Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет «Комп'ютерні технології і системи»
(назва факультету)

Кафедра «Електронні обчислювальні машини»
(повна назва кафедри)

Пояснювальна записка

до кваліфікаційної роботи
бакалавра
(ступінь вищої освіти)

на тему: Розробка засобів ідентифікації та аутентифікації систем контролю фізичного доступу

за освітньою програмою Кібербезпека
зі спеціальності: 125 Кібербезпека
(шифр і назва спеціальності)

Виконав: студент групи: КБ1811

_____ / Микита СЕМЕНОВ /
(підпис студента) (Ім'я ПРІЗВИЩЕ)

Керівник: _____ / доцент, Денис ОСТАПЕЦЬ /
(підпис) (посада, Ім'я ПРІЗВИЩЕ)

Нормоконтролер: _____ / ст. викладач, Володимир ДЗЮБА /
(підпис) (посада, Ім'я ПРІЗВИЩЕ)

Консультанти:

_____ _____ / /
(назва розділу) (підпис) (посада, Ім'я ПРІЗВИЩЕ)

_____ _____ / /
(назва розділу) (підпис) (посада, Ім'я ПРІЗВИЩЕ)

_____ _____ / /
(назва розділу) (підпис) (посада, Ім'я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Дніпро –2022 рік

Ministry of Education and Science of Ukraine
Ukrainian State University of Science and Technologies

Faculty «Computer technologies and systems»
(faculty)

Department «Electronic computers»
(department)

Explanatory Note
to Master's Thesis
first (bachelor's)
(higher education degree)

on the topic: Development of identification and authentication systems for physical access control systems

according to educational curriculum Кібербезпека

in the Speciality: 125 Cybersecurity
(speciality and its code)

Done by the student of the group: KB1811 / Nikita Semenov /
(name, surname)

Scientific Supervisor: / Associate Professor, Denis Ostapets /
(position, name, surname)

Normative controller : / Senior lecturer, Volodymyr Dziuba /
(position, name, surname)

Supervisors

(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)
(Chapter title heading)	/ / (position, name, surname)

Dnipro – 2022

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи
Кафедра: ЕОМ
Рівень вищої освіти: Перший (бакалаврський)
Освітня програма: Кібербезпека
Спеціальність: 125 Кібербезпека
(шифр та назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ЕОМ
(підпис) Ігор ЖУКОВИЦЬКИЙ (Ім'я ПРІЗВИЩЕ)
Дата 22.06.2022р.

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра
(ступінь вищої освіти)

студенту Семенову Микиті Сергійовичу
(Прізвище, Ім'я По батькові)

1. Тема роботи: Розробка засобів ідентифікації та аутентифікації систем контролю фізичного доступу.

Керівник роботи: Остапець Денис Олександрович, к.т.н, доцент
(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від "07" 12 2021 р. № 67ст
2. Строк подання студентом роботи: 13.06.2022 р.
3. Вихідні дані до роботи:
Методи ідентифікації та аутентифікації користувачів;
Структура системи контролю фізичного доступу
4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):
4.1 Аналітична частина:
Аналіз методів ідентифікації та аутентифікації користувачів
4.2 Основна частина:
- Огляд методів та засобів аутентифікації та ідентифікації в системах контролю доступу;
- Функціонування та інформаційна структура системи;
- Розробка апаратної частини;
- Розробка програмної частини;
- Перевірка працездатності системи.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
- Порівняльний аналіз методів аутентифікації та ідентифікації;

- Склад системи;
- Інформаційна структура системи;
- Вибір апаратних засобів;
- Схема пристрою;
- Основні алгоритми програм;
- Приклади роботи системи

6. Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав: (підпис консультанта, дата)	Завдання прийняв: (підпис студента, дата)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд методів та засобів аутентифікації та ідентифікації в системах контролю доступу	25.04.22	20%
2	Функціонування та інформаційна структура	05.05.22	15%
3	Розробка апаратної частини	19.05.22	20%
4	Розробка та налагодження програмного забезпечення	06.06.22	40%
5	Реферат, вступ, висновки	13.06.22	5%
6	Подання кваліфікаційної роботи до кафедри	13.06.22	
7	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	23.06.22	

Студент _____ (підпис) Микита СЕМЕНОВ (Ім'я ПРІЗВИЩЕ)

Керівник роботи _____ (підпис) Денис ОСТАПЕЦЬ (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи бакалавра: 52с., 32 рис., 2 табл., 4 додатка, 18 джерел.

Об’єкт розробки – програмно-апаратні засоби майнової ідентифікації та аутентифікації системи контролю фізичного доступу.

Мета роботи – розробка засобів ідентифікації та аутентифікації системи контролю фізичного доступу.

Проаналізовано методи та засоби ідентифікації та аутентифікації в системах контролю доступу. На основі проведеного аналізу обрано два методи майнової ідентифікації та аутентифікації: за допомогою RFID-карт та за одноразовим паролем з використанням смартфону. Розглянуто типові схеми систем контролю доступу на базі RFID та розроблено схеми функціонування системи, наведено інформацій структуру системи. Обрано апаратні засоби для реалізації системи та розроблено схему з’єднань елементів системи. Обрано засоби розробки програмної частини системи, необхідні бібліотеки та розроблена програмна частини системи, наведені блок-схеми роботи системи та перевірена працездатність.

Ключові слова: C, C++, КОНТРОЛЬ ФІЗИЧНОГО ДОСТУПУ, ARDUINO, IOT, TELEGRAM, ОДНОРАЗОВИЙ ПАРОЛЬ, RFID, ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ

ЗМІСТ

ВСТУП

Питання безпеки фізичного доступу піднімаються щодня, у різноманітних сферах: у побуті, для захисту периметру підприємства від небажаних відвідувачів, для допуску у те чи інше приміщення, тощо. Для цього використовуються засоби ідентифікації та аутентифікації: біометричні, парольні та майнові, які можна комбінувати між собою. Робота присвячена питанню ідентифікації та аутентифікації в системах контролю фізичного доступу. Тому тема цієї роботи є актуальною.

Тема роботи затверджена наказом по університету №67ст від 07.12.2021 р.

Метою роботи є розробка засобів ідентифікації та аутентифікації системи контролю фізичного доступу.

Основні положення роботи доповідались та були схвалені на XV Міжнародній конференції «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті» у 2021 році (див. додаток А).

Представлена робота складається зі вступу, 5 розділів та висновків.

У розділі 1 представлений огляд систем контролю доступу та аналіз засобів ідентифікації та аутентифікації. Розглянуто загальну структуру систем та її складових. Для описаних засобів майнової ідентифікації проведено порівняльний аналіз.

У розділі 2 наведено типи систем контролю доступу з майновими ідентифікаторами, сформовано склад системи та здійснено опис методів які буде реалізувати система.

У розділі 3 здійснено вибір апаратної частини системи, описано характеристики спеціальних модулів та підключення системи. Також наведено схему з’єднань елементів системи.

У розділі 4 здійснено вибір середовища та мови програмування для розробки програмної частини системи. Розроблено блок-схеми роботи окремих функцій та програмне забезпечення системи.

У розділі 5 виконано перевірку працездатності системи, показано ідентифікацію та аутентифікацію за допомогою карти RFID, одноразового паролю та роботу с ботом.

В додатках Б, В наведено вихідні коди програм.

1 ОГЛЯД МЕТОДІВ ТА ЗАСОБІВ АУТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

1.1 Загальні відомості

Більшість компаній у своїй повсякденній діяльності стикається із завданням виключити несанкціонований доступ на свою територію і в приміщення, а також отримати інформацію про те, де саме знаходяться в даний момент співробітники і численні відвідувачі. Вирішити ці завдання можна за допомогою автоматизованої системи контролю та управління доступом (СКУД).

У широкому сенсі СКУД - це сукупність апаратно-програмних засобів і організаційних заходів. Її головне завдання - автоматизувати процес санкціонованого контрольованого доступу і обліку співробітників, відвідувачів і транспортних засобів на території підприємства[1].

Всі системи контролю та управління доступом поділяють за принципом роботи:

- Автономні;
- Мережеві;
- Змішані.

Основною характеристикою автономної СКУД є контролер. Крім цього, в цьому виді систем є:

- джерело живлення;
- зчитувач (магнітний або штриховий);
- виконавчий пристрій.

Такі системи мають невисоку вартість, яка обумовлена простотою їх роботи. Основними завданнями автономних систем є організація входу-виходу на територію шляхом збору та зберігання інформації.

Відмінною характеристикою мережевих СКУД є можливість віддаленого управління. При цьому ПО, яке встановлено в системі дозволяє працювати з інформацією, здійснюючи її аналіз. Крім пропускної функції, мережеві СКУД можуть виконувати ідентифікацію осіб з правом доступу, обмеження, облік робочого часу службовців підприємства, контроль і облік відвідувачів, облік

зарплат і т.д. Також сучасні СКУД виробляють комплексний підхід до організації безпеки: здатні інтегруватися з системами безпеки - сигналізації, пожежної, відеоспостереження, систем аварійного освітлення.

Системи такого роду проявили свою ефективність на великих об'єктах, з багаторівневою системою охорони.

Змішані або комбіновані СКУД також має можливість віддаленого управління, крім цього, продовжує працювати навіть тоді, коли зв'язок з центром управління втрачена або мережеве обладнання тимчасово виявилося непрацездатним[2].

Чим складнішою (комплексної) є СКУД, тим більше у неї функціональних можливостей. Наприклад, можна в реальному часі відстежувати переміщення співробітників по планам приміщень, можна контролювати пожежну безпеку, можна здійснювати «фотобейджінг» - зіставлення особи відвідувача з його фотографією, можна автоматично розпізнавати номери автомобільного та залізничного транспорту і контролювати його проїзд.

1.2 Огляд методів ідентифікації та аутентифікації

Бувають методи ідентифікації трьох видів:

- Парольні
- Біометричні
- Майнові

Найбільш популярними парольними методами на даний момент є:

- Методи, що використовують постійний (багаторазово використовуються) паролі
- Методи, що використовують одноразові (динамічно змінюються) паролі [3].

На сьогодні популярними методами біометрії являються:

- **Аутентифікація за відбитками пальців**

Переваги засобів аутентифікації за відбитками пальців - простота використання, зручність та надійність. Весь процес ідентифікації здійснюється

швидко та не вимагає особливих зусиль від користувачів. Вірогідність помилки при ідентифікації користувача набагато менша порівняно з іншими біометричними методами[4].

- **Аутентифікація за рисами обличчя**

Біометрія по геометрії особи (аналіз характерних точок на обличчі людини) є другою за поширеністю на ринку біометричних систем. Вона являє собою дистанційний контроль, тому не вимагає безпосереднього контакту з людиною, особа якою встановлюється.

- **Аутентифікація за будовою вен**

Біометрія за будовою вен пальця, долоні, руки має високу ступінь технічної досконалості і складна з точки зору обходу системи, так як важко створити муляж біометричного ознаки[5].

Популярні методи майнової ідентифікації:

Виділяють кілька типів речових ідентифікаторів:

- Ідентифікатори з перфораційним кодуванням;
- Карти ідентифікаційні Wiegand;
- Безконтактні ідентифікатори RFID (технологія Proximity);
- Ідентифікаційні Smart-карти (карти з штучним інтелектом);
- Електронні ключі iButton (Touch Memory);
- Ідентифікаційні карти з магнітним кодуванням;

Найменшою імітостойкость володіють системи, що використовують такі типи ідентифікаторів:

- Ідентифікатори з перфораційним кодуванням;
- Електронні ключі iButton (Touch Memory) типу DS1990A;
- Ідентифікаційні карти з магнітним кодуванням.

Найкращу імітостойкость демонструють системи з такими типами ідентифікаторів:

- Електронні ключі iButton (Touch Memory), за винятком типу DS1990A (немає захисту від копіювання даних);

- Ідентифікаційна карта Wiegand;
- Ідентифікаційна Smart-карта.

Пасивні майнові методи ідентифікації

- Ідентифікаційна картка з магнітним кодуванням

Карти із магнітними смужками почали використовувати ще на початку 70-х років. Тоді магнітні смужки наносилися на ідентифікаційні картки з паперу та плівки, а також на кредитні картки. Карти з магнітною смужкою широко використовуються у всьому світі. Ця технологія залишається домінуючою у США, де вона застосовується для обробки платежів, а також у контрольно-пропускних системах.

Магнітна смуга може бути двох видів: HiCo, LoCo.

HiCo - це скорочення означає **High Coercivity (високий рівень коерцитивності).** Магнітні смужки HiCo забезпечують найвищий рівень захисту даних на магнітній смужці від зовнішніх магнітних полів. Такі магнітні смужки складніше кодувати порівняно з магнітними смужками LoCo, тому що для процесу кодування потрібна більш висока потужність. Цим пояснюється більш висока вартість карток з магнітними смужками HiCo.

LoCo - це скорочення означає **Low Coercivity (низький рівень коерцитивності)**. Такі карти простіше кодувати, і вони коштують менше карток з магнітними смужками HiCo[6].

- Електронний ключ iButton

Кожна така мікросхема укладена в сталевий герметичний циліндричний корпус і має унікальний реєстраційний номер (ID), що записується в процесі виготовлення у постійний внутрішній пристрій. Кількість комбінацій ID досягає 256 трильйонів - цього більш ніж достатньо, щоб унеможливити випадковий підбір[7].

- Безконтактний ідентифікатор RFID

RFID – технологія, яка для автоматичної ідентифікації об'єктів використовує радіохвилі. Вона може розпізнавати як живі істоти, а й неживі предмети,

наприклад, транспортні засоби, контейнери, одяг та багато іншого. Іншим прикладом Auto-ID є штрих-коди або біометричні методи (сканування сітківки ока, використання відбитків пальців), а також система оптичного розпізнавання символів та ідентифікація голосу.

Основа роботи технології: взаємодія RFID-мітки (RFID-тега) та RFID-зчитувача (RFID-рідера). RFID-мітка – мініатюрний чіп, який зберігає унікальний номер тега та інформацію та має можливість для передачі даних RFID-рідеру. Як тільки RFID-мітка потрапляє в зону дії RFID-рідера, рідер фіксує факт передачі даних, зчитує інформацію з мітки та передає її до облікової системи, яка аналізує дані за заздалегідь заданими алгоритмами[8].

При цьому між RFID-міткою та RFID-рідером може бути відстань до 300 метрів (системи, що працюють на відстані від 5 до 300 метрів відносять до систем далекої ідентифікації, від 20 см до 5 м – ідентифікації середньої дальності, до 20 см – системи ближньої ідентифікації).

1.3 Аналіз майнових методів аутентифікації та ідентифікації

У цій кваліфікаційній роботі вирішено використовувати майнові методи аутентифікації, тому що вони на даний момент мають найбільшу популярність та порівняно невелику ціну серед методів ідентифікації. При цьому популярні як пасивні методи, так і активні з використанням одноразових паролів.

Порівняльна характеристика пасивних ідентифікаторів наведена в таблиці 1.1.

Таблиця 1.1 – Порівняльна характеристика пасивних ідентифікаторів

Методи ідентифікації / Критерії	Ідентифікація по матеріальному коду		
	Безконтактний ідентифікатор RFID	Електронні ключі iButton	Ідентифікаційна картка з магнітним кодуванням
Достовірність зчитування	+++	+++	+
Стійкість до копіювання	++	+	++
Імітостійкість	+++	+	+
Продуктивність (пропускна здатність)	+++	+++	++

Закінчення таблиці 1.1

Стійкість до зовнішніх впливів	+++	+++	+++
Зручність використання	+++	++	++
Вартість виробництва і експлуатації	+++	+++	+++

Примітки. У таблиці використовуються наступні позначення відповідних відносних критеріїв оцінки:

“+” – відносно низька;

“++” – відносно середня.;

“+++” – відносно висока.

З наведених вище методів обрано RFID-мітки оскільки дані мітки можуть бути перезаписані та доповнюватись багато разів, вони можуть зчитуватись на значній відстані та мають відносно високий рівень захищеності. Як активний засіб аутентифікації обрано смартфон, на який надсилатиметься одноразовий пароль. Виходячи з наведених вище аспектів системи можливо розробити постановку задачі (див. Додаток Г).

1.4 Висновки за розділом

В розділу наведені основні поняття систем контролю доступу. Наведено огляд відомих методів ідентифікації та аутентифікації. За результатами порівняння майнових ідентифікаторів обрано RFID-мітки та як активний засіб аутентифікації обрано смартфон з одноразовим паролем.

2 ФУНКЦІОНУВАННЯ ТА ІНФОРМАЦІЙНА СТРУКТУРА СИСТЕМИ

2.1 Аналіз схем систем контролю доступу на базі RFID

RFID успішно використовується у рішеннях, що забезпечують контроль доступу. Рішення такого типу характеризується таким:

1) Мітка містить унікальні ідентифікаційні дані та переміщується разом з об'єктом або людиною для отримання доступу (наприклад, мітка, прикріплена на лобове скло автомобіля, вбудована у нагрудне посвідчення або впроваджена під шкіру людини);
2) Ідентифікаційні дані мітки зчитуються в пунктах контролю доступу (для того, щоб потім ретранслювати ідентифікатор у систему безпеки, що видає дозвіл на дійсний доступ)

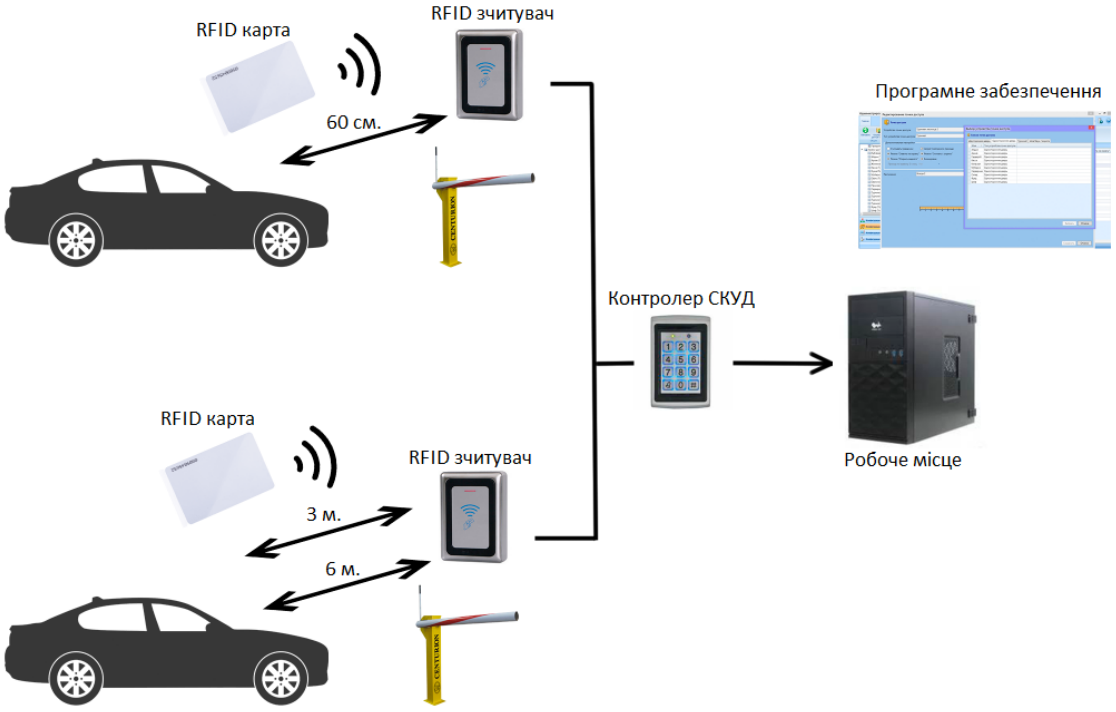

Рисунок 2.1 – Приклад системи контролю доступу на базі RFID

Цей тип прикладних систем є відносно зрілим у порівнянні з деякими іншими переважаючими типами систем з позицій RFID технології та систем, що відносяться до неї. Однією з ознак зрілості технології є існування стандартів для

неї. Стандарт на карти доступу ISO 15693 (ISO SC17/WG8) широко прийнятий у системах контролю доступу, що випускаються, для частоти 13,56 МГц.

Ось деякі добре відомі приклади прикладних систем, що належать до цього типу:

- Системи охорони периметра та будівлі,
- Системи доступу на автостоянки.

У другій системі пасивна RFID мітка прикріплюється до автомобіля (наприклад, на лобове скло), якому потрібен доступ до системи автостоянки. Коли водій під'їжджає цією машиною до в'їзду на автостоянку, рідер зчитує унікальні дані мітки та ретранслює їх у систему доступу. Ця система залежить від дозволу на доступ, пов'язаного з даними мітки, або надає, або забороняє доступ до паркувальної зони.

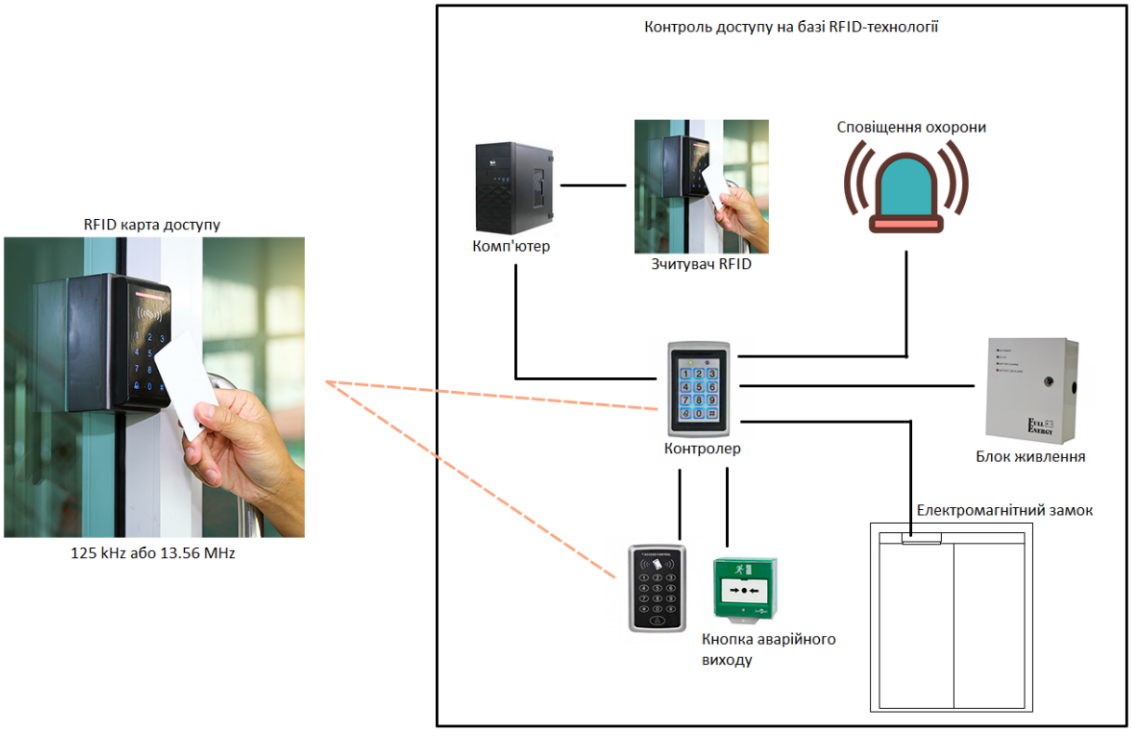

Рисунок 2.2 – Приклад системи з пасивною міткою RFID

Якщо доступ надано, то відкриваються в'їзна брама і автомобіль допускається в паркувальну зону. Зазвичай для такої прикладної системи використовуються пасивні позначки з частотою 13,56 МГц. Також використовуються активні та напівактивні RFID мітки, якщо потрібний великий радіус дії та вдосконалений

захист. Перший із вищенаведених представників цього типу систем одна із найпоширеніших.

Серед біометричних ідентифікаторів найбільш привабливі системи, що використовують не менше двох методів ідентифікації з включенням біометрії за будовою вен пальця і руки[9].

2.2 Склад та функціонування системи

Система, що розробляється, складається зі зчитувача карт, контролеру та матричної клавіатури. Структурну схему системи приведено на рисунку 2.3.

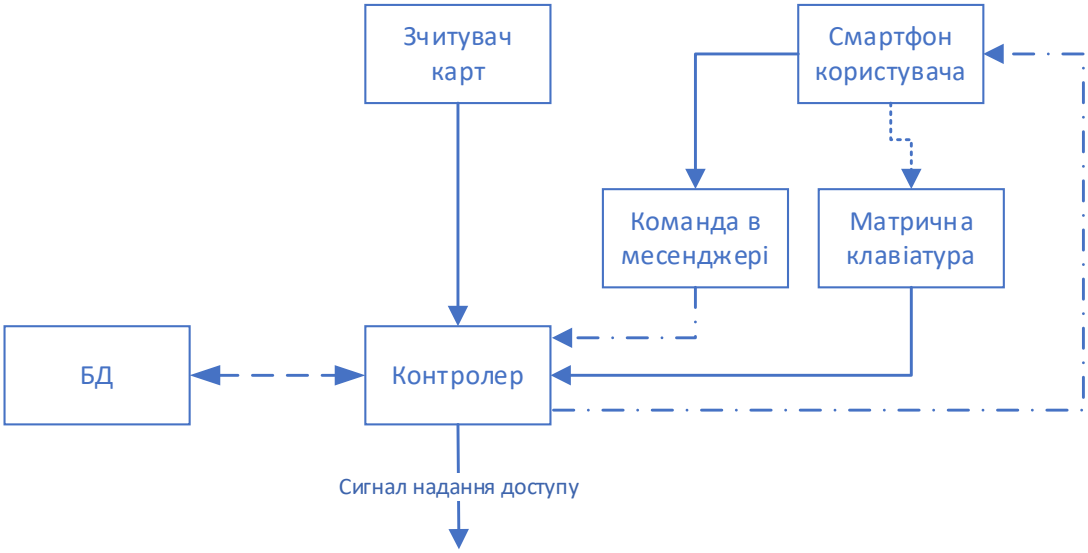

Рисунок 2.3 – Структура системи

Система буде реалізувати зчитування карт за допомогою зчитувача карт та послідуючу перевірку даних з карти, або очікувати повідомлення від користувача в месенджері для генерації одноразового паролю. Якщо ідентифікатор користувача який працює з системою співпадає з ідентифікатором який існує в базі даних йому відправляється в месенджер згенерований одноразовий пароль, після цього користувач має вводити на матричну клавіатуру одноразовий пароль. Система на основі отриманих даних приймає рішення, відправляти сигнал на надання доступу. Функціональна схема приведена на рисунку 2.4.

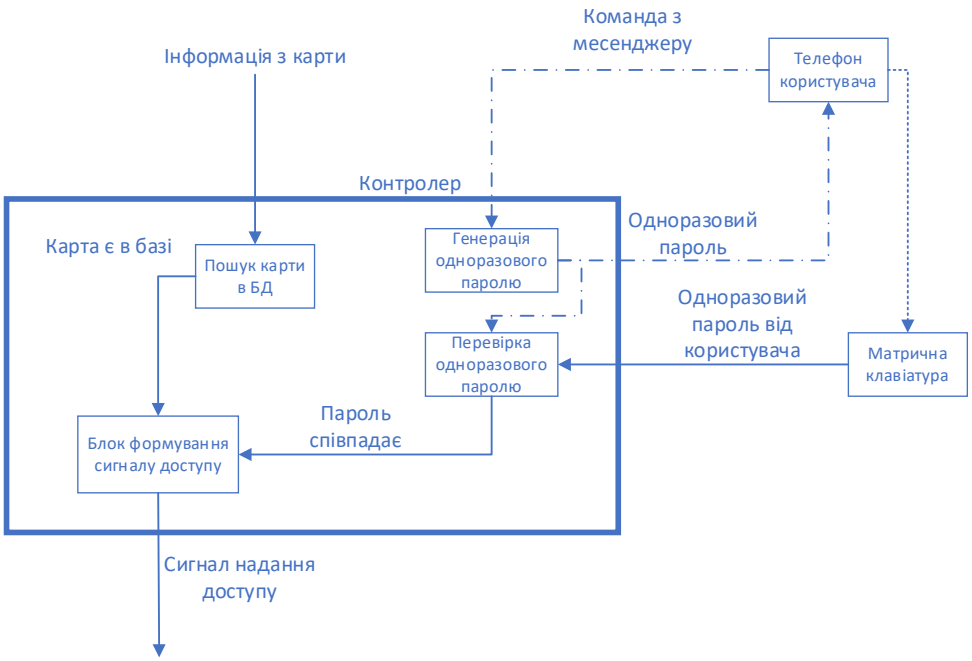

Рисунок 2.4 – Функціонування системи

Передбачається, що на смартфоні користувача встановлено Телеграм. Управління виконується за допомогою команд телеграм бота. Смартфон підключається до контролера за допомогою мережі Wi-Fi. Користувачі які існують в базі даних системи мають доступ до ідентифікації за допомогою карти або одноразового паролю, але додав рівні доступу для користувачів можливо розширити можливості системи та зробити її більш гнучкою, так, наприклад користувач який має адміністративний рівень доступу (далі адміністратор) працює з системою через команди месенджеру може мати змогу переглянути базу даних користувачів, обирати та змінювати певну інформацію в базі даних користувачів та заносити оновлену базу даних до пам’яті системи.

Виходячи з перерахованих вище дій із системою можна створити таблицю процедур які можуть бути реалізовані в системі (див. табл. 2.1).

Таблиця 2.1 – Основні процедури

Назва процедури	Рівень доступу	Що виконує
start	Більше або дорівнює 0	Виводить загальний список команд для користувача

Закінчення таблиці 2.1

oneTimePassword	Більше або дорівнює 0	Генерує одноразовий випадковий пароль для користувача
adminMenu	Більше 1	Виводить список команд для адміністратора
showDataBase	Більше 1	Виводить базу даних користувачів
changeUsersRFID	Більше 1	Дозволяє змінювати RFID-картку обраного користувача
changeUsersUID	Більше 1	Дозволяє змінювати унікальний ідентифікатор телеграму обраного користувача
changeUsersAccessLevel	Більше 1	Дозволяє змінювати рівень доступу обраного користувача
Зчитування даних із зчитувача карт	-	Отримує дані з карти
Порівняння даних з карти із даними що є в системі	-	Порівнює отримані дані зі зчитувача з даними які існують в базі даних
Подання сигналу для надання доступу	-	Подає сигнал надання доступу
Прийом команд з месенджеру	-	Отримує та визначає команди з месенджеру

2.1 Інформаційна структура

База даних складається з 4-х параметрів, таких як логін користувача, унікальний ідентифікатор акаунта в месенджері, тип доступу користувача та RFID-ключ персональної карти доступу. Структура бази даних та типів які використовуються наведено на рисунку 2.5.

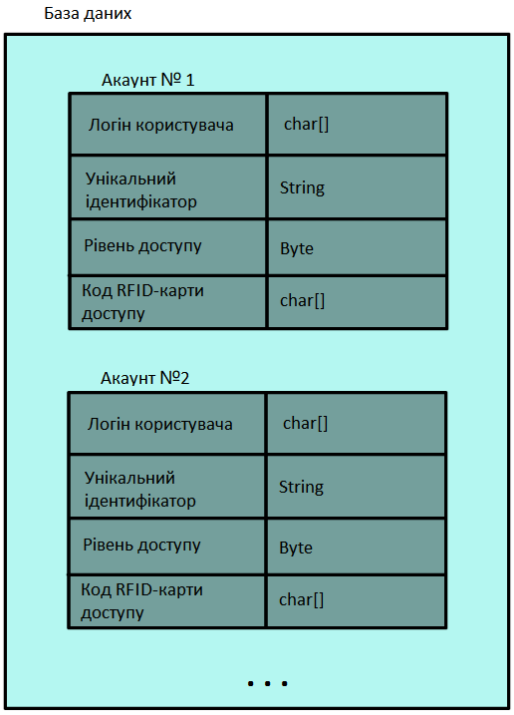

Рисунок 2.5 – Структура бази даних

Зміна даних у системі реалізуватиметься за допомогою спеціальних команд в месенджері які будуть відповідати за певний параметр в базі даних. Адміністратор обирає команду після чого вводить за допомогою матричної клавіатури індекс користувача, дані якого необхідно змінити та вводить нову інформацію через зчитувач карт якщо необхідно змінити персональну карту користувача або через матричну клавіатуру якщо необхідно змінити числові параметри, такі як ідентифікаційний номер месенджеру та рівень доступу.

2.2 Висновки за розділом

Проведено аналіз популярних схем систем контролю на базі RFID. Наведено склад системи, порядок функціонування системи та структуру бази даних.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ

3.1 Вибір апаратних засобів системи

В якості контролеру системи було обрано модуль ESP8266 з модифікацією плати розробника NodeMCU (рисунок 3.1) який являє собою UART-WiFi модуль з ультра низьким споживанням енергії. Сам чіп спроектований для пристроїв зі світу інтернет речей, а дана плата дозволяє спростити розробку, тому що на ній вже реалізовано підключення по USB. Крім цього плата має прошивку NodeMCU, що дозволяє програмувати її за допомогою мови Lua або за допомогою Arduino IDE. Схему контактів плати наведено на рисунку 3.2.

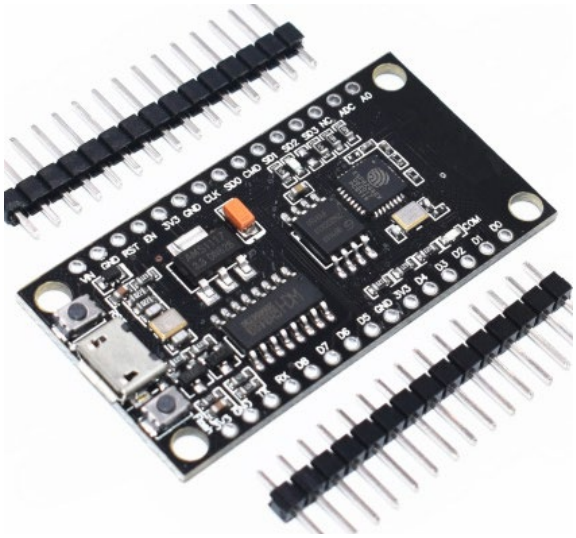

Рисунок 3.1 – Модуль ESP8266 з модифікацією NodeMCU

Характеристика модуля[10]**:**

- Wi-Fi 802.11 b / g / n
- Підтримка STA / AP / STA + AP режимів
- Вбудований стек протоколів TCP / IP з підтримкою множинних клієнтських підключень (до 5)
- D0 ~ D8, SD1 ~ SD3: можуть бути використані як GPIO, PWM, IIC, тощо.
- Ток на вивод: 15 мА
- AD0: 1 виведення АЦП

- Живлення: 4.5 - 9В (10В максимум), живлення від USB з наданням отладочного інтерфейсу
- Споживання: обмін даними: ~ 70 мА (200 мА максимум), очікування: <200 мкА
- Діапазон робочих температур: -40 ~ +125 ° C
- Швидкість передачі 110-460800 б/сек

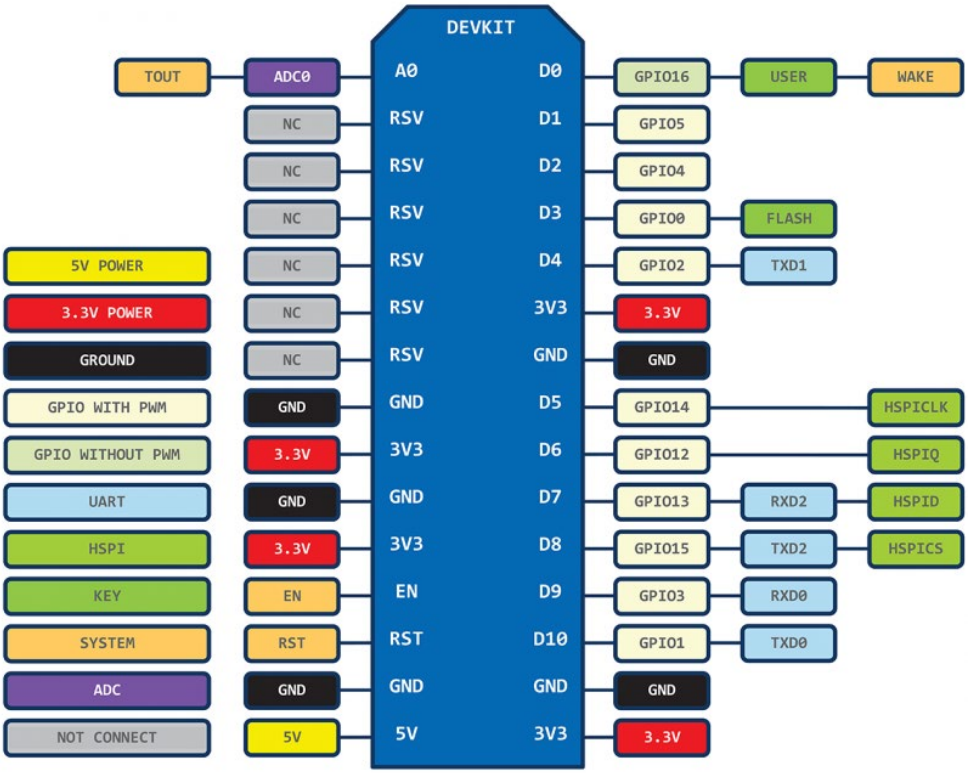

Рисунок 3.2 – Схема контактів плати NodeMCU

В якості зчитувача карт було обрано модуль RFID RC522. Тому що даний модуль легко інтегрується в систему та може використовуватись для різних комерційних цілей, в тому числі контроль доступу та автоматичної ідентифікації. Як виглядає модуль наведено на рисунку 3.3.

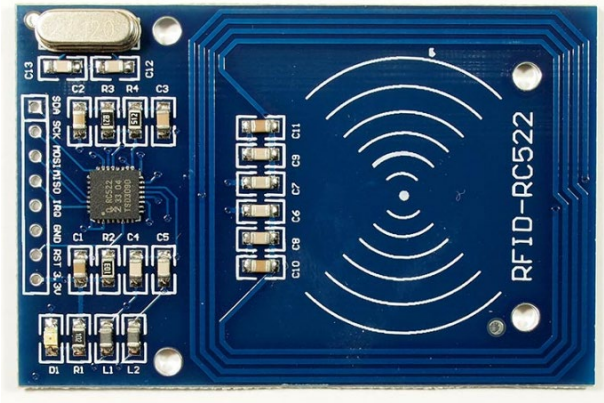

Рисунок 3.3 – Модуль RFID RC522

Даний модуль потребує підключення до NodeMCU за такою схемою [11]:

- Vcc – 3V3
- RST – D0
- GND – GND
- MISO (Master Input Slave Output) – D6
- MOSI (Master Output Slave Input) – D7
- SCK (Serial Clock) – D5
- SS/SDA (Slave select) – D8

Схему контактів модуля наведено на рисунку 3.4.

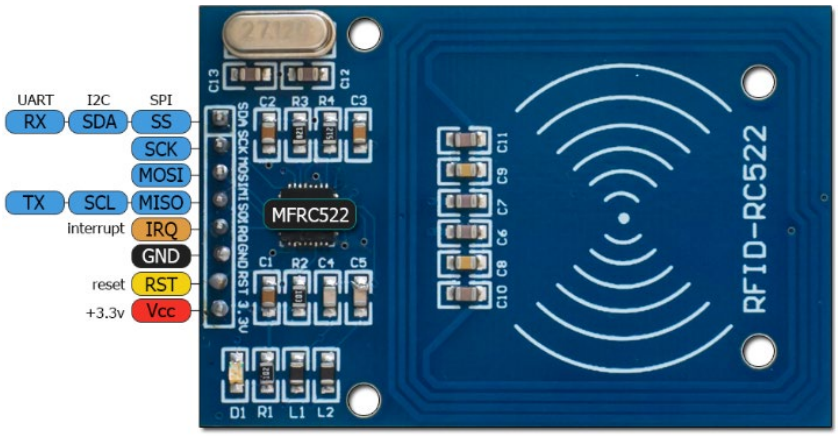

Рисунок 3.4 – Схема контактів модуля RFID RC522

Характеристики модуля [12]**:**

- Напруга живлення : 3.3V
- Струм: 13-26mA
- У режимі очікування: 10-13ma

- У сплячому режимі: менше 80 мкА
- Робоча частота: 13.56MHz
- Дальність зчитування: 0 ~ 60 мм
- Інтерфейс: SPI, максимальна швидкість передачі 10Мбіт/с

В якості матричної клавіатури було обрано мембранну клавіатуру на 16 кнопок (рисунок 3.5), такий вибір обумовлений можливістю розширювати системний комплекс під особисті потреби компанії, де 10 кнопок використовуються для чисел, 2 для вводу в контролер даних та 4 пусті, які можливо запрограмувати під особисті потреби.

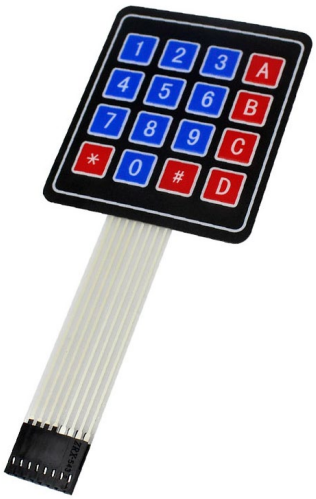

Рисунок 3.5 – Мембрана клавіатура 4x4

Також, через те, що модуль RC522 використовує майже всі Digital порти на NodeMCU, які потребує мембрана клавіатура, було вирішено використовувати Arduino Uno. Схема плати Arduino Uno наведена на рисунку 3.6. [13]

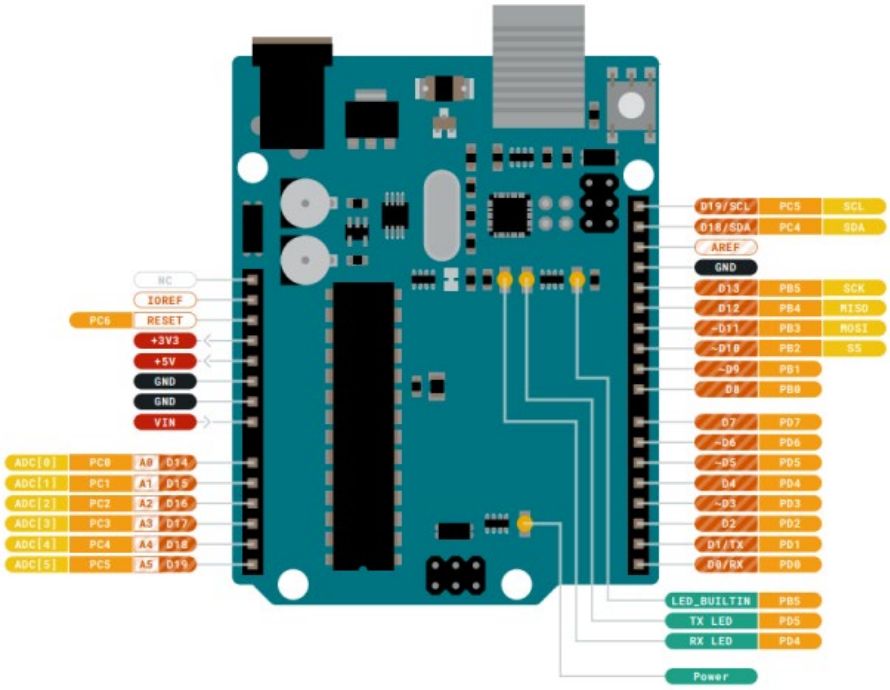

Рисунок 3.6 – Схема контактів Arduino Uno

3.2 Розробка схеми пристрою

Arduino Uno має достатньо Digital портів для підключення до неї мембранної клавіатури на 16 кнопок. Схема підключення мембранної клавіатури до плати Arduino Uno наведено на рисунку 3.7.

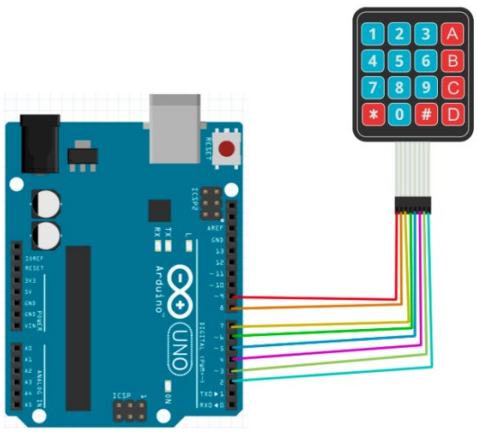

Рисунок 3.7 – Підключення мембранної клавіатури до Arduino Uno

NodeMCU може використовуватись як єдиний спосіб живлення системи, але для більш стійкої роботи системи рекомендується використовувати 2 способи

живлення, один для Arduino Uno, та другий для NodeMCU. Підключення Arduino Uno до модуля ESP8266 NodeMCU наведено на рисунку 3.8.

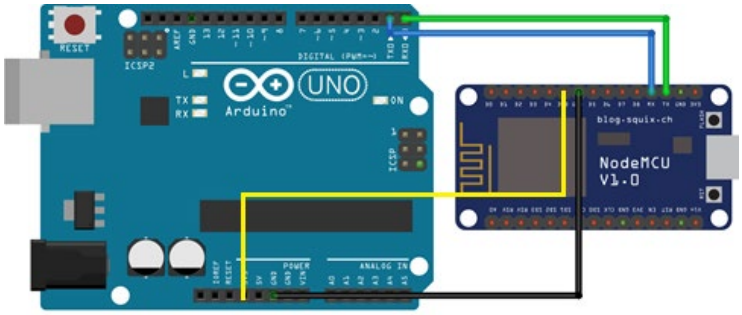

Рисунок 3.8 – Підключення Arduino Uno до модуля ESP8266 NodeMCU

Для демонстрації подання сигналу для надання доступу користувачу використано діод Led який підключено до NodeMCU та резистор на 10k.

Загальна схема системи наведена на рисунку 3.9

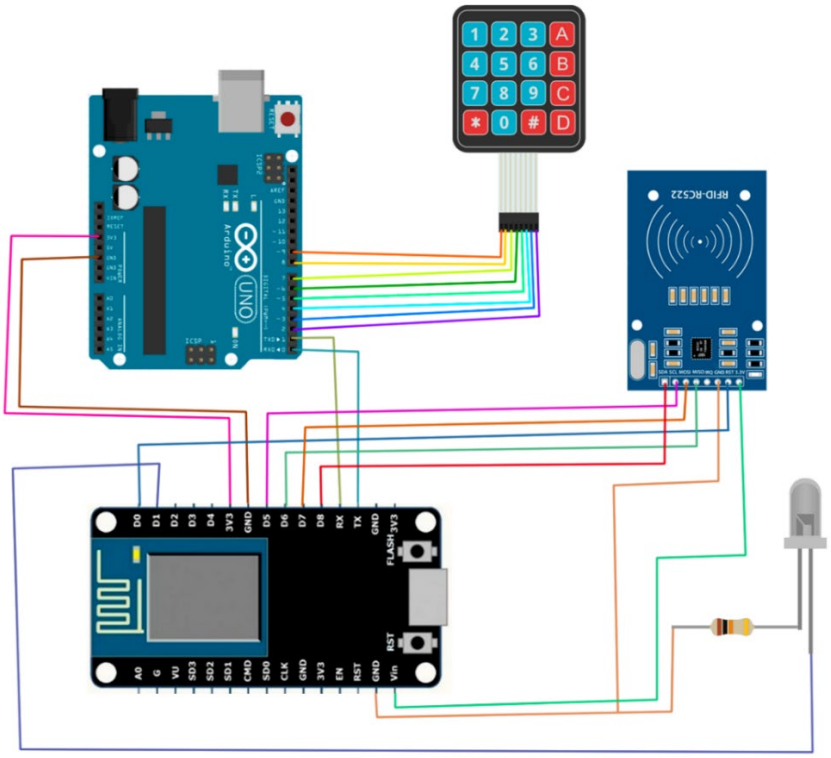

Рисунок 3.9 – Схема з’єднань елементів системи

Також для стабілізації напруги на діод було використано резистор на 10k.

3.3 Висновки за розділом

Обрано апаратну частину системи. Розроблено схеми підключення окремих частин системи та загальну схему підключення системи.

4 РОЗРОБКА ПРОГРАМНОЇ ЧАСТИНИ

4.1 Вибір засобів розробки програмного забезпечення

Як середовище для програмування системи було обрано Arduino IDE[14]. В якості мови програмування було обрано мову програмування C/C++ яка скомпонована з бібліотекою AVR Libc.

Бібліотека AVR Libc надає можливість працювати з великою кількістю різноманітних мікроконтролерів, до списку яких входить ATmega328 яка знаходиться в Arduino Uno[15].

Для програмування ESP8266 використано бібліотеку ESP8266WiFi[16] також для зв'язку з Telegram була обрана бібліотека UniversalTelegramBot[17] у зв'язку з її швидкістю роботи, функціональності та надійним зв'язком між системою та Telegram. Також для зв'язку системи з Wi-Fi використана бібліотека WiFiClientSecure[18] яка в свою чергу відповідає за безпечне з'єднання за допомогою TLS(SSL). Існує три способи встановлення безпечного з'єднання за допомогою бібліотеки WiFiClientSecure:

- Використання сертифікату кореневого центру сертифікації (CA)
- Використання кореневого сертифікату CA плюс сертифікату клієнта та ключа
- Використання попереднього спільного ключа (PSK)

В даній кваліфікаційній роботі використано сертифікат кореневого центру сертифікації, цей метод аутентифікує сервер і узгоджує зашифроване з'єднання. Це та сама функціональність, що реалізована у вашому веб-переглядачі, коли ви підключаєтеся до сайтів HTTPS.

4.2 Розробка програмного забезпечення ESP8266 з модифікацією NodeMCU

Узагальнений алгоритм роботи системи представлений на рисунку 4.1. Загальний код системи наведений у додатку Б.

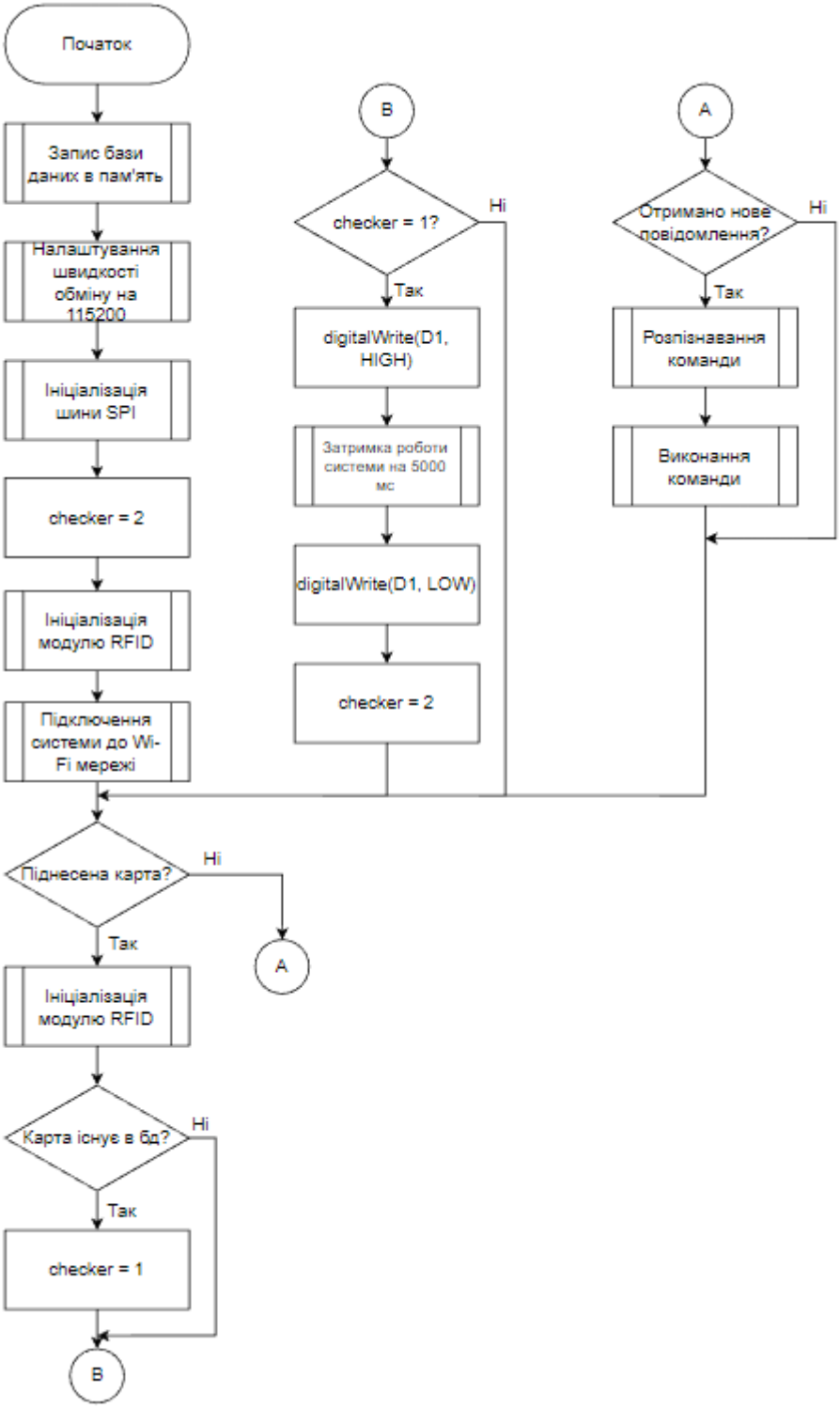

Рисунок 4.1 – Узагальнений алгоритм роботи системи

Процес отримання даних з RFID-карти та перевірки з базою даних показано на рисунку 4.2.

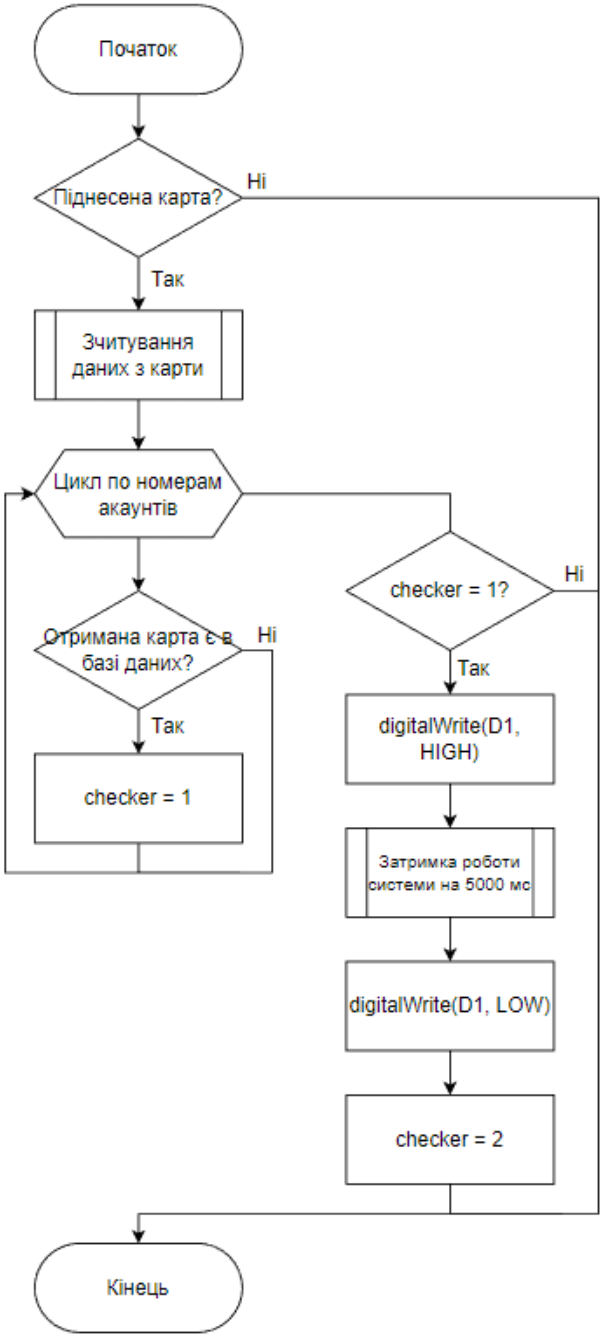

Рисунок 4.2 – Узагальнений алгоритм перевірки RFID-карти

4.3 Розробка програмного забезпечення Arduino UNO

Для передачі інформації про стан нажатої кнопки з Arduino Uno до NodeMCU був написаний алгоритм для передачі стану нажатої кнопки на клавіатурі через Serial з’єднання з NodeMCU (рисунок 4.3). Код для передачі інформації про стан нажатої кнопки наведений у додатку В.

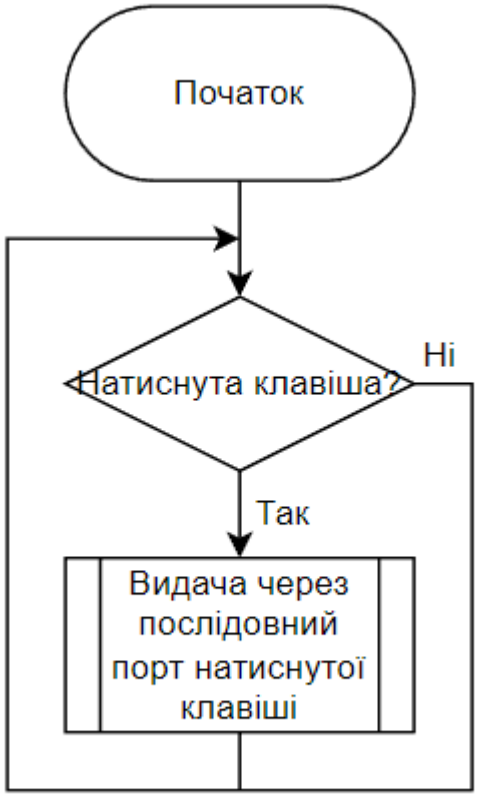

Рисунок 4.3 – Узагальнений алгоритм обробки клавіатури на базі Arduino UNO

4.4 Розробка програмного забезпечення Telegram боту

В якості месенджеру використано Telegram тому що сервіс побудований на шифруванні MTProto та дозволяє легко створювати ботів будь-яких цілей, в тому числі для отримання випадкових одноразових паролів та роботи з системними комплексами різних рівнів складності.

Команда /start перевіряє доступ користувача до цієї команди та якщо він має доступ то виводить користувачу інформацію про доступні команди звичайним користувачам. Функціональність цієї команди показана на рисунку 4.4.

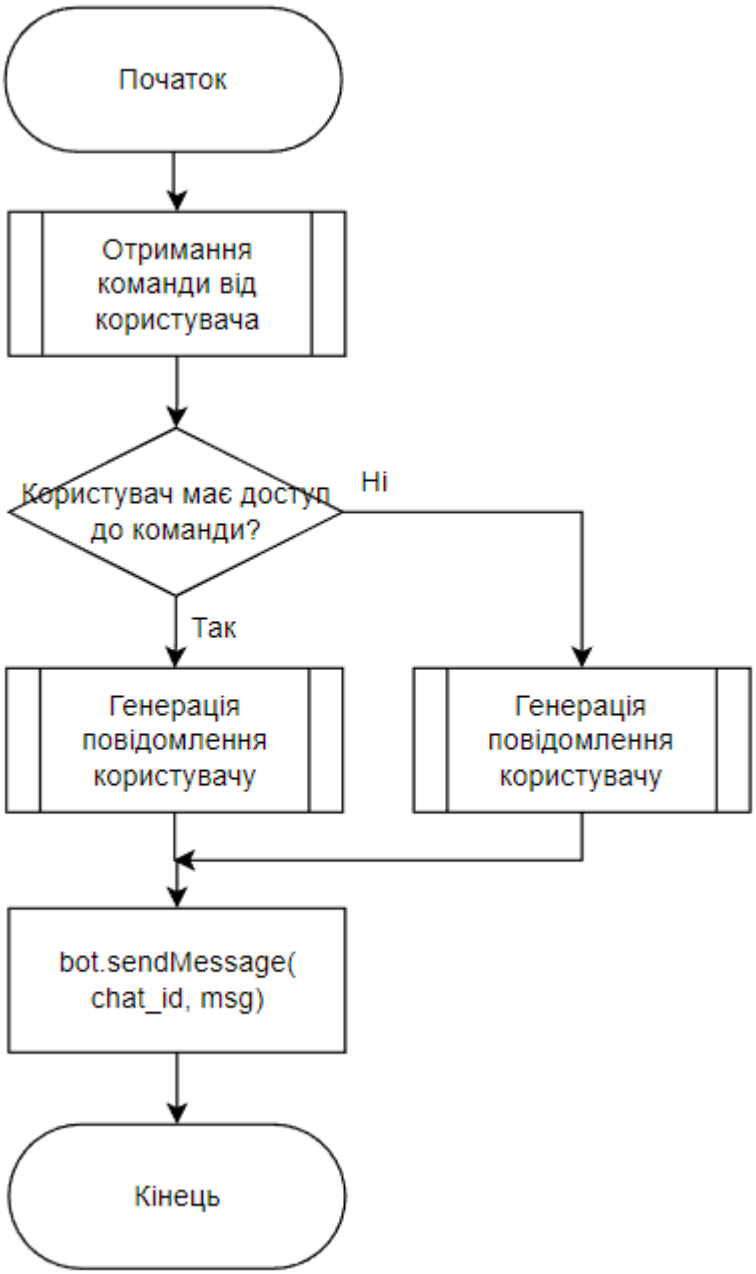

Рисунок 4.4 – Узагальнений алгоритм виконання команди /start

Команда /oneTimePassword якщо користувач має доступ до цієї команди генерує одноразовий випадковий пароль в границях від 1000 до 10000 та зберігає отримане число, після чого відправляє користувачу повідомлення з паролем та очікує від користувача вводу цього паролю. Функціональність цієї команди показана на рисунку 4.5.

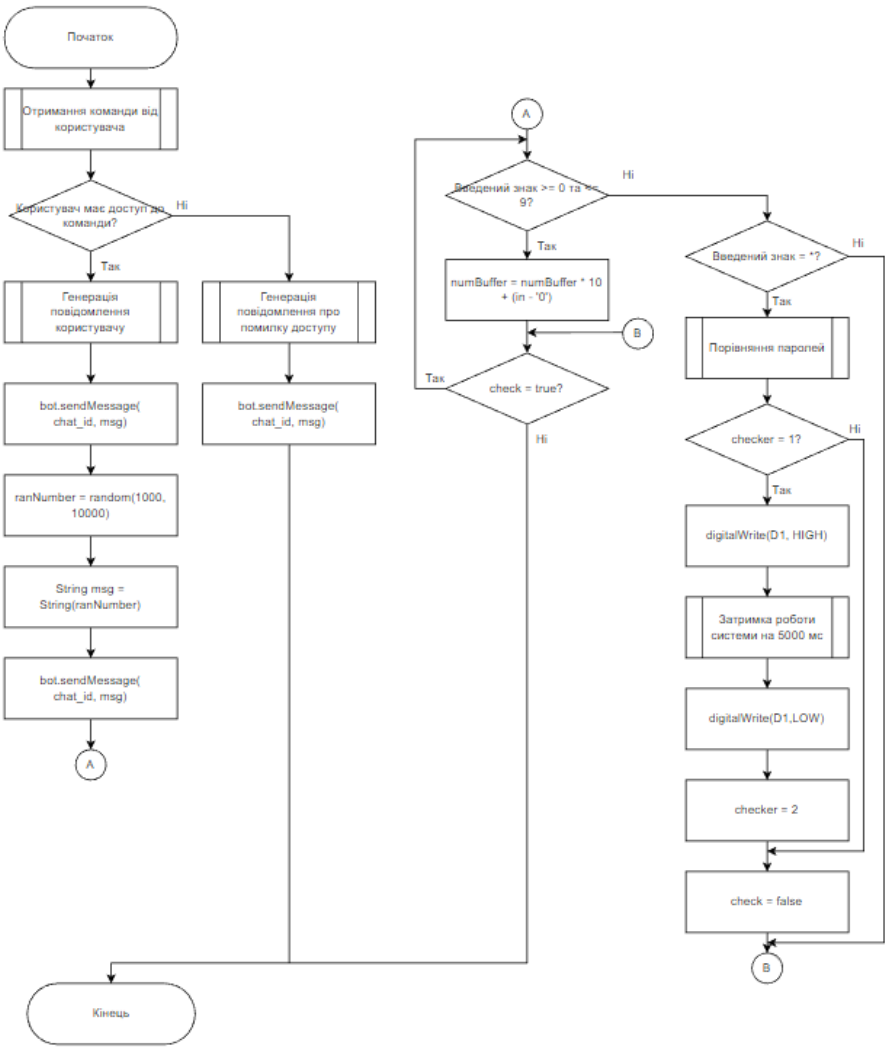

Рисунок 4.5 – Узагальнений алгоритм виконання команди /oneTimePassword

Команда /adminMenu виводить користувачу інформацію про доступні команди адміністратору системи якщо користувач має до цієї команди доступ. Функціональність цієї команди ідентична команді /start.

Команда /showDataBase отримує з енергонезалежної пам’яті системи інформації про користувачів які існують в базі даних, та виводить їх інформацію по одному за повідомлення.

Команда /changeUsersRFID дозволяє перезаписати інформацію про RFID-карту обраного користувача на нову піднесену до зчитувача картку.

Команда /changeUsersUID дозволяє перезаписати інформацію про унікальний ідентифікатор обраного користувача. Введення нового ідентифікатору відбувається за допомогою набору ідентифікатора на мембранній клавіатурі.

Команда /changeUsersAccessLevel дозволяє перезаписати інформацію про рівень доступу обраного користувача. Введення нового рівня доступу відбувається за допомогою мембранної клавіатури. Функціональність цієї команди ідентична команді /changeUsersUID.

4.5 Висновки за розділом

У розділі обрано середовище для програмування системи, необхідні бібліотеки та розроблено програмну частину системи. Наведено блок-схеми роботи системи.

5 ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ СИСТЕМИ

5.1 Перевірка роботи з картами RFID

При використанні RFID-карти зі зчитувачем виводиться в консоль унікальний ідентифікатор карти та порівнюється з базою даних, якщо дані з карти збігаються з тими, що є в базі даних, виводиться повідомлення про доступ та рядок того користувача, що приклав карту до зчитувача. Дана функціональність показана на рисунку 5.1 та рисунку 5.2.

```
15:52:26.423 -> 499251B8
15:52:26.423 -> Reading user's structure from EEPROM by adr: 1
15:52:26.423 -> login1234 439082372 1 5ABA8E16
15:52:26.423 -> Reading user's structure from EEPROM by adr: 37
15:52:26.423 -> login2345 394216598 2 499251B8
15:52:26.423 -> Reading user's structure from EEPROM by adr: 73
15:52:26.423 -> login3456 653862438 0 2ABA8E16
15:52:26.423 -> Reading user's structure from EEPROM by adr: 109
15:52:26.423 -> login4567 551078295 0 3ABA8E16
15:52:26.423 -> Reading user's structure from EEPROM by adr: 145
15:52:26.423 -> login5678 551078295 0 6ABA8E16
15:52:26.457 -> Access Allowed
15:52:26.457 -> login2345 394216598 2 499251B8
```

Рисунок 5.1 – Перевірка RFID карти яка існує в базі даних

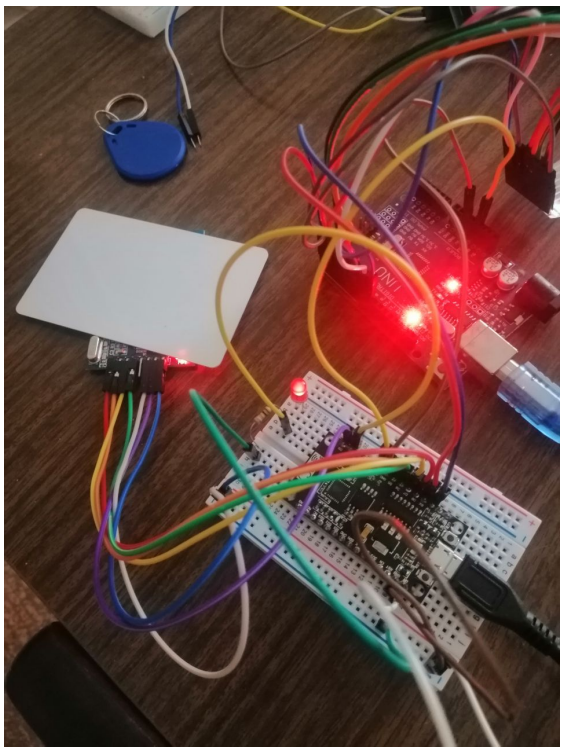

Рисунок 5.2 – Подача сигналу дозволу доступу

Якщо карта не існує в базі даних, нічого не виводиться, це показано на рисунку 5.3 та рисунку 5.4.

```
15:53:18.562 -> 1ABA8E16
15:53:18.562 -> Reading user's structure from EEPROM by adr: 1
15:53:18.562 -> login1234 439082372 1 5ABA8E16
15:53:18.562 -> Reading user's structure from EEPROM by adr: 37
15:53:18.595 -> login2345 394216598 2 499251B8
15:53:18.595 -> Reading user's structure from EEPROM by adr: 73
15:53:18.595 -> login3456 653862438 0 2ABA8E16
15:53:18.595 -> Reading user's structure from EEPROM by adr: 109
15:53:18.595 -> login4567 551078295 0 3ABA8E16
15:53:18.595 -> Reading user's structure from EEPROM by adr: 145
15:53:18.595 -> login5678 551078295 0 6ABA8E16
```

Рисунок 5.3 – Перевірка RFID карти яка не існує в базі даних

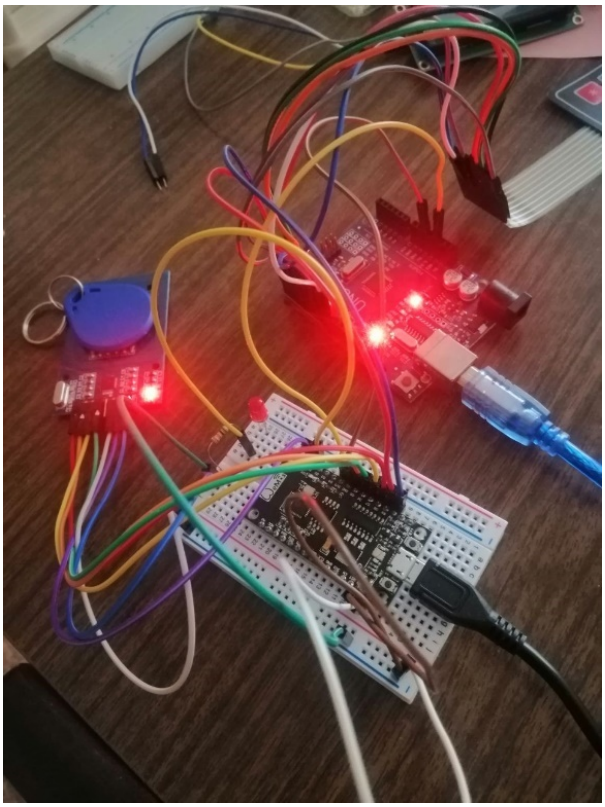

Рисунок 5.4 – Спроба отримання сигналу доступу без відповідної карти

5.2 Перевірка роботи з ботом

Спроба виконати команду за допомогою телеграм бота, до якої користувач не має доступу, приведе до помилки, яка показана на рисунку 5.5

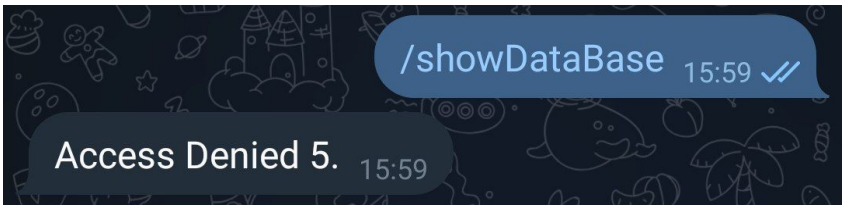

Рисунок 5.5 – Спроба виконати команду без прав доступу

Виконання команди /start приведено на рисунку 5.6.

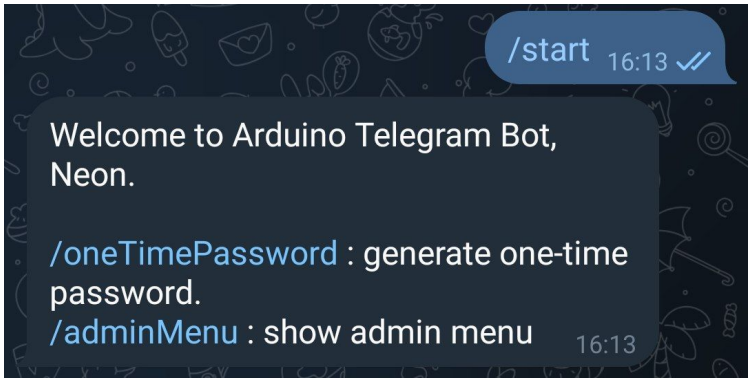

Рисунок 5.6 – Виконання команди /start

Виконання та перевірка працездатності команди /oneTimePassword приведено на рисунку 5.7 та 5.8.

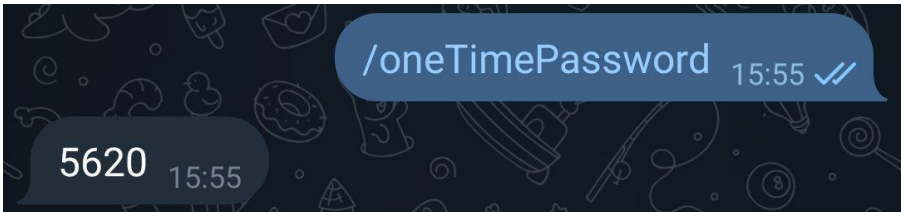

Рисунок 5.7 – Отримання одноразового паролю

```
15:55:45.364 -> got response
15:55:45.364 -> handleNewMessages 1
15:55:46.342 -> 5620
15:55:49.528 -> 5
15:55:49.528 -> 6
15:55:50.174 -> 2
15:55:51.161 -> 0
15:55:51.769 -> Access Allowed
```

Рисунок 5.8 – Введення одноразового паролю та отримання доступу

Перше число це згенерований одноразовий пароль який зберігається в системі, послідуючі це послідовне введення користувача за допомогою мембранної клавіатури, при натисканні відповідної кнопки для відправки даних в систему, вона перевіряє введений пароль з тим, що був згенерований після чого надає доступ або виводить в консоль помилку доступу.

Виконання команди /adminMenu приведено на рисунку 5.9.

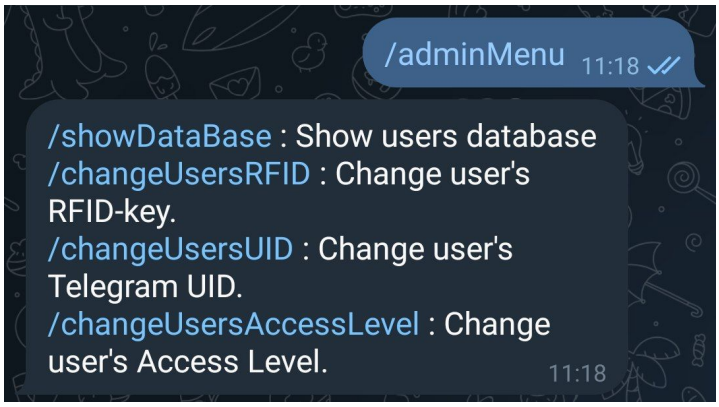

Рисунок 5.9 – Виконання команди /adminMenu

Виконання команди /showDataBase приведено на рисунку 5.10.

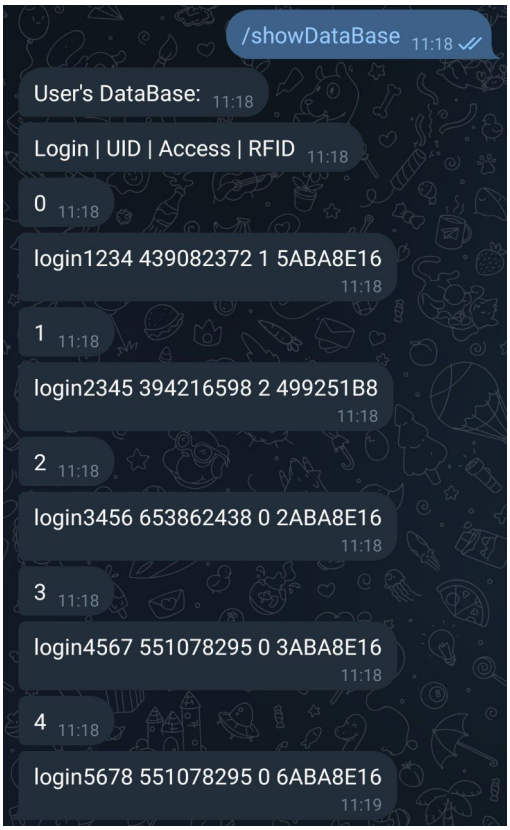

Рисунок 5.10 – Виконання команди /showDataBase

Виконання та перевірка працездатності команди /changeUsersRFID приведено на рисунку 5.11.

```
11:22:17.657 -> got response
11:22:17.657 -> handleNewMessages 1
11:22:17.657 -> Enter User index:
11:22:19.014 -> 2
11:22:20.097 -> 22
11:22:20.132 -> Поднесите новую карту для считывания
11:22:20.609 -> 1ABA8E16
11:22:20.609 -> 12
11:22:20.609 -> 2ABA8E16
11:22:20.609 -> 9
11:22:20.609 ->
11:22:20.609 -> 1ABA8E16
11:22:20.609 -> Было записано в БД
11:22:20.644 -> Чтение пользовательской структуры из EEPROM по адресу: 1
11:22:20.644 -> login1234 439082372 1 5ABA8E16
11:22:20.644 -> Чтение пользовательской структуры из EEPROM по адресу: 37
11:22:20.644 -> login2345 394216598 2 499251B8
11:22:20.644 -> Чтение пользовательской структуры из EEPROM по адресу: 73
11:22:20.644 -> login3456 653862438 0 1ABA8E16
11:22:20.644 -> Чтение пользовательской структуры из EEPROM по адресу: 109
11:22:20.677 -> login4567 551078295 0 3ABA8E16
11:22:20.677 -> Чтение пользовательской структуры из EEPROM по адресу: 145
11:22:20.677 -> login5678 551078295 0 6ABA8E16
```

Рисунок 5.11 – Заміна RFID карти користувача

Перше число це індекс акаунту користувача якому потрібно замінити RFID-карту, далі йде піднесена карту до зчитувачу та карта яка буде замінена. Після чого виводиться оновлена база даних користувачів.

Виконання та перевірка працездатності команди /changeUsersUID приведено на рисунку 5.12.

```
.1:28:37.089 -> 113456789
.1:28:37.089 -> 12
.1:28:37.089 -> 653862438
.1:28:37.089 -> 12
.1:28:37.089 ->
.1:28:37.089 -> 113456789
.1:28:37.124 -> Было записано в БД
.1:28:37.124 -> Чтение пользовательской структуры из EEPROM по адресу: 1
.1:28:37.124 -> login1234 439082372 1 5ABA8E16
.1:28:37.124 -> Чтение пользовательской структуры из EEPROM по адресу: 37
.1:28:37.124 -> login2345 394216598 2 499251B8
.1:28:37.124 -> Чтение пользовательской структуры из EEPROM по адресу: 73
.1:28:37.158 -> login3456 113456789 0 2ABA8E16
.1:28:37.158 -> Чтение пользовательской структуры из EEPROM по адресу: 109
.1:28:37.158 -> login4567 551078295 0 3ABA8E16
.1:28:37.158 -> Чтение пользовательской структуры из EEPROM по адресу: 145
.1:28:37.158 -> login5678 551078295 0 6ABA8E16
```

Рисунок 5.12 – Заміна унікального ідентифікатору користувача

Перше число це введений новий ідентифікатор, далі йде старий ідентифікатор який буде замінений. Після чого виводиться оновлена база даних.

Виконання та перевірка працездатності команди /changeUsersAccessLevel приведено на рисунку 5.13.

```
11:33:16.828 -> 0
11:33:16.828 -> 1
11:33:16.828 -> Чтение пользовательской структуры из EEPROM по адресу: 1
11:33:16.828 -> login1234 439082372 1 5ABA8E16
11:33:16.828 -> Чтение пользовательской структуры из EEPROM по адресу: 37
11:33:16.828 -> login2345 394216598 2 499251B8
11:33:16.828 -> Чтение пользовательской структуры из EEPROM по адресу: 73
11:33:16.828 -> login3456 653862438 1 2ABA8E16
11:33:16.863 -> Чтение пользовательской структуры из EEPROM по адресу: 109
11:33:16.863 -> login4567 551078295 0 3ABA8E16
11:33:16.863 -> Чтение пользовательской структуры из EEPROM по адресу: 145
11:33:16.863 -> login5678 551078295 0 6ABA8E16
```

Рисунок 5.13 – Заміна рівню доступу користувача

Перше число це новий рівень доступу користувача, далі йде старий рівень доступу який буде замінений. Після чого виводиться оновлена база даних.

5.3 Висновки за розділом

У розділі наведено проведено перевірку та налагодження працездатності. За результатами перевірки встановлено, що програмне забезпечення працездатне.

ВИСНОВКИ

В роботі розроблено засоби ідентифікації та аутентифікації системи контролю фізичного доступу з використанням технології RFID та одноразових паролів.

В роботі наведено визначення основних понять сучасних методів та систем аутентифікації та ідентифікації в системах контролю фізичного доступу. Розглянуті методи ідентифікації та аутентифікації, проведено аналіз майнових засобів, за результатом аналізу для реалізації роботи обрано RFID-мітки та одноразові паролі з використанням смартфону.

Описано функціонування системи та її інформаційна структура. Для посилення захисту з’єднання між системою та мережею Wi-Fi прийнято рішення використовувати відповідну бібліотеку WiFiClientSecure.

Обрані модулі, необхідні для роботи системи, створені відповідні схеми підключень.

Обрано середовище розробки та мову для реалізації програм. Розроблено програмне забезпечення системи в режимах зчитування карти та вводу одноразового паролю, також розроблені відповідні процедури для корегування даних користувачів, створені відповідні блок-схеми. Перевірена працездатність програмного забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Что такое СКУД и когда система контроля и управления доступом необходима? [Електронний ресурс] – 2021. – Режим доступу до ресурсу: https://ohholding.com.ua/stock/chto-takoe-skud-i-kogda-sistema-kontrolja-i-upravlenija-dostupom-neobhodima
2. Виды систем контроля и управления доступом (СКУД). [Електронний ресурс] // Компанія Карабинер. – 2018. – Режим доступу до ресурсу: https://karabiner.ua/stati/vidy-sistem-kontrolya-i-upravleniya-dostupom-skud/
3. Richard E. Smith - Authentication: From Passwords to Public Keys 1st Edition. 2001.
4. Ідентифікація та аутентифікація. [Електронний ресурс] – 2015. – Режим доступу до ресурсу: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/metodi-autentifikaciie
5. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2015. – 492 с.
6. Пластикова карта з магнітною смугою. [Електронний ресурс]. // Компанія Vostok. – 2016. – Режим доступу до ресурсу: https://www.vostok.dp.ua/ukr/infa1/glossary/plastik_karta_m/
7. iButton – products. [Електронний ресурс]. // Компанія maxim integrated. – 2020. – Режим доступу до ресурсу: https://pdfserv.maximintegrated.com/en/an/AN937.pdf
8. Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition / Klaus Finkenzeller ; translated by Dorte Muller. – 3rd ed.
9. Контроль доступа на базе RFID-технологии. [Електронний ресурс]. // Компанія Смарт Системы – 2020. – Режим доступу до

ресурсу:http://asupro.com/gps-gsm/system/access-control-based-rfid-technology.html

10. NodeMCU ESP8266. [Електронний ресурс]. // Компанія Components101. – 2022. – Режим доступу до ресурсу: https://components101.com/development-boards/nodemcu-esp8266-pinout-features-and-datasheet
11. Using an RFID module with an ESP8266 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.aranacorp.com/en/using-an-rfid-module-with-an-esp8266/
12. RC522 RFID Module. [Електронний ресурс]. // Компанія Components101. – 2022. – Режим доступу до ресурсу: https://components101.com/wireless/rc522-rfid-module
13. Arduino UNO R3. [Електронний ресурс]. // Документація до модулю. – 2022. – Режим доступу до ресурсу: https://docs.arduino.cc/resources/datasheets/A000066-datasheet.pdf
14. Arduino IDE. [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.arduino.cc/en/software
15. AVR Libc Home Page. [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.nongnu.org/avr-libc/
16. ESP8266WiFi Library. [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://arduino-esp8266.readthedocs.io/en/latest/esp8266wifi/readme.html
17. Universal-Arduino-Telegram-Bot. [Електронний ресурс]. – 2021. – Режим доступу: https://github.com/witnessmenow/Universal-Arduino-Telegram-Bot
18. Arduino-ESP32. [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://github.com/espressif/arduino-esp32/tree/master/libraries/WiFiClientSecure