

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій і технічного захисту інформації
(повна назва)

Кафедра Радіотехнологій інформаційно-комунікаційних систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

РОЗРОБКА ПРИСТРОЮ ІДЕНТИФІКАЦІЇ ІНДИВІДУАЛЬНОГО ДОСТУПУ

(тема)

Виконав:
студент 3 курсу, групи ТРРТу-21-1

Родітелєв О.М.

(прізвище, ініціали)

Спеціальність 172 Телекомунікації та
радіотехніка

(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма радіотехніка

(повна назва освітньої програми)

Керівник ст. викл. Штих І.А .

(посада, прізвище, ініціали)

Допускається до захисту

В.о. зав. кафедри

(підпис)

Зарудний О.А.

(прізвище, ініціали)

2024 р.

Не містить відомостей заборонених до відкритого публікування

Керівник _____ ст. викл. Штих І.А.

Студент _____ Родітелєв О.М.

Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій і технічного захисту інформації

Кафедра Радіотехнологій інформаційно-комунікаційних систем

Рівень вищої освіти перший (бакалаврський)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма радіотехніка
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____» _____ 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові РОДИТЄЛЄВУ ОЛЕКСАНДРУ МИХАЙЛОВИЧУ
(прізвище, ім'я, по батькові)

1. Тема роботи РОЗРОБКА ПРИСТРОЮ ІДЕНТИФІКАЦІЇ ІНДИВІДУАЛЬНОГО ДОСТУПУ

затверджена наказом університету від 27 травня 2024 р. № 498 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 21 червня 2024 р.

3. Вихідні дані до роботи _____

Провести аналіз основних елементів для пристрою ідентифікації.

Розробити пристрій ідентифікації індивідуального доступу.

4. Перелік питань, що потрібно опрацювати в роботі _____

Вступ

1. Аналіз персоналізуючих систем.

2. Вибір пристроїв для системи персонізації.

3. Розробка системи обліку персоналізації.

Висновки. Перелік джерел посилання. Додатки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
 Комп'ютерна презентація – слайди у форматі Power Point

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна частина	ст. викл. Штих І.А.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	06.05.2024	виконано
2	Підбір літератури за темою роботи	07.05.-09.05.2024	виконано
3	Аналіз персоналізуючих систем	10.05.-23.05.2024	виконано
4	Вибір пристроїв для системи персонізації	24.05.-29.05.2024	виконано
5	Розробка системи обліку персоналізації	30.05.-08.06.2024	виконано
6	Оформлення презентаційного матеріалу	09.06.-10.06.2024	виконано
	підготовка до захисту у ЕК		

Дата видачі завдання **06 травня 2024 р.**

Студент _____
 (підпис)

Керівник роботи _____
 (підпис)

О.М. Родітелєв

ст. викл. І.А. Штих

РЕФЕРАТ

Кваліфікаційна робота бакалавра складається з пояснювальної записки, що містить 73 сторінок тексту, 16 рисунків, 2 таблиця, 17 джерел посилання і 4 додатки.

ЗАПІРНИЙ МЕХАНІЗМ. МІКРОКОНТРОЛЕР ARDUINO. WEMOS D1 MINI. ВЕБСЕРВЕР. WI-FI.

Мета роботи: створити проєкт для доступу та реєстрації відвідуваності приміщення. Розробка даного проєкту ведеться на базі мікроконтролера Arduino, в середовищі розробки Arduino IDE.

У першому розділі було проведено дослідження системи обліку відвідуваності, вибір запірної пристрою і технології дистанційного відстеження.

У другому розділі був зроблений вибір основних пристроїв, що використовуються в системі, а саме: об'єкта управління, ключа ідентифікації та радіочастотного зчитувача.

У третьому розділі було послідовно описаний алгоритм розробки системи обліку відвідуваності.

THE ABSTRACT

The qualification work of the bachelor consists of an explanatory note containing 73 pages of text, 16 figures, 2 table, 17 literary sources and 4 appendices.

LOCKING MECHANISM. ARDUINO MICROCONTROLLER. WEMOS D1
MINI. WEBSERVER. WI-FI.

The purpose of the work: to create a project for access and registration of audience attendance. The development of this project is based on the Arduino microcontroller, in the Arduino IDE development environment.

In the first section, a study of the attendance accounting system, the choice of a locking device and remote tracking technology was carried out.

In the second section, the main devices used in the system were selected, namely: control object, identification key and radio frequency reader.

In the third chapter, the algorithm for developing the attendance accounting system was consistently described.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	8
ВСТУП.....	9
1 АНАЛІЗ ПЕРСОНАЛІЗУЮЧИХ СИСТЕМ	10
1.1 Види запиірних пристроїв.....	10
1.2 Дистанційний моніторинг системи персоналізації	14
1.3 Види дистанційного моніторингу	15
2 ВИБІР ПРИСТРОЇВ ДЛЯ СИСТЕМИ ПЕРСОЛІНАЗАЦІЇ	20
2.1 Класифікація замків з електронною картою	20
2.2 RFID зчитувач	24
2.3 Вибір об’єкта управління	31
3 РОЗРОБКА СИСТЕМИ ОБЛІКУ ПЕРСОНАЛІЗАЦІЇ	40
3.1 Організація взаємодії Wi-Fi Wemos D1 Mini і RC522.....	41
3.2 Робота сервоприводу	45
3.3 Створення та експлуатація вебсервера.....	51
ВИСНОВКИ.....	56
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	57
ДОДАТОК А – ЛІСТИНГ КОДУ ДЛЯ RC522.....	60
ДОДАТОК Б – ПУБЛІКАЦІЯ ЗА ТЕМОЮ РОБОТИ (СЕРТИФІКАТ).....	64
ДОДАТОК В – СЛАЙДИ ПРЕЗЕНТАЦІЇ	66
ДОДАТОК Г – ВІДОМІСТЬ КВАЛІФІКАЦІЙНОЇ РОБОТИ	72

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ,
ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

- DVI (Digital Visual Interface) – цифровий відеоінтерфейс;
- FTP (File Transfer Protocol) – протокол передачі файлів через мережу;
- GPIO (General-Purpose Input/Output) – інтерфейс для зв'язку між компонентами комп'ютерної системи;
- HDMI (High Definition Multimedia Interface) – інтерфейс для мультимедіа високої чіткості;
- HTML (HyperText Markup Language) – мова гіпертекстової розмітки;
- IEEE (Institute of Electrical and Electronics Engineers) – інститут інженерів електротехніки та електроніки;
- LAN (Local Area Network) – локальна комп'ютерна мережа;
- MOSI (Master Out Slave In) – вихід ведучого, вхід веденого;
- PHP (Hypertext Preprocessor) – скриптова мова загального призначення;
- OSI (Open System Interconnection) – еталонна модель взаємодії відкритих систем;
- RFID (Radio Frequency IDentification) – радіочастотна ідентифікація;
- RCA (Radio Corporation of America) – стандартний тип з'єднувачів, що широко застосовується в аудіо- та відеотехніці;
- SD (Secure Digital) – формат карт пам'яті;
- SPI (Serial Peripheral Interface) – послідовний периферійний інтерфейс;
- USB (Universal Serial Bus) – універсальна послідовна шина;
- Wi-Fi (Wireless Fidelity) – технологія бездротової мережі;
- ДНК – дезоксирибонуклеїнова кислота;
- ЕОМ – електронно-обчислювальна машина;
- ЛОС – локальна обчислювальна мережа;
- ПЗП – постійно запам'ятовуючий пристрій;
- САПР – система автоматизованого проєктування і розрахунку.

ВСТУП

З появою приватної власності з'явилася необхідність оберігати її від чужих зазіхань. Для цього і були придумані двері і замки. Замки для входних дверей і відповідно ключі до замків з'явилися у ранніх цивілізацій, про що можна прочитати в стародавніх міфах. Але стародавні замки для входних дверей були великих розмірів і досить примітивної конструкції, а ось принцип їх роботи використовувався при виготовленні перших штифтових замків. Стародавні пристосування для замикання входних дверей виготовлялися з підручного матеріалу, такого як очерет, волокна, дерево або вже пізніше з металу [1].

Метою роботи є створення системи управління завірним пристроєм, яка володіє можливістю введення обліку персоналізації. Практична значимість даної роботи тим вище, чим бажання керуючого персоналом зручно відстежувати відвідуваність робочого місця або приміщення з обмеженим рівнем доступу. Кожен відповідальний за будь-яке приміщення, будь-то склад, архів, лабораторія або ж звичайний кабінет бажає бути в курсі відвідуваності даного приміщення, але не завжди має можливість. Дана система націлена не тільки на надання такої можливості, але і забезпечення зручності відстеження з використанням сучасних технологій.

У цьому проекті була розроблена саме така система, безсумнівно, має аналоги на сучасному ринку, але протиставляє їм простоту використання і конкурентну ціну. Об'єктом дослідження була технологія обліку персоналізації і заміни відкриття дверей ключами на відкриття дверей з використанням радіочастотної ідентифікації, вже повсюдно поширеною в сучасному суспільстві. Предметом дослідження була реалізація даної технології за допомогою контролера фірми Arduino і зчитувача карток RC522.

1 АНАЛІЗ ПЕРСОНАЛІЗУЮЧИХ СИСТЕМ

З появою приватної власності з'явилася необхідність оберігати її від чужих зазіхань. Для цього і були придумані двері і замки. Замки для входних дверей і відповідно ключі до замків з'явилися у ранніх цивілізацій, про що можна прочитати в стародавніх міфах. Але стародавні замки для входних дверей були великих розмірів і досить примітивної конструкції, а ось принцип їх роботи використовувався при виготовленні перших штифтових замків. Стародавні пристосування для замикання входних дверей виготовлялися з підручного матеріалу, такого як очерет, волокна, дерево або вже пізніше з металу [1].

Але прогрес, як відомо, не стоїть на місці і стосується практично всього, що сьогодні оточує людей. І механізм відкриття дверей не виняток. Зараз відбувається перехід від звичайних механічних ключів до різного роду автоматичному відкриттю дверей при ідентифікації відвідувача [1].

1.1 Види запірних пристроїв

В даний час еволюція відбувається практично з усім, чим сьогодні користується людство. Дверні замки входять в число технологій, яким вимирання не загрожує, і, тому, дана технологія також знаходить свій розвиток в переході від уже морально застарілих механічних ключів до більш сучасним методам відкриття дверей. Електронний тип замків – один з цих методів. Електронні замки, в свою чергу, бувають наступних типів [1]:

- кодові електронні замки;
- електронний замок з карткою;
- біометричні замки.

Більшість сучасних замкових систем поєднують в собі кілька механізмів або їх комбінацію, це захищає їх від злому підбором ключа, відмичкою або із застосуванням грубої сили. Крім того, якщо замок має функцію перекодування,

при крадіжці ключа досить, не змінюючи замок, змінити розташування елементів всередині сердечника і виготовити новий дверний ключ, щоб виключити несанкціоноване проникнення за допомогою старого [1].

1.1.1 Кодовий замок

Кодовий замок – замок, для відкриття якого необхідно ввести код доступу з клавіатури. Правильний код доступу зберігатися в пам'яті пристрою. Переваги даного типу замку [1]:

- відсутність ключа, який можна втратити, і який зловмисник може за відсутності власника скопіювати [1];
- можливість швидкої зміни коду, яку можна виробляти щодня [1];
- можливість швидкої передачі коду іншій особі без залучення сторонніх осіб (майстерні з виготовлення ключів) і одночасно без втрати доступу самому [1].

Недоліки:

- код можна забути. Код зазвичай забувається після того, як він тривалий час не використовувався. Проте, його можна записати, але тоді збільшується ймовірність, що код дізнається сторонній [1];
- код можуть підглянути при введенні. Тому при введенні коду необхідно зберігати скритність [1];
- часто в якості кодів використовуються дати (народження), адреси, загальновідомі числа, що спрощує злом коду, методом підбору [1].

1.1.2 Електронний замок з картою

Електронний замок з картою – сучасне рішення для забезпечення доступу в офіс тільки співробітникам компанії. Система відкриває двері при піднесенні магнітної картки, або магнітного чіпа. Даний замок може бути встановлений на двері будь-якого типу [1].

До переваг електромагнітного замка відносяться:

- легкість записи і видалення даних співробітників з карт, що дуже зручно при зміні користувачів [1];

- високий рівень безпеки та довговічності [1];

До недоліків можна віднести:

- можлива втрата ідентифікуючої картки або чіпа [1];

- періодично, необхідна заміна акумулятора [1].

1.1.3 Біометрична аутентифікація

Методи аутентифікації, засновані на вимірі біометричних характеристик людини, забезпечують близько (100%) ідентифікацію, вирішуючи проблеми різних можливостей втрати та забуття паролів і персональних ідентифікаторів. Прикладами використання даних методів є системи ідентифікації користувача по малюнку райдужної оболонки ока, відбитками долоні, формам вух, по почерку, по запаху, за тембром голосу і навіть по структурі ДНК [2].

Передовим напрямком є використання біометричних характеристик в побуті людини, таких як: розрахункових картках, жетонах-пропусках і засобах стільникового зв'язку. Наприклад в країнах Європи, при розрахунку в деяких передових магазинах пред'явник картки кладе палець на сканер на підтвердження, що картка дійсно належить йому [2].

У той же час біометрична аутентифікація має певні недоліки [2]:

- отриманий шаблон порівнюється ні з результатом первісної обробки, а з тим, що надійшло до місця порівняння результатів. Під час передачі можуть виникнути певні перешкоди, та навіть підміна [2];

- первинна база шаблонів може бути підмінена зловмисником;

- також потрібно враховувати різницю між застосуванням біометрії на контрольованій території, та в умовах, коли, наприклад, до пристрою сканування можуть скористатися фальшивим муляж і т.д. [2];

– більшість біометричних даних людини змінюються (як в результаті старіння, так і травм, опіків, порізів, хвороби, ампутації і т.д.), Так що база шаблонів потребує постійного оновлення, а суттєво ускладнює контроль та роботу і для користувачів, і для адміністраторів [2];

– якщо ваші біометричні дані викрадають або їх компрометують, то це, як правило, на все життя і подалі вони є ненадійними . Навіть паролі, при їх ненадійності, в будь-який момент можна змінити. Палець, очі або голос змінити не можна, принаймні швидко [2];

– біометричні характеристики людини - є унікальними ідентифікаторами, але їх не можна зберегти в секреті [2].

1.1.4 Обґрунтування вибору заперного пристрою

Даний проєкт планується використовувати в середовищі, де з ним працюватимуть велика кількість людей. Відповідно, використання кодового замка в даному випадку вельми невиправдано, тому що захистити код даного замку від поширення буде проблематично, якщо не сказати неможливо. Також зберігання коду доступу в однієї людини напевно почне доставляти незручність, як цій людині, так і всім бажаючим потрапити в приміщення. Використання біометричної аутентифікації для вирішення цих проблем підходить ідеально: «ключ» доступу в приміщення унікальний і просто передати його або втратити ніяк не вийде. Але у цього методу є ряд недоліків при реалізації в даному проєкті. Перший з них – це ціна на комплектуючі даного замку. Ціна на середньостатистичний сканер відбитка пальця в 3-4 рази перевищує ціну на середньостатистичний радіочастотний зчитувач, і, в 4-5 разів на клавіатуру введення для кодового замка. Другим недоліком є складність процедури внесення в базу даних біометричних параметрів кожного з осіб, допущених в приміщення. Складність присутній як в технічному плані, так і в плані вибору відповідальних за це приміщення, тому що число людей, які мають право доступу до цього приміщення має бути вибрано оптимально.

Оскільки чим більше людей має доступ до аудиторії, тим менше шанс так і в плані вибору відповідальних за це приміщення, тому що число людей, які мають право доступу до цього приміщення має бути вибрано оптимально. Оскільки чим більше людей має доступ до аудиторії, тим менше шанс так і в плані вибору відповідальних за це приміщення, тому що число людей, які мають право доступу до цього приміщення має бути вибрано оптимально. Оскільки чим більше людей має доступ до аудиторії, тим менше шанс виявитися в ситуації, коли в зоні досяжності не виявиться жодного «Носія ключа». Але, з іншого боку, велике число людей, які мають право доступу в закриті приміщення, нівелює сенс фінансових витрат на даний датчик, а також, при будь-яких порушеннях або надзвичайних пригодах, ускладнює пошук відповідального за їх причину. З огляду на обстановку, в якій дана система повинна буде функціонувати, логічним буде вибрати замок з електронною картою. Даний вид замку підходить по цінній категорії складових, зручності контролю поширення ключів, видалення ключів з бази даних і внесення ключів в базу даних.

1.2 Дистанційний моніторинг системи персоналізації

На сьогоднішній день дистанційне відстеження стрімко розвивається і застосовується в багатьох сферах життєдіяльності людей. Дистанційне відстеження - це передача інформації від об'єкта управління до оператора, що знаходиться на відстані. Дистанційне відстеження поступово заповнює системи автоматизації, так як не завжди є можливість безпосередньо спостерігати за об'єктом управління, наприклад, якщо об'єкт рухається або перебуває на значній відстані або в агресивному середовищі [3].

Дистанційне відстеження за системою управління затворним механізмом необхідно, в першу чергу, для безпеки об'єкта. При будь-яких надзвичайних подій, які порушення в приміщенні, обладнаному системою з дистанційним відстеженням, набагато простіше знайти відповідального за цю подію. Сучасні

технології дозволяють створити дистанційне керування в домашніх умовах при незначних витратах на складові системи [3].

1.3 Види дистанційного моніторингу

Реалізація дистанційного спостереження за затворним механізмом має широкий спектр, все залежить від переслідуваної мети. Бути це може двері від гаража, будинку, квартири і також це може бути сейф. Названі далеко не всі можливості застосування такого відстеження [4].

Передача відбувається за допомогою різних способів транспортування цифрової інформації від джерела до одержувача. Перерахуємо найпопулярніші з них [4]:

- передача інформації по каналу Ethernet;
- передача інформації по інфрачервоному каналу;
- передача інформації з використанням технології Bluetooth;
- передача інформації за допомогою Wi-Fi.

1.3.1 Технологія Ethernet

Ethernet – технологія пакетної передачі даних для інформаційних електронних мереж та комп'ютерних систем. Стандарти Ethernet визначають дротяні з'єднання і електричні сигнали на фізичному рівні, формат кадру та протоколи управління доступом до інформаційного середовища - на канальному рівні моделі OSI. Ethernet в основному описується стандартами IEEE групи 802.3. Ethernet став найпоширенішою технологією ЛВС в середині 1990-х років [4].

Назва «Ethernet» (буквально переводиться «Ефірна мережа» або «середовище мережі») відображає основний принцип роботи цієї технології: все, що передається одним пристроєм, одночасно приймається всіма іншими [4].

В наш час практично підключення відбувається через комутатори, так що кадри, що відправляються одним вузлом, доходять лише до адресата (виняток становлять передачі на широкомовна адресу) - це підвищує швидкість роботи і безпеку мережі. Ранні версії технології Ethernet використовували в якості середовища передачі коаксіальний кабель, але з часом він був повністю витіснений оптоволоконном і крученою парою. Справа в тому, що коаксіальний кабель - поділюване середовище передачі. Важлива особливість розділяється середовища: її можуть використовувати одночасно кілька інтерфейсів, але передавати в кожен момент часу повинен тільки один. За допомогою коаксіального кабелю можна з'єднає не тільки 2 комп'ютери між собою, але і більш двох, без застосування активного обладнання. Така топологія називається шина. Однак якщо хоча б два вузла на одній шині почнуть одночасно передавати інформацію, то їх сигнали накладуться один на одного і приймачі інших вузлів нічого не розберуть [4].

1.3.2 Передача інформації по ІЧ каналу

Інфрачервоний канал - канал передачі даних, що не вимагає для свого функціонування провідних з'єднань. У комп'ютерній техніці зазвичай використовується для з'єднання комп'ютерів з периферійними пристроями [4].

На відміну від радіоканалу, інфрачервоний канал нечутливий до електромагнітних завад, і це дозволяє використовувати його в виробничих умовах. До недоліків інфрачервоного каналу відносяться висока вартість приймачів і передавачів, де потрібно перетворення електричного сигналу в інфрачервоний і назад, а також низькі швидкості передачі. В умовах прямої видимості інфрачервоний канал може забезпечити з'єднання на відстанях в декілька кілометрів, але найбільш зручний він для зв'язку комп'ютерів, що знаходяться в одному приміщенні, де відображення від стін кімнати дає стійку і надійну зв'язок. Найбільш природний тип топології тут - «Шина» (тобто переданий сигнал одночасно отримують всі абоненти). Ясно, що, маючи таку

кількість недоліків, інфрачервоний канал не зміг отримати широкого розповсюдження [4].

Переваги даного способу передачі інформації [4]:

- не вимагає проводів;
- нечутливий до електромагнітних завад;
- на відміну від радіозв'язку, не вимагає ліцензування в інспекції електрозв'язку.

Недоліки:

- необхідність знаходження приймача і передавача в прямої видимості [4];
- висока вартість приймачів і передавачів невисока швидкість передачі даних [4].

1.3.3 Передача інформації за допомогою технології Bluetooth

Технологія Bluetooth стала першою технологією, що дозволяє забезпечити бездротову персональну мережу передачі даних WPAN. Вона дає змогу здійснювати передачу даних і голосового повідомлення по радіоканалу на невеликі відстані, до 100 метрів, в вільному діапазоні частот 2,4 ГГц і з'єднувати портативні пристрої, при відсутності прямої видимості. Технологія Bluetooth підтримує як з'єднання типу «точка-точка», так і «точка-багато точок». Два або більше користувача можуть використовувати один і той же канал пристрою утворення пікомережа. Один з пристроїв працює як сервер, а решта – як клієнти. В одній пікомережі можуть бути до семи активних клієнтів, при цьому інші клієнти пристрої знаходяться в стані «очікування», залишаючись синхронізованими з сервером [4].

У кожній пікомережі діє тільки один сервер, проте клієнтські пристрої можуть входити в різні пікомережі. Крім того, сервер однієї пікомережі може бути клієнтом в інший [4].

В наш час на ринку представлен велика кількість компаній, що пропонують модулі BlueTooth, а також компоненти для самостійної реалізації апаратної частини Bluetooth-пристроїв [4].

1.3.4 Технологія Wi-Fi

На початку використання установка технології Wireless LAN використовувалася там, де розгортання кабельної системи вважалося неможливо або економічно нерентабельним. На даний час у більшості компаній та організаціях використовується Wi-Fi, так як швидкість роботи мережі вже перевищує 100 Мбіт / сек, та нові прилади перевищують цю цифру в декілька разів . Користувачі мають можливість переміщатися між точками доступу , без втрати покриття мережі Wi-Fi. Мобільні пристрої оснащені модулями Wi-Fi прийнятно-передавальними пристроями, можуть підключатися до локальної мережі і отримувати доступ в Інтернет через точки доступу або хот-споти. Стандарт IEEE 802.11 є основним стандартом для побудови бездротових локальних мереж. Цей стандарт постійно розвивається та вдосконалювався, і в даний момент є ціле сімейство, до якого відносять специфікації IEEE 802.11 з літерними індексами аз. Однак тільки чотири з них (a, b, g, i) є основними і використовуються найчастіше у виробників обладнання, інші ж (з-f, hn) представляють собою більш досканале , або виправлення прийнятих специфікацій. Теоретично 802.11n здатний забезпечити швидкість передачі даних до 480 Мбіт/с [4].

1.3.5 Вибір технології дистанційного моніторингу

Вибір технології для дистанційного відстеження в даній системі здійснювався з урахуванням наступних факторів [4]:

- надійність роботи в закритому приміщенні;
- протяжність дії технології;

– поширеність пристроїв для дистанційного відстеження серед передбачуваних операторів;

– цінова категорія компонентів системи;

– зручність створення інфраструктури для передачі даних;

Для постійної експлуатації даної системи нам необхідна технологія, яка б надійно функціонувала в приміщенні, так щоб переданий сигнал впевнено проходив через стіни. З огляду на це, рішення використання інфрачервоного каналу для передачі даних стає ненадійним, незважаючи на позитивні сторони даної технології. Технологія Ethernet поступається іншим видам в зручності прокладки інфраструктури для передачі даних і в протяжності дії технології. Технологія Wi-Fi мають потенційно вищу швидкістю передачі даних, ніж Bluetooth. Але дана характеристика не грає великої ролі в системі, що розробляється, тому що обсяг даних з яким даній системі доведеться працювати транслюватиметься обома технологіями за однаковий інтервал часу. З метою зробити роботу цієї системи зручною для більшої кількості людей, доцільніше буде зробити вибір на користь технології Wi-Fi. Цей вид передачі даних набагато більш поширений в порівнянні з Bluetooth. До того ж Wi-Fi продовжує набирати свою популярність, тому що на сьогоднішній день Wi-Fi модуль вбудований практично в усьому мобільних телефонах, ноутбуках і навіть деяких електронних книгах [4].

Така поширеність дозволить реалізувати по-справжньому дистанційну систему стеження.

2 ВИБІР ПРИСТРОЇВ ДЛЯ СИСТЕМИ ПЕРСОЛІНАЗАЦІЇ

В даному проєкті планується реалізувати систему, що складається з 4 основних компонентів, що взаємодіють через об'єкт управління, роль якого виконуватиме мікроконтролер.

2.1 Класифікація замків з електронною картою

Існує велика різноманітність фізичних методів безконтактної ідентифікації об'єкта, що підходять для даної мети. Найбільшого вжитку набули варіації на електромагнітному способі реалізації. Преважна ознака даних систем – це є рамки електромагнітних антен, що перешкоджають прохід. Різниця є лише в конструкції міток [5].

2.1.1 Електромагнітні системи

Мітки (рисунок 2.1) представлені в виді двох (або більше) смужок на паперовій наклеїці.

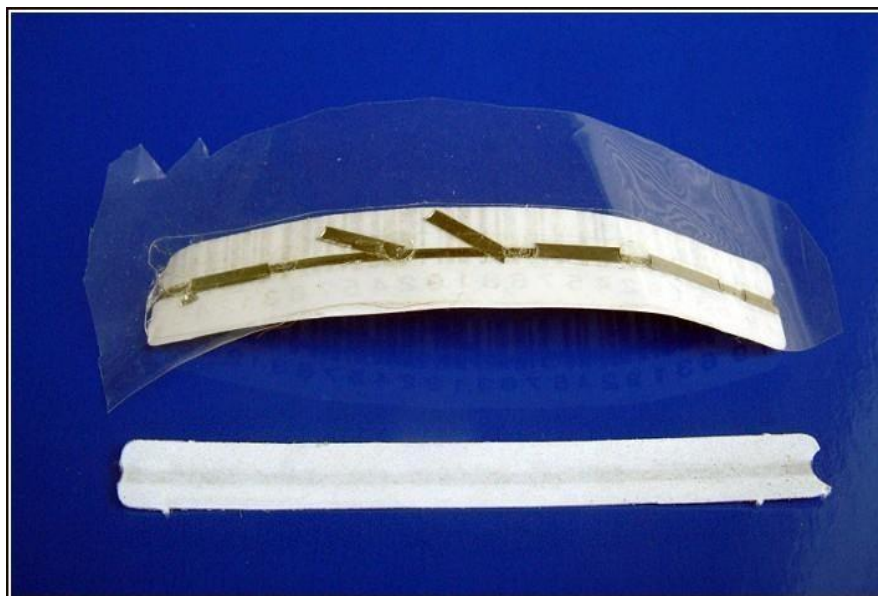


Рисунок 2.1 – Електромагнітна мітка

Перша смужка зроблена з матеріалу з великим магнітострикційним ефектом. Тому коли вона потрапляє в змінне магнітне поле, то починає працювати як нелінійний елемент і в магнітному полі з'являються гармоніки робочих частот, які і стають основною ознакою крадіжки. Друга смужка працює як «вимикач» для першої. Вона виготовлена з феромагнетичного матеріалу, який може є намагнічений, як постійний магніт. І коли смужка намагнічена, то вона порушує магнітострикцію першої смужки завдяки ефекту магнітного насичення матеріалу. Таким чином деактивація мітки полягає в її намагнічування. Мітку можна повторно активувати розмагнічуванням. Цей вид міток особливо люблять використовувувати на книги – вони тонкі, також вони зручні в бібліотеках: деактивує при видачі, реактивується після повернення [5].

2.1.2 Акустомагнітні системи

Пристрій (рисунок 2.2) цих міток сильно схоже на магнітні, але різниться принцип детектування мітки. Сенс в тому, що вільне положення магнітострикційному смужки в пустотілої мітці дозволяє їй здійснювати вільні механічні коливання під дією магнітного поля [5].



Рисунок 2.2 – Акустомагнітна мітка

При цьому механічна добротність системи на частоті накачування вибирається максимально можливою, і смужка продовжує коливатися деякий час після зняття накачування. При цьому, згідно з тим же магнітострикційному ефекту, тепер уже смужка створює змінне магнітне поле, яке і реєструється системою. Магнітна смужка бере участь в механічному резонансі, тому ці мітки активуються намагнічуванням і деактивуються розмагнічуванням. Оскільки намагнічування має бути певним за величиною і напрямком, то повторна активація таких міток не передбачено [5].

2.1.3 Радіочастотні системи

Мітка (рисунок 2.3) представлена як коливальний контур з котушки індуктивності і конденсатора, виготовлених з фольги на паперовій основі. Принцип роботи базується на вимірюванні добротності коливального контуру стаціонарної рамки, тому коли в поле його котушки вносять котушку коливального контуру мітки [5].



Рисунок 2.3 – Радіочастотна мітка

Деактивація міток цього типу здійснюється електричним пробоем фольгового конденсатора. Для цього потрібно внести мітку в сильне магнітне

поле робочої частоти. Повторно активувати мітку цього типу вже неможливо. Мітки на паперовій основі легко знищити (порвати) або обійти за допомогою металевої пластини (наприклад, великої монети), притиснувши її до мітки. Тому для дорогих речей мітки випускають у вигляді великого і міцного пластикового брелка. Такі мітки є багаторазовими, коливальний контур в них зроблений на порядок якісніше, деактивувати мітку вандалізмом стає складніше і наявність мітки стає можливо визначити навіть візуально співробітниками. Мітки такого типу часто використовуються в магазинах одягу та господарчих товарів. Системи цього типу використовують робочу частоту 8,2 МГц [5].

2.1.4 Обґрунтування вибору ключа ідентифікації

Перераховані мітки схожі за принципом роботи і своїми характеристиками. Вибір міток здійснювався, керуючись поширеністю міток і складністю комунікації з обраним мікро контролером. З даних трьох типів міток найбільш поширені радіочастотні мітки. Вони використовуються в банківських картах, електронних пропусках, картах проїзду в метро. Використання даного типу міток в розроблюваної системі надає можливість модернізувати яку-небудь з цих карт, внісши номер обраної карти в базу даних. Що стосується складності зв'язування з мікро контролером, то радіочастотний ідентифікатор RC522 є одним з найпопулярніших зчитувачів при реалізації подібного роду проєктів. Це обумовлено наступними факторами [5]:

- відносно невисока вартість;
- наявність бібліотек в середовищі програмування, що сильно полегшує підключення та експлуатацію даного датчика [5];
- даному датчику необхідно харчування 3.3В, що ідеально підходить для використання з Arduino Uno і подібними контролерами [5].

2.2 RFID зчитувач

2.2.1 Сфера використання

Технологія RFID – це сучасна технологія, що базується на використанні радіочастотного електромагнітного випромінювання. Технологія використовується для ідентифікації та обліку об'єктів. Радіочастотна мітка, як правило, є мініатюрною пристроєм. Ця пристрій зібрано з двох елементів: мікрочіпа, на якому зберігаються дані, і антени, за допомогою якої мітка отримує і роздає ці дані. Якщо в RFID-позначці вбудоване власне джерело живлення, то ці мітки є активними. Якщо в мітці відсутній вбудований джерело живлення, то, ці мітки є пасивними. Пасивні мітки є в більшій мірі поширеними, ніж активні [6].

У пам'яті RFID-мітки зберігається її власний індивідуальний та унікальний номер, який використовується для ідентифікації, а також необхідною інформацією, завантажені користувачем. Спочатку інформація на мітці відсутня і зберігається тільки унікальний ID. Коли радіопозначка з'являється в радіусі дії ідентифікатора, інформація, що у ньому, зчитується спеціальним приладом, який крім функції читання також має функцію запису інформації на мітку [6].

Радіомітки з вбудованим джерелом живлення витрачають на передачу даних енергію даного джерела. Даний тип міток запрограмований на випромінювання сигналу з певною періодичністю, наприклад, 1 раз за 10 секунд. Відстань, на якому можлива ідентифікація подібних RFID- міток, може досягати ста метрів. Пасивні RFID-мітки, тобто радіопозначки без джерела живлення, витрачають на передачу даних енергію поля пристрої ідентифікації. Передача інформації відбувається тоді, коли мітка накопичить енергію, необхідну для цього. Відстань виявлення пасивних міток набагато менше і володіє залежністю від потужності пристрою, як правило, радіус дії знаходиться в проміжку 0,05-8 метрів [6].

Область використання радіочастотної ідентифікації постійно збільшується. Особливо дана технологія поширена в галузях, де необхідний контроль за переміщеннями об'єктів в реальному часі, здатність працювати в тяжких та жорстких умовах експлуатації, безпомилковість, швидкість і надійність.

2.2.2 Компоненти RFID-системи

Радіочастотні мітки – пристрої, що володіють можливістю зберігання та передачі даних. У пам'яті кожної радіомітки міститься її індивідуальний ідентифікаційний код. Також, деякі радіомітки мають можливість перезапису збережених даних [6].

Зчитувачі – пристрої, які зчитують дані з міток і, при необхідності, записують на них інформацію. Ці прилади можуть використовуватися обліковою системою як постійно, так і експлуатуватися незалежно від неї [6].

Облікова система – ПЗ, яке використовується для накопичення та аналізу інформації, отриманої з радіоміток. Також дана система об'єднує всі компоненти в систему. Багато в наші дні сучасні облікові системи (програми сімейства 1С, корпоративні інформаційні системи - MS Ахарта, R3Com) вже сумісні з RFID-технологією і не вимагають спеціальної доопрацювання [6].

2.2.3 Класифікація RFID міток

Як вже було доведено, радіочастотна ідентифікація затребувана в безлічі виробничих сфер. Щоб дані системи ефективно функціонували в будь-якій застосовується області, було розроблено велику кількість різних за виконання радіоміток. Умовно всі ці мітки класифікуються наступним чином [6]:

– за наявності живлення: активні - для передачі інформації використовують енергію вбудованого джерела живлення, радіус реєстрації таких міток досягає ста метрів; пасивні - радіопозначки, що використовують

для різних дій з даними енергію, що випромінюється пристроєм ідентифікації, радіус дії міток цього типу досягає 9 метрів [6];

– за видами пам'яті: тільки для читання (RO) - інформація на мітку записується лише один раз, при виробництві, даний тип міток використовується тільки для ідентифікації, записати будь-яку інформацію в мітки для читання не можна, також їх практично неможливо підробити; запис одного разу, читання багаторазово (WORM) - крім унікального ідентифікатора даний тип радіоміток містить блок одноразово записаної інформації, надалі інформацію з цього блоку можна зчитувати багаторазово; для читання і запису (RW) - такі RFID - мітки зберігають унікальний ідентифікатор і кілька блоків пам'яті, призначених для читання і перезапису інформації, дані в подібних радіомітках можуть бути перезаписані багаторазово [6];

– за видом виконання: самоклеючі паперові або лавсанові мітки; стандартні пластикові карти; дискові; різні види брелків; спеціальне виконання для тяжких та жорстких умов експлуатації [6].

В наш час існує велика кількість різноманіття міток, тому відповідне виконання можна підібрати для індивідуального завдання, в залежності від потреб коистувача [6].

2.2.4 Класифікація RFID зчитувачів

Прилади для зчитування даних з міток також можуть бути декількох типів [6].

За виконанням пристрою для зчитувача діляться на:

– стаціонарні зчитувачі (рисунок 2.4). Стаціонарні зчитувачі зазвичай прикріплюються нерухомо на стінах, порталах і в інших технічних відповідних місцях. У порівнянні з переносними, зчитувачі такого типу зазвичай мають більшу зоною читання і потужністю і здатні одночасно обробляти дані з декількох десятків міток [6];



Рисунок 2.4 – Приклад стаціонарного зчитувача

– мобільні зчитувачі (рисунок 2.5). Вони на відміну мають меншу дальність дії і переважно не мають постійного зв'язку з програмою контролю. Данний тип зчитувачів має внутрішню пам'ять, в яку записуються дані з прочитаних міток (потім цю інформацію можна використовувати та відобразити на різноманітні пристрої) і, також як і попередній тип, здатні записувати дані в мітку [6];



Рисунок 2.5 – Приклад мобільного зчитувача

– настільні зчитувачі (рисунок 2.6). Зовні, настільний RFID зчитувач дуже схожий на роутер. Застосовуються в таких приміщеннях як бібліотеки, місцях роздрібної торгівлі та інших різноманітних областях [6];



Рисунок 2.6 – Приклад настільного зчитувача

– портальні зчитувачі (рисунок 2.7). Портальний RFID-зчитувач складається з двох вертикальних стійок, всередині яких встановлені 4 приймально-передавальні антени (по 2 в кожній). Антени створюють зону реєстрації RFID-міток, повністю перекриває весь прохід між стійками. RFID-зчитувач може працювати автономно або під управлінням від зовнішнього програмного забезпечення [6].

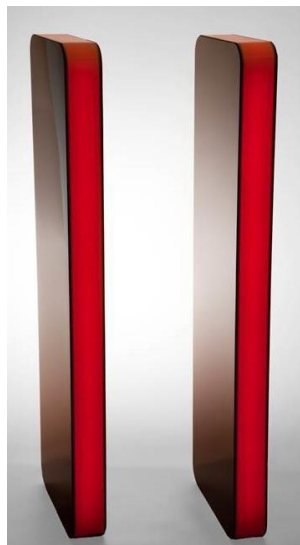


Рисунок 2.7 – Приклад мобільного зчитувача

Переваги RFID:

– відсутність необхідності в прямій видимості. У зчитувача типу RFID немає необхідності в прямій видимості мітки, щоб сприймати її дані. Взаємне становище мітки і зчитувача в просторі абсолютно не грає ролі [6];

– порівняно більша відстань читання. Цей тип міток може зчитуватися на значно більшій відстані, ніж мітки створені іншими технологіями [6];

– великий обсяг зберігання даних в порівнянні з іншими. RFID-мітка зберігає інформацію в значно більшому обсязі, ніж, наприклад, ніж штрих-код. До 10 Кбайт можуть зберігатися на мікросхемі площею в 1 квадратний сантиметр [6];

– функція ідентифікації більше, ніж однієї мітки. Промислові зчитувачі можуть одночасно ідентифікувати кілька десятків міток цього типу в секунду, використовуючи так звану антиколізійну функцію [6];

– велика міцність та стійкість впливу навколишнього середовища. Пасивні мітки мають відносно необмежений термін експлуатації [6];

– інтелектуальне різноманіття. Мітки цього типу можуть використовуватися для виконання багатьох інших завдань, а не тільки лише для того, щоб бути просто запам'ятовуваним пристроєм і носієм даних [6];

– високий ступінь захищеності. Унікальний захищений ідентифікатор, що записується на мітку при виробництві та є гарантом високого ступеня захисту міток від підробки [6].

Недоліки RFID зчитувачів. При роботі з ідентифікацією за допомогою радіочастоти, необхідно враховувати деякі фізичні обмеження. До яких відносяться: неможливість розміщення під металевими і екрануючими поверхнями, взаємні колізії, схильність до перешкод у вигляді сильних електромагнітних полів [6].

Допускається екранування при розміщенні на металевих поверхнях. RFID-мітки схильні до впливу металу. Це зовсім не виключає застосування RFID, але призводить до необхідності використання дорогих міток,

розроблених спеціально під задані цілі, такі як установки на металеві поверхні або до нестандартних способів закріплення міток на об'єкті [6].

2.2.5 Радіочастотний зчитувач RC522

У роботі для ідентифікації різних радіочастотних безконтактних міток використовується сканер RFID RC522 (рисунок 2.8). Даний сканер дозволяє виявити і зчитувати ідентифікатори безконтактних карт, міток, пропусків стандарту 13,56 МГц на відстані до 10 см. При зв'язуванні з мікроконтролером дозволяє створити ряд цікавих проектів: пропускні системи, електронні замки, складський облік і багато іншого [7].

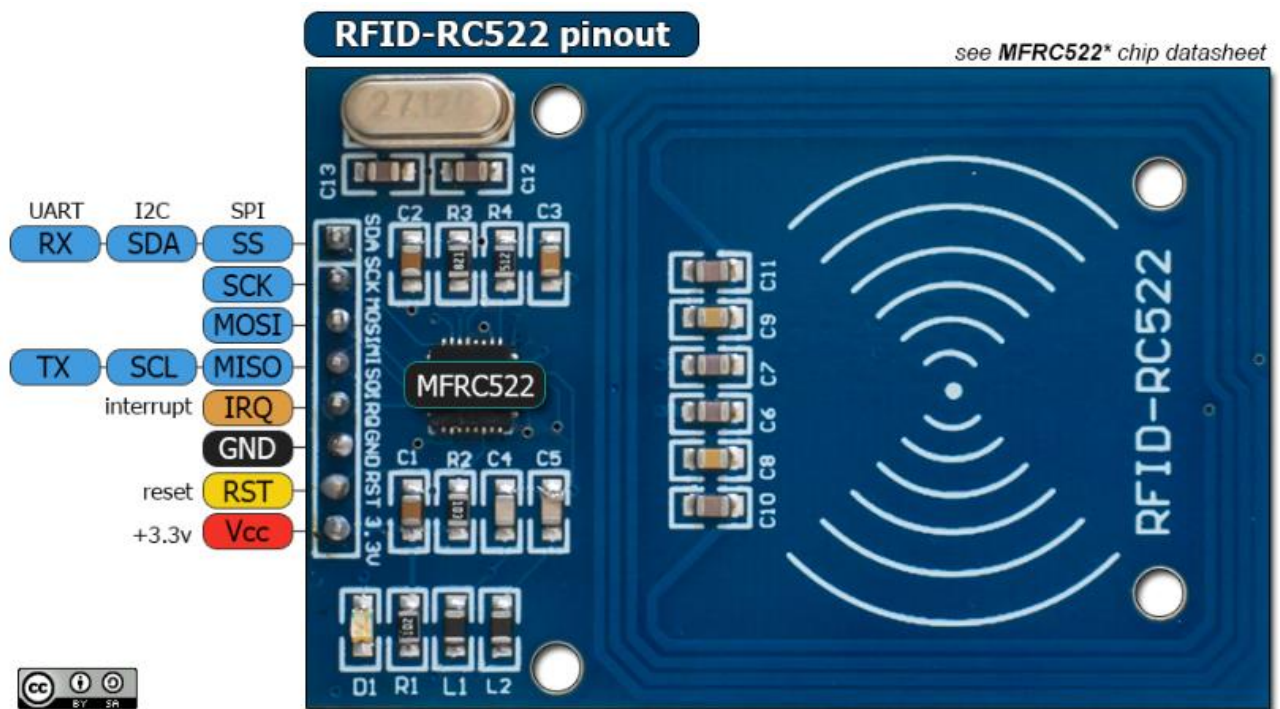


Рисунок 2.8 – Радіочастотний зчитувач RC522

Основні характеристики [7]:

- заснований на мікросхемі MFRC522;
- напруга живлення: 3,3V;
- струм: 13-26 mA;

- у режимі очікування: 10-13 ma;
- у сплячому режимі: менше 80 мкА;
- робоча частота: 13.56 MHz;
- дальність зчитування: 0 ~ 60 мм;
- інтерфейс: SPI, максимальна швидкість передачі 10 Мбіт/с;
- розмір: 40мм x 60 мм;
- читання і запис RFID-міток.

RFID-модуль 13.56 МГц з SPI-інтерфейсом. Даний модуль може бути використаний для різних радіоаматорських і комерційних застосувань, в тому числі для контролю доступу, автоматичної ідентифікації, робототехніки, відстеження речей, платіжних систем і т.д. У комплекті до модуля йде 2 RFID-мітки - у вигляді карти і брелку [7].

2.3 Вибір об'єкта управління

Контролер – це мініатюрний комп'ютер з набором входів і виходів, що працює по заздалегідь написаній програмі. Мікросхема контролера обов'язково присутня в комп'ютерній миші, телефоні, плеєрі і пульті, так само як в практично будь-якому сучасному електронному пристрої [8].

Контролер – річ сама по собі універсальна. До входів можна підключити як звичайні кнопки (пульт), так і температурні датчики (кондиціонер), модулі бездротового зв'язку (телефон) і навіть електрогітару (цифровий процесор ефектів). Виходи також можуть управляти чим завгодно. Завдання контролера – вимірювати електричну напругу на входах і подавати напругу на виходи відповідно до програми [8].

Для реалізації даного проекту будемо вибирати об'єкт управління між мікроЕОМ Raspberry Pi і контролером Arduino.

Розглянемо кожен з пристроїв в деталях і виділимо свої плюси і мінуси при використанні в даному проекті.

2.3.1 Raspberry Pi

Raspberry Pi – це вид одноплатних комп'ютерів, тобто різні частини комп'ютера, які зазвичай розташовуються на окремих платах, тут представлені на одній. До того ж ця плата має відносно невеликий розмір – приблизно 8,5*5,5 см. Raspberry Pi – недорога платформа – середня ціна за одну становить всього \$35, а для новітньої версії A+ взагалі \$20. Продаж даних платформ почався порівняно недавно – на початку 2012 р, сьогодні це найбільш популярна платформа своєї області, продано вже більше 3,5 млн примірників Raspberry Pi [8].

Raspberry Pi випускається в двох версіях – А і В. Версія В на сьогоднішній день більш популярна. Порівняння версій і основні характеристики Raspberry Pi [8]:

- процесор ARM11, Broadcom BCM2835, 700 МГц;
- оперативна пам'ять - 256 Мб у А, 512 Мб у В;
- USB входи/виходи – 1 у А, 2 у В;
- SD вхід;
- RCA вихід;
- HDMI вихід;
- Ethernet вхід/вихід – є тільки у В;
- Audio вихід;
- GPIO контакти.

Для початку роботи з даною мікроЕОМ потрібна SD-карта, із завантаженою операційною системою. Рекомендується використовувати карту з об'ємом від 4 до 32 Гб. Для організації інтерфейсу з користувачем необхідні монітор, з роз'ємом HDMI, DVI або RCA, кабель з даним інтерфейсом, USB-клавіатура і USB-миша. Raspberry Pi є видом повнофункціонального комп'ютера. Він володіє всіма властивостями справжнього комп'ютера: виділеним процесором, пам'яттю і графічним драйвером для виведення через HDMI. На ньому працює спеціальна версія операційної системи Linux. Тому на

даному пристрої легко встановити більшість програм для операційної системи Linux. Після невеликої праці – і Raspberry Pi можна буде використовувати як повноцінний медіа-сервер або емулятор відеоігор. Хоча в ньому і відсутнє внутрішнє сховище даних, на цьому електронному пристрої можна використовувати смарт-карти в якості флеш-пам'яті, яка обслуговує всю систему. Таким чином, доволі швидко можна вивантажувати для налагодження різні версії операційної системи або програмних оновлень. Також цей пристрій забезпечує незалежне з'єднання в мережі, тому його можна налаштувати і для доступу по SSH або пересилати на нього файли по протоколу FTP [8].

Raspberry Pi для роботи потрібно постійна напруга 5V, більш того, робота даної мікроЕОМ завершується програмним процесом – як у звичайного комп'ютера. Raspberry Pi складно переносити з місця на місце, так як ви не зможете просто вставити в нього дві батарейки AA. Для роботи цього комп'ютера необхідно забезпечити безперебійне живлення, а також підключити додаткове обладнання, яке гарантує подачу постійного струму [8].

У Raspberry Pi є вбудований Ethernet-порт, який забезпечує легкий доступ до будь-якої мережі і практично не вимагає налаштувань. Провести бездротовий Інтернет на Raspberry Pi також не складає труднощів: для цього достатньо придбати USB-адаптер для модуля Wi-Fi і встановити відповідний драйвер. Як тільки це зроблено, можна приступати до використання операційної системи для підключення до вебсерверів, обробленню HTML або просто що-небудь писати в Інтернеті. Також Raspberry Pi можна використовувати як для створення віртуальної приватної мережі, так і в якості сервера друку [8].

2.3.2 Контролер Arduino

Порівнюючи плати Arduino і Raspberry Pi має сенс відразу сказати, що плати Arduino – це мікроконтролери, а не повноцінні комп'ютери. На них немає операційної системи як такої, Arduino просто виконує код, що інтерпретується

прошивкою. В даному випадку, відсутні базові інструменти, що надаються операційною системою, але, з іншого боку, таке безпосереднє виконання нескладного коду протікає простіше, а при роботі не виникає ніяких затримок, яких помилок, пов'язаних з операційною системою [9].

Основне призначення плати Arduino – взаємодія з сенсорами і пристроями, тому Arduino відмінно підходить для апаратних проєктів, де потрібно просто реагувати на різні сигнали сенсорів і ручне введення. Може здатися, що в цьому немає нічого особливого, проте на ділі Arduino - складна віртуальна система, яка значно полегшує керування пристроями. Вона відмінно підходить саме для організації взаємодії інших пристроїв і виконавчих механізмів, де повноцінна операційна система просто не потрібно, так як мова йде просто про отримання сигналів з сенсорів і реагуванні на них [9].

Як приклад характеристик, наведемо основні характеристики найбільш популярною і універсальної серії контролерів Arduino – Uno [10]:

- мікроконтролер ATmega328 [10];
- робоча напруга 5 В [10];
- рекомендована вхідна напруга 7-12 В (граничне 6-20 В) [10];
- 14 контактів для цифрового сигналу (6 з яких можуть бути використані як виходи ШІМ) [10];
- 6 аналогових входів [10];
- постійний струм через вхід/вихід 40 мА [10];
- постійний струм для виведення 3,3 В 50 мА [10];
- Flash-пам'ять 32 Кб (ATmega328), з яких 0,5 Кб використовуються для завантажувача [10];
- ОЗУ 2 Кб (ATmega328) [10];
- EEPROM 1 Кб (ATmega328);
- тактова частота контролера 16 МГц [10].

Arduino Uno може живитись як від USB підключення, так і від зовнішнього джерела: батарейки або звичайної електричної мережі. Джерело визначається автоматично. Платформа може працювати при наявності напруги

від 6 до 20 В. Однак при напрузі менше 7 В робота може бути нестійкою, а напруга більше 12 В може призвести до перегріву і пошкодження. Тому рекомендований діапазон: 7-12 В [10].

На Arduino доступні наступні контакти для доступу до живлення [10]:

- Vin надає той же вольтаж, що використовується для живлення платформи. При підключенні через USB буде дорівнює 5 В [10];

- 5V надає 5 В незалежно від вхідної напруги. На цій напрузі працює процесор. Максимальний допустимий струм, одержаний за цього контакту – 800 мА [10];

- 3,3 V надає 3,3 В. максимально допустимий струм, одержуваний з цього контакту – 50 мА [10];

- GND – земля [10].

Arduino починає виконувати код відразу після включення і припиняє роботу відразу, як тільки відключити плату від джерела живлення. Щоб розширити функціонал пристрою з Arduino, необхідно підключити периферійні пристрої безпосередньо до контактів самої плати Arduino, або до плат розширень для неї [9].

Для Arduino існують сотні різноманітних модулів, кожен з яких призначений для вирішення специфічного завдання, може взаємодіяти з тими чи іншими сенсорами, а також з іншими модулями, які разом утворюють повноцінний керуючий блок [9].

На жаль, система Arduino без додаткових модифікацій не пристосована для роботи в мережі інтернет [9].

Щоб встановити надійне з'єднання, вона вимагає або підключення додаткових модулів до плати, або використання модифікацій платформи з відразу вбудованими необхідними модулями. Як вже говорилося вище, Arduino має велику кількість сумісних модулів. Відповідно, знайти і підключити необхідний Wi-Fi модуль не буде важким завданням [9].

2.3.3 Обґрунтування використання контролера

При відомому і чітко поставленому завданню завжди простіше вибрати основні і периферійні пристрої для використання в проєкті. Основне завдання в цьому проєкті полягає в обробці сигналів з сенсора і подальша зміна значень на периферійних пристроях, а саме сервоприводи. Платформа Arduino проста в обслуговуванні і не вимоглива в живленні. У середовищі Arduino IDE, врахувавши те, що потрібно автономна робота платформи, можна скласти код, який дозволить використовувати пристрій, при цьому не виключаючи і абсолютно не втручаючись в його роботу [10].

Наведемо аргументи на користь платформи Arduino в порівнянні з мікроЕОМ Raspberry Pi. Основними плюсами даного одноплатного контролера в порівнянні з Arduino є продуктивність, багатозадачність, зручність роботи з інтернетом, наявність вибору мови програмування, робота з відео, звуком. Недоліками - швидкість реакції в швидкодіючих проєктах і коротка тривалість роботи від акумулятора. З переваг даного мікрокомп'ютера може знадобитися зручність роботи з даними з інтернет протоколами, але інші переваги в даній роботі абсолютно не критичні. До того ж, з огляду на сотні мА, які Raspberry Pi споживає при своїй роботі на нормальне функціонування, доцільність використання даного мікрокомп'ютера сходить нанівець. До того ж, Raspberry Pi для ефективної взаємодії з різними пристроями вимагає спеціального програмного забезпечення. Використання даної мікроЕОМ виправдано при вирішенні таких завдань, які було б логічно виконувати на персональному комп'ютері. Raspberry Pi спрощує управління потоком операцій в різних ситуаціях [10]:

2.3.4 Вибір модифікації Arduino

Після того як було вирішено зробити Arduino центральним елементом системи, яка розробляється, належить зробити вибір модифікації Arduino. Вибір

належить зробити між Arduino Uno з модулем Wi-Fi ESP8266 і платою Wemos D1 Mini. Жодного з цих рішень не має значної переваги перед іншим. У плату Wemos D1 Mini виробником був вбудований абсолютно такий же модуль ESP8266, з бездротовим інтерфейсом Wi-Fi 802.11 b/g/n. Нижче опишемо особливості даної модифікації.

У даній модифікації платформи Arduino Uno, на платформі розташовані 11 контактів. Але, на відміну від оригіналу, не всі з них можуть бути використані для цифрового введення і виведення. Всі вони працюють з напругою 3,3 В, і розраховані на струм до 40 мА. Також кожен контакт має вбудований, але відключений за замовчуванням резистор на 20 - 50 кОм. Деякі контакти мають додаткові ролі [10]:

- Serial: 0-й і 1-й. Дані контакти позначаються «RX» і «TX» і використовуються для прийому і передачі даних по USB, або між декількома платформами [10];

- D0 - D8 можуть використовуватися для отримання вхідних цифрових сигналів і передачі вихідних. Також кожен з цих контактів може використовуватися як один з портів послідовного периферійного інтерфейсу (SPI) [10].

На Arduino доступні наступні контакти для доступу до живлення:

- Vin надає той же вольтаж, що використовується для живлення платформи. При підключенні через USB буде дорівнює 5 В [10];

- 5V надає 5 В незалежно від вхідної напруги. На цьому напрузі працює процесор. Максимальний допустимий струм, одержаний на цьому контакті – 800 мА [10];

- 3,3V надає 3,3 В. Максимальний допустимий струм, одержаний на цьому контакті – 50 мА [10];

- G – земля.

Крім цього на платі є вхідний контакт Reset. Його установка в логічний нуль призводить до скидання процесора. Це аналог кнопки Reset звичайного комп'ютера [10].

Список перерахованих контактів Wemos D1 і їх основні функції представлені в таблиці 2.1.

Таблиця 2.1 – Контакти Wemos D1 і їх функції [11]

Контакт	Функції	Позначення Відповідно до ESP-8266
TX	TXD	TXD
RX	RXD	RXD
A0	Аналогове введення (3,3 В максимум)	A0
D0	Цифрове введення / виведення	GPIO16
D1	Цифрове введення / виведення	GPIO5
D2	Цифрове введення / виведення, канал отримання даних	GPIO4
D3	Цифрове введення / виведення, підтягування	GPIO0
D4	Цифрове введення / висновок, підтягування, вбудований світлодіод	GPIO2
D5	Цифрове введення / виведення, тактовий сигнал	GPIO14
D6	Цифрове введення / висновок, передача даних від відомого до ведучого	GPIO12
D7	Цифрове введення / висновок, передача даних від ведучого до відомого	GPIO13
D8	Цифрове введення / виведення, вибір відомого	GPIO15
G	Земля	GND
5V	Живлення 5 В	-
3V3	Живлення 3,3 В	3,3V
RST	Скидання	RST

ESP8266 – мікроконтролер китайського виробника Espressif з інтерфейсом Wi-Fi. Крім Wi-Fi мікроконтролер відрізняється важливою для даного проекту можливістю виконувати програми з зовнішньої flash-пам'яті з інтерфейсом SPI. Цей чип вбудований в плату Wemos D1 і використовується для взаємодії з Wi-Fi з Web сервером [11].

Мікроконтролер не має на кристалі енергонезалежної пам'яті. Виконання програми ведеться із зовнішнього SPI ПЗП шляхом динамічного підвантаження необхідних ділянок програми в кеш інструкцій. Підвантаження відбувається апаратно, прозоро для програміста. Підтримується до 16 МБ зовнішньої пам'яті програми. Можливий інтерфейс Standard, Dual або Quad SPI [11].

3 РОЗРОБКА СИСТЕМИ ОБЛІКУ ПЕРСОНАЛІЗАЦІЇ

Система обліку відвідуваності буде складатися з п'яти основних взаємодіючих компонентів. Функціональна схема даної системи зображена на рисунку 3.1.

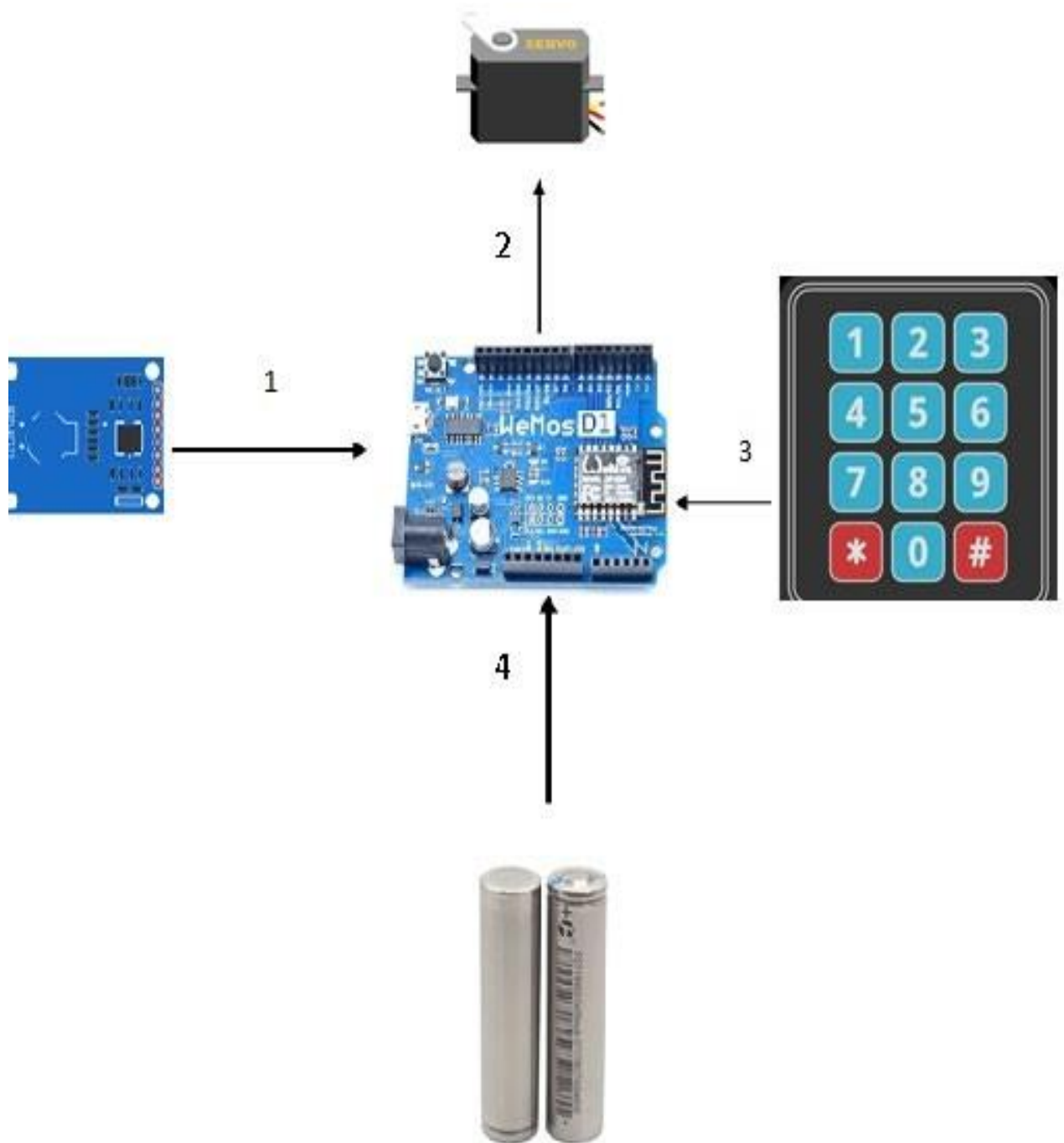


Рисунок 3.1 – Функціональна схема системи обліку відвідуваності

Алгоритм роботи системи:

- сигнал про наявність мітки приходить з RFID зчитувача на мікроконтролер;
- мікроконтролер відправляє запит на вебсервер з базою даних, запитуючи, чи має права доступу власник даної мітки;
- вебсервер відповідає на запит. Далі можливі два варіанти розвитку подій: або власнику дозволено відвідати приміщень, або відмова в доступі. Якщо відбувається відмова в доступі, то система не виробляє ніяких дій, в очікуванні наступного сеансу ідентифікації;
- якщо власник мітки має доступ в приміщення, то мікроконтролер відправляє сигнал на сервопривід відкрити двері, за умови, що вона була закрита, або навпаки, закрити двері, якщо вона була відкрита;
- на вебсервер, створений платою Wemos D1 Mini, відправляється інформація про час відвідування і унікальний номер карти.

3.1 Організація взаємодії Wi-Fi Wemos D1 Mini і RC522

3.1.1 Опис SPI

Платформа Wemos D1 Mini і радіочастотний ідентифікатор RC522 зв'язуються по послідовному периферійному інтерфейсу SPI. SPI – один з найпопулярніших інтерфейсів для виконання послідовного обміну даними між мікросхемами. Поряд з не менш поширеним I2C, і є найбільш широко-використовуваних інтерфейсів для з'єднання мікросхем. Даний тип інтерфейсу був розроблений для організації простого і швидкого обміну даних між компонентами системи – мікроконтролерами і периферійними пристроями (рисунок 3.2) [12].

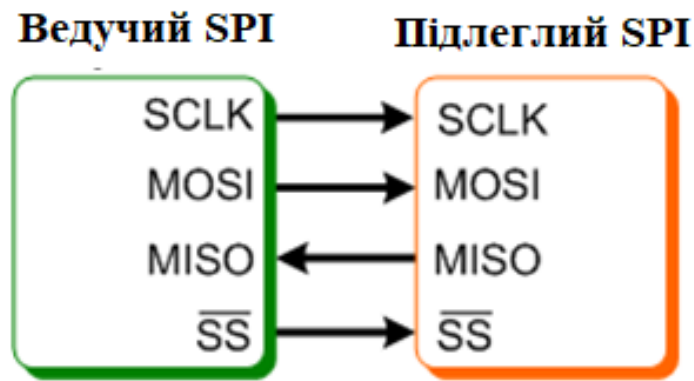


Рисунок 3.2 – Приклад пристроїв, пов'язаних SPI

На шині завжди є один ведучий пристрій і кілька підлеглих, master і slave відповідно. Інтерфейс використовує такі лінії для обміну даними [12]:

- SCK - Serial Clock: тактовий сигнал;
- MOSI - Master Output, Slave Input: дані від ведучого до підлеглого;
- MISO - Master Input, Slave Output: дані від підлеглого до ведучого;
- SS (SDA) - Slave Select: вибір підлеглого; встановлюється ведучим.

На початку роботи, ведучий пристрій встановлює низький рівень сигналу на тій лінії SDA, на якій знаходиться потрібний йому підлеглий пристрій. В даному проєкті буде тільки один підлеглий пристрій - RC522, відповідно, на початку кожного сеансу роботи на контакті SDA у даного пристрою низький рівень сигналу. Після цього, ведучий пристрій задає такт за допомогою синхронізуючого виходу SCK. З кожним тактом по каналах зв'язку MOSI і MISO передається потрібний рівень сигналу від ведучого до підлеглого і від підлеглого до ведучого, відповідно. Для завершення сеансу передачі даних, провідний пристрій відправляє високий рівень сигналу по каналу SDA. SPI являється повнодуплексною шиною – дані передаються одночасно в обидва боки. Типова швидкість роботи шини лежить в межах 1-50 МГц. Завдяки подібній винятковій простоті алгоритму передачі, SPI отримав широке розповсюдження в самих різних електронних пристроях - наприклад, в датчиках, чипах пам'яті, радіомодулях, і т.д. [12].

3.1.2 Підключення Wi-Fi модуля Wemos D1 Mini і RC522

В даному проєкті платформа Wemos D1 Mini і радіочастотний ідентифікатор RC522 з'єднуються 7 проводами «тато-мама». Підключення відбувається за схемою, яка представлена на рисунку 3.3.

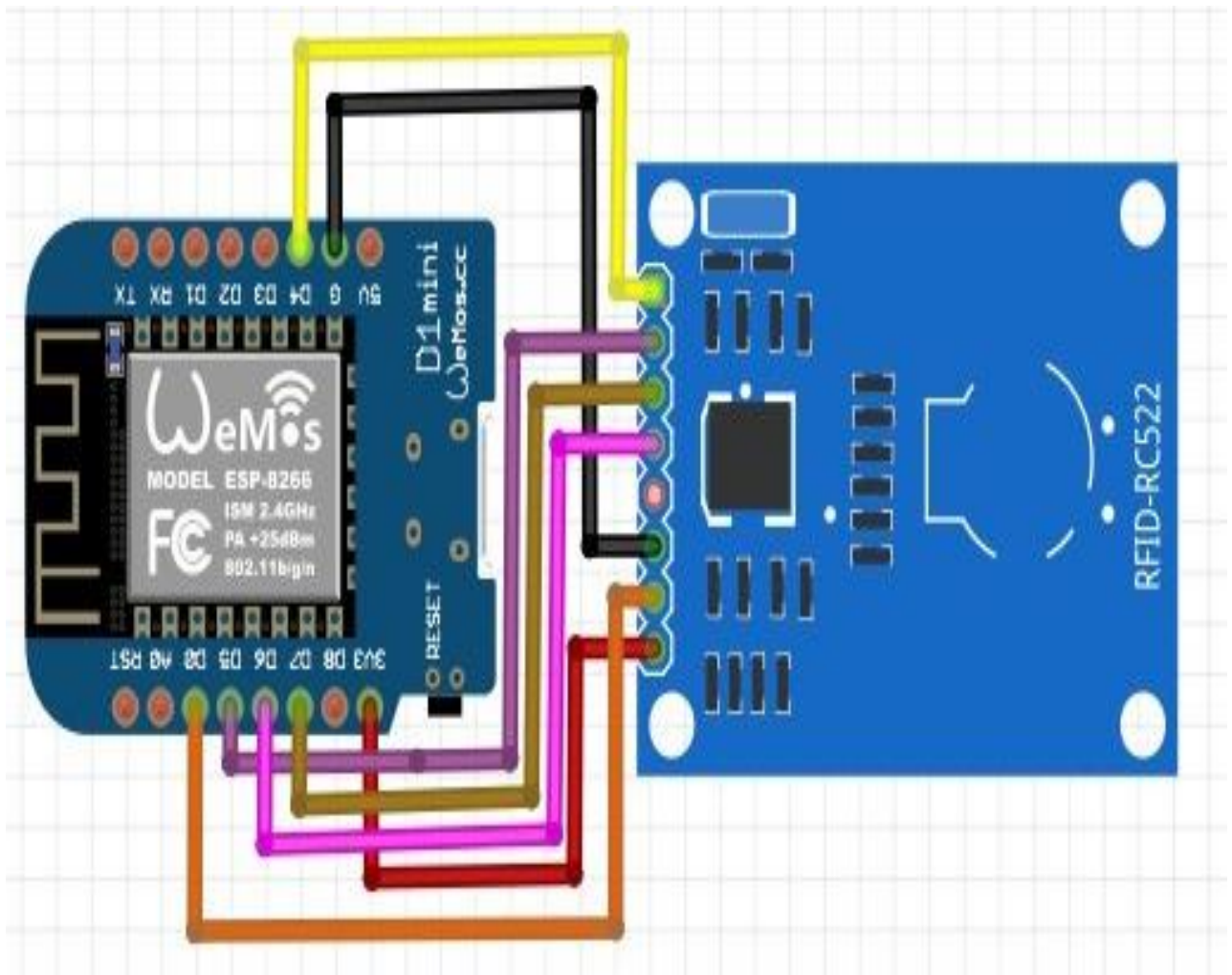


Рисунок 3.3 – Схема з'єднання RC522 і Wemos D1 Mini

В таблиці 3.1 представлена інформація щодо способів з'єднання контактів Wemos D1 Mini і RC522, які в свою чергу продемонстровані на рисунку 3.3.

Таблиця 3.1 – З'єднання контактів Wemos D1 Mini і RC522 [12]

RFID RC522	Wemos D1 Mini
RST	GPIO2
SDA	GPIO4
MOSI	GPIO13
MISO	GPIO12
SCK	GPIO14
3,3V	3,3V
GND	GND

3.1.3 Програмування в Arduino IDE

Arduino IDE – це програма, яка дозволяє складати програми в зручному текстовому редакторі, компілювати їх в машинний код, і завантажувати на всі версії Arduino [13].

Додаток є повністю безкоштовним, а завантажити його можна на офіційному сайті спільноти Arduino. В даному середовищі програмування використовується мова C ++ [13].

Для того, щоб контролер і ідентифікатор могли спілкуватися між собою за допомогою цього середовища програмування, необхідно завантажити та встановити з офіційного сайту Arduino бібліотеку «RFID Library for MFRC522» Дана бібліотека необхідна для того, щоб в Arduino IDE з'явилися команди для взаємодії з RC522 [13].

На рисунку 3.4 предсталено алгоритм роботи програмного коду RC522, який представлений в Додатку А.

В даному коді реалізована ідентифікація картки або чипу, оснащених радіочастотним передавачем і запис в масив унікального коду.

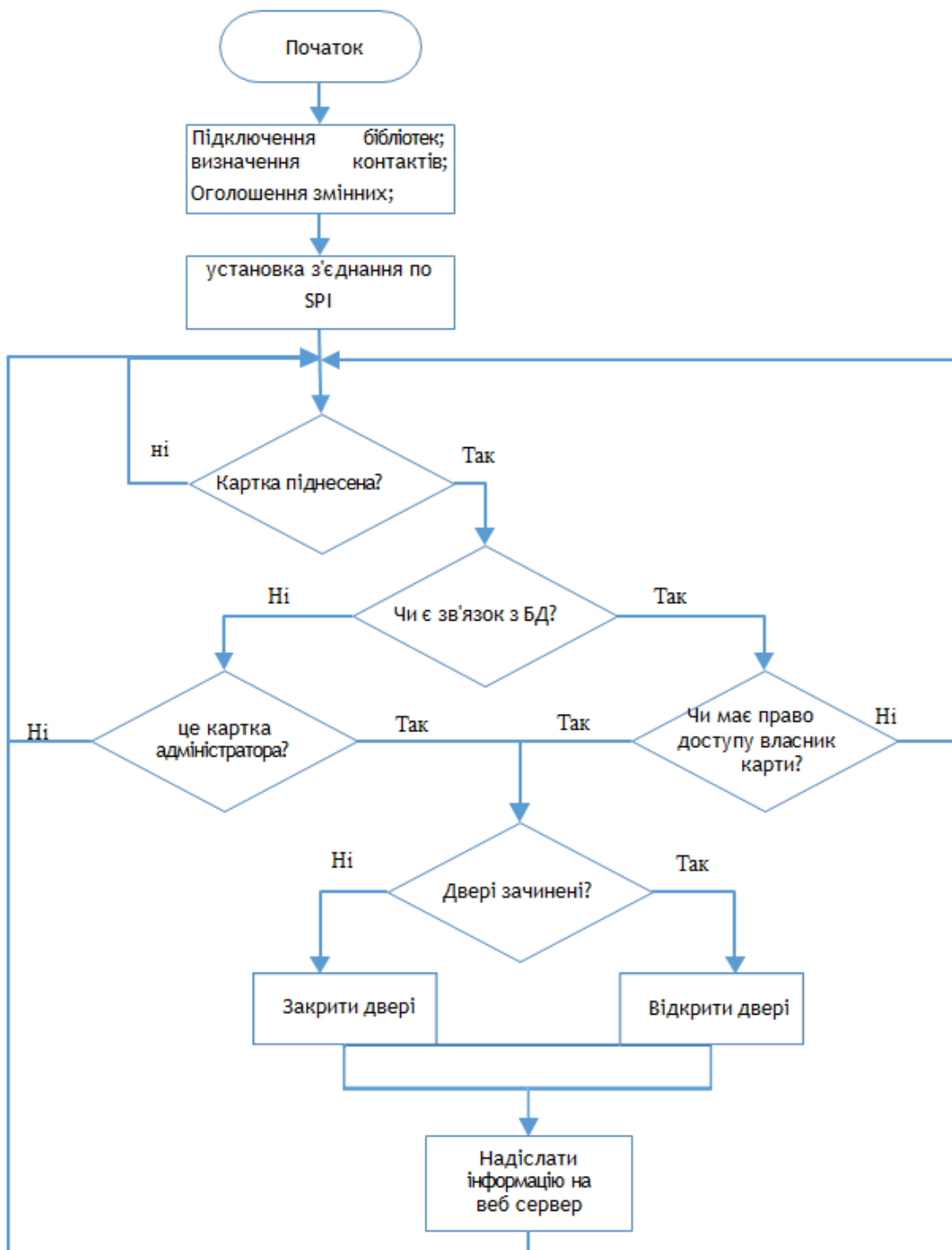


Рисунок 3.4 – Схема алгоритму роботи коду RC522

3.2 Робота сервоприводу

Під сервоприводом частіше всього мають на увазі механізм з електромотором, який можна змусити повернутися на заданий кут і утримувати це положення [14].

Якщо більш докладніше, сервопривід – це пристрій з управлінням через негативний зворотний зв'язок, що дозволяє з великою точністю керувати параметрами руху. Сервоприводом є будь-який тип механічного приводу, що має в складі датчик (положення, швидкості, зусилля і т.п.) і блок управління приводом, автоматично підтримує необхідні параметри на датчику і пристрої відповідно до заданого зовнішнього значення [14].

Алгоритм роботи сервоприводу:

- сервопривід отримує на вхід значення керуючого параметра, наприклад, кут положення [14];
- блок управління порівнює це значення зі значенням на своєму датчику;
- на основі результату порівняння привід виробляє деяку дію, наприклад: поворот, прискорення або уповільнення так, щоб значення з внутрішнього датчика стало якомога ближче до значення параметра, який задається [14].

Найбільш поширені сервоприводи, які утримують заданий кут і сервоприводи, що підтримують задану швидкість обертання [14].

Сервоприводи мають кілька складових частин (рисунок 3.5) [14].

Привід – це електромотор, який має редуктор. Щоб перетворювати електричну енергію в механічну (поворот), необхідний електромотор. Проте частіше всього швидкість обертання мотора буває занадто великою для використання на практиці. Тому щоб знизити швидкість, використовується редуктор - механізм з шестернею, тобто передає і перетворює крутний момент [14].

Включаючи та вимикаючи цей вид електромотору, можна обертати вихідний вал – кінцеву шестерню сервоприводу, до якої також можна прикріпити будь-що, чим в подальшому планується керувати. Але, щоб положення контролювалося пристроєм, необхідний датчик зворотного зв'язку, який буде перетворювати кут повороту назад в електричний сигнал. Для цього дуже часто використовується потенціометр. При повороті його бігунка відбувається зміна його опору, пропорційне куту повороту потенціометра.

Таким чином, за його допомогою можна встановити поточний стан механізму [14].

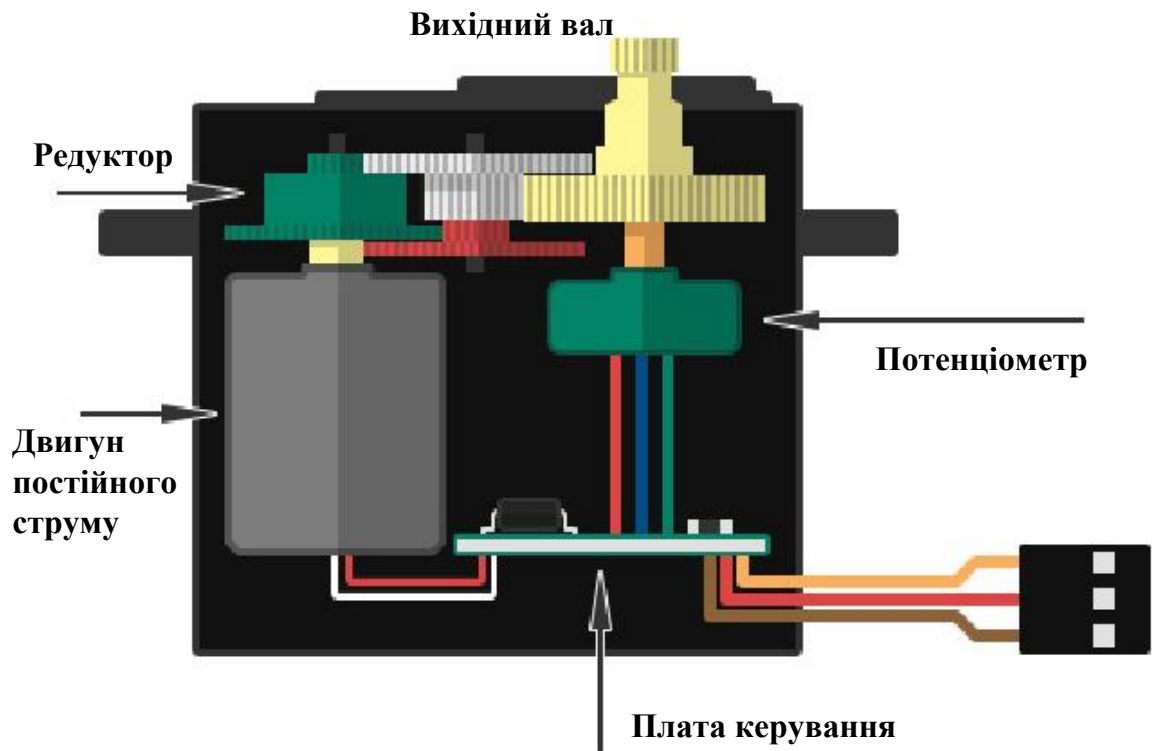


Рисунок 3.5 – Механізм сервоприводу

Крім електромотора, редуктора і потенціометра в сервопривід входить електронна начинка, що відповідає за прийом зовнішнього параметра, тобто зчитування значень з потенціометра, та їх порівняння включення/вимикання двигуна. Саме вона і відповідає за підтримання негативного зворотного зв'язку. До самого сервоприводу тягнуться три дроти. Два з них відповідають за живлення мотора, третій відповідає за керуючий сигнал, який використовують для виставлення положення пристрою [14].

3.2.1 З'єднання сервоприводу і Arduino

Сервопривід, який використовується в даному проєкті, володіє трьома контактами:

- живлення;

- контакт для керуючого сигналу;
- GND – земля.

На рисунку 3.6 представлено з'єднання сервоприводу і Wemos D1 Mini.

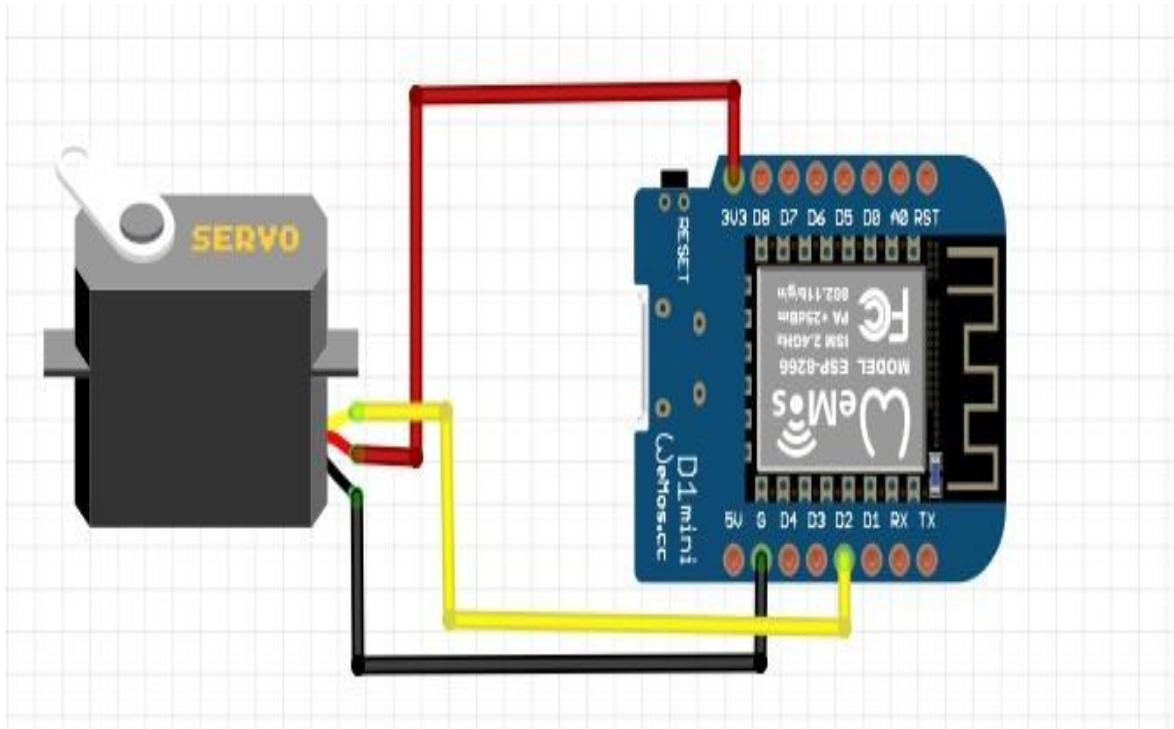


Рисунок 3.6 – Схема з'єднання сервоприводу і Wemos D1 Mini

На контакт для керуючого сигналу з контролера приходить сигнал, що повідомляє сервоприводу кут, на який необхідно повернути вихідний вал. Для використання команд для управління сервоприводом, необхідно підключити стандартну бібліотеку в Arduino IDE і створити об'єкт класу Servo:

```
#include <Servo.h> Servo servo.
```

В області завдання налаштувань програми необхідно задати контакт, який буде використовуватись як вихід для керуючого сигналу, що посилається на сервопривід:

```
void setup ()
{ servo.attach (0);
}
```

Після підключення бібліотеки і створення змінних можна користуватися командою «Servo.write», яка повідомляє сервоприводу кут для повороту. Приклад використання в створеному проєкті:

```
If (is_door_open == false)
  {Servo.write (180); is_door_open = true; Serial.println ( "Opening
  ..."); } Else {servo.write (60); is_door_open = false; Serial.println ( "Closing
  ...");}
```

В даному уривку коду відбувається перевірка умови «відриті двері?», якщо ця умова невірна, тобто двері закриті, то сервопривід повертається на певний кут, обертаючи ручку замка на такий кут, щоб ригель повністю пішов в тіло замку, таким чином відбувається відкриття дверей. Якщо умова «Відриті двері?» вірна, то сервопривід також повертає вихідний вал на деякий кут, повертаючи ригель в початкове положення і, тим самим, закриваючи двері.

3.2.2 Розробка принципової та друкованої плати

Для проєктування друкованої плати та принципової схеми буде використовуватися програмне забезпечення Eagle [15].

Eagle – це система для проєктування електричних принципових схем та друкованих плат, яка була розроблена компанією CadSoft Computer GmbH. Програма дозволяє експортувати та імпортувати файли до інших систем автоматизованого проєктування і розрахунку (САПР) [15].

Можливості САПР EAGLE: модуль електронних принципових схем та модуль друкованих плат [15].

Модуль електронних принципових схем дозволяє створювати принципові електричні схеми, проєктувати складні електронні системи. Дозволяє переключати анотацію на модуль друкованої плати. Файли зберігаються у форматі .SCH, а компоненти зберігаються в бібліотеках пристроїв з розширенням .LBR. Має вбудовані блоки [15]:

- схемний редактор (використовується для розміщення компонентів на схемі, прокладення з'єднань) [15];
- контролер бібліотек (дозволяє додавати, налаштовувати та створювати власні бібліотеки) [15];
- ERC модуль (перевірка електричних правил, перевіряє узгодження схеми, а саме з'єднання елементів між собою, коректність з'єднання живлення та розриви на електричній схемі, неузгодження принципової схеми та друкованої плати) [15].

Модуль друкованих плат дозволяє створити друковану плату. Якщо електрична принципова схема була вже зібрана, то модуль автоматично підзавантажує необхідні компоненти та зв'язки між ними. Має вбудовані блоки [15]:

- DRC (перевірка правил проектування, в цьому місці потрібно задекларувати необхідні правила для друкованої плати. Наприклад, ширина доріжок, параметри отворів тощо) [15];
- Autorouter (автотрасування доріжок, дозволяє автоматично прокласти маршрути для доріжок, враховуючи задані правила) [15];
- Ratsnest (оптимізація, оцінюється маршрут повітряних з'єднань та створюється найоптимальніший маршрут) [15].

Важливою можливістю програми є створення GERBER файлів. GERBER – спеціальний файловий формат, який представляє собою спосіб опису проєкту друкованої плати для виготовлення фотошаблонів на різноманітному обладнанні. Майже все сучасне обладнання дозволяє зчитувати файли у цьому форматі [15].

Практично всі компанії виробники друкованих плат приймають на замовлення GERBER файли.

3.3 Створення та експлуатація вебсервера

В даному проєкті планується використовувати два невеликих вебсервера – один на персональному комп'ютері, для зберігання бази даних унікальних ключів і прав доступу, інший – створений платформою Wemos D1 Mini, для зберігання історії відвідування даного приміщення.

3.3.1 Створення вебсервера на персональному комп'ютері

Для створення і експлуатації вебсервера на персональному комп'ютері необхідно додаткове програмне забезпечення.

Програма Apache буде виконувати функції http сервера. Саме з її допомогою і буде функціонувати вебсервер. Ця програма виконує всі необхідні функції, під її керівництвом працює більшість ресурсів мережі. Створений сервер не виняток, в силу гнучкості і універсальності Apache, для створення вебсервера буде використана саме ця утиліта [16].

Web-сервер Apache є самостійним, некомерційним, вільно розповсюджуваним продуктом. Продукт підтримує безліч можливостей, багато з яких реалізовані як скомпільовані модулі, які розширюють основні функціональні можливості. Вони різняться від серверної підтримки мов програмування до схем аутентифікації. Існують інтерфейси для підтримки мов програмування Perl, Python, Tcl і PHP [16].

Популярні методи стискування на Apache включають зовнішній модуль `mod_gzip`, створений для зменшення розміру вебсторінок, переданих по HTTP.

Функції віртуального хостингу дозволяють одній інсталяції Apache обслуговувати різні вебсайти. Наприклад, одна машина, з однією інсталяцією Apache може одночасно містити `www.example.com`, `www.test.com`, `test47.test-server.test.com` і так далі [16].

Ядро Apache включає в себе основні функціональні можливості, такі як обробка конфігураційних файлів, протокол HTTP і система завантаження

модулів. Ядро (на відміну від модулів) повністю розробляється Apache Software Foundation, без участі сторонніх програмістів [16].

Теоретично, ядро apache може функціонувати в чистому вигляді, без використання модулів. Однак, функціональність такого рішення вкрай обмежена [16].

Ядро Apache повністю написано мовою програмування C [16].

Система конфігурації Apache заснована на текстових конфігураційних файлах. Має три умовних рівня конфігурації [16]:

- конфігурація сервера (файл `httpd.conf`) [16];
- конфігурація віртуального хоста (файли `httpd.conf` с версії 2.2, `extra / httpd-vhosts.conf`) [16];
- конфігурація рівня директорії (файл `htaccess`) [16];

Має власну мову конфігураційних файлів, заснований на блоках директив. Практично всі параметри ядра можуть бути змінені через конфігураційні файли. Більша частина модулів має власні параметри. Частина модулів використовує у своїй роботі конфігураційні файли операційної системи (наприклад `/etc/passwd` і `/etc/hosts`). Крім цього, параметри можуть бути задані через ключі командного рядка [16].

Після налаштування Apache, в панелі швидкого доступу з'являється ярлик Apache Monitor, при успішному запуску вебсервера, там можна побачити наступну інформацію (рисунок 3.7).

Тепер, якщо в браузері, в пошуковому рядку вписати «localhost» або IP адреса 127.0.0.1, то на екран виведеться наступна напис «Hello? World!» (рисунок 3.8).

Текст цієї програми, написаний мовою PHP, зберігається за замовчуванням в папці, де був створений сервер і називається `index.php`.

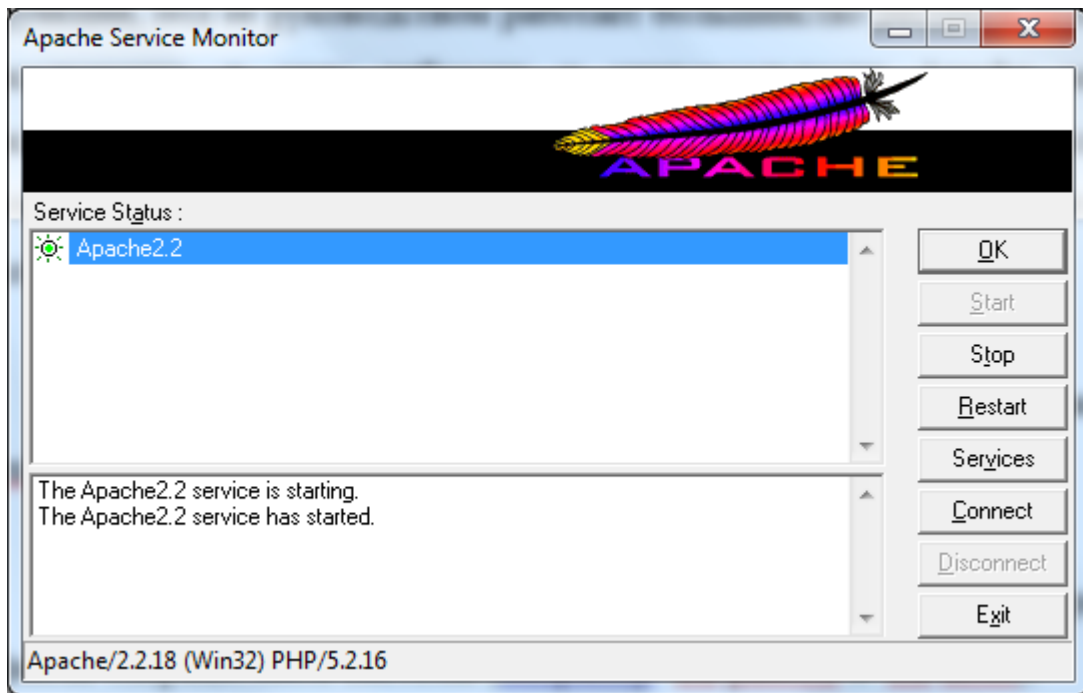


Рисунок 3.7 – Apache Monitor



Рисунок 3.8 – Підключення до вебсервера Apache

3.3.2 Підключення до вебсервера з платформи Wemos D1 Mini

Для створення вебсервера з платформи Wemos D1 Mini використовується середовище програмування Arduino IDE. Для початку, необхідно підключити скачати і підключити бібліотеку для використання, інтегрованого wi-fi модуля. Щоб підключити бібліотеку необхідно ввести команду:

```
#include <ESP8266WiFi.h>.
```

Для підключення до мережі Wi-Fi здійснюється за допомогою команди WiFi.begin (ssid, password), де ssid – ім'я мережі, а password – пароль для даної

мережі. Опис інших команд бібліотеки ESP8266.h, які використовуються для створення програми:

- `client.println ()` – друкує дані на монітор порту сервера, до якого підключений клієнт;

- `WiFi.localIP ()` – повертає IP-адресу Wi-Fi мережі, до якої підключено даний пристрій;

- `WiFi.status ()` – повертає інформацію про стан підключення до мережі.

Список варіантів значень, що повертаються представлені нижче:

- `client.connect (ip, port)` – команда для приєднання до певного вебсервера по його IP. Також вказується порт, по якому буде відбуватися підключення. Для успішного підключення цей порт повинен бути вільний і доступний для встановлення зв'язку з його допомогою. Найчастіше для цих цілей використовуються порти 80 і 443;

- `client.available ()`, `client.read ()` – команди, часто використовуються в зв'язці. Параметр `.available ()` повертає кількість байт, доступних для читання. Дана команда перевіряє, чи прийшла якась інформація при запиті від клієнта до сервера. Параметр `.read` зчитує інформацію, відправлену від сервера клієнту.

Список варіантів значення команди `WiFi.status ()`:

- `WL_CONNECTED`: повертається, якщо встановлення зв'язку з wi-fi мережею пройшло успішно;

- `WL_NO_SHIELD`: даний статус присвоюється, якщо платформа не може знайти пристрій для зв'язку з Wi-Fi;

- `WL_IDLE_STATUS`: це тимчасовий статус, який присвоюється під час виконання команди `WiFi.begin ()`. Статус буде зберігатися в такому вигляді, поки не скінчиться число спроб з'єднання (в результаті присвоїти статус `WL_CONNECT_FAILED`) або з'єднання успішно встановиться (відбудеться присвоєння статусу `WL_CONNECTED`);

- `WL_NO_SSID_AVAIL`: повертається, коли немає доступної мережі з таким ім'ям;

- WL_SCAN_COMPLETED: використовується при скануванні Wi-Fi мереж, повідомляє про те, що сканування завершилося успішно;
- WL_CONNECT_FAILED: даний статус присвоюється після закінчення числа спроб з'єднання з мережею;
- WL_CONNECTION_LOST: цей статус повідомляє про те, що з'єднання з мережею втрачено;
- WL_DISCONNECTED: повертається, якщо сталося відключення від мережі Wi-Fi.

ВИСНОВКИ

На будь-якому підприємстві і в кожній організації є приміщення, в яких зберігається апаратура або документи з обмеженими правами доступу. Безсумнівно, людина, відповідальна за збереження подібного роду речей, зацікавлений в тому, щоб доступ до них залишався в установлених межах, з метою підтримки максимального рівня безпеки.

В кваліфікаційній роботі була розроблена система автоматичної персоналізації та відвідуваності приміщень, сейфів, шкафів, тумбочок на основі Arduino. У даній системі були використані наступні елементи:

- мікроконтролер Wemos D1 Mini;
- RFID – зчитувач моделі RC522;
- сервопривід;
- запірний пристрій;
- база даних на вебсервері.

Поставлена мета роботи, а саме, створення системи обліку персоналізації з можливістю дистанційного відстеження, була успішно досягнута.

Дана система, яка розроблялась, може бути впроваджена на абсолютно будь-яких підприємствах і організаціях, зацікавлених у підвищенні безпеки будь-якого приміщення. Відмінною особливістю даної системи є наявність взаємодії пристрої ідентифікації з віддаленим веб сервером за допомогою технології Wi-Fi.

Для поліпшення даної системи, необхідно додати можливість відстеження відвідуваності за допомогою Wi-Fi не тільки по локальній мережі, але і з будь-якої іншої мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Замки з карткою доступу. [Електронний ресурс] – Режим доступу: <https://bezpeka.club/access-card-locks/> (дата звернення: 18.05.2024)
2. Коваль Л.Г., Злепко С.М., Новіцький Г.М., Крекотень Є.Г. Методи і технології біометричної ідентифікації за результатами літературних джерел. [Електронний ресурс] – Режим доступу: https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf (дата звернення: 17.05.2024)
3. Кіндій В.А., Парамуд Я.С. Алгоритмічно-програмні засоби моніторингу часу роботи працівника за комп'ютером. Комп'ютерні системи та мережі. 2022. Вип. 4, №1. С. 59-66. (дата звернення: 19.05.2024)
4. Комп'ютерні мережі. [Електронний ресурс] – Режим доступу: <https://e-tk.lntu.edu.ua/mod/page/view.php?id=3539> (дата звернення: 19.05.2024)
5. Протикражні радіочастотні системи: опис, характеристики і відгуки. [Електронний ресурс] – Режим доступу: <http://xn--80aimveh.pp.ua/nauka/16867-protikrazhn-radochastotn-sistemi-opis-harakteristiki-vguki.html> (дата звернення: 20.05.2024)
6. Радіочастотна ідентифікація. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%96%D0%BE%D1%87%D0%B0%D1%81%D1%82%D0%BE%D1%82%D0%BD%D0%B0_%D1%96%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F (дата звернення: 20.05.2024)
7. RFID модуль RC522 з карткою доступу для Arduino. [Електронний ресурс] – Режим доступу: <https://arduino.ua/prod649-rfid-modyl-rc522-s-kartochkoi-dostupa-dlya-arduino> (дата звернення: 10.06.2024)
8. Могильний С.Б. Мікрокомп'ютер Raspberry Pi – інструмент дослідника: посібник.– К.: 2014. –340 с. ISBN 978-617-7133-48-2
9. Don Wilcher. Arduino Electronics Blueprints. - Packt Publishing: 2015. – 252 p. ISBN:9781784392116, 1784392111

10. Характеристики Arduino Uno. [Електронний ресурс] – Режим доступу: <https://forum.arduinka.biz.ua/viewtopic.php?t=7> (дата звернення: 20.05.2024)

11. Wi-Fi модуль WeMos D1 mini на чіпі ESP-12F ESP8266. [Електронний ресурс] – Режим доступу: <https://www.mini-tech.com.ua/ua/wemos-d1-mini> (дата звернення: 28.05.2024)

12. ЛЕКЦІЯ 4. Послідовний інтерфейс передачі даних SPI. [Електронний ресурс] – Режим доступу: https://learn.ztu.edu.ua/pluginfile.php/322028/mod_resource/content/1/Лекція_4_SPI.pdf (дата звернення: 28.05.2024)

13. Arduino IDE. [Електронний ресурс] – Режим доступу: <https://itmaster.biz.ua/electronics/arduino/arduino-ide.html> (дата звернення: 28.05.2024)

14. Цифровий сервопривід із аналогового, або як керувати його параметрами. [Електронний ресурс] – Режим доступу: <https://arduino.ua/art168-cifrovii-servoprivid-iz-analogovogo-abo-yak-keryvati-iogo-parametrami> (дата звернення: 28.05.2024)

15. Eagle – САПР. [Електронний ресурс] – Режим доступу: <http://radio-hobby.org/modules/instruction/eagle> (дата звернення: 08.06.2024)

16. Apache HTTP Server. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Apache_HTTP_Server (дата звернення: 08.06.2024)

17. Blynk Документація. [Електронний ресурс] – Режим доступу: <https://shoorik007.github.io/> (дата звернення: 08.06.2024)