Хмельницький національний університет
Факультет інформаційних технології
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Програмно-технічний засіб керування доступом до дверного замку на базі ESP8266
Назва теми

КвРКІ.2001125.01.17.01 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Комп'ютерна інженерія та програмування»
Назва

Виконав: студент III курсу, група КІ2с–20–1 _____ А.Г. Балан
Підпис Ініціали, прізвище

Керівник _____ О.В. Боровик
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

«5» червня 2023 р.

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"11" 01 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Балан Андрій Григорович

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Програмно-технічний засіб керування доступом до дверного замку на базі ESP8266

Керівник проекту (роботи) Боровик О.В., професор кафедри КПС

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.03.2023 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 07.06.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих засобів керування доступом до дверного замку

Проєктування та апаратна реалізація програмно-технічного засобу керування доступом до дверного замку на базі ESP8266

Програмна реалізація програмно-технічного засобу керування доступом до дверного замку на базі ESP8266

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Креслення сценарію керування доступом до дверного замку у Node-red

Схема електрична принципова

Монтажна схема

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийн
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання « 11 » 01 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2023	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2023	виконано
3	Робота над розділом 1 – Аналіз відомих засобів та рішень	01.03.2023	виконано
4	Робота над розділом 2 – Проєктування апаратної чатини програмно-технічного засобу	01.04.2023	виконано
5	Робота над розділом 3 – Проєктування та реалізація програмної чатини програмно-технічного засобу	30.04.2023	виконано
6	Оформлення пояснювальної записки згідно вимог	20.05.2023	виконано
7	Попередній захист ВКР	25.05.2023	виконано
8	Захист ВКР на засіданні ЕК	Червень 2023 року	

Студент Підпис Балан А.Г. Ініціали, прізвище

Керівник проекту (роботи) Підпис Боровик О.В. Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
1		КвРКІ. 2001125.01.17.01ПЗ	Текстові документи			
			Пояснювальна записка	55		
			Графічні матеріали			
2		КвРКІ. 2001125.01.17.01Е8	Креслення сценарію керування доступом до дверного замку у Node-red	1		
3		КвРКІ. 2001125.01.17.01Е2	Схема електрична принципова	1		
4		КвРКІ. 2001125.01.17.01Е4	Монтажна схема	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ. 2001125.01.17.01 ПЗ		
Розробив		Балан А.Г.		05.06	Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Боровик О.В.				У	1	1
Н. контр.		Лисенко С.М.				ХНУ, КІ2с-20-1		
Затв.		Говорущенко		05.06				

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Програмно-технічний засіб керування доступом до дверного замку на базі ESP8266».

Автор роботи: *Балан Андрій Григорович*

Керівник роботи: *Боровик Олег Васильович.*

Пояснювальна записка: *55 с.*, 37 *рис.*, 1 *табл.*, 3 *дод.*, 60 *джерел.*

Графічна частина: 3 креслення.

ESP8266, КЕРУВАННЯ ДОСТУПОМ ДО ДВЕРНОГО ЗАМКУ, RFID МІТКА.

Мета кваліфікаційної роботи: є розробка програмно-технічного програмно-технічного засобу керування доступом до дверного замку на базі ESP8266.

У сучасному світі програмно-технічний засіб керування доступом до дверних замків на базі ESP8266 є актуальною і важливою темою. Забезпечення безпеки приміщень і обмеження доступу до них є першочерговим завданням для багатьох організацій і приватних осіб. Із зростанням інтелектуальних технологій та Інтернету речей, використання мікроконтролерів, таких як ESP8266, для розробки програмно-технічних засобів керування доступом стає все більш популярним. Це дозволяє створювати розумні системи, що об'єднують безпеку та зручність управління, а також забезпечує можливість віддаленого контролю і моніторингу. Такі системи можуть бути застосовані в різних сферах, включаючи житлові будинки, офіси, громадські споруди, готелі та інші об'єкти, де необхідна ефективна та безпечна система контролю доступу.

Підпис студента

Дата

05.06.2023

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АЦП – Аналого-цифровий перетворювач

ІТ – Інформаційна технологія

КС – Комп’ютерна система

КФС – Кібер-фізична система

ПЗ – Програмне забезпечення

ПТЗ – Програмно-технічний засіб

ЦАП – Цифро-аналоговий перетворювач

MQTT – Message queuing telemetry transport

ВСТУП

У сучасному світі програмно-технічний засіб керування доступом до дверних замків на базі ESP8266 є актуальною і важливою темою. Забезпечення безпеки приміщень і обмеження доступу до них є першочерговим завданням для багатьох організацій і приватних осіб. Із зростанням інтелектуальних технологій та Інтернету речей, використання мікроконтролерів, таких як ESP8266, для розробки програмно-технічних засобів керування доступом стає все більш популярним. Це дозволяє створювати розумні системи, що об’єднують безпеку та зручність управління, а також забезпечує можливість віддаленого контролю і моніторингу. Такі системи можуть бути застосовані в різних сферах, включаючи житлові будинки, офіси, громадські споруди, готелі та інші об'єкти, де необхідна ефективна та безпечна система контролю доступу.

Якщо порівнювати звичайний RFID зчитувач із програмно-технічним засобом керування доступом на базі ESP8266, то останній має ряд переваг, зокрема:

– Простота автентифікації користувачів: Засіб може вимагати введення паролю, коду або використання біометричних даних для перевірки прав доступу користувача. Це забезпечує надійну захист від несанкціонованого доступу.

– Гнучке управління дверима: Засіб може відкривати або закривати двері залежно від доступу користувача. Це дозволяє зручно керувати доступом до приміщень і забезпечує ефективну організацію робочих процесів.

– Журналювання доступу: Система може записувати інформацію про кожен вхід або вихід користувача, створюючи журнал доступу. Це дозволяє відстежувати події, виявляти незвичайну активність та забезпечувати безпеку приміщень.

– Віддалений доступ: Завдяки з'єднанню Wi-Fi, програмно-технічний засіб може забезпечувати віддалений доступ до системи керування. Користувачі можуть керувати доступом через мобільні додатки або веб-інтерфейс, навіть якщо вони знаходяться далеко від приміщення.

– Інтеграція з іншими системами: Програмно-технічний засіб може легко інтегруватися з іншими системами безпеки або автоматизації, такими як системи відеоспостереження, системи контролю доступу до паркування або системи управління освітленням. Це дозволяє створювати комплексні рішення для забезпечення безпеки та зручності в різних середовищах.

Таким чином, програмно-технічний засіб керування доступом на базі ESP8266 надає ряд переваг що проявляється у спрощені процесу автентифікації користувачів, забезпечуючи надійний захист від несанкціонованого доступу. Крім того, засіб забезпечує гнучке управління дверима, дозволяючи відкривати або закривати їх залежно від доступу користувача, що сприяє зручному керуванню доступом до приміщень.

Метою роботи є розробка програмно-технічного програмно-технічного засобу керування доступом до дверного замку на базі ESP8266.

Об’єктом дослідження є процеси керування доступом до дверного замку із використанням мікроконтролера.

Предметом дослідження є програмно-технічний засіб керування доступом до дверного замку на базі ESP8266.

.

1 АНАЛІЗ ВІДОМИХ ЗАСОБІВ ТА РІШЕНЬ КЕРУВАННЯ ДОСТУПОМ ДО ДВЕРНОГО ЗАМКУ

1.1 Системи контролю доступу до дверей

Система контролю доступу до дверей – це просто система, яка дозволяє контролювати, хто може відкривати двері. Це дозволяє підприємствам, державним установам, лікарням тощо не лише керувати доступом до охоронюваних територій, але й створювати ефективну систему керування відвідувачами. Хоча традиційні латунні замки та ключі певною мірою відповідають наведеному вище визначенню, система контролю доступу до дверей – це сучасна електронна система з передовою технологією, яка контролюється системою контролю доступу.

Існує кілька методів класифікації дверних систем контролю доступу. Ці методи покладаються на параметри входу та комбінації компонентів у системі. Розглянемо найдокладніші з них. У випадку із класифікацією за складністю комбінацій вирізняють:

– Система управління дверима: найпростіший тип, призначений для заміни традиційних систем замків і ключів електронним ключем. Перевагою є зниження витрат і усунення проблеми втрати ключа: інформацію про втрачений електронний ключ можна просто видалити із системи.

– Система контролю доступу на основі правил/ролей: наступний рівень в ієрархії, цей тип дозволяє призначати правила та ролі відповідно до того, який доступ буде надано. Правила можуть бути створені на основі посад співробітників або спеціальних вимог, встановлених у компанії.

– Система контролю доступу на основі правил/ролей + безпеки: забезпечує такий самий рівень контролю, як і доступ на основі правил/ролей, а також дає додатковий відгук про безпеку об’єкта. Цей тип відстежує положення дверей і сповіщає вас, якщо двері залишили відкритими або їх відкрили без належного використання облікових даних.

Системи контролю доступу до дверей працюють, дозволяючи вхід за допомогою надійних замків, які відкриваються, коли користувач правильно представляє свій спосіб доступу. На сьогоднішній день існують різні варіанти способів доступу та зняття замка дверей, що включають у себе:

– Ключові картки або брелки: Користувачі отримують ключові картки або брелоки, які містять електронну ідентифікаційну інформацію. Ці картки або брелоки зберігаються близько до замка, і якщо їх ідентифікатор збігається з даними системи, замок розблокується (рис. 1.1). Даний спосіб доступу є одним із найбільш поширених та найбільш простих. Проте головним недоліком цього способу керування доступом є відсутність функції логування даних.

Рисунок 1.1 – Система доступу до дверей на основі картки

– Кодові клавіатури: Замки можуть мати вбудовані кодові клавіатури, на яких користувачі вводять певний код доступу. Якщо введений код збігається з програмованим кодом, замок відкривається (рис. 1.2).

Рисунок 1.2 – Система доступу до дверей на основі клавіатури

– Біометричні системи: Деякі системи контролю доступу використовують біометричні дані для ідентифікації користувачів. Це можуть бути відбитки пальців, розпізнавання обличчя або сканування сітківки ока. Якщо біометричні дані збігаються з даними системи, замок відкривається. Цей спосіб є одним із найбільш інтелектуальних способів у якому можуть використовуватись методи машинного навчання для розпізнавання біометричних даних користувачів. Проте, очевидним недоліком даного методу є підвищена імовірність хибного спрацювання (або не спрацювання взагалі) системи (наприклад в процесі ідентифікації за обличчям).

Рисунок 1.3 – Система доступу до дверей на основі біометричних даних

– Відеодзвінки: В деяких системах контролю доступу до дверей використовуються відеодзвінки (1.4). Користувачі натискають на кнопку дзвінка, а зовнішня камера дозволяє їм бачити, хто стоїть за дверима. Якщо користувач визнає особу та надає дозвіл, замок розблокується.

Рисунок 1.4 – Система доступу до дверей на основі відодзвінків

Таким чином, для систем контролю доступу можна виділити наступні властивості:

– Логування: Системи контролю доступу зазвичай ведуть журнал доступу, в якому фіксуються всі події, пов'язані з входами та виходами користувачів. Це дозволяє вести детальний облік та моніторинг доступу до приміщень.

– Часові обмеження: Системи контролю доступу можуть бути налаштовані на обмеження доступу в певні періоди часу. Наприклад, користувач може мати доступ до приміщення лише певними днями тижня або протягом обмеженого часу.

– Управління правами доступу: Адміністратори системи можуть налаштовувати рівні доступу для різних користувачів або груп користувачів. Це дозволяє обмежити доступ до певних приміщень або зон для певних користувачів, забезпечуючи гнучкість і контроль.

– Сигналізація та сповіщення: У разі спроби несанкціонованого доступу або інциденту система контролю доступу може спрацювати сигналізацію та надіслати сповіщення адміністраторам або відповідним службам безпеки.

– Централізоване управління: Багато систем контролю доступу мають централізовану консоль керування, що дозволяє адміністраторам централізовано керувати налаштуваннями, правами доступу та моніторити стан системи в реальному часі.

– Інтеграція з іншими системами: Системи контролю доступу можуть інтегруватись з іншими системами безпеки, такими як системи відеоспостереження, пожежної сигналізації або системи керування присутністю. Це дозволяє створити комплексну систему безпеки з централізованим керуванням.

1.2 Складові системи контролю доступу до дверей

Існує два основних компоненти систем контролю доступу до дверей: програмне та апаратне забезпечення.

– Програмне забезпечення є ключовим компонентом, який робить сучасні системи контролю доступу безпечними та зручними. Програмне забезпечення дозволяє контролювати, хто має доступ до яких областей, коли; він навіть може встановити час відкриття та закриття дверей. Програмне забезпечення відстежує діяльність у вашому закладі: ви можете бачити, які співробітники отримували доступ до яких зон і як довго. Таким чином, ви можете побачити загальну картину того, як відбувається доступ і чи не зловживають ним.

– Облікові дані – це картки доступу, ідентифікаційні значки та брелоки, які ідентифікують людей і надають їм доступ. З розвитком технологій смартфони та інші розумні пристрої також можна використовувати як облікові дані через технологію Bluetooth. Крім того, якщо потрібно змінити умови

доступу, це можна легко зробити за допомогою програмного забезпечення системи.

– Зчитувачі – це обладнання, яке «зчитує» облікові дані та порівнює їх із базою даних у програмному забезпеченні контролю доступу. Читач – це те, що надає або відмовляє у доступі.

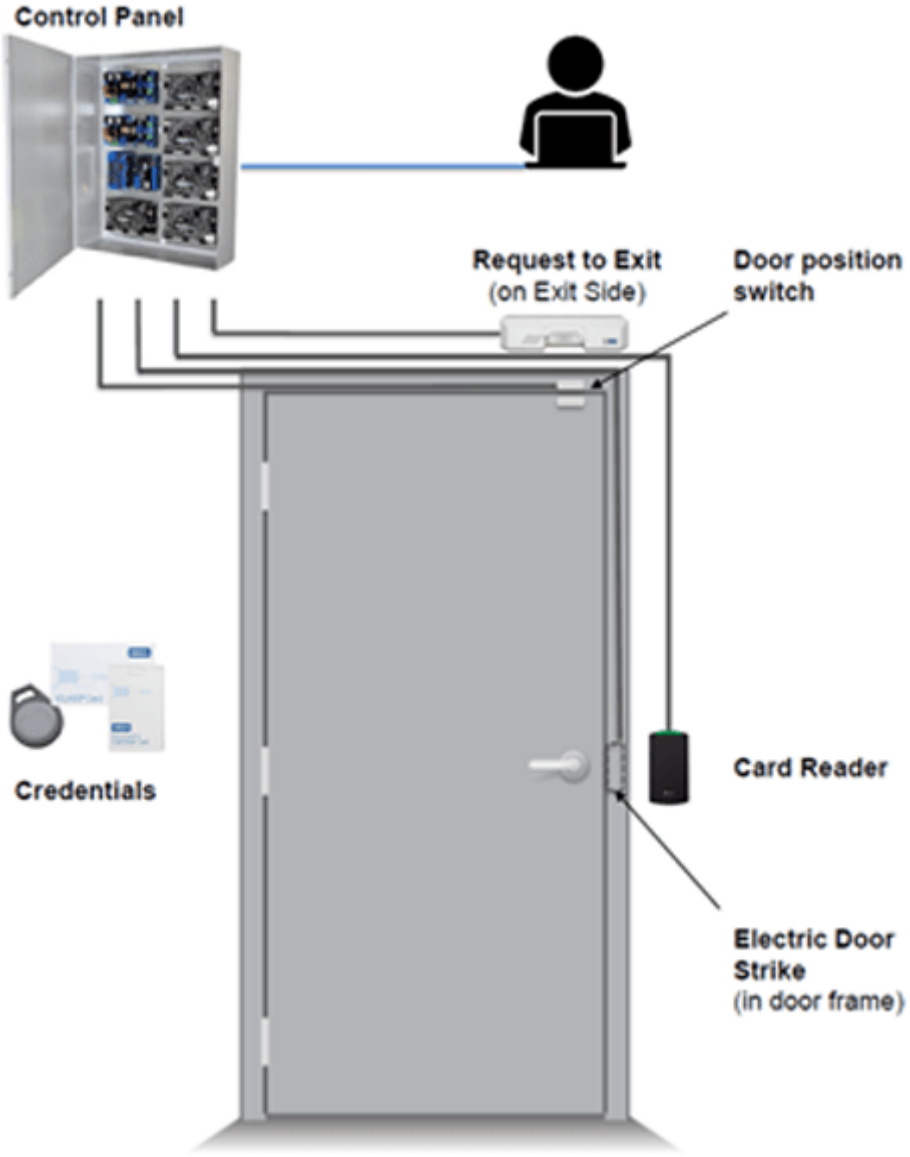


Рисунок 1.5 – Узагальнена структура системи керування доступом до дверей

– Страйки – це електронні механізми, які відкривають двері чи ворота у відповідь на підтвердження авторизованого доступу зчитувачем. Тепер, коли

ми знаємо компоненти систем контролю доступу до дверей, давайте розглянемо, як ці компоненти задіяні в процесі.

– Серевер. Незалежно від того, використовується локальний сервер чи хмарний, сервер зберігає та керує списком схвалених облікових даних, виданих окремим особам. Цей білий список можна оновлювати за потреби, щоб відобразити зміни у політиці безпеки. Сервер також зберігає всі дані про вхід і вихід, що дозволяє отримати інформацію для подальшого використання. Внутрішні сервери, як правило, містять спеціальний термінал, і ними неможливо керувати з іншого місця. Хоча це досить безпечно, його також дорожче встановити та обслуговувати. Як правило, потрібна спеціальна IT-команда, щоб оновити систему та переконатися, що все працює безперебійно. Хмарні системи контролю доступу, такі як Brivo OnAir, пропускають локальний сервер і розміщують білий список доступних токенів.

1.3 Класифікація ідентифікаторів та зчитувачі

У системах контролю доступу можна видділити наступні ідентифікатори:

– Картка перфорована: Цей тип ідентифікатора складається з двошарової пластмасової картки, яка не деформується. Інформація записується на цій картці за допомогою пробивання спеціальних отворів під час її виготовлення. Зчитування інформації здійснюється за допомогою оптичних або механічних зчитувачів. Хоча цей тип ідентифікатора є простим і недорогим, він майже не забезпечує секретності коду і легко підробляється. Картка перфорована має обмежений термін служби, який зазвичай становить 1-2 роки.

– Картка зі штриховим кодом: Ця картка містить смуги іншого кольору на своєму поверхні, що утворюють кодову послідовність за заданою шириною та відстанню між смугами. Кодова послідовність наноситься на картку під час виготовлення (зазвичай за допомогою генератора випадкових чисел) і може бути змінена. Інформацію з цієї картки можна зчитувати за допомогою

оптичних зчитувачів, таких як інфрачервоні або лазерні. Найпоширеніші системи штрихового кодування - код 39 (3 з 9) та код 25 (2 з 5).

– Картка магнітна: Цей тип картки має магнітну смугу, на якій записаний код. Картка магнітна є самоочищувальною і не залишає оксидів на зчитувачі. Крім того, код, записаний на магнітній смузі, може бути легко перезаписаний за бажанням користувача. Якщо картка загублена, можна швидко, дешево і без проблем замінити її на нову картку з тим самим кодом. Для зчитування коду з картки використовується магнітний зчитувач, принцип роботи якого подібний до зчитувача звичайного магнітофону: інформація зчитується під час переміщення картки між магнітними головками зчитувача. Картки з магнітною смугою є відносно недорогими, але не є дуже надійними, оскільки існує ризик підробки. До їхніх недоліків можна також віднести необхідність механічного контакту при зчитуванні з головками зчитувача, що може скоротити термін служби картки (середній термін служби становить близько 1 року), а також потребу в обережному поводженні, оскільки записана інформація може бути спотворена або знищена при впливі слабких магнітних полів та високих температур навколишнього повітря, перевищуючи 80 °С.

– Брелки з електронними ключами “Touch Memory” є зручними і компактними інструментами контролю доступу. У них міститься мікросхема, на яку записуються усі необхідні дані. Для запису, додавання або видалення ключів використовується майстер-ключ з контролера. Інформація зчитується, коли ключ торкається до зчитувача. Як правило, мікросхема живиться вбудованою батареєю, яка забезпечує тривалий термін служби, що може сягати кілька років, але в кінцевому підсумку ключ все ж потребує заміни. Ключі є досить надійними і стійкими до механічних і електромагнітних впливів (порушень). Вони широко використовуються у системах контролю доступу із невеликою кількістю користувачів та великою кількістю дверей (або інших об’єктів доступу), що потребують контролю.

– Картка безконтактна (Proximity) – це картка, яка містить в собі мікросхему (чіп) з записаною інформацією. Інформація з таких карт зчитується

за допомогою радіочастотного методу на відстані від 5 до 90 см (для автомобільних ідентифікаторів цього типу відстань зчитування може досягати 2 м). Картки цього типу поділяються на активні та пасивні. У пасивних картках інформація записується один раз на всю тривалість їх використання, тоді як у активних картках можлива зміна інформації в мікросхемі. Пасивні картки отримують енергію від зчитувача, мають необмежений термін служби і їх не можна підробити. Активні картки мають вбудовані незамінні батареї, і зазвичай їх термін роботи становить до 10 років. Хоча ці картки менш надійні, ніж Віганд-картки, вони зручніші у використанні. Зчитувач може бути прихований за неметалевою стіною. Ця технологія поєднує ефективний контроль зі свободою переміщення. Інформація з картки може бути зчитана навіть тоді, коли вона знаходиться в гаманці або кишені. Недоліком є неможливість використання таких карток у місцях із сильним електромагнітним полем.

1.4 Аналіз відомих програмно-технічних засобів керування доступом до дверного замку

Тема застосування пристроїв керування електронним замком є досить поширеною. Розглянемо детальніше відомі програмно-технічні засоби керування доступом до дверного замку.

У роботі [1] запропоновано систему керування дверним замком на базі мікроокнтролера Atmega 328p (мікроконтролерна плата Arduino). Запропонований програмно-технічний засіб включав у себе використання наступнимх компонентів: LCD дисплею 16x2, 4x4 клавіатури, серво мотору та 5 В джерела живлення. Основною особливістю даного проекту є організація доступу за допогою паролю.

Ще одним проектом для керування доступом до дверного замку є [2]. Автором було запропоновано систему, що складалася із Arduino Nano, сервомотору, Bluetooth модуля, а також джерела живлення. Керування

доступом здійснюється із Android або Windows систем, за дпопомогою Bluetooth Terminal або TeraTerm відповідно.

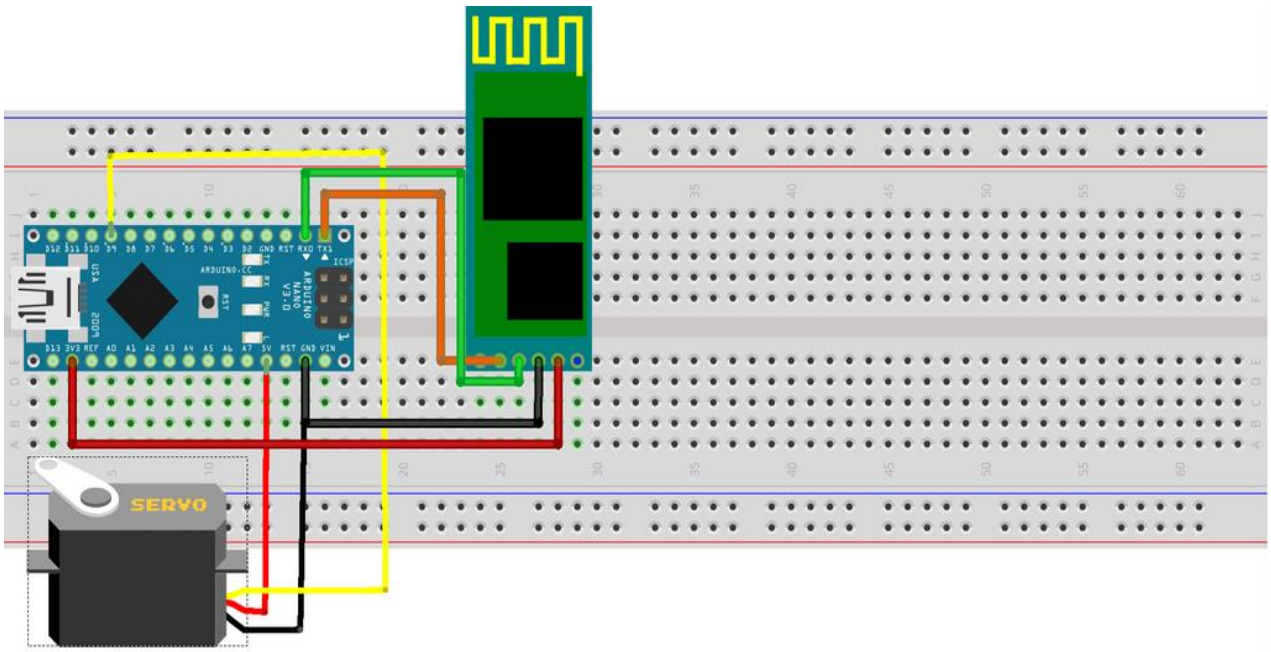


Рисунок 1.6 – Керування доступом за допогою Bluetooth модуля

У роботі [3] запропоновано керування дверним замком за допомогою RFID Master Card із функцією EEPROM на основі мікроконтролерної плати Arduino. Система використовує модуль зчитування RFID RC522 для зчитування карток і брелків RFID та електромагнітний дверний замок для блокування або розблокування дверей. Функціональність пристрою дозволяє додавати або видаляти кілька RFID-карт із системи. Головна картка використовується для виконання адміністративних завдань, таких як додавання або видалення карток. Ця функція забезпечує гнучкість і зручність, оскільки користувачі можуть додавати або видаляти карти за потреби без необхідності перепрограмувати всю систему. Друковану схему запропонованого авторами засобу керування замком наведено на рис. 1.7.

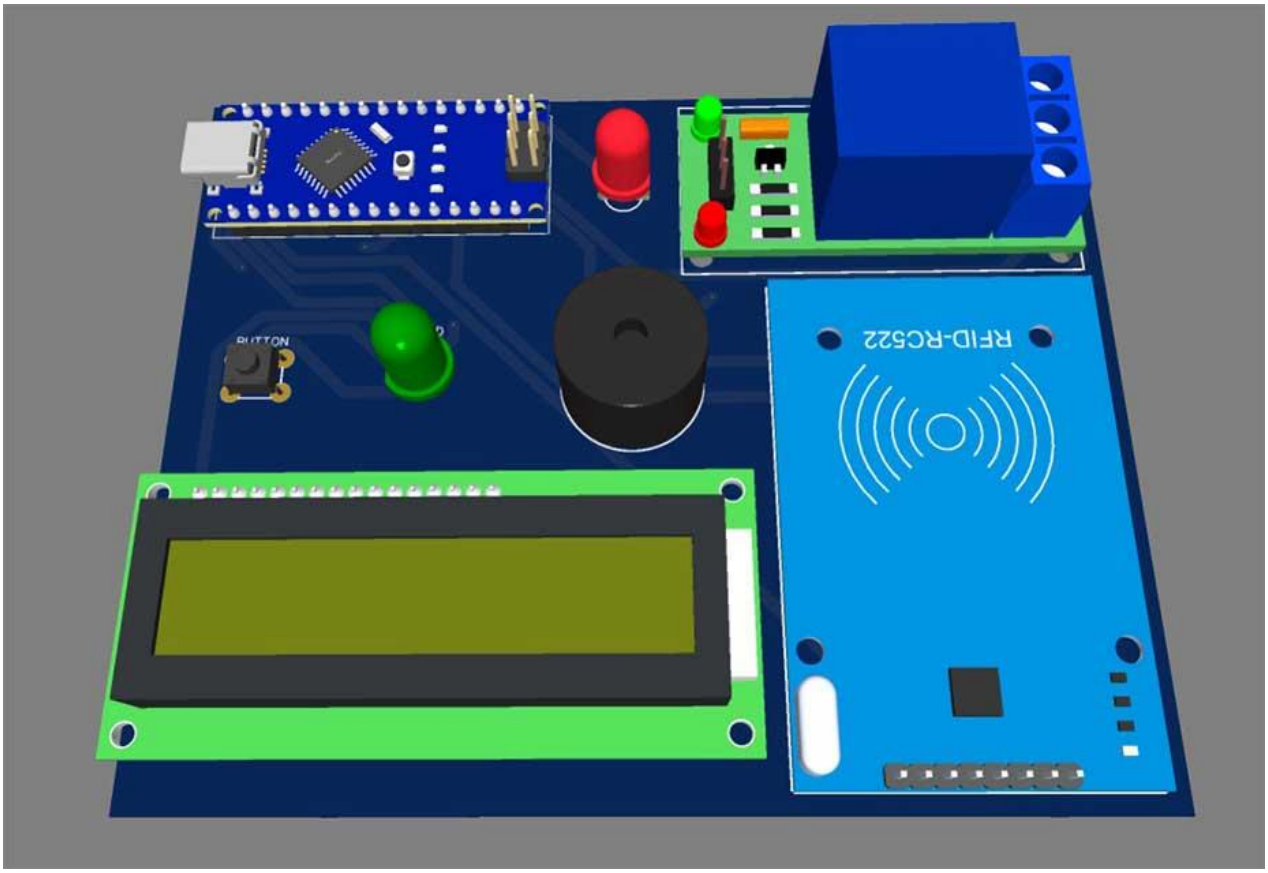


Рисунок 1.7 – Друкована плата пристрою [3]

У роботі [4] запрпоноапно систему автоматичного вдкривання воріт для гаражу. У цьому проекті використовується PIR-датчик для автоматичного відкривання або закривання дверей, який сприймає інфрачервону енергія, яку продукує людське тіло. Коли хтось наближається до дверей, інфрачервона енергія, яку сприймає датчик PIR, змінюється та активує датчик, щоб автоматично відкривати та закривати двері. Далі сигнал надходить на мікроконтролер для управління дверима. Принципова схема запропонованого пристрою автоматичного відкривання та закривання дверей показана на рис. 1.8. Схема побудована з використанням мікроконтролерної плати Arduino UNO, 16×2 LCD, датчиком PIR, з’єднувальними проводами, макетною платою, резистором 1 кОм, джерелом живлення, драйвером двигуна та DVD.

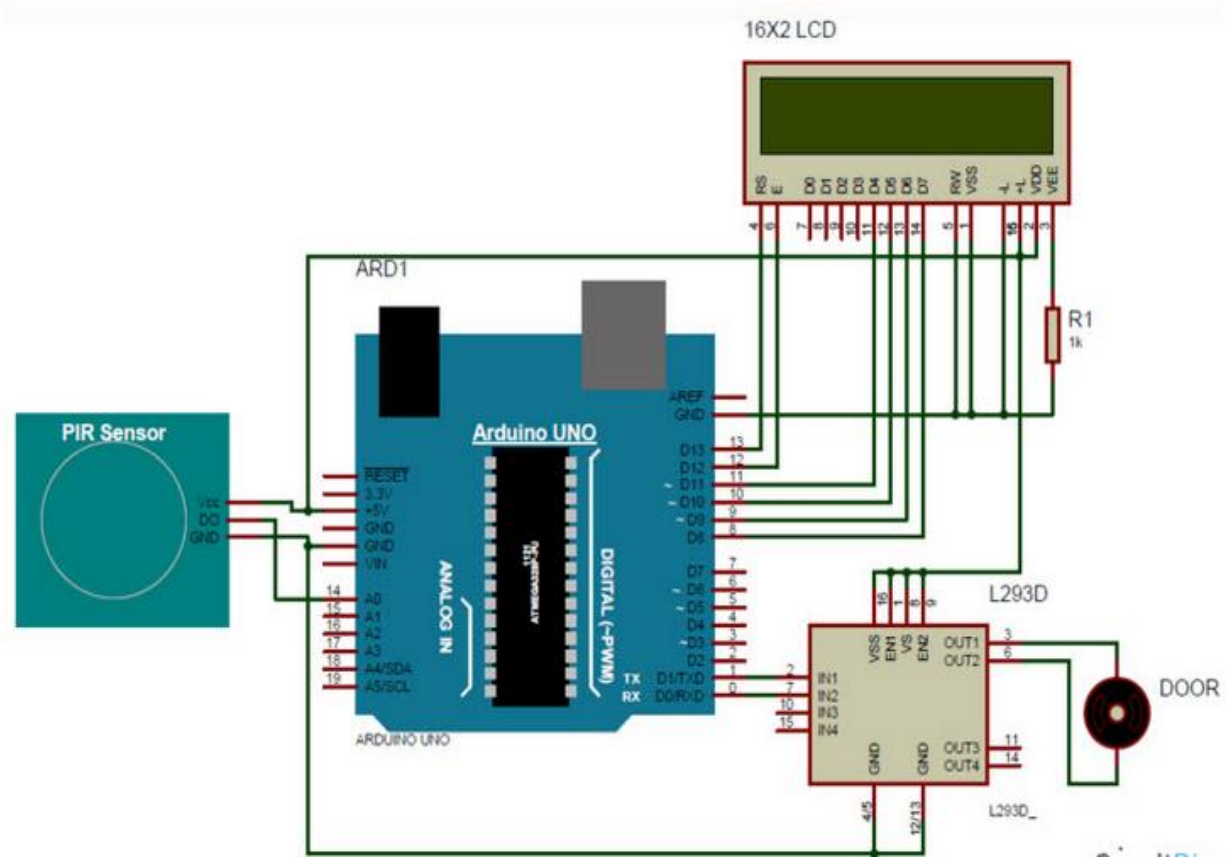


Рисунок 1.8 – Принципова схема пристрою автоматичного відкриття воріт гаражу

Таким чино було проведено огляд відомих програмно-технічних засобів керування доступом до дверного замку. Головним недоліком всіх розглянутих засобів є відсутність збереження інформації про доступ користувачів, тобто інформація про мітку не зберігається у системі, що унеможливлю подальший аналіз даних про спроби доступу до дверного замку.

1.5 Постановка задачі

Процес забезпечення безпеки приміщень і обмеження доступу до них є першочерговим завданням для багатьох організацій і приватних осіб. Із зростанням інтелектуальних технологій та Інтернету речей, використання мікроконтролерів, таких як ESP8266, для розробки програмно-технічних засобів керування доступом стає все більш популярним. Це дозволяє створювати розумні системи, що об’єднують безпеку та зручність управління, а також забезпечує можливість віддаленого контролю і моніторингу. Тому, для розробки програмно-

технічного засобу доступу до дверного замку на базі ESP866 потрібно виконати ряд етапів:

1. Провести аналіз предметної області та механізмів керування доступом до дверних замків та інших об’єктів, провести визначення їх слабких та сильних сторін.

2. Визначити функції та проаналізувати вимоги до проектованого програмно-технічного засобу керування доступом до дверного замкуу на базі ESP8266;

3. Провести аналіз та здійснити вибір складових для проектування програмно-технічного засобу;

4. Зпроєктувати структуру, схему електричну принципову та монтажну схему програмно-технічного засобу керування доступом до дверного замку на базі ESP8266.

5. Реалізувати функції керування доступом до дверного замку.

6. Оцінити вартість програмно-технічного засобу керування доступом до дверного замку на базі ESP8266.

2 ПРОЄКТУВАННЯ ТА АПАРАТНА РЕАЛІЗАЦІЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ ДОСТУПУ ДО ДВЕРНОГО ЗАМКУ НА БАЗІ ESP8266

2.1 Формування вимог до програмно-технічного засобу доступу до дверного замку на базі ESP8266

У процесі проектування будь-якої системи чи пристрою, визначення функціональних вимог є одним з перших етапів, оскільки ці вимоги встановлюють, які конкретні функції повинні бути реалізовані в цій системі. Якісно сформульовані функціональні вимоги мають велике значення, оскільки вони визначають цілі та обмеження проекту, а також слугують основою для подальшого проєктування, розробки та випробування системи. Детально визначені функціональні вимоги також допомагають забезпечити якість системи, оскільки вони дозволяють провести більш точне тестування та валідацію реалізованих функцій. Це дозволяє виявити та виправити можливі проблеми та недоліки ще на ранніх етапах розробки, що забезпечує високу якість кінцевої системи.

Визначимо основні функційні вимоги до проектованого програмно-технічного пристрою доступу до дверного замку на базі ESP8266 наступним чином:

– Доступ до дверного замку по RFID мітці.

– Перевірка зчитаної RFID мітки із списком відомих міток та відхилення доступу, якщо мітка відсутня у списку.

– Сповіщення власника програмно-технічного пристрою про спробу доступу до дверного замка неавторизованого користувача у вигляді СМС повідомлення.

– Виведення інформації про доступ до дверного замку у інформаційну панель у вигляді: мітка часу, RFID мітка, ім’я користувача.

Також, увагу звернемо на нефункційні вимоги, які відображатимуть характеристики засобу, такі як його вартість, зручність використання, масштабованіст, тощо. Таким чином, проєктований програмно-технічний засіб має відповідати наступним вимогам:

– Низька вартість пристрою у порівнянні із відомими аналогами на ринку.

– Можливість, за потреби, масштабування (наприклад, доступ не тікльи до одних дверей, а інших об’єктів будинку – вікна, ворота, тощо).

– Мати можливість працювати в автономному режимі і забезпечувати можливість підключення до зовнішніх джерел живлення.

– Можливість легкого оновлення складових компонентів пристрою.

Таким чином, був встановлений набір вимог, який включає функціональні та нефункціональні вимоги, що дозволяють визначити, якими характеристиками та функціями повинен володіти проектований програмно-технічний засіб доступу до дверного замку на базі ESP8266.

2.2 Будова програмно-технічного засобу доступу до дверного замку на базі ESP8266

Ґрунтуючись на попередньо сформованих функційних та нефункційних вимогах запропоновано узагальнену структуру програмно-технічного засобу керування доступом до дверного замку на базі ESP8266, схему якої наведено на рис. 2.1.

Запропонований програмно-технічний засіб керування доступом до дверного замку на базі ESP8266 складається із наступних компонентів:

– Мікроконтролерна плата ESP8266. Даний модуль використовується як мікроконтролер, який відповідає за керування та координацію роботи всієї системи. Він забезпечує комунікацію з модулем RFID для зчитування ідентифікаційних карток або брелків, а також контролює роботу реле, що керує електричним замком. Також мікроконтролер ESP8266 виконує роль посередника у

завданні збереження та обробки даних, передаючи та приймаючи дані через Wi-Fi мережу.

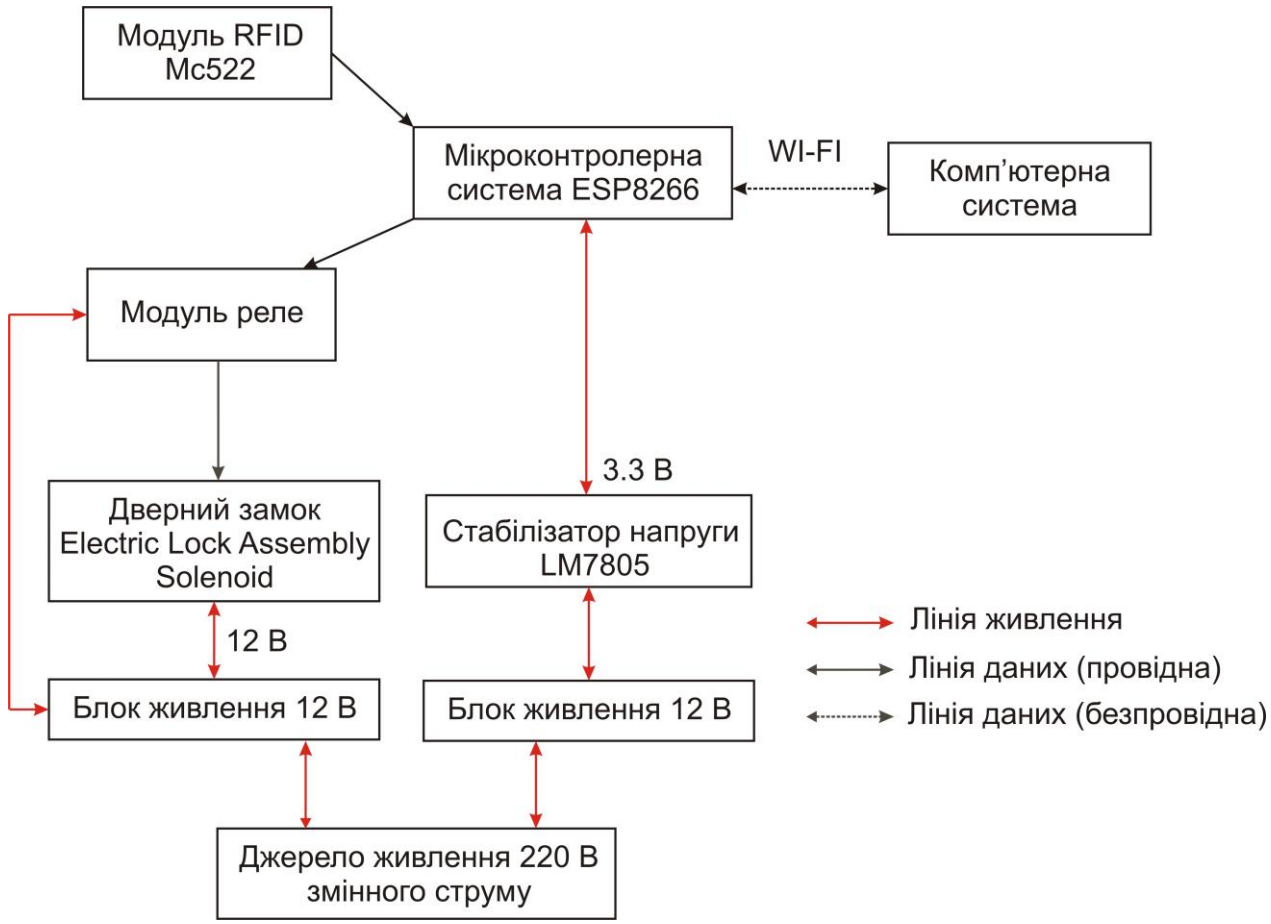


Рисунок 2.1 – Узагальнена структурна схема програмно-технічного засобу доступу до дверного замку на базі ESP8266

– Модуль реле. Модуль реле у даному програмно-технічного засобі виконує завдання керування електричним замком. Реле є електромеханічним пристроєм, який дозволяє переключати електричне з'єднання між двома контактами при наявності зовнішнього сигналу. У контексті системи керування дверним замком, реле використовується для фізичного відкриття або закриття замка. ESP8266, який виступає в ролі мікроконтролера, може надсилати сигнал до модуля реле, щоб активувати його. Коли реле отримує цей сигнал, воно змінює свій стан і відповідно вмикає або вимикає електричний замок, дозволяючи або забороняючи доступ до двері. Таким чином, модуль реле є проміжним елементом

між мікроконтролером ESP8266 та електричним замком, і відповідає за фізичне виконання команд керування замком, що забезпечує контроль доступу до приміщення.

– Електронний дверний замок. Електронний дверний замок виконує завдання фізичного блокування або розблокування дверей у системі керування доступом. Його призначення полягає в контролі фізичного доступу до приміщення, дозволяючи або обмежуючи проходження користувачів.

– Комп'ютерна система. Виступає в ролі сервера, який отримує дані від ESP8266. Передбачає розгортання середовища створення сценарії керування Node red та брокера mosquitto. Після отримання мітки та перевірки її присутності здійснює надсилання сигналу на ESP8266, що у свою чергу активує або деактивує дверний замок. Встановлений брокер керує роботою двох топіків: ESP8266/RFID (комп'ютерна система підписана на даний топік) та ESP8266/status (комп'ютерна система публікує керуючі сигнали).

– Стабілізатор напруги. Завдання стабілізатора напруги LM7805 у цій системі полягає у забезпеченні стабільної постійної напруги для живлення електронних пристроїв, зокрема ESP8266. У цій системі, стабілізатор LM7805 використовується для забезпечення сталої напруги живлення ESP8266 мікроконтролера. ESP8266 працює з напругою живлення 3.3 В, тому стабілізатор перетворює 5 В постійного струму на потрібну напругу для безперебійної роботи мікроконтролера. Це дозволяє забезпечити стабільне живлення ESP8266 незалежно від коливань вхідної напруги, забезпечуючи надійну та стійку роботу пристрою.

2.3 Схема електрична принципова програмно-технічного засобу доступу до дверного замку на базі ESP8266

Електрична принципова схема використовується для графічного зображення та опису зв'язків та взаємодії електронних компонентів в електричному пристрої або системі. Вона надає важливу інформацію про

компоненти, їхні функції, з'єднання та послідовність операцій. Електрична принципова схема дозволяє розуміти, як працює пристрій або система на рівні сигналів і електричних з'єднань. Ця схема включає в себе символи компонентів (наприклад, мікросхеми, резистори, конденсатори, транзистори, тощо), з'єднання між ними та напрямок потоку сигналів. В результаті проєктування було запропоновано схему електричну принципову програмно-технічного засобу доступу до дверного замку на базі ESP8266, яку приведено на рис. 2.2.

У запропонованій схемі контакт 3,3 В модуля RFID MFRC522 підключений до модуля Wifi Nodemcu ESP8266, контакт RST модуля RFID підключений до цифрового контакту 2, контакту GND модуля RFID підключено до контакту заземлення модуля Nodemcu, контакт IRQ не підключено, контакт MISO підключено до цифрового контакту D6, контакт MOSI підключений до цифрового контакту D7, контакт SCK модуля RFID підключений до D5, і, нарешті, контакт SDA модуля RFID MFRC522 з'єднаний з цифровим контактом D4 модуля Wi-Fi Nodemcu ESP8266.

Електронний дверний замок 12 В керується за допомогою одноканального релейного модуля. Відповідно до схеми, контакт GND електронного дверного замка з'єднаний із землею джерела живлення. У той час як контакт 12 В електронного замка з'єднаний із загальним контактом релейного модуля, а нормально відкрита ніжка (NO) релейного модуля з'єднана з джерелом живлення 12 В. Подавши сигнал керування на релейний модуль здійснюється керування (відкриття або закриття) електронним дверним замком. Модуль реле керується за допомогою контакту D0 Wifi-модуля Nodemcu ESP8266.

Також у пристрій додано регульований блок живлення 5 В на основі стабілізатора напруги LM7805, яке використовується для живлення модуля Nodemcu. J1 – це гніздо живлення, до якого підключається джерело живлення 12 В. На вході та виході регулятора напруги підключені два конденсатори ємністю 470 мкФ. Резистор на 330 Ом з'єднаний послідовно зі світлодіодом 2,5 В (використовується як обмежуючий резистор для обмеження струму). Провідник від виходу регулятора напруги під'єднується до контакту Vin модуля Nodemcu, а

провідник від заземлення джерела живлення підключається до контакту заземлення модуля Nodemcu.

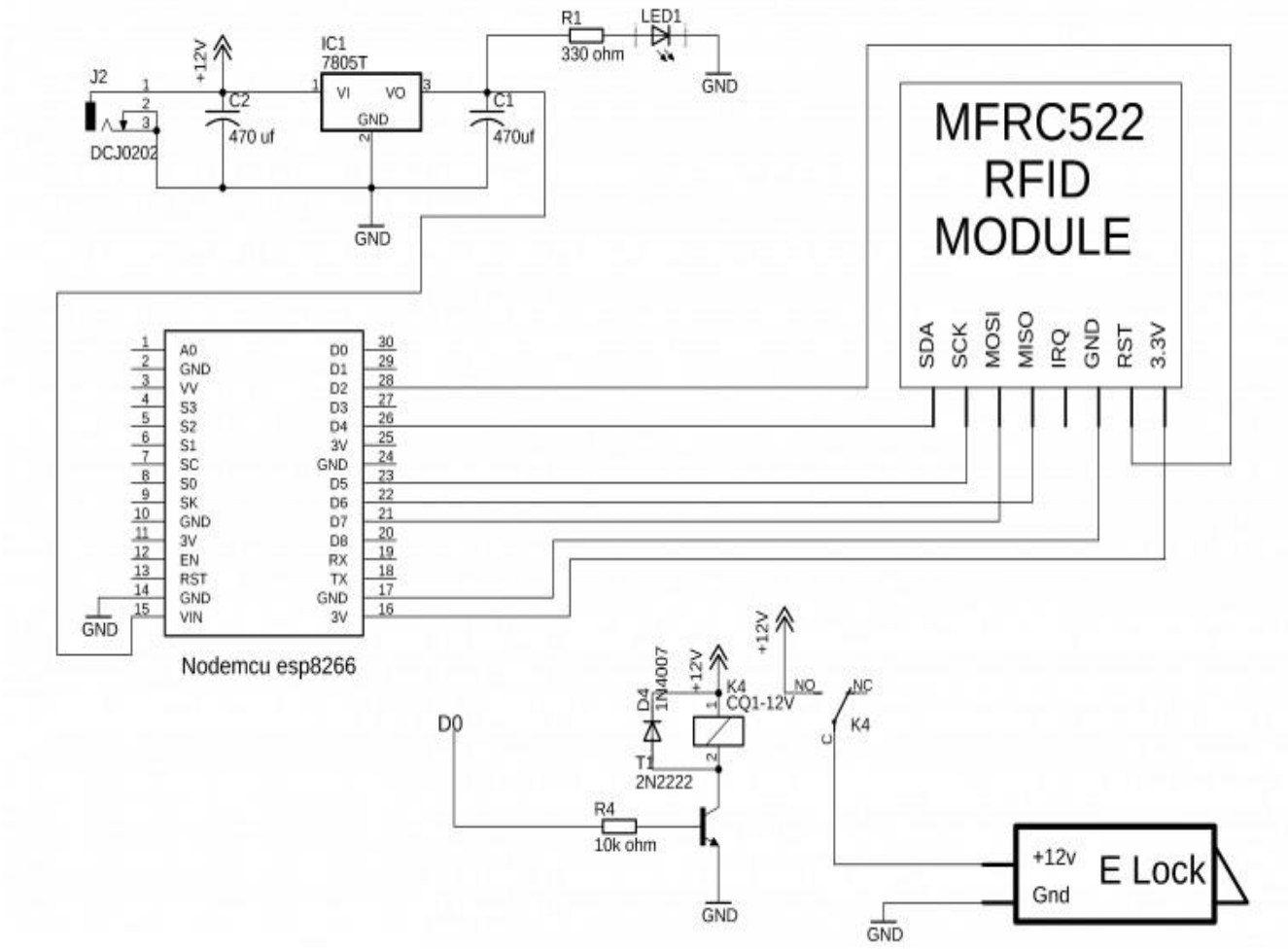


Рисунок 2.2 – Схема електрична принципова програмно-технічного засобу доступу до дверного замку на базі ESP8266

2.4 Монтажна схема програмно-технічного засобу керування доступом до дверного замку

Для розробки монтажної плати використовувалась САПР Fritzing, яка є системою автоматизованого проєктування. Дана САПР надає зручний інтерфейс, який спрощує процес створення монтажних плат та електричних схем. Fritzing має широкий вибір компонентів, включаючи популярні електронні компоненти

(мікросхеми, давачі, модулі, тощо), що дозволяє легко використовувати стандартні компоненти для швидкого створення схем та монтажних плат.

Монтажну схему програмно-технічного засобу керування доступом до дверного замку наведено на рис. 2.3.

Запропонований програмно-технічний засіб складається із таких апаратних компонентів як ESP8266, модуля RFID rc522, електричного дверного замку (живлення 12 В) та модуля реле. Окрім того додатково у схему додано два електролітичні конденсатори 470 пФ. Ці електролітичні конденсатори використовуються разом зі стабілізатором напруги, таким як LM7805, з метою фільтрації і стабілізації напруги. Основна їх функція полягає в тому, щоб згладити коливання напруги на вході стабілізатора і забезпечити стабільний та безшумний вихідний струм. Коли вхідна напруга проходить через стабілізатор, вона може мати деякі шуми, коливання або високочастотні перешкоди. Електролітичні конденсатори допомагають згладити ці коливання та шуми, фільтруючи їх і забезпечуючи стабільну напругу на виході стабілізатора. Також у схему додано світлодіод, який підключено через обмежуючий резистор. Даний світлодіод використовується для індикації живлення пристрою.

Для живлення пристрою у схему додано два гнізда живлення типу female. Одне гніздо, через стабілізатор напруги, живить мікроконтролерну плату ESP8266 та RFID модуль. Через інше гніздо під’єднується живлення електричного замку, яким керує модуль реле.

Констуртивно проектований програмно-технічний пристрій виконано наступним чином: біля електронного замку розташовується RFID модуль. Вгорі дверей у пластиковому корпусі розташовується плата керування, що складається із ESP8266, релейного модуля та стабілізатора напруги. У корпусі є отвори під живлення від 12 В блока живлення та інформаційні провідники. Конструктивний вигляд проектованого програмно-технічного засобу керування доступом до дверного замку на базі ESP8266 зображено на рис. 3.4.

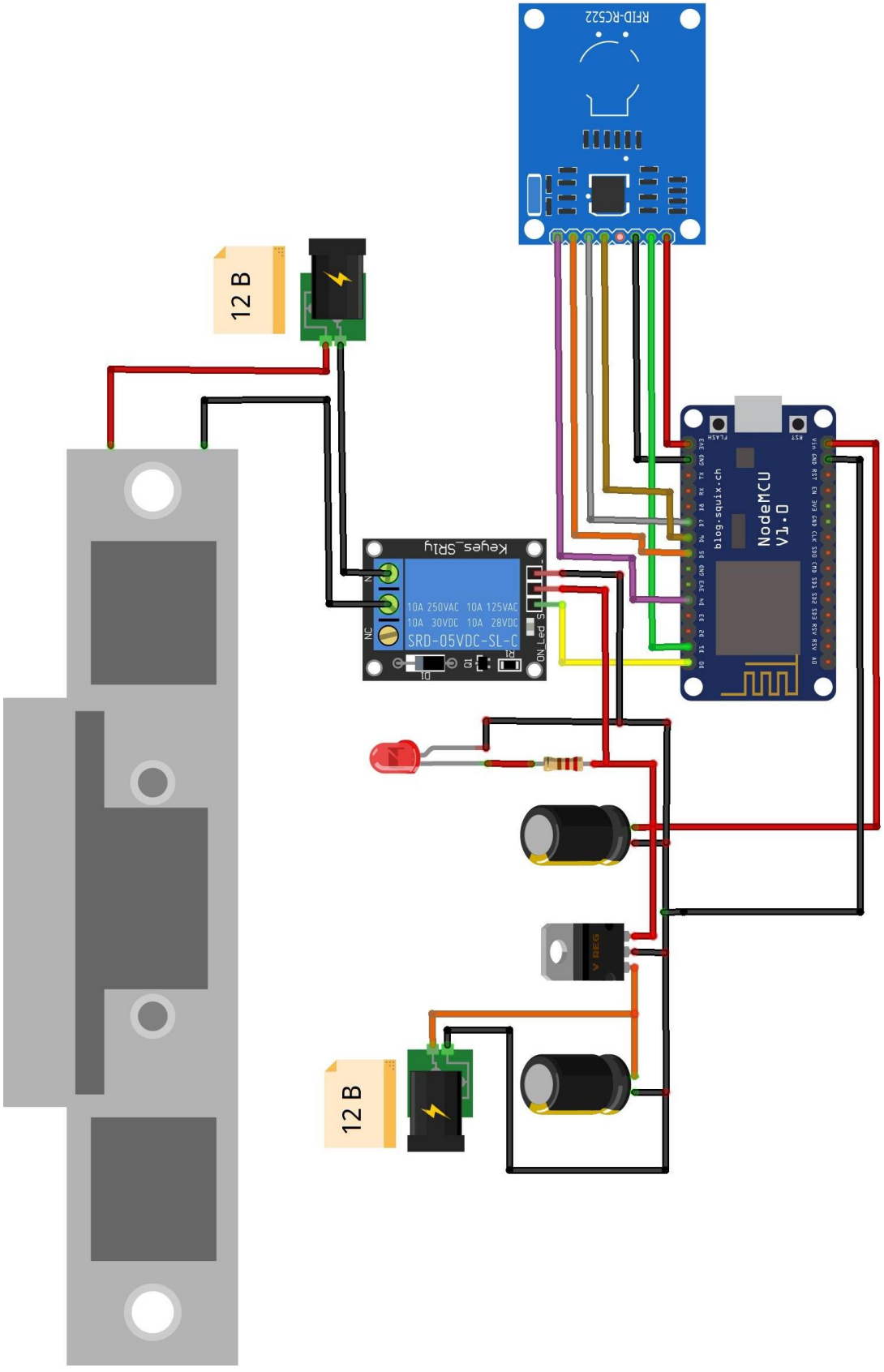


Рисунок 2.3 – Монтажна схема програмно-технічного засобу керування доступом до дверного замку на базі ESP8266

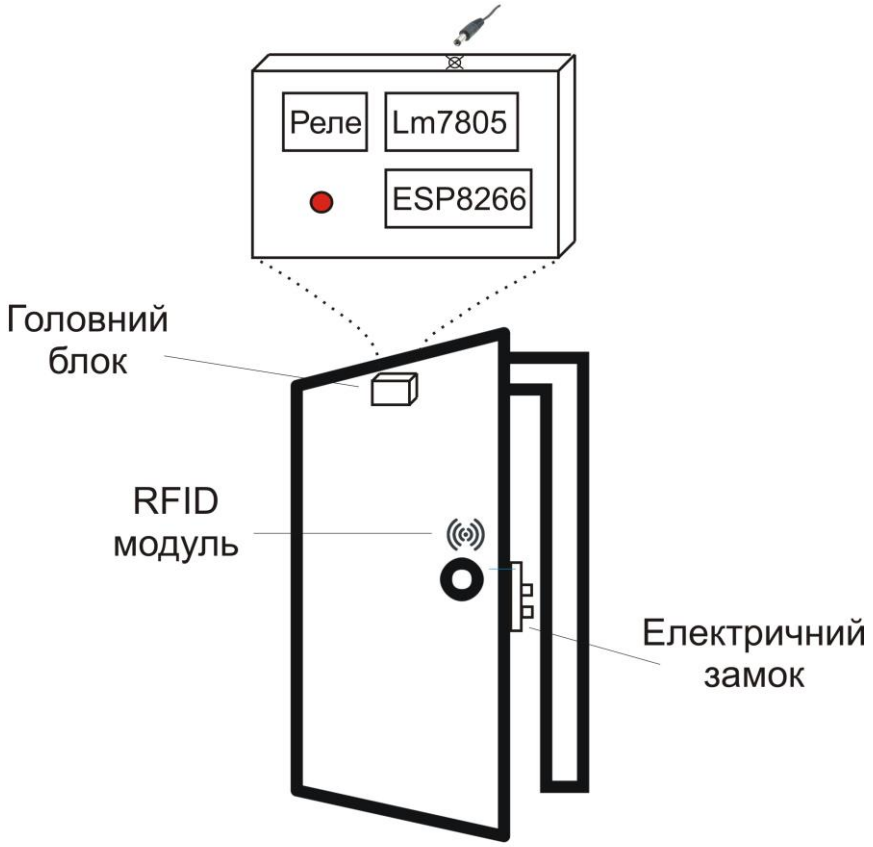


Рисунок 2.4 – Конструктивний вигляд проектованого програмно-технічного засобу керування доступом до дверного замку на базі ESP8266

2.5 Огляд обраних рішень

Ґрунтуючись на запропонованій раніше структуру програмно-технічного засобу керування доступом до дверного замку на базі ESP8266 розглянемо детальніше необхідні апаратні та програмні компоненти.

2.5.1 Огляд обраних апаратних рішень

Запропонований програмно-технічний засбі керування доступом до дверного замку на базі ESP8266 складається із таких апаратних компонентів як мікроконтролерна система ESP8266, модуля зчитування RFID міток rc522, одноканального модуля реле srd-05vdc-sl-c та стабілізатора напруги LM7805.

ESP8266 – це мініатюрний Wi-Fi модуль, що базується на мікроконтролері ESP8266EX (рис. 2.5). Він став популярним серед розробників завдяки своїй високій продуктивності, низькій вартості та широким можливостям для підключення до Інтернету. ESP8266 підтримує протоколи Wi-Fi, TCP/IP, і може виконувати роль клієнта або точки доступу. Цей модуль має вбудовану пам'ять для зберігання програмного коду та данних, що дозволяє розробникам виконувати програми без необхідності використання зовнішнього мікроконтролера. ESP8266 має вбудований 32-бітний мікропроцесор з тактовою частотою до 160 МГц, а також GPIO (виводи загального призначення), які дозволяють підключати різноманітні сенсори, актуатори та інші зовнішні пристрої. Цей модуль підтримує роботу з різними платформами розробки, такими як Arduino, і має велику спільноту розробників, що активно ділиться знаннями та проектами, що робить його привабливим для реалізації різних інноваційних проектів, таких як системи IoT, домашні автоматизації, датчики та багато іншого.

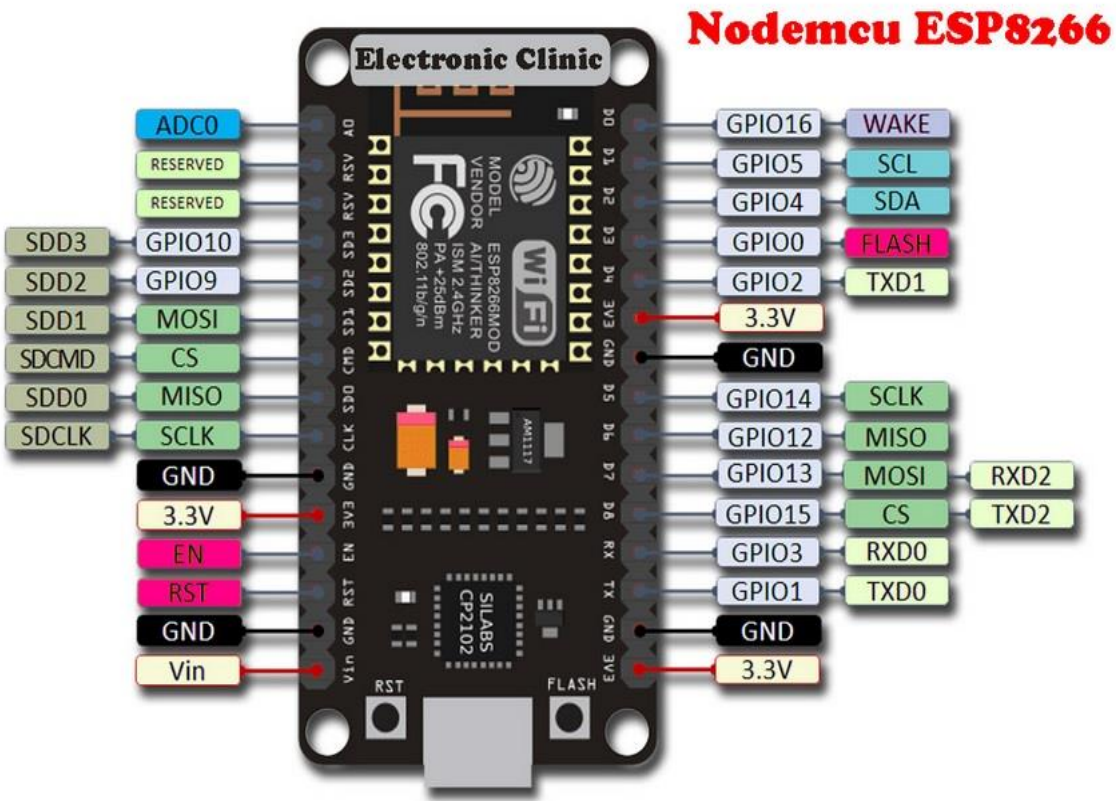


Рисунок 2.5 – Призначення контактів ESP8266

Також можна виділити наступні характеристики мікроконтролерної плати ESP8266:

– Мікропроцесор: Вбудований 32-бітний процесор Tensilica Xtensa LX106 з тактовою частотою до 160 МГц.

– Wi-Fi: Підтримка бездротового зв'язку стандарту Wi-Fi 802.11 b/g/n з можливістю підключення до мережі як клієнт або точка доступу.

– Пам'ять: Вбудована флеш-пам'ять для зберігання програмного коду та данних. Варіанти з різним обсягом пам'яті доступні (наприклад, 512 Кб або 4 Мб).

– Ввід/вивід: GPIO (виводи загального призначення) для підключення зовнішніх пристроїв, таких як сенсори, актуатори, дисплеї та інші периферійні пристрої.

– Аналоговий ввід: Має один аналоговий вхідний пін для зчитування аналогових сигналів.

– Інтерфейси: Підтримка UART, SPI, I2C та інших інтерфейсів для комунікації з іншими пристроями.

– Живлення: Робоче напруга від 3.3 В, але потребує стабілізованого живлення. Також можлива робота в полегшеному режимі для забезпечення енергозбереження.

– Підтримка платформ розробки: ESP8266 може бути програмований з використанням різних платформ розробки, таких як Arduino IDE, MicroPython, NodeMCU і багато інших.

– Вбудовані функції безпеки: Підтримка шифрування WPA/WPA2 для безпечного підключення до Wi-Fi мережі.

Для безконтактного зчитування RFID міток використовувався модуль RC522 (рис. 2.1). Цей модуль заснований на інтегральній схемі MFRC522 від компанії NXP і працює на частоті 13,56 МГц. Він використовує радіочастотні електромагнітні хвилі для передачі даних, зчитування та запису. Модуль може працювати з різними типами RFID транспондерів, такими як картки і брелки, які мають пам'ять 1 КБ і сумісні з частотою 13,56 МГц. Він є невеликим за розміром і працює з низькою напругою, а також постачається з інтерфейсом SPI, що

дозволяє легко інтегрувати його з різними мікроконтролерами, такими як ATTiny, Arduino, ESP8266, Raspberry Pi та іншими. Зазвичай модуль RC522 доступний на ринку або в Інтернеті як комплект, який включає в себе модуль зчитування RC522, RFID-картку, брелок та необхідні роз'єми для підключення.

Модуль або трансивер RFID-зчитувача RC522 – це пристрій зчитування/запису, здатний зчитувати/записувати дані з/на транспондер RFID. Він складається з 3 ключових компонентів, це мікросхема MFRC522, кварцевий генератор 27,12 МГц, а також антена.

RC522 побудований на мікросхемі MFRC522. Ця мікросхема характеризується низьким енергоспоживанням, низькою вартістю, а також малим розміром. MFRC522 IC підтримує різні типи тегів RFID, зокрема MIFARE 1K, MIFARE 4K, MIFARE Mini та інші картки та теги на основі стандартного протоколу ISO/IEC14443. Окрім того, він підтримує більш швидкісний безконтактний зв’язок серії Mifare, швидкість дуплексного зв’язку до 424 кбіт/с. MFRC522 IC працює на частоті 13,46 МГц з робочим діапазоном до 50 мм залежно від розміру антени та налаштування. Мікросхема MFRC522 підтримує послідовний зв’язок SPI, UART і I2C із хостом (наприклад мікроконтролер, як Arduino).

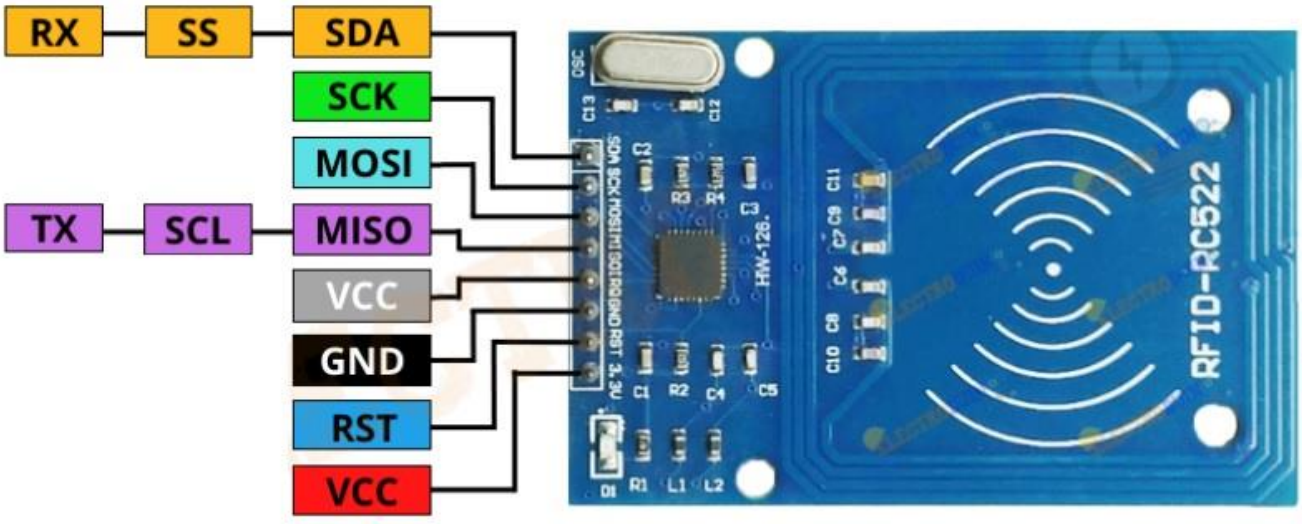


Рисунок 2.6 – Призначення контактів RFID модуля rc522

Модуль rc522 має вісім контактів:

VCC: Контакт джерела живлення для модуля. Модуль працює в діапазоні напруг від 2,5 до 3,3 вольт. Є можливість підключити його до вихідного контакту 3,3 В мікроконтролера (наприклад Arduino або ESP8266).

RST: контакт скидання є входом для скидання та вимкнення модуля. Коли на цей вивід подати низький сигнал, здійснюється відключення живлення, що тим самим призводить до вимкнення всіх внутрішніх споживачів струму, включаючи генератор, і вхідні контакти модуля від'єднуються від зовнішньої периферії.

GND: контакт заземлення модуля. Даний контакт потрібно підключити його до контакту заземлення мікроконтролера.

IRQ: це контакт переривання, який сповіщає мікроконтролер про пробудження модуля, коли мітка RFID потрапляє в його діапазон. Це допомагає модулю переходити в сплячий режим для забезпечення економії енергії.

MISO / SCL / Tx: коли ввімкнено інтерфейс SPI, цей вивід діє як Master-In-Slave-Out, коли ввімкнено інтерфейс I2C, вивід діє як послідовний годинник, а коли ввімкнено інтерфейс UART, виступає як послідовний вихід даних.

MOSI: це контакт Master Out Slave In для зв'язку SPI

SCK: Це штифт послідовного годинника. Він приймає тактові імпульси, що надаються майстром шини SPI, тобто мікроконтролером.

SS / SDA / RX: цей контакт діє як послідовний вхід (SS) під час зв'язку SPI, SDA під час I2C і Rx під час UART.

Для керування електронним дверним замком задіяно релейний модуль. У даному пристрої було обрано релейний модуль SRD-05VDC-SL-C.

Модуль реле SRD-05VDC-SL-C має три контакти для під'єднання високої напруги (NC, C і NO), які підключаються до пристрою, яким потрібно керувати. Інша сторона має три контакти низької напруги (земля, Vcc і сигнал), які підключаються до мікроконтролера.

Всередині реле знаходиться перемикач на 120-240 В, який підключений до електромагніту. Коли реле отримує сигнал HIGH на сигнальному штифті,

електромагніт стає зарядженим і переміщує контакти перемикача у відкрите або закрите положення.

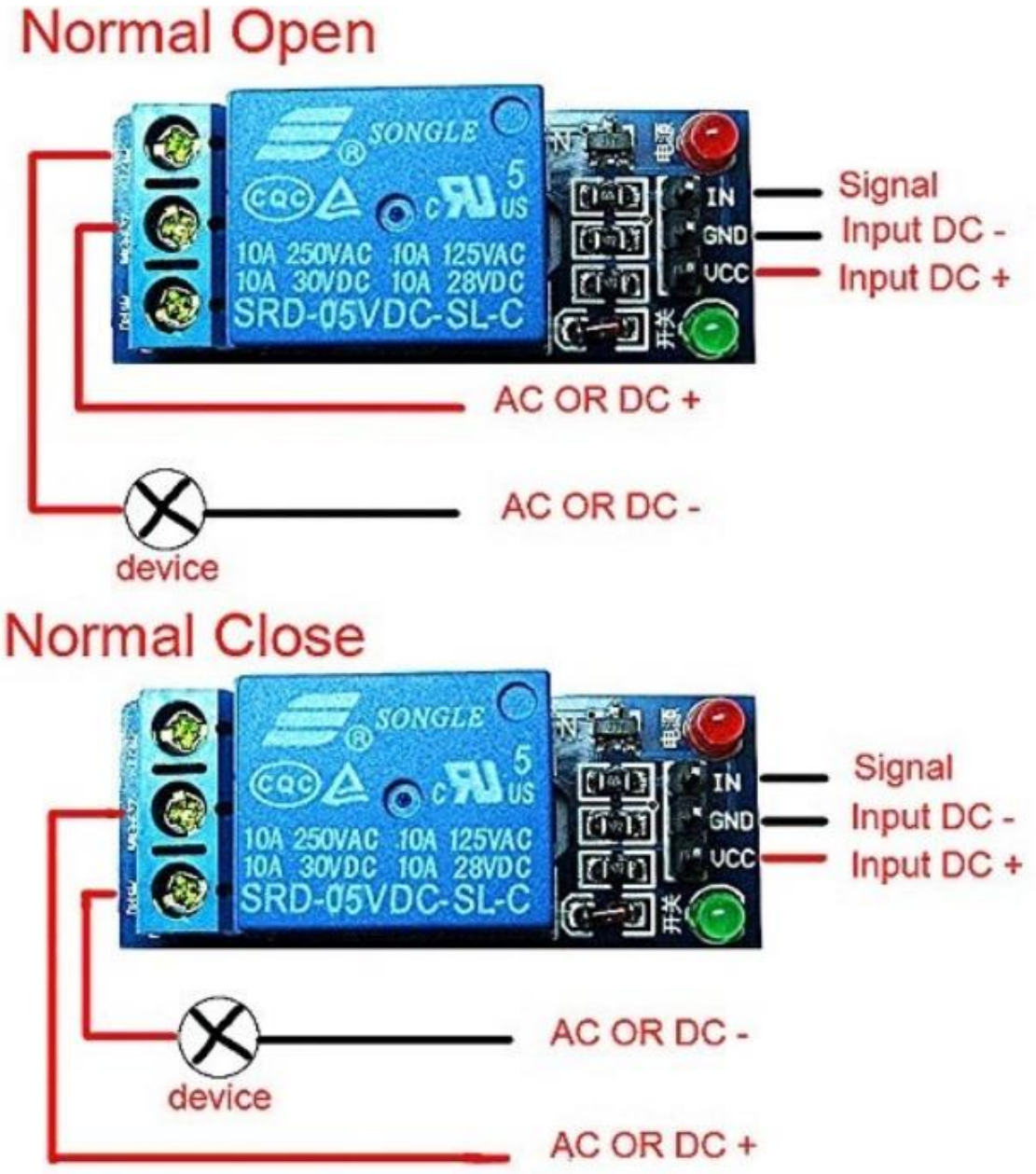


Рисунок 2.7 – Релейний модуль SRD-05VDC-SL-C та підключення контактів до NO та NC відповідно

Реле має всередині два різних типи електричних контактів – нормально розімкнені (НО) і нормально замкнуті (НЗ). Контакт, який використовуватиметься, залежатиме від того, чи потрібно, щоб сигнал 5 В увімкнув чи вимкнув перемикач. Струм живлення 120-240 В надходить на реле на

загальній клемі (C) в обох конфігураціях. Щоб використовувати нормально розімкнуті контакти, слід використовувати клему NO. Щоб використовувати нормально замкнуті контакти, використовуйте клему NC.

У нормально розімкненій конфігурації, коли реле отримує сигнал HIGH, перемикач 120-240 В замикається і дозволяє струму протікати від клеми C до клеми NO. Сигнал LOW вимикає реле та припиняє струм. Отже, якщо потрібно, щоб сигнал HIGH вмикав реле, слід використовувати нормально розімкнену клему.

У нормально закритій конфігурації сигнал HIGH розмикає вимикач і перериває струм 120-240 В. Сигнал LOW замикає перемикач і дозволяє струму протікати від клеми C до клеми NC. Тому, потрібно, щоб сигнал HIGH вимкнув струм 120-240 В, слід використовувати нормально закриту клему.

В якості електричного замку було обрано 12V Iron Door Drawer Tongue Down Electric Lock Assembly Solenoid Slim Rustproof (рис. 2.2). Головна особливість цього замка полягає у забезпеченні безпеки та контролю доступу. Він може використовуватись для різних застосувань, таких як сейфи, шафи, шухляди, автоматичні двері та інші пристрої, де необхідно забезпечити замикання та розмикання.

Характеристиками 12V Iron Door Drawer Tongue Down Electric Lock є:

– Напруга живлення: 12 Вольт.

– Тип замка: Електричний соленоїдний замок.

– Корпус: Виготовлений з міцної сталі з високою стійкістю до корозії (rustproof).

– Компактний розмір: Дозволяє зручне встановлення та інтеграцію в різноманітні пристрої.

– Надійність: Висока міцність і довговічність.

– Енергоефективність: Використовує невелику кількість електроенергії для роботи.

– Легке керування: Замок може бути відкритий або закритий за допомогою подачі або припинення подачі живлення.

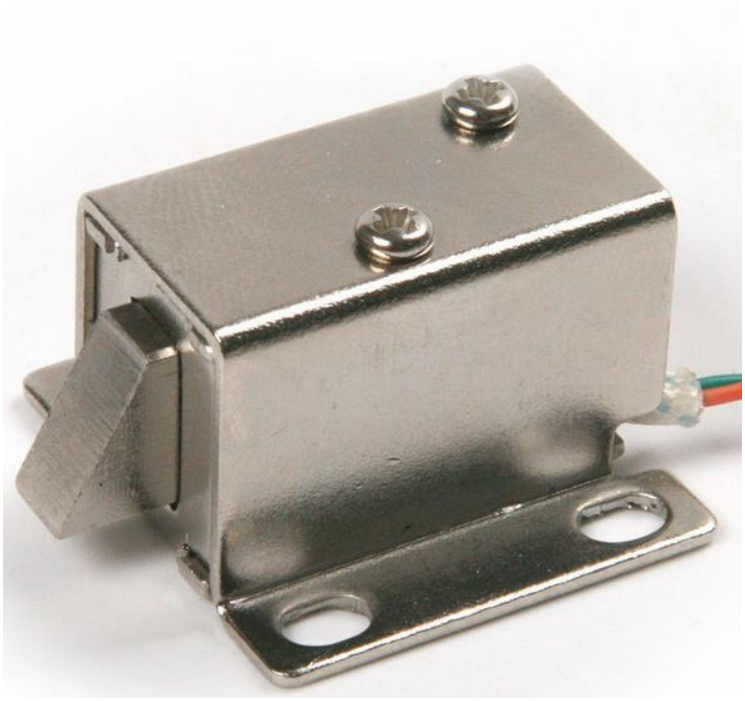


Рисунок 2.8 – Електричний замок 12V Iron Door Drawer Tongue Down Electric Lock Assembly Solenoid Slim Rustproof

Для живлення мікроконтролерної плати ESP8266 використано стабілізатор напруги LM7805 (рис. 2.9). LM7805 – це триконтактний лінійний стабілізатор напруги, який працює зі змінним струмом. Це звичайний компонент у схемах, які потребують позитивних стабілізаторів напруги.

Регулятор 7805 випускається в різних версіях. Версія TO-92 виготовлена з пластику, тому краще працює з ланцюгами малої потужності. Версія T-O3 поставляється в суцільнометалевому корпусі для полегшення тепловідведення. Для даного програмно-технічного засобу використано LM7805 в корпусі TO-92.

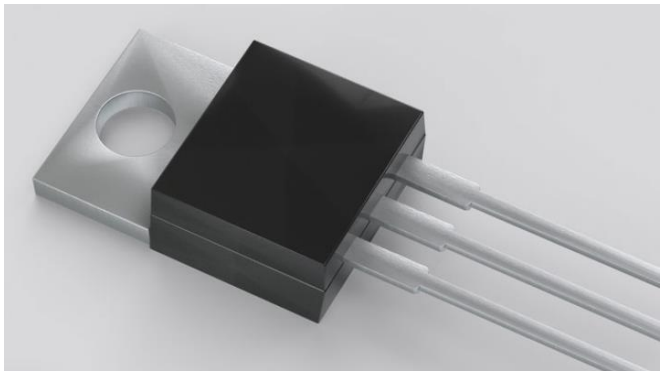


Рисунок 2.9 – Стабілізатор напруги LM7805

Основними властивостями Стабілізатор напруги LM7805 є:

– Вхідна напруга: від 7В до 25В

– Вихідна напруга: 5В

– Максимальний вихідний струм: 1,5А

Таким чином проведено огляд апаратних компонентів, що використовуються у програмно-технічногому засобі керування дверним замком на базі мікроконтролерної плати ESP8266

2.5.2 Аналіз обраних програмних рішень

З метою створення сценаріїв керування дверним замком у проектованому програмно-технічному пристрої задіяно комп’ютерну систему на якій розгорнуто Node red. Node-RED – це візуальний інструмент для програмування відкритого вихідного коду, який дозволяє візуально створювати потокові програми (flows). Він призначений для розробки та виконання потокових додатків Інтернету речей (IoT), веб-серверів, автоматизації робочих процесів, обробки даних та інтеграції систем.

Основне призначення Node-RED полягає у спрощенні розробки складних програмних логік із використанням графічного інтерфейсу. Замість традиційного написання коду, ви можете створювати вузли (nodes) та з'єднувати їх для визначення логіки програми. Кожен вузол виконує певну функцію або операцію і обмінюється даними з іншими вузлами у потоці даних.

Основними ключовими властивостями Node-RED є:

– Візуальний інтерфейс: Node-RED надає інтуїтивно зрозумілий графічний інтерфейс, де ви можете створювати, змінювати та керувати потоковими програмами без потреби писати код.

– Велика бібліотека вузлів: Node-RED має широкий вибір вбудованих вузлів, які представляють різноманітні функції і сервіси, такі як зчитування даних з датчиків, керування пристроями IoT, робота з базами даних, веб-службами

тощо. Крім того, спільнота Node-RED активно розробляє сторонні вузли, що розширюють функціональність платформи.

– Легка інтеграція: Node-RED забезпечує простий спосіб інтеграції з різними пристроями, системами та сервісами. Ви можете легко взаємодіяти зі смарт-пристроями, хмарними платформами, базами даних, веб-службами та багатьма іншими системами. Node-RED має набір вузлів, які дозволяють вам з'єднуватися з популярними сервісами, такими як Twitter, Facebook, Slack, Google Cloud та іншими. Це робить його ідеальним інструментом для створення розширених додатків, які взаємодіють з різними платформами та сервісами.

– Розширюваність: Node-RED дає можливість створювати власні вузли, які відповідають вашим потребам. Ви можете створювати вузли на основі ваших власних функцій, бібліотек або сервісів, що дозволяє розширити функціональність платформи та адаптувати її до конкретних вимог проекту.

– Підтримка візуалізації: Node-RED має вбудовану підтримку візуалізації даних. Ви можете створювати графіки, діаграми, інтерактивні інтерфейси та інші візуальні елементи для відображення та моніторингу даних, що проходять через ваші потокові програми.

– Підтримка розподіленої архітектури: Node-RED може бути використаний у розподіленому середовищі, де кожен вузол виконується на окремому пристрої або сервері. Це дозволяє створювати складні системи, які включають багато вузлів, що співпрацюють між собою.

2.6 Налаштування програмних компонентів

Для подальшої реалізації функції програмно-технічного засобу керування дверним замком слід виконати налаштування таких програмних компонентів як середовище розробки Arduino IDE та брокер mosquitto.

Для налаштування Arduino IDE слід виконати наступні кроки:

– Встановити Arduino IDE: Завантажити та встановити останню версію Arduino IDE з офіційного веб-сайту Arduino (https://www.arduino.cc/en/software).

– Встановити ESP8266 додатковий пакет: Відкрити Arduino IDE та перейти у головному меню до "File" (Файл) -> "Preferences" (Параметри). У полі "Additional Boards Manager URLs" (Додаткові URL-адреси менеджера плат) вставте наступну URL-адресу: http://arduino.esp8266.com/stable/package_esp8266com_index.json (рис. 2.10, 2.11).

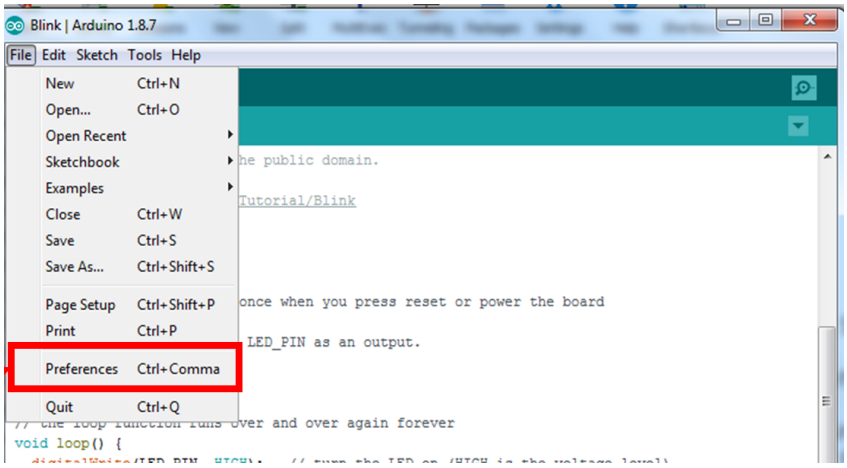


Рисунок 2.10 – Встановлення додаткового пакету для ESP8266

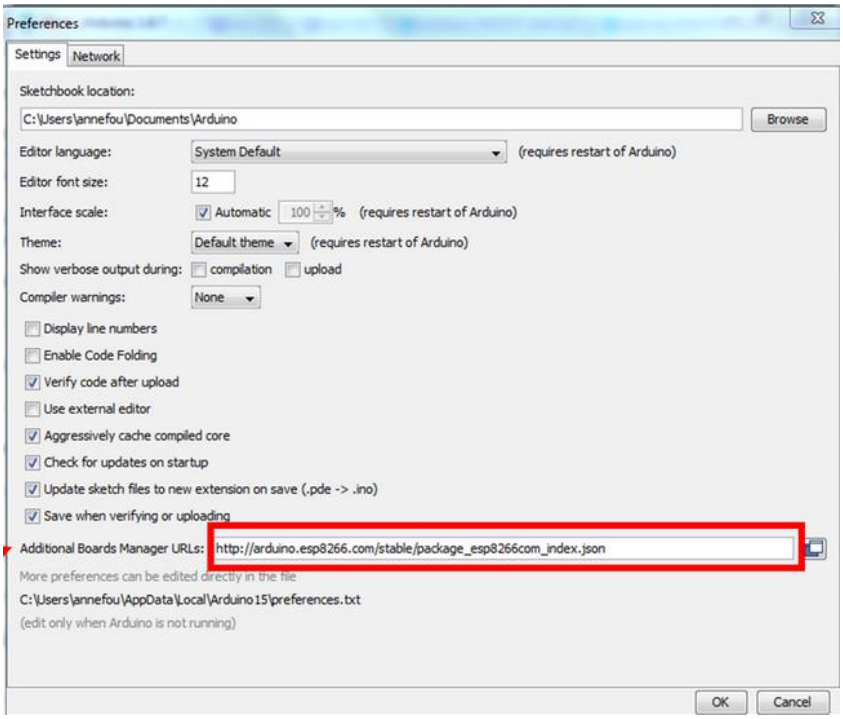


Рисунок 2.11 – Встановлення додаткового пакету для ESP8266

– Встановити ESP8266 пакет: Слід перейти до "Tools" (Інструменти) -> "Board" (Плата) -> "Boards Manager" (Менеджер плат). У пошуковому полі ввести

"esp8266" і виберіть "esp8266 by ESP8266 Community". Далі натиснемо "Install" (Встановити), щоб встановити пакет (рис. 2.12).

Рисунок 2.12– Вибір плати ESP8266

– Виберіть ESP8266 плату: Після встановлення пакету ESP8266 перейдіть до "Tools" (Інструменти) -> "Board" (Плата) та виберіть вашу ESP8266 плату зі списку доступних плат. Наприклад, "NodeMCU 1.0 (ESP-12E Module)".

– Вибрати правильний порт: Для цього слід підключити ESP8266 до комп’ютера за допомогою USB-кабелю. Далі перейти до "Tools" (Інструменти) -> "Port" (Порт) та вибрати правильний порт COM або /dev/ttyUSB для ESP8266 (рис. 2.13).

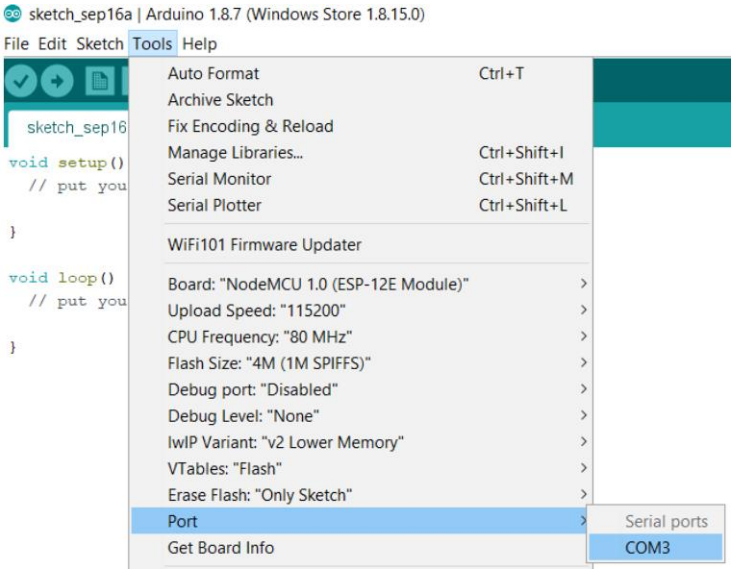


Рисунок 2.13 – Вибір порту

Далі виконаємо встановлення брокера mosquitto, що надасть змогу здійснити комунікацію між комп’ютерною системою та ESP8266.

З цією метою у терміналі введемо наступні команди:

sudo apt update.

sudo apt install -y mosquitto mosquitto-clients

Далі активуємо функцію автоматичного запуску mosquitto при завантаженні системи:

sudo systemctl enabled mosquitto.service

Наступним кроком виконаємо запуск брокера шляхом введення наступної команди:

mosquitto

Успішне встановлення та роботу брокера можна таож перевірити за допомогою двох клієнтів командного рядку для підписки та публікації повідомлень – mosquitto_sub та mosquitto_pub відповідно.

2.7 Висновки до розділу 2

Таким чином визначено перелік вимог та запропоновано узагальнену стуркутру програмно-технічного засобу доступу до дверного замку на базі ESP8266. Здійснено вибір апаратних та програмних компонентів, а також запропоновано схеми електричну принципову та монтажну. Запропоновано конструктивний вигляд проектованого програмно-технічного засобу керування доступом до дверного замку на базі ESP8266

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ КЕРУВАННЯ ДОСТУПОМ ДО ДВЕРНОГО ЗАМКУ НА БАЗІ ESP8266

3.1 Програмна реалізація програмно-технічного засобу керування доступом до дверного замку

Програмна реалізація функції програмно-технічного засобу керування доступом до дверного замку включає розподіл процесів функціонування даного засобу на дві частини: процеси збору даних та процеси обробки даних. Організація процесу збору даних передбачає реалізацію функціоналу зчитування даних із RFID карти та надсилання даних по протоколу MQTT, що функціонує поверх Wi-Fi на комп'ютерну систему. Організація процесу обробки даних перевчає реалізацію сценарії управління засобами візульаного середовища роботи із потоками Node red. Таким чином дані збирають на стороні мікроконтролерної системи ESP8266, до якого підключено RFID давач, а аналіз цих даних здійснюється на стороні комп'ютерної системи.

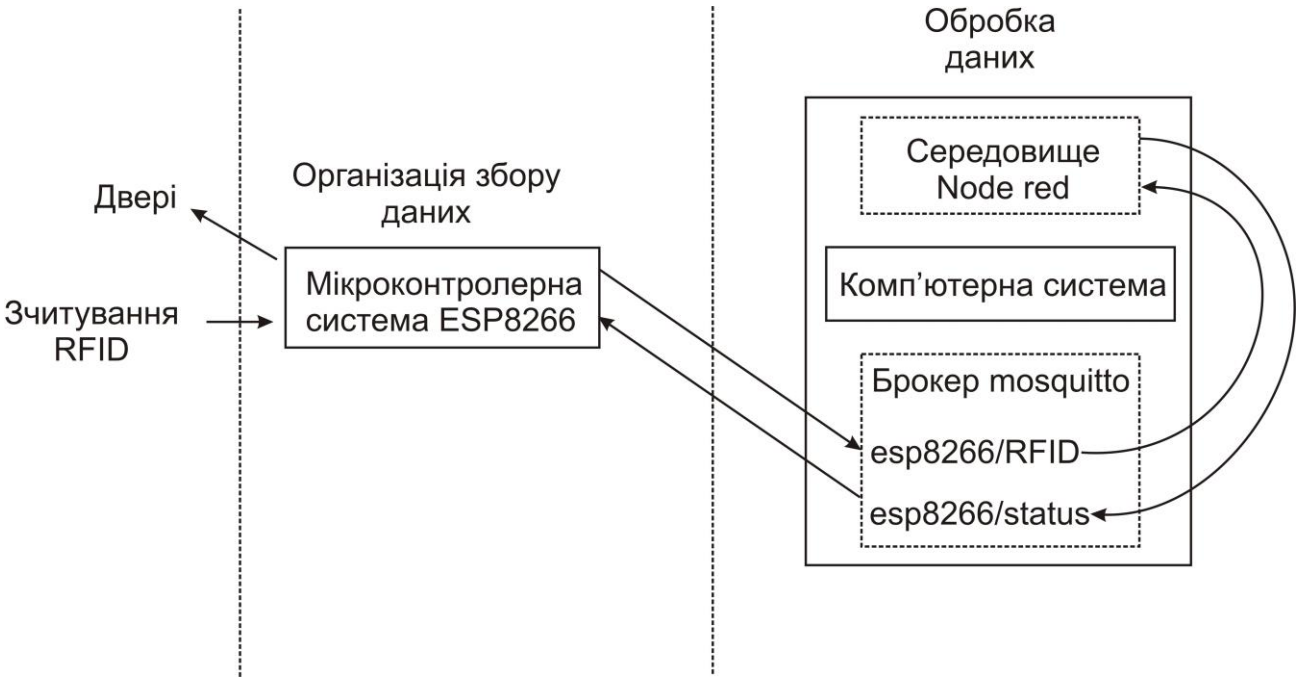


Рисунок 3.1 – Організація збору даних та обробка даних у програмно-технічному засобі керування доступом до дверного замку

Розглянемо детальніше процеси збору даних та процеси обробки даних.

3.1.1 Реалізація процесу збору даних із використанням мікроконтролерної системи ESP8266

Процес збору даних із залученням мікроконтролерної системи ESP8266 передбчає реалізацію функціоналу отримання RFID мітки, надсилання її із використанням протоколу MQTT на комп’ютерну систему, а також отримання результату перевірки та подання відповідного сигналу на дверний замок, що під’єднаний до модуля реле. Розглянемо детальніше прошивку мікроконтролерної системи ESP8266.

Спочатку виконаємо підключення необхідних бібліотек для роботи із ESP8266, mc522 та MQTT. Далі налаштуємо пароль та ssid для WiFI, а також MQTT параметри брокера.

```
#include <ESP8266WiFi.h>
#include <PubSubClient.h>
#include <MFRC522.h>
// Налаштування параметрів WiFi
const char* ssid = "_WiFiSSID";
const char* password = "_WiFiPassword";
// Налаштування MQTT Broker
const char* mqttServer = "_MQTTBroker";
const int mqttPort = 1883;
const char* mqttUser = "_MQTTUsername";
const char* mqttPassword = "_MQTTPassword";
```

Далі визначимо контакти до яких під’єднано RFID RC522 та створимо об’єкт RC522.

```
#define SS_PIN D4
#define RST_PIN D3
MFRC522 mfrc522(SS_PIN, RST_PIN);
```

Також визначимо контакт, до якого під’єднано реле та створимо esp8266 клієнта:

```
#define RELAY_PIN D2
WiFiClient espClient;
PubSubClient client(espClient);
```

У функції setup виконаємо початкові налаштування контактів та виклики відповідних функцій ініціалізації.

```
void setup() {
  Serial.begin(115200);
  pinMode(RELAY_PIN, OUTPUT);
  digitalWrite(RELAY_PIN, LOW);  // Вимкнути реле спочатку
  setupWiFi();
  setupMQTT();
  setupRFID();
}
```

Визначимо також функцію setupRFID, яка буде виконувати ініціалізацію mc522:

```
void setupRFID() {
  SPI.begin();
  mfrc522.PCD_Init();
  Serial.println("RFID module initialized");
}
```

Реалізуємо функцію loop:

```
void loop() {
  if (!client.connected()) {
    reconnectMQTT();
  }
  client.loop();
```

```
  // Зчитування мітки RFID
  if (mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial()) {
    String rfidUID = "";
    for (byte i = 0; i < mfrc522.uid.size; i++) {
      rfidUID.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? "0" : ""));
      rfidUID.concat(String(mfrc522.uid.uidByte[i], HEX));
    }

    Serial.print("RFID UID: ");
    Serial.println(rfidUID);

    publishRFID(rfidUID);

    mfrc522.PICC_HaltA();
    mfrc522.PCD_StopCrypto1();
  }
}
```

У даному коді в функції loop() відбувається основний цикл виконання програми на платі ESP8266. Основні кроки циклу наступні:

– Перевірка підключення до MQTT-сервера: Умова !client.connected() перевіряє, чи платформа ESP8266 підключена до MQTT-сервера. Якщо підключення втрачено, виконується функція reconnectMQTT(), яка відновлює підключення до сервера.

– Обробка MQTT-повідомлень: Виклик client.loop() виконує обробку вхідних та вихідних MQTT-повідомлень. Цей виклик необхідний для забезпечення зв'язку з MQTT-сервером та обміну даними.

– Зчитування мітки RFID: Умова mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial() перевіряє, чи була знайдена нова мітка RFID. Якщо так, то виконується наступний блок коду.

– Отримання ідентифікатора мітки RFID: Виконується цикл для зчитування байтів ідентифікатора мітки RFID з об'єкту mfrc522. Байти конвертуються у шістнадцятковий формат і з'єднуються у рядок rfidUID. Цей рядок представляє ідентифікатор мітки RFID.

– Публікація ідентифікатора мітки RFID: Виклик функції publishRFID(rfidUID) публікує ідентифікатор мітки RFID на топік esp8266/RFID за допомогою клієнта MQTT.

– Завершення операцій з міткою RFID: Виклики mfrc522.PICC_HaltA() та mfrc522.PCD_StopCrypto1() припиняють роботу з міткою RFID та готують модуль RC522 до зчитування наступної мітки.

Таким чином даний код виконує циклічно зчитування міток RFID та публікацію їх ідентифікаторів на MQTT-сервері.

Також визначимо функцію publishRFID, яка виконує публікацію повідомлення мітки у топік esp8266/RFID:

```
void publishRFID(String rfidUID) {
    String topic = "esp8266/RFID";
    char payload[rfidUID.length() + 1];
    rfidUID.toCharArray(payload, sizeof(payload));

    if (client.publish(topic.c_str(), payload)) {
        Serial.println("RFID tag published");
    }
    else {
        Serial.println("Failed to publish RFID tag");
    }
}
```

У функції callback описуєтьяс логіка роботи ESP8266 у випадку, якщо буде отримано повідомлення, тобто фактично підписка на топік. В даному випадку здійснюєтьяс підписка на топік esp8266/status. Для цього слід спочатку отримати

повідомлення та зберегти його у змінній message. Далі якщо було отримано повідомленн зі значенням "on" виконується команда digitalWrite(RELAY_PIN, HIGH) для увімкнення реле, а при отриманні значення "off" виконується команда digitalWrite(RELAY_PIN, LOW) для вимкнення реле.

```
void callback(char* topic, byte* payload, unsigned int length) {
    Serial.print("Message received on topic: ");
    Serial.println(topic);

    String message = "";
    for (unsigned int i = 0; i < length; i++) {
        message += (char)payload[i];
    }

    Serial.print("Message payload: ");
    Serial.println(message);

    String statusTopic = "esp8266/status";
    if (message.equals("on")) {
        digitalWrite(RELAY_PIN, HIGH); // Увімкнути реле
       Serial.println("Relay turned on");
    }
    else if (message.equals("off")) {
        digitalWrite(RELAY_PIN, LOW); // Вимкнути реле
        Serial.println("Relay turned off");
    }
}
```

3.1.2 Реалізація процесу обробки даних на основі створення сценаріїв керування доступом до дверного замку у середовищі Node red

Реалізацію процесу обробки даних на основі створення сценаріїв керування доступом до дверного замку у середовищі Node red розпочнемо із створення інформаційної панелі. Для цього створимо новий шаблон Layout. Далі натиснемо на кнопку tab. В результаті буде створено новий шаблон із назвою Tab4.

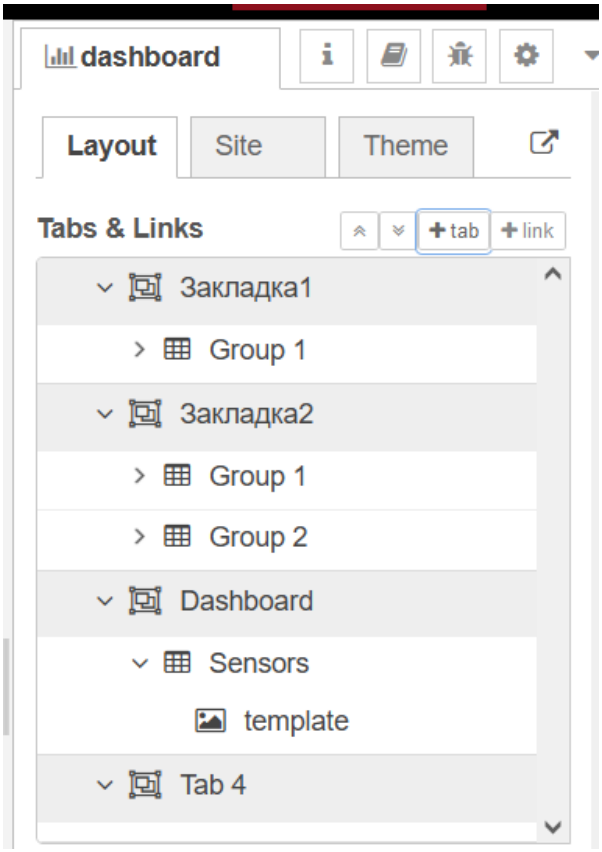


Рисунок 3.2 – Створення шаблону інформаційної панелі в Node red

Після цього слід до створеного шаблону додати нову групу. Для цього наводимо на створений шаблон, після чого тискаємо на кнопку Group (рис. 3.3). Перейменуємо назву Group1 в Список користувачів.

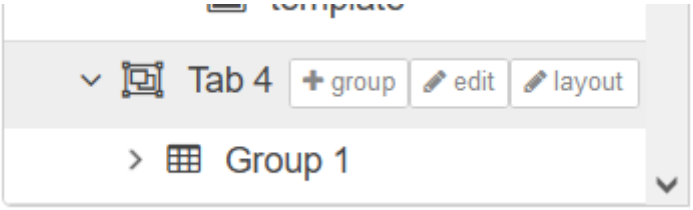


Рисунок 3.3 – Створення групи для інформаційної панелі в Node red

Далі додамо два блоки для обміну даними по протоколу MQTT. Один із них буде вхідний (буде здійснювати підписку на топік esp8266/RFID), і нший – вихідний (виконуватиме публікацію повідомлень у топік esp8266/status). Властивості блоків MQTT приведено на рис. 3.4 та рис. 3.5.

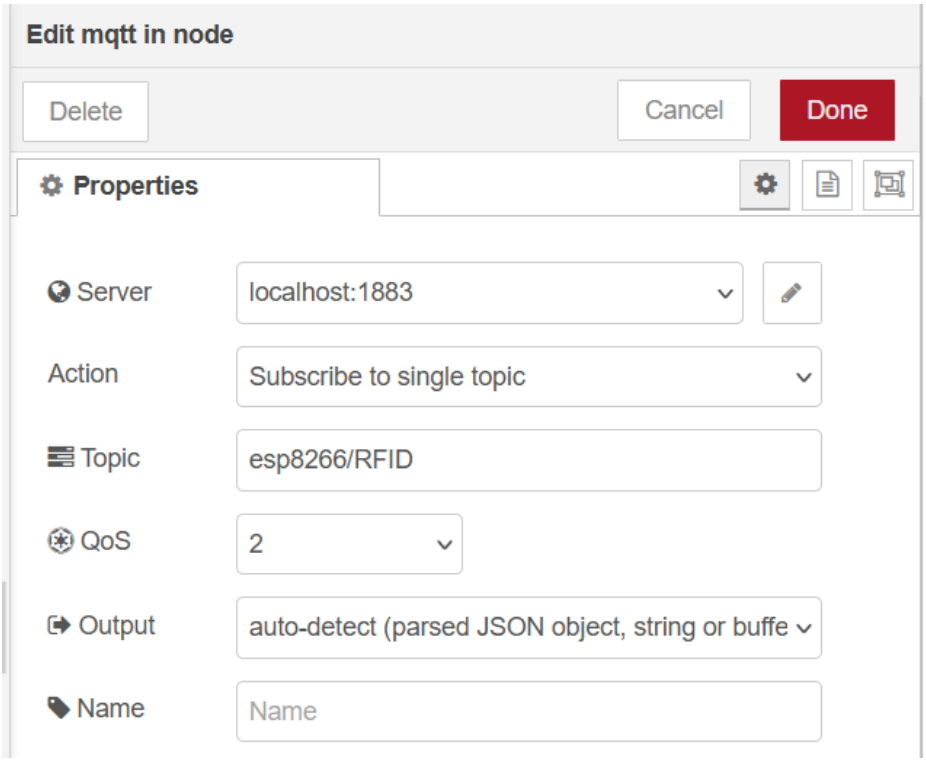


Рисунок 3.4 – Властивості блоку MQTT in esp8266/RFID

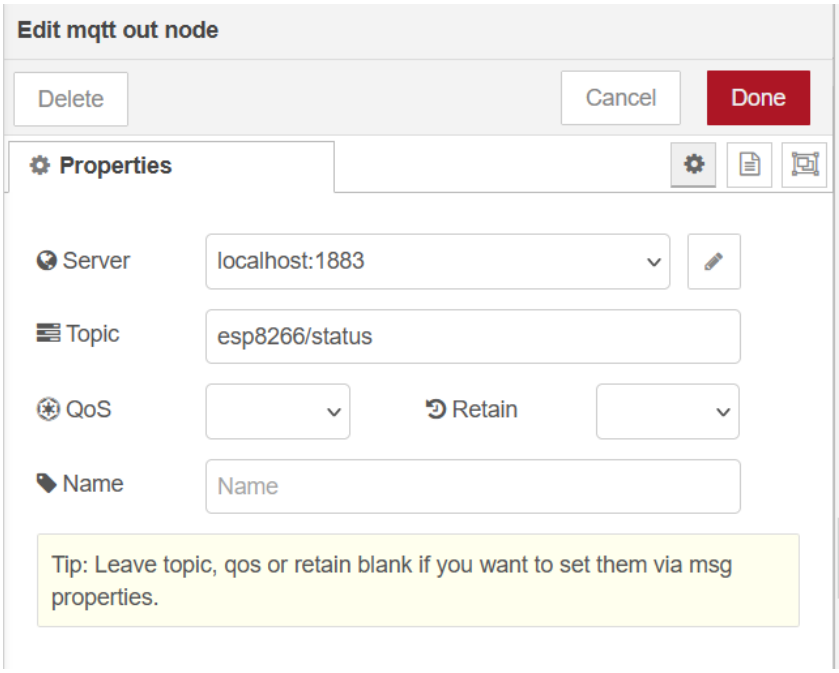


Рисунок 3.5 – Властивості блоку MQTT in esp8266/status

Між заданими двома MQTT блоками додамо блок function та дамо йому назву CheckUser. Основним призначенням даного блоку є безпосередня реалізація процесу обробки даних для керування доступом до дверного замку.

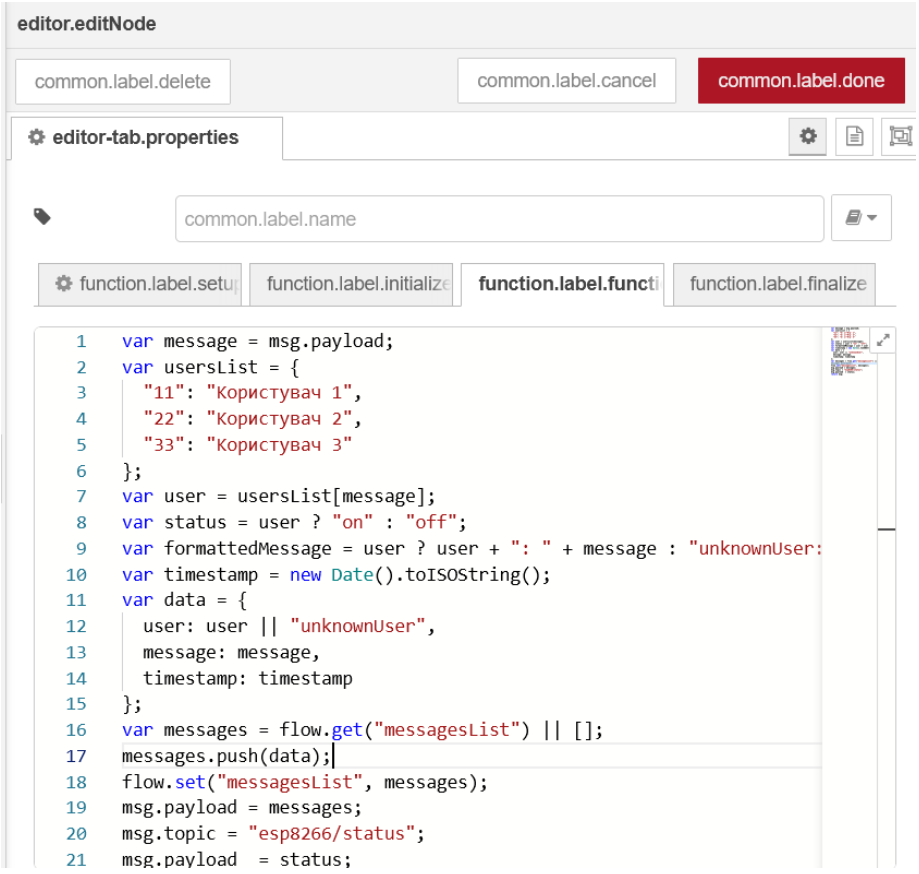


Рисунок 3.6 – Властивості блоку CheckUser

Розгялнемо алгоритм роботи даного блоку.

Спочатку оголошується змінна message, яка ініціалізується значенням msg.payload. В даному випадку msg.payload вважається вхідним повідомленням, яке надійшло до цього вузла. Далі створюється об'єкт usersList, який містить список користувачів, що присутні у системі. Ключі у цьому об'єкті відповідають ідентифікаторам користувачів, а значення – їх іменам. Далі змінна user отримує ім'я користувача, яке відповідає отриманому повідомленню message. Якщо ідентифікатор користувача знайдений в списку usersList, то в змінній user буде збережено відповідне ім'я користувача. В іншому випадку, значення user буде визначено як undefined, що відповідатиме не ідентифікованому користувачу. Далі дійснюється визначення змінної status, яке може отримати значення «on», якщо user має значення (тобто користувач знайдений), або «off» у протилежному випадку. Це статус, який показує, чи було знайдено відповідного користувача. Відповідне повідомлення буде опубліковано у топік esp8266/status.

Далі слід визначити змінну (formattedMessage), яка міститеме сформатоване повідомлення, і яке складатиметься із імені користувача (якщо воно доступне) і самого повідомлення. Якщо користувач не знайдений, використовується префікс «unknownUser».

Наступним кроком сформуємо порцію даних, яка публікуватиметься в інформаційну панель у вигляді: <RFID мітки, Користувач, Часова мітка>. Тому з цією метою створимо об'єкт data, який міститиме інформацію про повідомлення. Властивість user містить ім'я користувача, якщо воно доступне, або значення "unknownUser" у протилежному випадку. Властивість message містить отримане повідомлення, а властивість timestamp містить час, коли було створено це повідомлення:

```
var data = {
  user: user || "unknownUser",
  message: message,
  timestamp: timestamp
};
```

Далі оголошується змінна messages, яка отримує значення списку повідомлень з контексту потоку (flow context). Якщо список не існує, створюється порожній список. Потім об'єкт data додається до цього списку, а оновлений список зберігається назад в контекст потоку. Далі властивість payload об'єкта msg оновлюється змінною messages, яка містить список повідомлень. Властивість topic оновлюється значенням «esp8266/status». Крім того, властивість payload знову оновлюється змінною status, яка містить статус "on" або "off". Нарешті, модифікований об'єкт msg повертається з вузла для подальшої обробки в інших вузлах потоку.

Таким чином результуючий код блоку CheckUser буде виглядати наступним чином:

```
var message = msg.payload;
var usersList = {
  "11": "Користувач 1",
  "22": "Користувач 2",
  "33": "Користувач 3"
};
var user = usersList[message];
var status = user ? "on" : "off";
var formattedMessage = user ? user + ": " + message : "unknownUser: " + message;
var timestamp = new Date().toISOString();
var data = {
  user: user || "unknownUser",
  message: message,
  timestamp: timestamp
};
var messages = flow.get("messagesList") || [];
messages.push(data);
flow.set("messagesList", messages);
```

```
msg.payload = messages;
msg.topic = "esp8266/status";
msg.payload  = status;
return msg;
```

Таким чином після додавання блоку function потік буде виглядати як зображено на рис. 3.7.

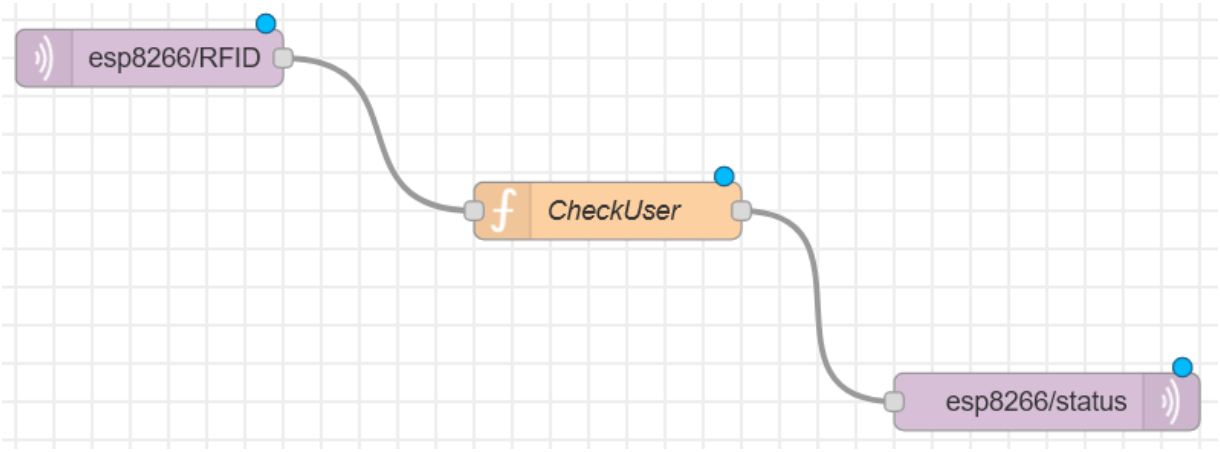


Рисунок 3.7 – Сценарій керування доступом до дверного замку у середовищі Node red

Наступним кроком реалізуємо відображення даних на інформаційній панелі (dashboard). Для цього додамо вузол template (рис. 3.8), основне призначення якого є формування розмітки сторінки.

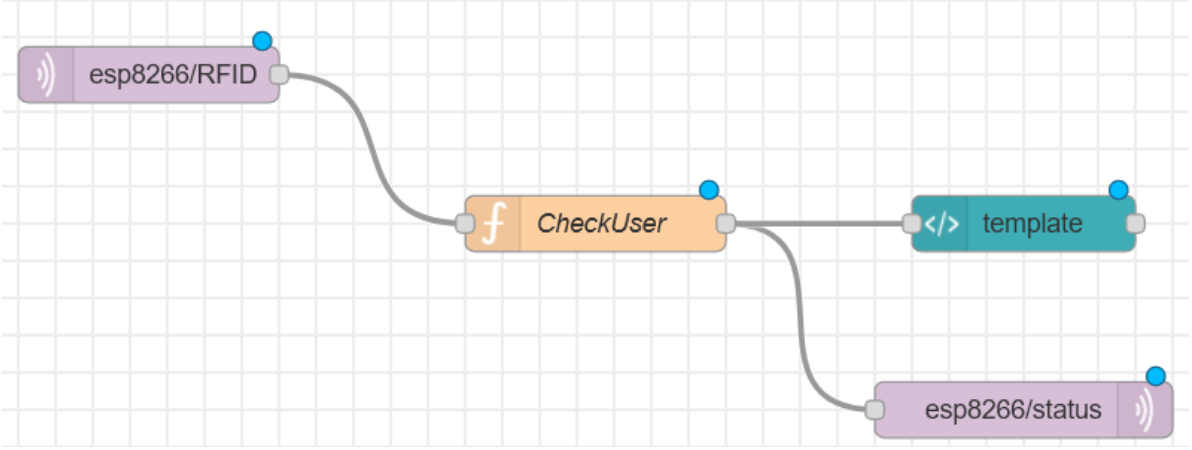


Рисунок 3.8 – Сценарій керування доступом до дверного замку у середовищі Node red із вузлом template

Властивсті вузла template наведено на рис. 3.9

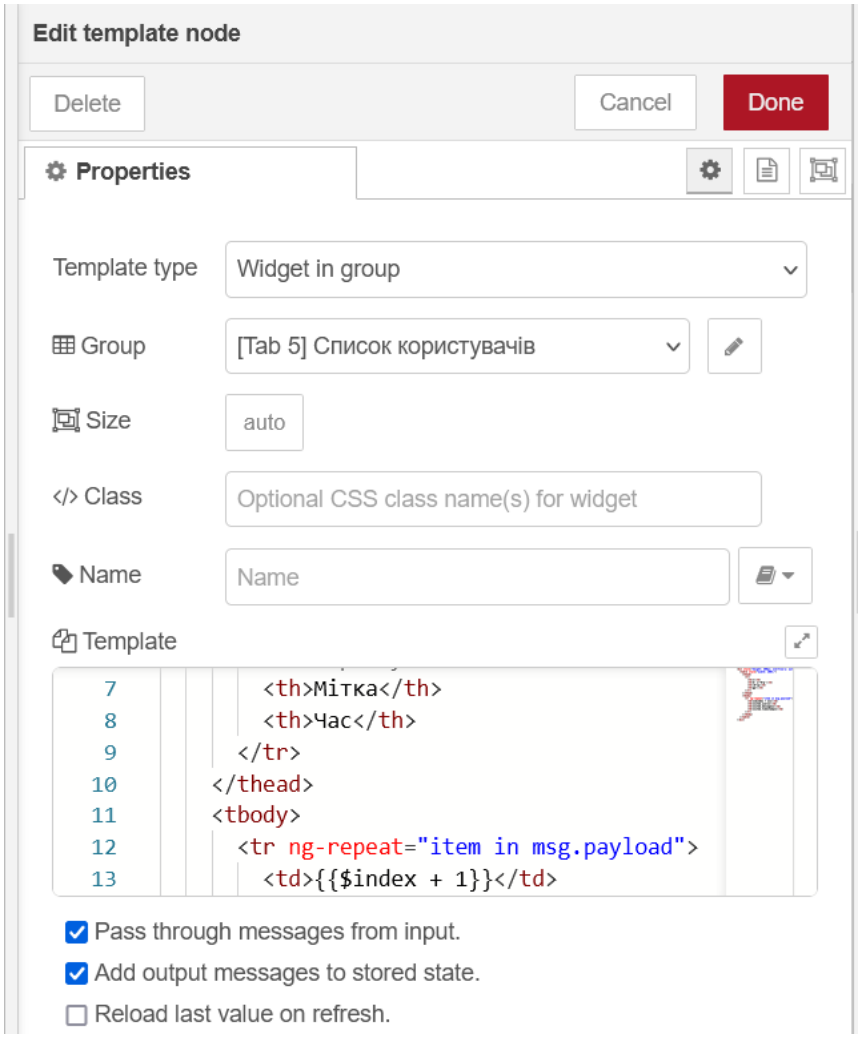


Рисунок 3.9 – Властивості блоку template

Розмітка даного блоку визначає створення таблиці, яка складається із чотирьох стовпців: №, Користувач, Мітка та Час:

```
<div style="height: 300px; overflow-y: auto;">
  <table style="width: 100%;">
    <thead>
      <tr>
        <th>№</th>
        <th>Користувач</th>
        <th>Мітка</th>
        <th>Час</th>
      </tr>
```

```
    </thead>
    <tbody>
      <tr ng-repeat="item in msg.payload">
        <td>{{$index + 1}}</td>
        <td>{{item.user}}</td>
        <td>{{item.message}}</td>
        <td>{{item.timestamp}}</td>
      </tr>
    </tbody>
  </table>
</div>
```

Таким чином в результаті буде створено сторінку інформаційної панелі, інтерфейсне вікно якої зображено на рис. 3.10.

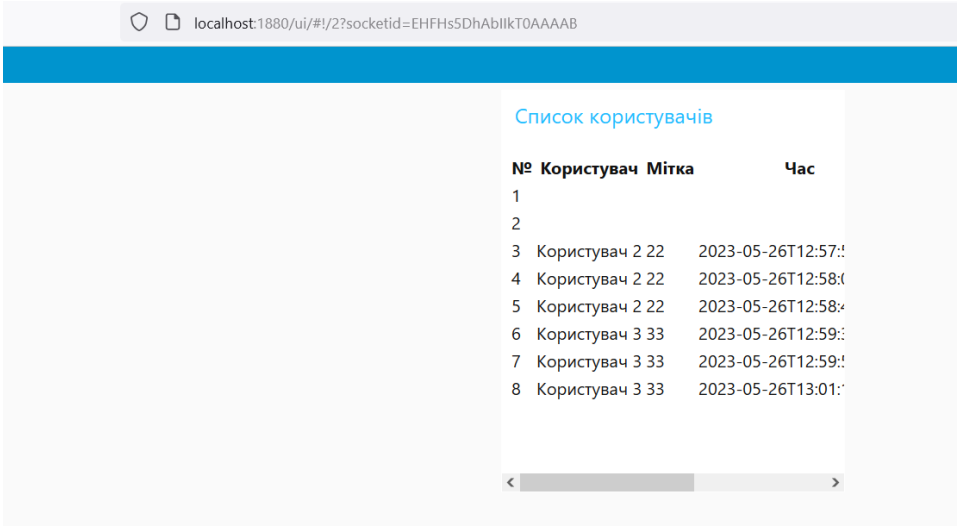


Рисунок 3.10 – Інтерфейсне вікно інформаційної панелі відображення результату доступу

Далі додамо функцію повідомлення користувача про спробу доступу не авторизованого користувача. Для цього скористаємось механізмом СМС. Виконаємо встановлення необхідних блоків для роботи із СМС шляхом виконання команди node-red-contrib-smstools (рис. 3.11).

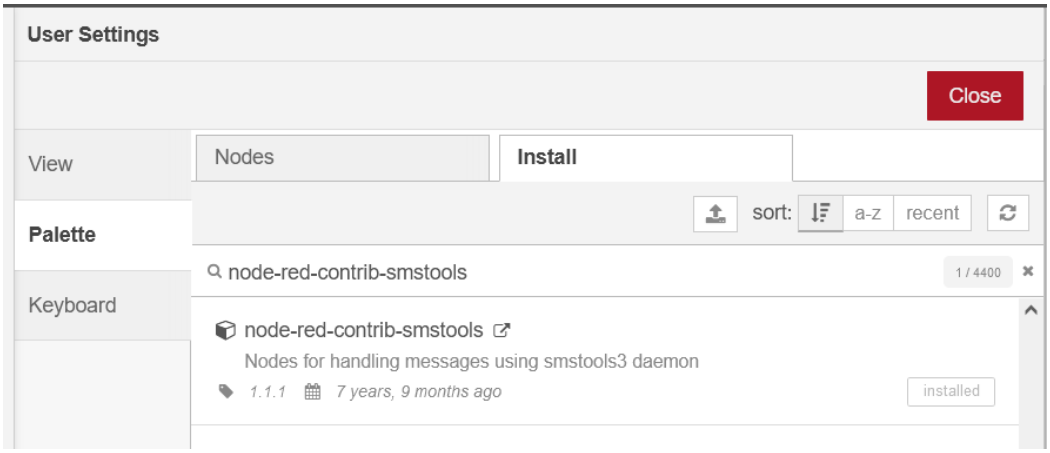


Рисунок 3.11 – Встановлення вузлів для роботи із СМС

Далі модифікуємо сценарій таким чином, щоб у випадку, якщо сценарій розпізнає не ідентифікованого користувача здійснювалось надсилання повідомлення за допомогою СМС. З цією метою додамо блоки Switch та SMS out. Властивості даних блоків забораження на рис. 3.12 та рис. 3.13

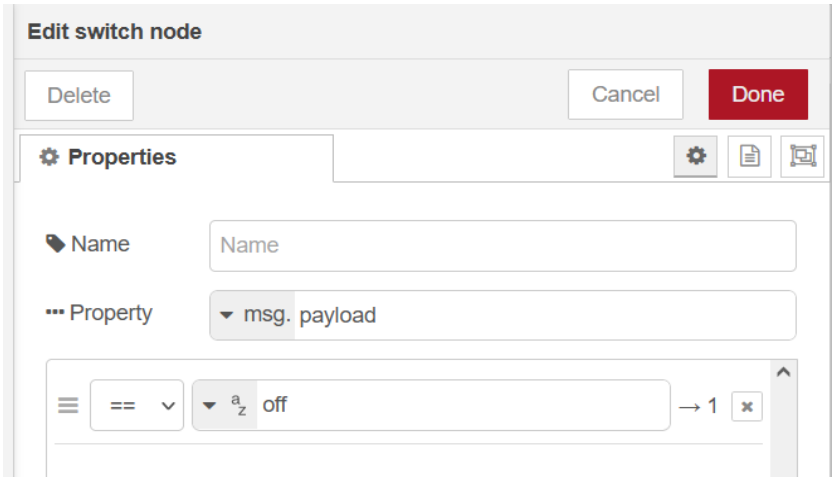


Рисунок 3.12 – Властивості вузла Switch

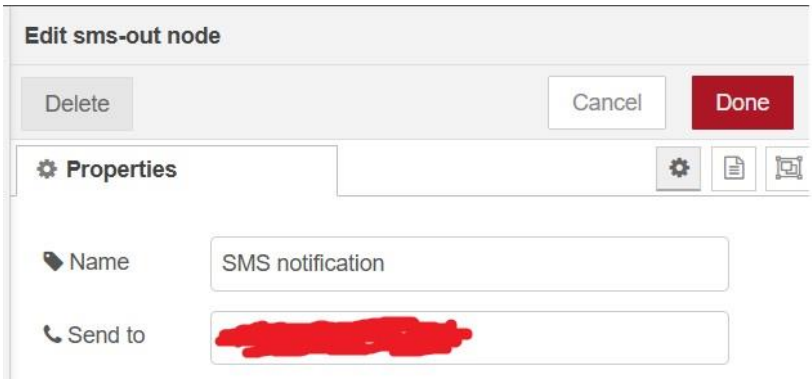


Рисунок 3.13 – Властивості вузла SMS out

Таким чином результаючий сценарій керування доступом до дверного замку (із додатковими вузлами для тестування) у середовищі Node red зображено на рис. 3.14.

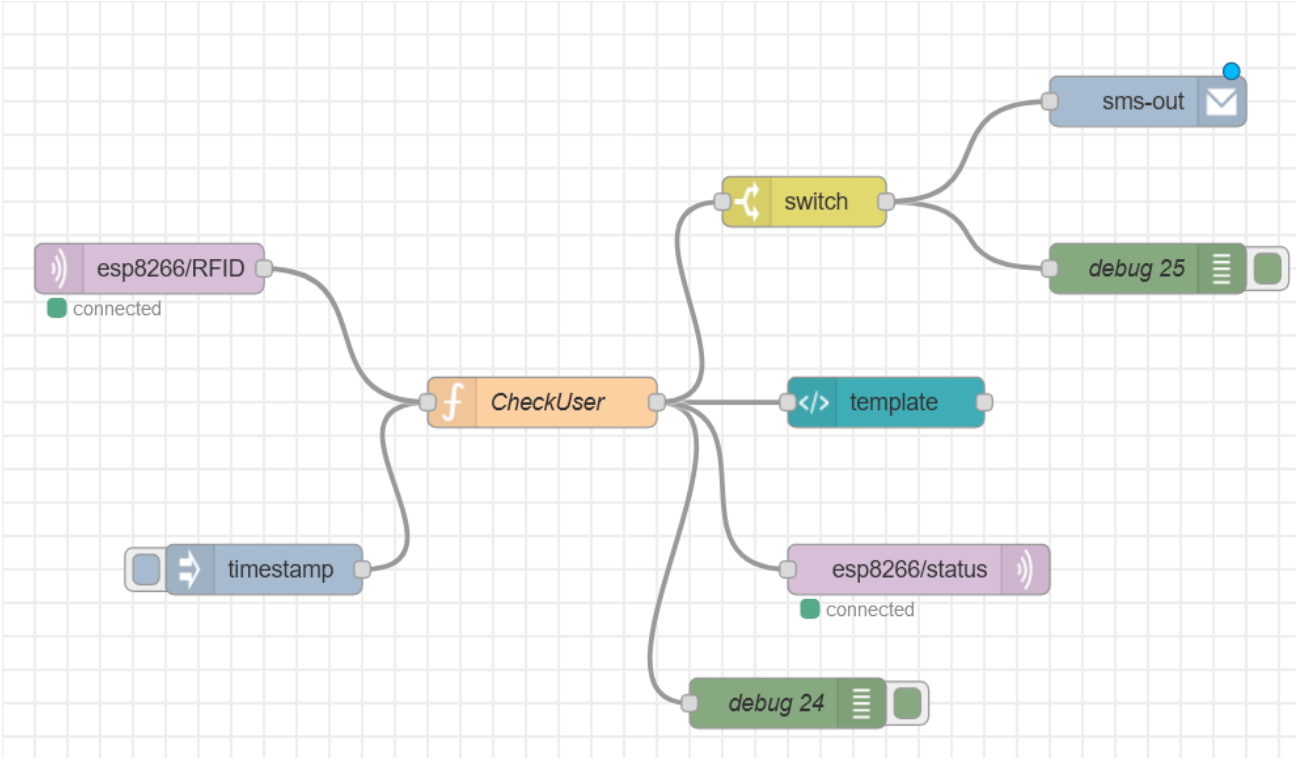


Рисунок 3.14 – Результуючий сценарій керування доступом до дверного замку у середовищі Node red

Для перевірки роботи сценарію скористаємось вбудованими функціями публікації повідомлень у mosquitto. З цією метою виконаємо команду mosquitto_pub –t esp8266/RFID –m “11”, де esp8266/RFID – назва топіка для публікації (рис. 3.15).

```
C:\Program Files (x86)\mosquitto>mosquitto_pub -t esp8266/RFID -m "11"

C:\Program Files (x86)\mosquitto>
```

Рисунок 3.15 – Публікація повідомлення у топік esp8266/RFID

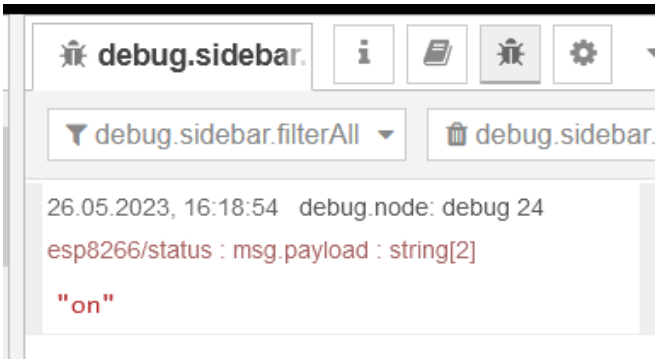


Рисунок 3.16 – Результат роботи сценарію із виведенням на консоль Node red

3.2 Оцінка вартості програмно-технічного засобу керування доступом до дверного замку на базі ESP8266

Оцінка вартості програмно-технічного засобу для керування доступом до дверного замку на базі ESP8266 складається із розрахунку вартості апаратної та програмної складової. Проте, оскільки використанні прогрмні продукти є безкоштовним програмним забезпеченням, оцінку вартості програмно-технічного засобу проведемо із врахуванням виключно апаратної складової.

Таблиця 3.1 – Оцінка вартості апаратних компонентів програмно-технічного засобу керування доступом до дверного замку на базі ESP8266

№	Компонент	Вартість, грн
1	Мікроконтролерна плата NodeMCU Lua V3, ESP8266, CH340	130
2	RFID модуль RC522 з карткою доступу 13.56МГц	81
3	Дверний замок 12V Iron Door Drawer Tongue Down Electric Lock Assembly Solenoid Slim Rustproof	185
4	Стабілізатор напруги LM7805	10
5	Реле модуль 1-канальний 5V	50
6	Роз’єм для підключення живлення DC-F з клемною колодкою 5,5x2,1мм	26
7	Конденсатори електролітичний алюмінієвий 47мкф	60

	50В 105С	
8	Резистори 220 Ом, 10 кОм	30
9	Набір провідників	52
10	Блок живлення 12V 2A із штекером 5.5*2.1 мм	130
Загалом		754

Таким чином загальна вартість програмно-технічного засобу керування доступом до дверного замку на базі ESP8266 складає 754 грн, що складає менше 20$. Якщо порівнювати вартість даного засобу із вартістю аналогів, що присутні на ринку, то зпроєктований засіб виходить дешевшим в декілька разів.

3.3 Висновки за розділом 3

Таким чином було здійснено реалізацію програмної складаової програмно-тезнічного засобу керування доступом до дверного замку на базі мікрокотролера ESP8266. Програмна реалізація функції програмно-технічного засобу керування доступом до дверного замку включає розподіл процесів функціонування даного засобу на дві частини: процеси збору даних та процеси обробки даних. Організація процесу збору даних передбачає реалізацію функціоналу зчитування даних із RFID карти та надсилання даних по протоколу MQTT, що функціонує поверх Wi-Fi на комп’ютерну систему. Організація процесу обробки даних перевчає реалізацію сценарії управління засобами візульаного середовища роботи із потоками Node red. Таким чином дані збирають на стороні мікроконтролерної системи ESP8266, до якого підключено RFID давач, а аналіз цих даних здійснюється на стороні комп’ютерної системи.

Також було проведено обрахунок вартості складових компонентів проектованого пристрою. Загальна вартість програмно-технічного засобу керування доступом до дверного замку на базі ESP8266 складає 754 грн, що складає менше за 20$.

ВИСНОВКИ

Створення програмно-технічного засобу керування доступом до дверних замків на базі ESP8266 є актуальною і важливою темою. Забезпечення безпеки приміщень і обмеження доступу до них є першочерговим завданням для багатьох організацій і приватних осіб. Із зростанням інтелектуальних технологій та Інтернету речей, використання мікроконтролерів, таких як ESP8266, для розробки програмно-технічних засобів керування доступом стає все більш популярним. Це дозволяє створювати розумні системи, що об’єднують безпеку та зручність управління, а також забезпечує можливість віддаленого контролю і моніторингу. Такі системи можуть бути застосовані в різних сферах, включаючи житлові будинки, офіси, громадські споруди, готелі та інші об'єкти, де необхідна ефективна та безпечна система контролю доступу.

За результатами виконання кваліфікаційної роботи було спроектовано програмно-технічний засіб керування доступу до дверного замку на базі мікроконтролера ESP8266. Слід відзначити, що однією із головних особливостей спроектованого пристрою є те, що його можна легко розширити, використавши багатоканальні модулі реле та декілька дверних замків. Це дозволить реалізувати контроль доступу одночасно до декількох дверей або інших об’єктів у приміщенні.

У першому розділі розглянуто системи контролю доступу до дверей, проведено аналіз відомих засобів керування доступу до дверних замків. Розглянуто класифікацію ідентифікаторів та зчитувачі, що використовуються для керування дверними замками.

У другому розділі було визначено перелік вимог та запропоновано узагальнену стуркутру програмно-технічного засобу доступу до дверного замку на базі ESP8266. Здійснено вибір апаратних та програмних компонентів, а також запропоновано схеми електричну принципову та монтажну. Запропоновано конструктивний вигляд проектованого програмно-технічного засобу керування доступом до дверного замку на базі ESP8266.

У третьому розділі здійснено реалізацію програмної складаової програмно-тезнічного засобу керування доступом до дверного замку на базі мікрокотролера ESP8266. Програмна реалізація функції програмно-технічного засобу керування доступом до дверного замку включає розподіл процесів функціонування даного засобу на дві частини: процеси збору даних та процеси обробки даних. Організація процесу збору даних передбачає реалізацію функціоналу зчитування даних із RFID карти та надсилання даних по протоколу MQTT, що функціонує поверх Wi-Fi на комп'ютерну систему. Організація процесу обробки даних перевчає реалізацію сценарії управління засобами візульаного середовища роботи із потоками Node red. Таким чином дані збирають на стороні мікроконтролерної системи ESP8266, до якого підключено RFID давач, а аналіз цих даних здійснюється на стороні комп'ютерної системи.

Також було проведено обрахунок вартості складових компонентів проектованого пристрою. Загальна вартість програмно-технічного засобу керування доступом до дверного замку на базі ESP8266 складає 754 грн, що складає менше за 20$. Якщо порівнювати вартість даного засобу із вартістю аналогів, що присутні на ринку, то зпроєктований засіб виходить дешевшим в декілька разів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Circuit Diget, Digital Keypad Security Door Lock using Arduino, URL: https://circuitdigest.com/microcontroller-projects/digital-keypad-security-door-lock-using-arduino.
2. Instructables, Bluetooth Door Lock (Arduino), URL: https://www.instructables.com/Bluetooth-Door-Lock-Arduino/.
3. IoT projectsideas, Arduino RFID Master Card Door Lock with EEPROM, URL: https://iotprojectsideas.com/arduino-rfid-master-card-door-lock-with-eeprom/.
4. Nwogu C., Eze M., Okunbor C., Design and Implementation of Access Door Control with Mo-bile Alert, *International Journal of Engineering & Technology* 9(2):480, 2020.
5. Mandeep K., Manjeet S., Neeraj M. and Parvinder S,. RFID Technology Principles, Advantages. Limitations and Its Applications. *International Journal of Computer and Engineering*, Vol3. No1, 2010. 1793-8163.
6. Shin S. S., Han, K. H., & Jin, K. Y,. Digital Door Lock on the Access Control System using OTP-based User Authentication. *International Journal of Digital Content Technology and its Applications*, 7(11), 2013, 436.
7. Sathish P. K. et al. Smart home automation using Raspberry PI 4. *AIP Conference Proceedings. 2463*. 020012.
8. Rahman M. M., Ali M. S., Akther M. S. Password Protected Electronic Lock System for Smart Home Security. *International Journal of Engineering Research & Technology*, 7(4), 2018, 541-544.
9. Altaf H., Muhammad H., Kamran. H. and Tabinda Z., Programming a microcontroller. *International Journal of Computer Applications*. Vol 155 (5), 2016, 21-26.
10. Шостак І. В., Данова М. О., Феоктистова О. І. Підхід до роботизації процесів функціонування системи «Розумний будинок» на основі Інтернету речей. *Інтегровані інтелектуальні робототехнічні комплекси* : матеріали XIII між нар. наук.-практ. конф. (19-20 трав., 2020 р., м. Київ) Київ, 2020, С.48-49.

11. Oloyede M., Adedoyin A. and Adewole K. Fingerprint Biometric Authentication for enhancing Staff Attendance System. *International Jour-nal of Applied Info. Systems*. 5 (3), 2013, 19-24

12. ESPRESIF, ESP8266, URL: https://www.espressif.com/en/products /socs/esp8266

14. Components 101. RC522 RFID Module URL: https://components101.com/wireless/rc522-rfid-module

15. Basri A. H. H. Ibrahim S. N., Malik N. A. and Asnawi A. L. Integrated Surveillance System with Mobile Application, *2018 7th International Conference on Computer and Communication Engineering (ICCCE)*, Kuala Lumpur, Malaysia – 2018, pp. 218-222

16. Boasheng Y., Honhmei L. and Xiaoling Y. Logic Conversion Method in Serial Data System, *Procedia Engineering*, 29, 2012, 1539-1543.

17. Haiwei C. and Shin-Tson W. Advanced Liquid Crystal Display with Supreme Image Qualities. *Journal: Liquid Crystals Today*. 28 (1), 2019, 4-11.

18. Samuel E. and Chukwuebuka E. Numerical simulation: controlling light emitting diodes from MATLAB. *International Journal of Computer Aided Engineering and Technology*, 2018, 10 (6), 2018. 748-761.

19. Hossain M. K., Biswas, P., Mynuddin, M., & Morsalin, S. Design and implementation of smart home security system. *International Journal of modern embedded system*, 2(6), 2014. 7-10.

20. Patchava V., Kandala H. B. and Babu P. R., A Smart Home Automation technique with Raspberry Pi using IoT, *2015 International Conference on Smart Sensors and Systems (IC-SSS)*, Bangalore, India, 2015, pp. 1-4

21. Глибовець А.М., Моголівський В.О. Аналіз систем підтримки розумного будинку. *Control systems and computers*. 2019. No 5(283). С. 30–37.

22. Arduino ua RFID модуль RC522 з карткою доступу для Arduino URL: https://arduino.ua/prod649-rfid-modyl-rc522-s-kartochkoi-dostypa-dlya-arduino

23. Конспект лекцій з дисципліни « Комп'ютерні системи» для студентів напряму підготовки «Комп'ютерна інженерія» / І. М. Лазарович. – Івано-

Франківськ : *Видавництво Прикарпатського національного університету імені Василя Стефаника*, 2014. – 190 с.

24. Mahamudul H., Islam M., Shameem A., Rana J. and Metselaar H., Modelling of PV module with incremental conductance MPPT controlled buck-boost converter, *2013 2nd International Conference on Advances in Electrical Engineering (ICAEE)*, 2013, pp. 197-202

25. Фурман І.О., Старовєров Р.М., Мельський Д.О. Огляд можливостей «розумного будинку» для покращання побутових умов та зменшення витрат на утримання домогосподарств. *Енергетика та комп'ютерно-інтегровані технології в АПК*. 2014. No 2. С. 79–80.

26. Valov N. and Valova I., Home Automation System with Raspberry Pi, *2020 7th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE)*, Ruse, Bulgaria, 2020, pp. 1-5

27. Wong D., Jones E. and Rubin G. (2018). Mobile Text alerts are an effective way of communicating emergency information to adolescents: Results from focus groups with 12 to 18 years olds. *Journal of Contingencies and Crisis Management.* Vol 26, 183-192.

28. Singh N. J. and Sidhu E., Raspberry pi based smart fire management system employing sensor based automatic water sprinkler, *2017 International Conference on Power and Embedded Drive Control (ICPEDC)*, 2017, pp. 102- 106.

29. Sathyakala G., Kirthika V. and Aishwarya B., Computer Vision Based Fire Detection with a Video Alert System, *2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018, pp. 0725-0727.

30. Bin Bahrudin M. S., Kassim R. A. and Buniyamin N., evelopment of Fire alarm system using Raspberry Pi and Arduino Uno, *2013 International Conference on Electrical, Electronics and System Engineering (ICEESE)*, 2013, pp. 43-48, doi: 10.1109/ICEESE.2013.6895040.

31. Верусь В.С., Кондратюк О.І., Ляшко С.С. Розумний будинок або автоматизована система керування житлом. *Студентський вісник Національного*

університету водного господарства та природокористування. 2019. Вип. 1(11). С. 119–122.

32. Raju L., Sowmya G., Srividhya S., Surabhi S., Retika M. K. and Reshmika Janani M., Advanced Home Automation Using Raspberry Pi and Machine Learning, *2021 7th International Conference on Electrical Energy Systems (ICEES)*, Chennai, India, 2021, pp. 600-605.

33. Mandeep K., Manjeet S., Neeraj M. and Parvinder S. RFID Technology Principles, Advantages. Limitations and Its Applications. *International Journal of Computer and Engineering*, Vol3. No1, 2011, 1793-8163.

34. Takahashi H. et al., Improvement of automatic fire extinguisher system for residential use, *2015 International Conference on Informatics, Electronics & Vision (ICIEV)*, 2015, pp. 1-4.

35. Swain K. B., Dash S. and Gouda S. S., Raspberry PI based Integrated Autonomous Vehicle using LabVIEW, *2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS)*, 2017, pp. 69-73, doi: 10.1109/SSPS.2017.8071567.

36. Lino R. The prototype of automated doors and windows by using voice commands, *Int. Seminar on Application for Technology of Information and Communication* (ISemantic) 323-326 2016.

37. Mohd Nor Azni, L. Vellasami, A. H Zianal, F. A Mohammed, N. N Mohd Daud, R. Vejasegaran, N. W. Basharudin, M. Jusoh, Ku Azir, P. L. Eh Kan, Home automation system with android application, *3rd Int. Conf. on Electronic Design (ICED)*, 2016. 299-303.

38. Nisan N., Schocken S. The Elements of Computing Systems, second edition: Building a Modern Computer from First Principles 2nd Edition, *The MIT Press*, 2021.

39. Yadin A. Computer Systems Architecture, Chapman and Hall, *CRC*, 2016. – 467 p.

40. Null L., Lobur Y. Essentials of Computer Organization and Architecture, *Jones & Bartlett Learning*; 5th edition, 2018, 744 p.

41. Rea P., Ottaviano E., Machado J. and Antosz K. Design, Applications, and Maintenance of Cyber-Physical Systems , *Engineering Science Reference*, 2021. 314 p.

42. Гайдукевич С.В., Семенова Н.П., Леськів Я.А. Особливості SMART-технологій на прикладі автоматизації житлового будинку, *Таврійський науковий вісник*. №1. 2022. С. 12-21.

43. Li B. S. X., Wan B., Wang C., Zhou X., Chen X. Definitions of predictability for cyber physical systems, *J. of Systems Architecture*. 2016.

44. Poliakov, M., Larionova, T. Control Systems with programmable logic controllers, Remote and virtual tools in engineering: textboo, General editorship Dr.Ing.Karsten Henke, aporizhzhya: Dike Pole, 2016, 250 p.

45. Натрошвілі С. Г., Натрошвілі Г. Р., Бабина Т. Г., Злотенко Б. М., Кулік Т. І. Комп'ютерно-інтегрована система керування природним і штучним освітленням розумного будинку, *Вісник Хмельницького національного університету. Серія : Технічні науки*, 2020, № 5 (289), С. 65-71.

46. Monk S. Programming Arduino Next Steps: Going Further with Sketches, *McGraw-Hill Education TAB*, 2018. 320 p.

47. Barrett S.F. Microchip AVR® Microcontroller Primer: Programming and Interfacing , *Morgan & Claypool Publishers*, 2019, 374 p.

48. Papazoglou P. M. An Educational Guide to the AVR Microcontroller Programming: AVR Programming::Demystified (Assembly Language) (Vol.1), *CreateSpace Independent Publishing Platform*, 2018. 274 p.

49. Hu Y., Tilke D., Adams T. et al. Smart home in a box: usability study for a large scale self-installation of smart home technologies. *J Reliable Intell Environ* 2. – 2016, pp. 93-106

50. Kravets A.G., Bolshakov A.A., M.V. Shcherbakov Cyber-Physical Systems: Industry 4.0 Challenges (Studies in Systems, Decision and Control, 260) , *Springer*; 1st ed., 2020., 349 p.

51. Nisan N., Schocken S. The Elements of Computing Systems, second edition: Building a Modern Computer from First Principles 2nd Edition, *The MIT Press*, 2021. 344 p.

52. Rhee J.H., Ma J.H., Seo J., Cha S.H., Review of applications and user perceptions of smart home technology for health and environmental monitoring, *J. Comput. Des. Eng*. No 9. 2022, pp. 857–889

53. Kayastha S. and Upadhyaya P., Design and Implementation of a Cost-Efficient Smart Home System with Raspberry Pi and Cloud Services, *2019 Artificial Intelligence for Transforming Business and Society (AITB)*, Kathmandu, Nepal, 2019, pp. 1-7.

54. Бабенко О. В. Актуальність технологій розумних будинків для підвищення енергоефективності економіки держави, *Матеріали XLVIII наук.-техн. конф. підрозділів Вінниц. нац. техн. ун-ту (НТКП ВНТУ-2019)* : зб. доп., Вінниця, 2019, С. 2920-2921

55. Balta-Ozkan N., Davidson R., Bicket M., Whitmarsh L., Social barriers to the adoption of smart homes, *Energy Policy*, Vol. 63, 2013, pp. 363-374

56. Степаненко О.І. Пасивний будинок – шлях до ефективного використання енергії , *Енергетика: економіка, технології, екологія*, 2014, №3, С. 56-58.

57. Valov N. and Valova I., Home Automation System with Raspberry Pi, *2020 7th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE)*, Ruse, Bulgaria, 2020, pp. 1-5

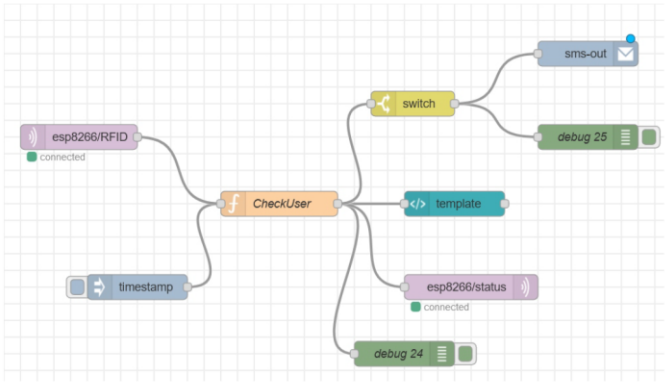
58. Sharma M., Assotally A. and Bekaroo G., RaspiMonitor: A Raspberry Pi Based Smart Home Monitoring System, *2022 3rd International Conference on Next Generation Computing Applications (NextComp)*, Flic-en-Flac, Mauritius, 2022, pp. 1-6.

59. Singh N. J. and Sidhu E., Raspberry pi based smart fire management system employing sensor based automatic water sprinkler, *2017 International Conference on Power and Embedded Drive Control (ICPEDC)*, 2017, pp. 102- 106.

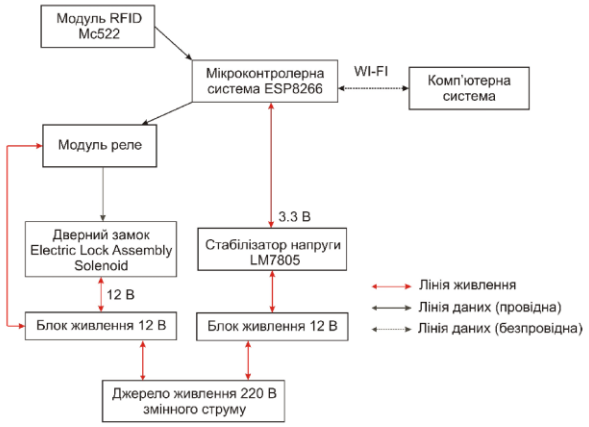
ДОДАТОК А
(обов’язковий)
Копія креслення «Креслення сценаріїв керування доступом до дверногозамку у Node-red»

КвРКІ. 2001125.01.17.01 Е8

Сценарій керування доступом до дверного замку у середовищі Node red



Узагальнена структурна схема програмно-технічного засобу доступу до дверного замку на базі ESP8266

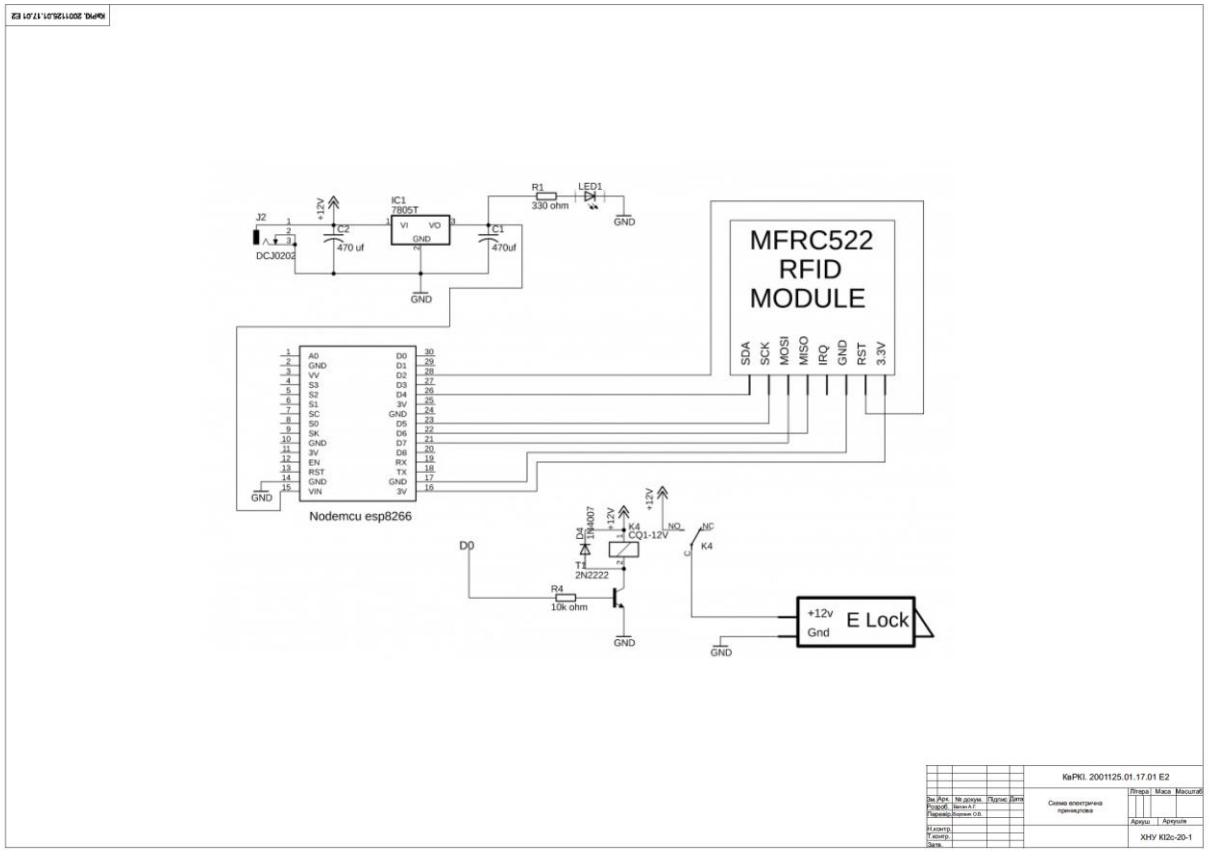


Зм.	Арк.	№ докум.	Підпис	Дата	КвРКІ. 2001125.01.17.01 Е8				
Розроб.		Білан А.Г.			Креслення сценаріїв керування доступом до дверного замку у Node-red		Літера	Маса	Масштаб
Перевір.		Боровик О.В.							
Н.контр.							Аркуш	Аркушів	
Т.контр.									
Затв.							ХНУ КІ2с-20-1		

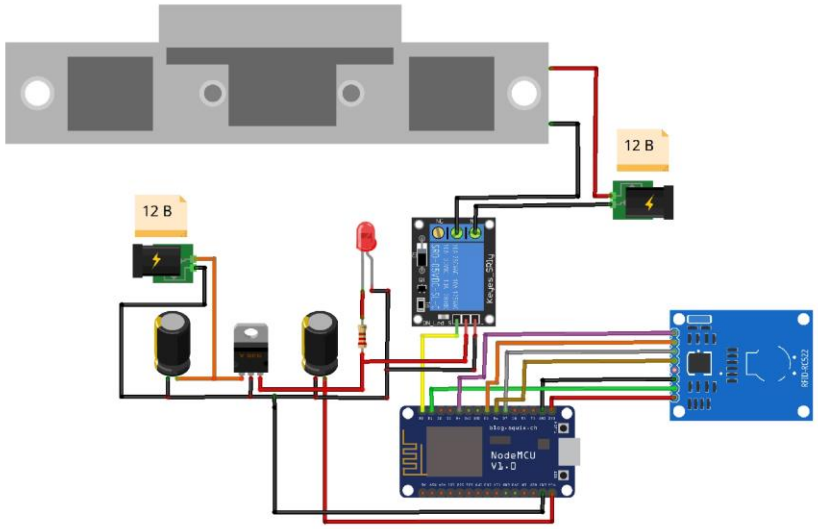
ДОДАТОК Б

(обов’язковий)

Копія креслення «Схема електрична принципова»



ДОДАТОК В
(обов’язковий)
Копія креслення «Монтажна схема»



КвРКІ. 2001125.01.17.01 Е4

Монтажна схема

ХНУ КІ2с-20-1

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1015375516

Дата перевірки:
01.06.2023 19:17:39 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
01.06.2023 19:21:49 EEST

ID користувача:
100005591

Назва документа: **Балан_Програмно-технічний засіб керування доступом до дверного замку на базі ESP8266**

Кількість сторінок: **69** Кількість слів: **10440** Кількість символів: **78621** Розмір файлу: **5.94 MB** ID файлу: **1015041352**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

17.6%
Схожість

Найбільша схожість: **12%** з джерелом з Бібліотеки (ID файлу: **1014850623**)

13.5% Джерела з Інтернету	902	Сторінка 71
12.8% Джерела з Бібліотеки	74	Сторінка 75

0.58% Цитат

Цитати	5	Сторінка 76

Не знайдено жодних посилань

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Підозріле форматування	14 сторінок

Thu Jun 01 18:17:56 EEST 2023, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 8.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 14%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114500 Назва: БКР Програмно-технічний засіб керування доступом до дверного замку на базі ESP8266 Додано в БД: 2023-06-01 Автора: А.Г. Балан Керівники: О.В. Боровик Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	70887	600	5840 (8%)	49 (8%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Балан Андрій Григорович

Тема: Програмно-технічний засіб керування доступом до дверного замку на базі ESP8266

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг дипломної роботи:

Кількість листів креслень 3; кількість сторінок записки 55

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано програмно-технічний засіб керування доступом до дверного замку на базі ESP8266

2. Висновок про відповідність роботи дипломному завданню Дипломний проект відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз предметної області та огляд відомих засобів керування доступом до дверного замку та інших об'єктів. У другому розділі наведено структуру проектованого засобу, здійснено вибір апаратної складової програмно-технічного засобу. У третьому розділі проведено реалізацію програмної програмно-технічного пристрою керування доступом до дверного замку на базі ESP8266

4. Позитивні сторони роботи: Запропоновано структуру та спроектовано програмно-технічний засіб керування доступом до дверного замку на базі ESP8266

5. Негативні сторони роботи: В запропонованій структурі програмно-технічного засобу відсутні функції індикації про статус дозволу (наприклад, можна було виводити інформацію на дисплей).

6. Оцінка графічного оформлення та пояснювальної записки роботи: пояснювальна записка та листи креслення виконані згідно діючих вимог

7. Відгук про роботу в цілому: В загальному робота виконана на задовільному рівні.

8. Інші зауваження: -

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої дипломної роботи вважаю, що робота заслуговує оцінки «задовільно» 3,25 (D)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) д.ф.-м.н., проф. зав. кафедри ІПЗ Бедрачок Л.П.

"5" червня 2023р.

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Балан Андрій Григорович
ПІБ здобувача вищої освіти

ФІТ, 3 курсу, групи КІ2с-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

"05" червня 2023 р. _____ (підпис)

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Програмно-технічний засіб керування доступом до дверного замку на базі ESP8266

Автор: Балан Андрій Григорович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Боровик Олег Васильвович, д.т.н, професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділі аналізу існуючих аналогів та відомих рішень, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) перелік використаних джерел кваліфікаційної роботи розпізнано як плагіат

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 17,6% і адресується до 976 першоджерела, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи О. В. Боровик

Гарант ОП С. М. Лисенко

Завідувач кафедри КІІС Т. О. Говорущенко