", "F8 08 89 0E"}
};

bool found = false;
for (Person p : persons) {
    if (RFID_code == p.uuid) {
        DateTimeParts dt = DateTime.getParts();
        String access_msg;
        access_msg += "\n✅ <b><u>Доступ Дозволено</u></b>";
        access_msg += "\n<b>UID тег:</b> " + p.uuid;
        access_msg += "\n<b>Ім'я:</b> " + p.name;
        access_msg += "\n<b>Прізвище:</b> " + p.surname;
        access_msg += "\n<b>Вік:</b> " + String(p.age);
        access_msg += "\n<b>Посада:</b> " + p.position;
        access_msg += "\n\n🔒 <b>Сповіщення про Успішний Доступ</b>";
        access_msg += "\n<b>Дата:</b> ";
    }
}

```

```

        access_msg += String(dt.getMonthDay() < 10 ? "0" : "") + String(dt.getMonth-
Day()) + " ";
        access_msg += String(months[dt.getMonth()]) + " ";
        access_msg += String(dt.getYear());
        access_msg += "\n<b>Час:</b> ";
        access_msg += String(dt.getHours() < 10 ? "0" : "") + String(dt.getHours()) +
":";
        access_msg += String(dt.getMinutes() < 10 ? "0" : "") +
String(dt.getMinutes());
        bot.sendMessage(CHAT_ID, access_msg, "HTML");

        digitalWrite(relayPin, LOW);
        delay(5000);
        digitalWrite(relayPin, HIGH);

        found = true;
        break;
    }
}

if (!found) {
    DateTimeParts dt = DateTime.getParts();
    String denied_msg;
    denied_msg += "\n⊗ <b><u>Доступ Заборонено</u></b>";
    denied_msg += "\n<b>UID тег:</b> " + RFID_code;
    denied_msg += "\n\n⚠ <b>Сповіщення про Спробу Доступу</b>";
    denied_msg += "\n<b>Дата:</b> ";
    denied_msg += String(dt.getMonthDay() < 10 ? "0" : "") + String(dt.getMonthDay())
+ " ";
    denied_msg += String(months[dt.getMonth()]) + " ";
    denied_msg += String(dt.getYear());
    denied_msg += "\n<b>Час:</b> ";
    denied_msg += String(dt.getHours() < 10 ? "0" : "") + String(dt.getHours()) +
":";
    denied_msg += String(dt.getMinutes() < 10 ? "0" : "") + String(dt.getMinutes());
    bot.sendMessage(CHAT_ID, denied_msg, "HTML");
}

mfrc522.PICC_HaltA();
mfrc522.PCD_StopCrypto1();

mfrc522.PCD_Init();

delay(1000);
}

```

		Кириєнко Є.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		61