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

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Кіберфізична система контролю доступу до підприємства на основі Esp8266
Назва теми

КвРКІ 220021.22.01.16 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 ІІІ курсу, група КІ2с-22-1 _____ Андрій ЛОЗОВЕЦЬКИЙ
Підпис Ініціали, прізвище

Керівник _____ Сергій ЛИСЕНКО
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата Ініціали, прізвище

До захисту допускаю:
зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис Ініціали, прізвище

«02» червня 2025 р.

Хмельницький 2025

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 Ольга ПАВЛОВА

" 10 " 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

ЛОЗОВЕЦЬКОМУ Андрію Анатолійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система контролю доступу до підприємства на основі Esp8266

Керівник проекту (роботи) ЛИСЕНКО Сергій Миколайович , д.т.н., проф.

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

Затверджена наказом ректора університету від 07.02.2025 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

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

Кіберфізична система контролю доступу до підприємства на основі Esp8266 та постановка задачі щодо її удосконалення

Елементна база кіберфізичної системи контролю доступу до підприємства на основі Esp8266

Реалізація кіберфізичної системи контролю доступу до підприємства на основі мікроконтролера Esp8266

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

Монтажна схема

Схема електрична принципова

Структурна схема

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийн
Нормоконтроль	Тетяна КИСІЛЬ, доцент кафедри КІІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІІС		

7. Дата видачі завдання «_10_»_____01_____2025 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Приміт
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2025	виконан
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2025	виконан
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2025	виконан
4	Робота над розділом 2 – вибір компонентів для проєктування кіберфізичної системи контролю доступу до підприємства на основі Esp8266	01.04.2025	виконан
5	Робота над розділом 3 – проєктування кіберфізичної системи контролю доступу до підприємства на основі Esp8266	29.04.2025	виконан
6	Оформлення пояснювальної записки згідно вимог	25.05.2025	виконан
7	Попередній захист ВКР	26.05.2025	виконан
8	Захист ВКР на засіданні ЕК	Червень 2025 року	

Студент _____ Андрій ЛОЗОВЕЦЬКИЙ
Підпис Ініціали, прізвище

Керівник роботи _____ Сергій ЛИСЕНКО
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 220021.22.01.16 ПЗ	Пояснювальна записка	60		
			Графічні матеріали			
2		КвРКІ 220021.22.01.16 Е8	Монтажна схема проєкту	1		
3		КвРКІ 220021.22.01.16 Е8	Схема електрична принципова	1		
4		КвРКІ 220021.22.01.16 Е8	Структурна схема проєкту	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 220021.22.01.16 ВП		
Розробив		Лозовецький			Відомість проєкту	Літера	Аркуш 1 / Аркушів 1
Перевір.		Лисенко				У	
Н. контр.		Кисіль		02.06.25		ХНУ, КІ2с-22-1	
Затв.		Павлова		02.06.25			

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберфізична система контролю доступу до підприємства на основі Esp8266».

Автор роботи: Андрій ЛОЗОВЕЦЬКИЙ.

Керівник роботи: Лисенко Сергій Миколайович.

Пояснювальна записка: 60 с., 34 рис., 7 табл., 5 дод., 58 джерел.

Графічна частина: 3 креслення.

КІБЕРФІЗИЧНА СИСТЕМА, ESP8266, ESP32, RFID, КОНТРОЛЬ ДОСТУПУ, GOOGLE SHEETS.

Метою дипломної роботи є створенння та реалізація проекту який покращить вже існуючі системи контролю доступу, а саме реалізувати кіберфізичну систему для контролю доступу до підприємства на основі Esp8266.

У сучасних умовах спостерігається зростаючий інтерес до впровадження надійних та безпечних систем контролю доступу до приміщень. Це пояснюється підвищеними вимогами до безпеки з боку як приватних осіб, так і підприємців, які прагнуть здійснювати ефективний контроль за переміщенням працівників та доступом до об'єктів інфраструктури. У зв’язку з цим багато компаній займаються розробкою та вдосконаленням відповідних технологічних рішень.

У межах даної кваліфікаційної роботи поставлено мету розробити технічно та програмно реалізовану кіберфізичну систему контролю доступу на основі мікроконтролера ESP8266 у поєднанні з RFID-зчитувачем. Основний акцент зроблено на підвищенні функціональності таких систем, оптимізації їхньої роботи та забезпеченні можливості інтеграції з мережею Інтернет для збереження даних і дистанційного моніторингу.

_____ 30.05.2025

Підпис студента Дата

ЗМІСТ

ВСТУП

У сфері невпинного стрімкого розвитку технологій стає все більшим попит на ефективні та спеціалізовані кіберфізичні системи, які можуть допомагати з автоматизацією та управлінням найрізноманітнішими типами задач у різних сферах життя.

Кіберфізичні системи це інтегровані рішення, що об'єднують фізичні процеси з комп’ютерними алгоритмами для досягнення високої ефективності, автоматизації та точності. Сфера їх застосування охоплює різні аспекти життя: від управління будівлями до промислових і освітніх систем.

Сучасне суспільство прагне до автоматизації й цифровізації процесів, що дозволяє економити час і ресурси, підвищуючи рівень комфорту та зручності. Одним із важливих напрямів є контроль відвідуваності на підприємствах, офісах або інших організаціях де потрібно постійно відслідковувати кількість працівників на робочих місцях, їхні запізнення чи не вчасне покидання робочого місця або відвідування тим чи іншим студентом навчального закладу та лекцій. Використання кіберфізичної системи на базі Esp8266 дозволяє створити ефективне, недороге та адаптивне рішення, здатне вирішувати завдання моніторингу відвідуваності та передачі даних у хмарні сервіси.

Основною метою цього проєкту є розробка системи для автоматизації збору та обробки даних про відвідуваність будь якого підприємства чи робочого простору із використанням мікроконтролера Esp8266, що передає інформацію про осіб які відвідували підприємство, години входу та виходу з підприємства, дату та їхні контактні данні в Google Sheets для аналізу й подальшого використання.

Особливістю цього проєкту є комбінація фізичних і цифрових компонентів що допомагає системі забезпечувати взаємодію електроних компонентів, що реєструють відвідування, із хмарним сервісом Google Sheets. Використання мікроконтролера Esp8266 є доступним і функціональним рішенням для побудови системи з можливістю передачі даних через Wi-Fi. Також сильними сторонами

системи є те що відвідуваність реєструється в режимі реального часу, а результати автоматично синхронізуються з Google Sheets для подальшого аналізу а адміністратор та користувачі можуть переглядати зібрані дані в Google Sheets, що робить систему зручною для моніторингу

Очікуваним результатом роботи системи є те що система дозволить ефективно контролювати та аналізувати відвідуваність персоналом чи студентами того чи іншого закладу, продемонструє принципи роботи сучасних кіберфізичних систем, інтегруючи апаратну й програмну частини.

Розробка даної кіберфізичної системи є важливим кроком у впровадженні доступних, швидких та надійних автоматизованих систем для повсякденного використання будь де та будь коли.

1 КІБЕРФІЗИЧНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ ДО ПІДПРИЄМСТВА НА ОСНОВІ ESP8266 ТА ПОСТАНОВКА ЗАДАЧІ ЩОДО ЇЇ УДОСКОНАЛЕННЯ

1.1 Аналіз структурних і функціональних особливостей кіберфізичної системи контролю доступу до підприємства на основі Esp8266

На початковому етапі важко усвідомити та уявити собі справжню діючу кіберфізичну систему, її складну будову, алгоритми, програмне забезпечення, сукупність різних деталів мікросхем та інших елементів. Система контролю доступу представленна як сукупність технологічних та програмних рішень спрямованих на забезпечення безпеки та комфорту доступу до приміщень та обєктів і контроль часу проведеного в цих приміщенях. В основі системи як і в кожній іншій кіберфізичній системі лежить мікроконтролер який забезпечує контроль виконання усіх функцій які має виконувати система в залежності від її типу та як її побудували та запрограмували. Мікроконтролер являє собою мозок системи, як мозок людини контролює рухи поведінку, емоції людей так і мікроконтролер обробляє усі вхідні сигнали та відправляє вихідний сигнал до компонентів з наказами, роби так чи не роби так якщо не поданий сигнал.

Спершу необхідно ознайомитися з мікроконтролером, дослідити його архітектуру та проаналізувати основні складові, що забезпечують функціонування центрального елемента системи (рисунок 1.1).

Рисунок 1.1 – Приклад мікроконтролера [1]

Мікроконтролер являє собою мікросхему яка включає в себе сам мікропроцесор який обробляє інформацію, оперативну пам’ять для забезпечення подачі інформації на обробку мікропроцесору та постійну пам’ять в якій зберігається багато інформації про сам мікроконтролер, його порти вводу та виводу інформації, та безпосередньо в цю пам’ять записується код який буде виконувати мікроконтролер. Мікроконтролери деколи ще називають однокристальними мікрокомп’ютерами оскільки їх зазвичай використовують для керування невеличкими електронними пристроями та компонентами. Чому мікроконтролери а не прості процесори як в ноутбуках чи компютерах. Відповідь очевидна, комп’ютерні процесори мають більший розмір вартість та набагато більше споживання енергії в порівнянні з мікроконтролерами які займають мало місця, енергоефективніші та використання цих контролерів пришвидшує час збірки простої кіберфізичної системи, оскільки вони і були створенні для виконання простих завдань.

Насправді мікроконтролери також використовуються в багатьох складних пристроях таких як телефони, смартфони, нове покоління автомобілів, сигналізаціях, датчиках газу чи диму, охоронних системах, системах збору та контролю інформації та ін. Їх основна мета швидко та надійно працювати і виконувати поставленні задачі, наприклад: вони керують різними системами автомобіля такими як гальмування чи ввімкнення вимкнення в автоматичному режимі світла в автомобілі чи виклик пожежних коли датчиком буде виявлено чадний газ або виклик служби газу при детекції високого показнику газу у приміщенні, також вони контролюють виклик охорони якщо на ваше підприємство проникли зловмисники. В цілому без мікроконтролерів не можливо уявити наш світ в теперішній час, та неможливо уявити жодну повноцінну кіберфізичну систему.

Перший мікроконтролер був не такий яким зараз користуємось часто та до яких звикли. Перший контролер розробив в 1971 році інженером англ. Gary W. Boone, він був одним з найкращих співробітників Texas Instruments, ця компанія

думаю знайома багатьом людям та інженерам, оскільки вона є одним з провідних компаній що виготовляє чіпи та контролери. У 1980 році компанія Intel, популярна і одна з двох компаній гігантів на даний час які виготовляють процесори та іншу електроніку, випускає перший мікроконтролер під назвою i8048 а пізніше того ж року його вдосконалену модель i8051 (рисунок 1.2). На той час це був прорив в області електроніки, можливості цього контролера вражали тому він і став революцією в розробці електроних систем та засобів. Термін кіберфізичні системи почав використовуватись у рамках четвертої промислової революції.

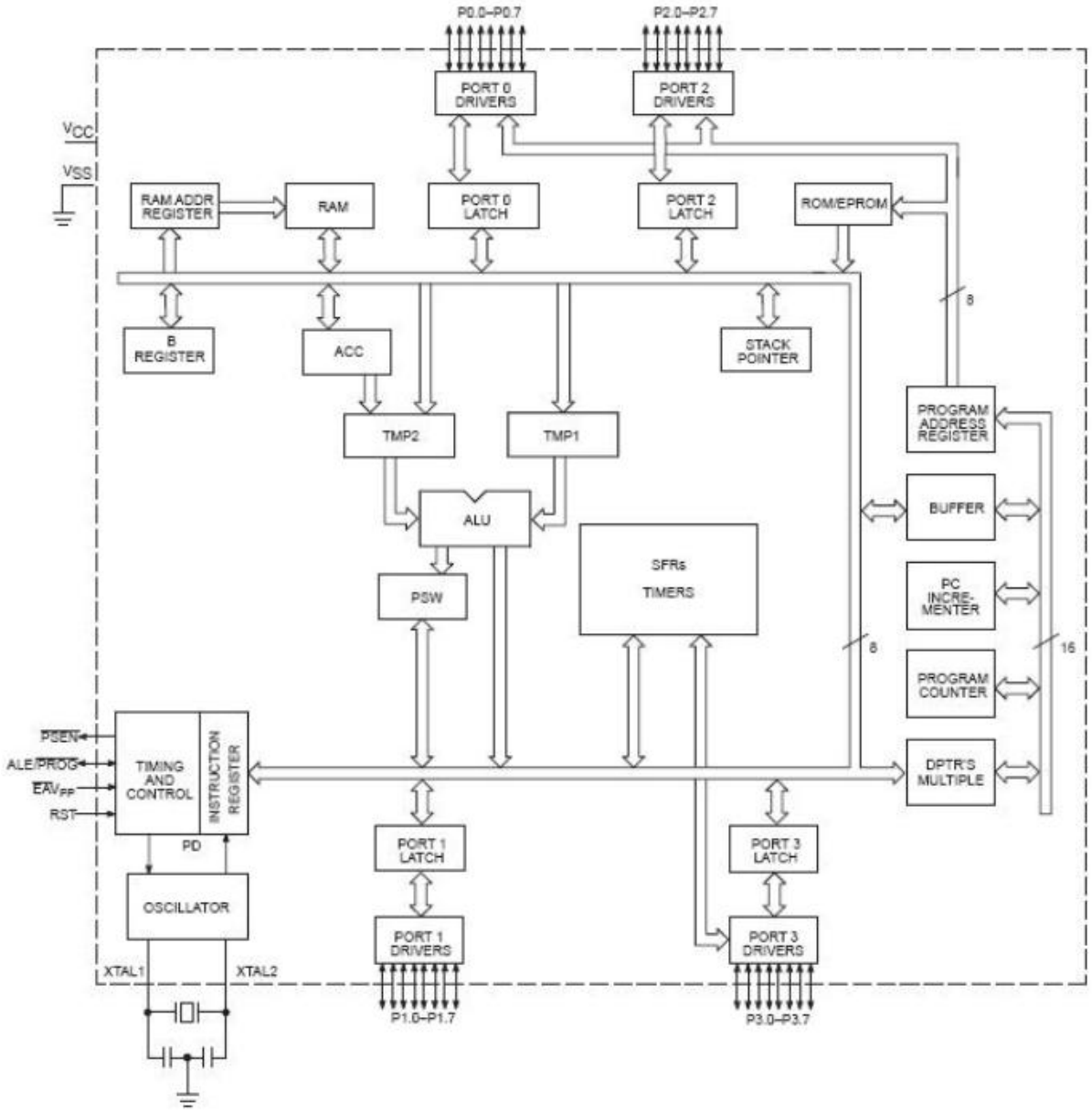


Рисунок 1.2 – Блок-схема мікроконтролера i8051[2]

На початку розробки та проектуванні мікроконтролера доводиться добре вимірювати та проектувати розмір та вартість контролера, цей баланс і є одним з важливих аспектів при розробці але є третій не менш важливий аспект, можна сказати головний, це ефективність та продуктивність мікроконтролера. Усі компанії та виробники намагаються зробити мікроконтролерами малими, гнучкими, ефективним та дешевими, в свою чергу користувачі від них вимагаємо саме цього, ціни якості та ефективності, хто б не хотів отримати ефективний контролер за низьку ціну.

В наш час створена велика кількість функціональних платформ на основі мікроконтролерів за допомогою яких можна створювати та проектувати багато цифрових додатків та кіберфізичних систем. Щоб краще познайомитись з цим сигментом візьмемо для прикладу платформу для розробки Arduino.

Вибір платформи Arduino можна обгрунтувати тим що в даний час ця платформа знаходиться у відкритому доступі для всіх користувачів та розробників і її можна замовити чи купити в будь-якій країні, переваги ардуіно в зручному та компактному розмірі та потужному мікропроцесорі що дозволяє створювати різні цифрові системи і робити їх компактними і зручними для використання.

На сьогоднішній день в світі існує різні формфактори цього типу плат з багатим складом периферії. Багато з них виконано на базі 8-розрядного мікроконтролера Atmel. Для прикладу цього різновиду платформ було обрано ArduinoUno, яка характеризується досить легким середовищем розробки, великим обсягом прикладів розробок та різних систем. Всі ці аспекти дозволяють створювати різної складності функціональні додатки.

Новачку-розробнику краще обрати Arduino, оскільки розробкою на базі цієї плати займається велика кількість користувачів, в результаті чого у відкритому доступі можна знайти достатню кількість готових рішень та проектів, а також контенту навчального характеру. Ці напрацювання будуть дуже доречними в процесі створення власних додатків, а сама платформа передбачає легкий та швидкий спосіб підключення периферії.

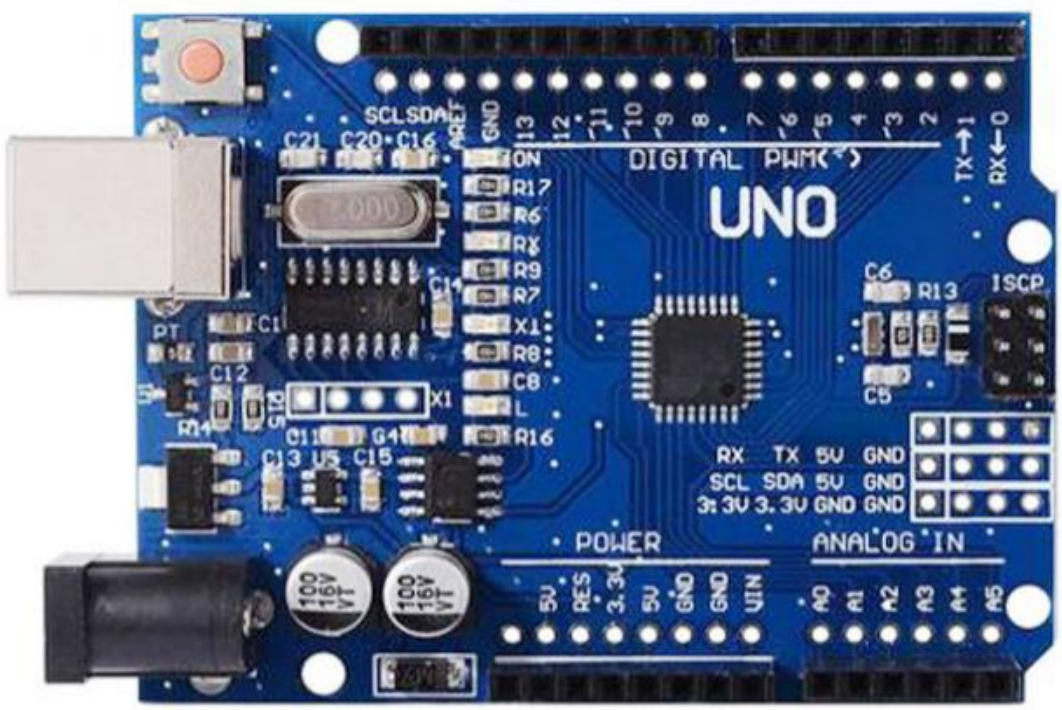


Рисунок 1.3 – Зовнішній вигляд плати Arduino UNO [3]

Плата Arduino Uno (рисунок 1.3) створена на основі мікроконтролера ATmega328P і слугує універсальною апаратною платформою для розробки вбудованих систем. Вона оснащена 14 цифровими входами/виходами, шість із яких підтримують режим широтно-імпульсної модуляції, а також має 6 аналогових входів, кварцовий резонатор на 16 МГц, USB-інтерфейс, роз'єм живлення, інтерфейс ICSP і кнопку скидання. Для початку роботи достатньо з'єднати пристрій із комп'ютером через USB-кабель або подати живлення за допомогою мережевого адаптера.

Основою розробки платформи Arduino була організація найпростішого зв'язку між датчиками, виконавчими механізмами та мікроконтролером без застосування додаткових схем та зєднань, що дозволило б навіть недосвідченому користувачу з базовими знаннями електроніки займатися створенням додатків або пристроїв. Arduino це достатня база для того, щоб отримати початковий досвід, який стане вірним помічником при створенні більш складних проектів і систем.

Розглянемо короткі характеристики плати Arduino UNO що наведено в (таблиці 1.1).

Таблиця 1.1 – Характеристика плати Arduino UNO

Платформа	ArduinoUno
Модель	R3
Орієнтовна ціна	5$
Габаритні розміри	7.5 × 5.3 см
Мікроконтроллер	ATmega328
Тактова частота	16 МГц
ОЗУ	2 Кбайт
Flash-память	32 Кбайт
EEPROM	1 Кбайт
Напруга живлення	7-12 В
Цифровілінії вводу/виводу	14
Аналогові входи	6(10-бітні)
Канали ШИМ	6
Інтерфейс TWI/I2C	2
Інтерфейс SPI	1
Інтерфейс UART	1
Інструменти розробки	Arduino IDE
Порт Ethernet	-
Вага	25 г
Мінімальне енергоспоживання	42 Ма (0.3 Вт)
Максимальна вхідна напруга	20 В
Роз’єм USB	Type D

Окрім мікроконтролерів в системах контролю доступу використовується один з найпопулярніших модулів це RFID-модуль. RFID-модуль популярний тим що він дозволяє відкривати доступ до підприємства не використовуючи звичайний усім відомий металевий ключ та заберає необхідність вводити код доступу при вході чи виході з будівлі підприємства.

Що ж таке RFDI-модуль. RFDI-модуль це пристрій за допомогою якого відбувається зчитування інформації чи запис інформації, він використовує технологію радіочастототної передачі та ідентифікації. Ці модулі дуже популярні у багатьох приміщення та закладах де потрібин надійний захист, швидка ідентифікація, та головне безконтактне відкриття дверей. На даний час RFID-модулів є велика кількість, наприклад:

- RC522;
- PN532;
- RDM6300;
- RDM8800.

Як бачимо модулів є досить велика кількість, що означає що система радіочастотної ідентифікації в сучасному світі стрімко та беззупинно розвивається. Радіочастотна ідентифікація стала незамінною у сучасному світі оскільки її якість та надійність дуже подобаються людям та підприємствам де вона необхідна. Система ідентифікації працює наступним чином, для цього потрібно сам модуль і ключ-карта так званий ключ, в ключ-карті записана вся інформація про людину та ключ доступу за допомогою якого відкриваються двері, людина підносить карту до зчитувача і якщо данні вірні то система моментально зчитує дані за допомогою радіочастотної ідентифікації та дозволяє доступ до приміщення.

З зображень наведених нище (рисунок 1.4) та (рисунок 1.5)можемо зрозуміти що модулі відрізняються один від одного зовнішнім виглядом, але основна різниця між ними полягає в тому що, вони не тільки відрізняються зовнішнім виглядом, формою, розміром але і функціоною складовою та особливостями, через особливості в використанні і було створено так багато видів цих модулів.

В таблиці (таблиця 1.2) наведено порівняльну характеристику основних переваг та недоліків та характеристик різних моделів RFID-зчитувачів.

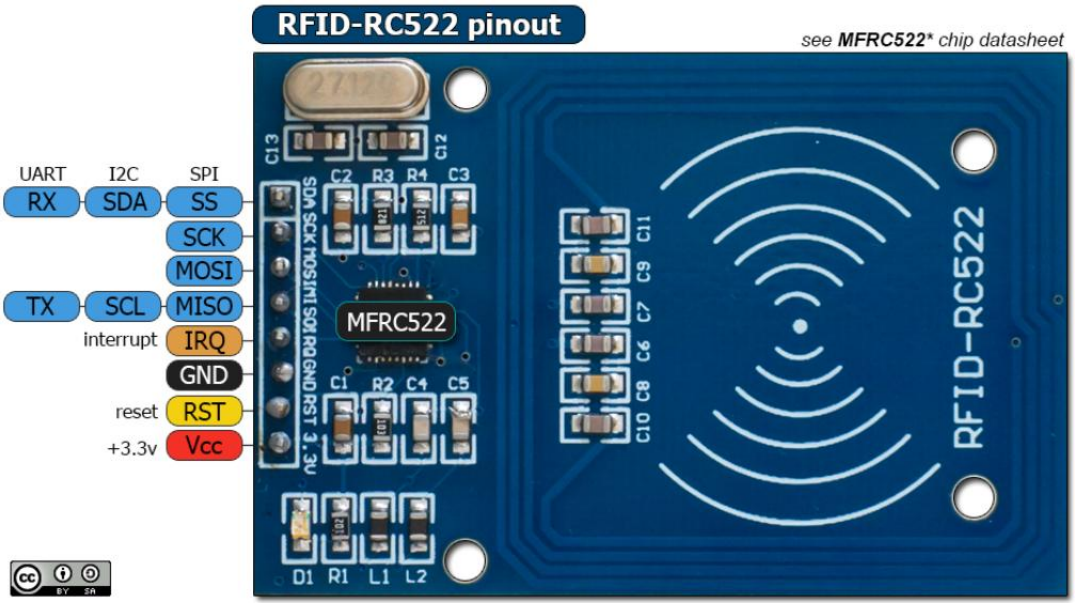


Рисунок 1.4 – Вигляд RFID-модуля RC522 [4]

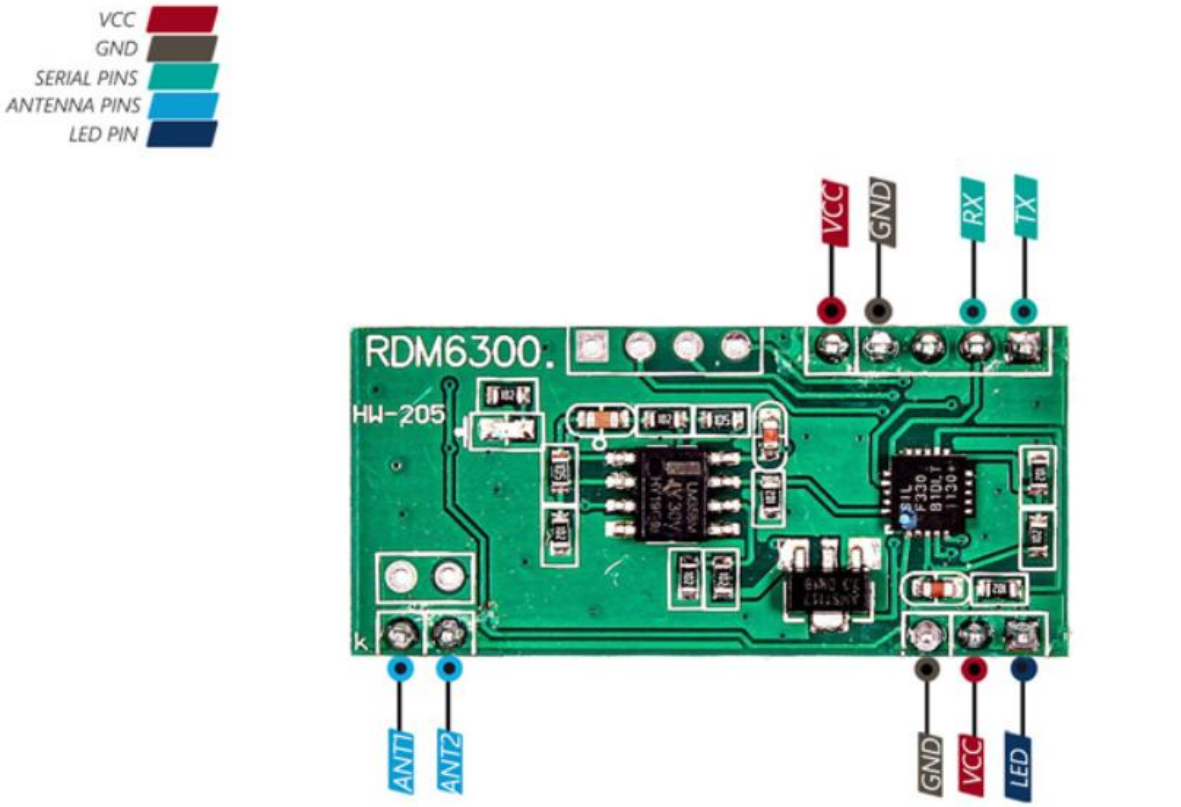


Рисунок 1.5 – Вигляд RFID-модуля RDM6300 [5]

Таблиця 1.2 – Порівняння характеристик популярних RFID-модулів

Назва модуля	Частота роботи	Стандарти	Інтерфейси	Відстань зчитування	Робоча напруга
RC522	13.56 МГц	ISO 14443A	SPI,I²C,UART	2-5 см	3.3 В
PN532	13.56 МГц	ISO 14443A/B, NFC	SPI, I²C, UART	1-7 см	3.3-5 В
RDM8800	13.56 МГц	ISO 14443A	UART	3-5 см	5 В
RDM6300	125кГц	EM4100	UART	8-10 см	5 В

Після детального розгляду різних компонентів з яких створюють та розробляють кіберфізичні системи можна нарешті розглянути та сформувати самий опис, що таке кіберфізична система та що вона собою являє.

Кіберфізична система це механізм, що контролюється або відстежується комп'ютерними алгоритмами і пов'язаний з Інтернетом та його користувачами. В кіберфізичних системах програмне забезпечення тісно повязане з фізичними предметами та компонентами. Компоненти кіберфізичної системи взаємодіють на різних часових та просторових рівнях та можуть мати різні, в залежності від системи моделі поведінки та взаємодіяти одна з одною різними шляхами, які можуть змінюватися в залежності від ситуації. Прикладами кіберфізичних систем можна вважати розумні енергосистеми, безпілотні автомобільні системи, автоматизовані системи керування, робототехнічні системи, самокеровані літальні апарати, відомі і популярні системи розумного будинку та ін.

Для прикладу можна проаналізувати працюючу кіберфізичну систему, це роботичний город у Мічіганському технологічному інституті, в якому команда роботів вирощує томати. Дана кіберфізична система має розділену сенсорну мережу (стан кожної рослини відстежується окремо та данні передаються на

сервер), навігацію, бездротовий зв'язок та власне роботів або ще як приклад Національна лабораторія штату Айдахо, що належить до підрозділів Міністерства енергетики США, вони у себе розробляють за участі приватних компаній та інших спонсорів гнучкі контрольні системи, які будуть застосовуватися на об'єктах критичної інфраструктури. Вся ця робота спрямована на створення комплексного підходу для аналізу тих багатьох аспектів діяльності, які не можуть бути підраховані кількісно, наприклад: кібербезпека, людські відносини, людські емоції, складні взаємозалежності та багато іншого.

1.2 Аналіз відомих автоматизованих систем контролю доступу

Аналіз відомих та працюючих систем керуванням та контролем доступу дає змогу детально розібрати систему, як вона працює, її переваги та недоліки, і не повторювати помилки які зробили розробники в своїх системах.

Для аналізу розглянемо кілька систем:

- SEVEN LOCK.
- RAYKUBE Tuya.
- PES Alabay.

Система доступу SEVEN LOCK (рисунок 1.6) має багато моделей своїх замків, в кожної моделі свої переваги та недоліки. Розглянемо для прикладу розумний дверний замок SEVEN LOCK SL-7740BF.

Замок сконструйовано надійно, корпус ергономічний та зручний, в ручку вмонтований сканер відбитка пальця, та у верхній частині кодовий замок і сканер карти доступу.

Керування та доступ електронним накладним замком SEVEN LOCK SL-7740BF black здійснюється:

1. Відбитком пальця, в базу можна записати 120 шт.
2. ПІН-кодом в базу можна записати 250 шт.
3. Картками / брелками MIFARE (1000 шт.).

4. Механічним ключем (2 шт.).
5. Bluetooth через безкоштовний мобільний додаток.
6. Брелком Bluetooth SEVEN LOCK SR-7716B smart.
7. Wi-Fi.
8. Піднесенням телефону до замка (за допомогою NFC мітки SEVEN R-90).
9. При інтеграції з розумним будинком SEVEN HOME/GOOGLE HOME/AMAZON ALEXA можна керувати замками за допомогою голосу чи смарт сценаріїв.

Рисунок 1.6 – Зовнішній вигляд замка SEVEN LOCK SL-7740BF [6]

RAYKUBE Tuya (рисунок 1.7) - Одна з поширених бюджетних систем контролю доступу китайського виробництва являє собою електронний замок, у якому сканер відбитків пальців інтегрований безпосередньо в ручку. Окрім цього, пристрій оснащений зчитувачем безконтактних карток, а також цифровою клавіатурою, що дозволяє вводити код доступу. Серед основних недоліків такої конструкції можна відзначити низьку продуктивність вбудованого контролера,

характерну для багатьох подібних рішень. Крім того, система функціонує не від блоку живлення або акумуляторів із можливістю підзарядки, а від стандартних батарейок, що суттєво знижує її зручність в експлуатації. Зовнішній вигляд пристрою справляє позитивне враження лише на початковому етапі використання, однак з часом матеріали корпусу втрачають свій вигляд через подряпини та інші механічні пошкодження, що зумовлює необхідність заміни замка.

Рисунок 1.7 – RAYKUBE Tuya [7]

PES Alabay (рисунок 1.8) Цей інтелектуальний замок призначений для вхідних дверей і поєднує функції відеодомофона з технологією розпізнавання обличчя. Система автоматичного замикання, реалізована через моторизований ригель, забезпечує високий рівень безпеки та дозволяє налаштовувати параметри з урахуванням індивідуальних вимог користувача. Ідентифікація особи може здійснюватися за допомогою FACE-ID, біометричного сканера відбитків пальців,

безконтактних карток стандарту MIFARE або NFC, а також через мобільний застосунок Smarta Lock.

Конструкція біометричного замка передбачає інтеграцію відео-вічка та системи розпізнавання обличчя, що розширює його функціональні можливості. Пристрій виготовлено з високоякісних матеріалів і адаптовано до встановлення на масивні металеві або дерев'яні двері. Завдяки надійному мотор-редуктору з внутрішньої сторони корпусу відбувається автоматичне висування сталевих ригелів, що ефективно запобігає силовому відкриванню чи натиску.

Усі компоненти електронної частини та механічної конструкції мають підвищений рівень захисту від вологи, що дозволяє експлуатацію пристрою в умовах підвищеної вологості за умови базового захисту від прямого контакту з водою, наприклад, за наявності козирка над дверима. Замок не оснащено натискною ручкою, а керування ригелями здійснюється виключно за допомогою моторного приводу, розташованого всередині, що істотно підвищує рівень стійкості до несанкціонованого втручання.

Рисунок 1.8 – PES Alabay [8]

1.3 Висновки

У процесі вибору тематики для кваліфікаційної роботи виник інтерес до сучасних систем контролю доступу, їхньої архітектури, принципів функціонування, а також до виявлення сильних і слабких сторін таких рішень. Поглиблене вивчення наявних реалізацій дало змогу сформувати розуміння їхніх конструктивних особливостей і технічних обмежень. На основі проведеного аналізу було виявлено низку можливостей для вдосконалення існуючих систем із урахуванням сучасних вимог до безпеки, надійності та зручності використання.

У сучасних умовах більшість компаній поступово відмовляються від традиційних механічних замків із використанням металевих ключів на користь електронних систем доступу, зокрема на базі технології RFID. Такий перехід сприяє підвищенню рівня захищеності об’єктів, а також забезпечує більшу зручність користування. Проте навіть сучасні реалізації систем доступу нерідко мають суттєві недоліки, зокрема відсутність ефективних механізмів протидії злому й несанкціонованому проникненню. Крім того, слабко розвинений або незручний інтерфейс ускладнює роботу з пристроєм, що негативно впливає на його популярність у деяких сферах застосування.

Однією з ключових проблем електронних замків, які використовують RFID-модулі, є нестабільність джерел живлення, що створює загрозу тимчасової втрати функціональності системи. Також значна частина таких рішень демонструє вразливість до атак із метою пошкодження обладнання або несанкціонованого доступу до приміщення, що ставить під загрозу безпеку майна. З огляду на новизну технології, багато користувачів не мають належного досвіду інтеграції подібних систем у власну інфраструктуру, що ускладнює повноцінне використання їхнього потенціалу. Крім того, складність процесу налаштування може стати бар’єром для пересічного користувача, що, у свою чергу, знижує загальний рівень захисту, який могла б забезпечити система за умови правильної конфігурації.

У наявних реалізаціях також часто спостерігається обмежений обсяг ресурсів, відсутність функціоналу для віддаленого керування, а також неможливість переглядати журнали подій, зокрема списки осіб, які здійснювали вхід або вихід. Ці обмеження суттєво звужують сферу ефективного використання таких систем і створюють потребу в їхньому вдосконаленні. Розгледівши ці проблеми, кваліфікаційна робота була зосереджена на розробку комплексного програмно-технічного засобу для забезпечення перегляду списку доступу до приміщення і контролю хто о котрій годині потрапляв в приміщення та коли покидав його, усе це буде організовано системою на основі дверей з RFID та мікроконтролера ESP8266 в домашньому середовищі. Метою є вирішення недоліку віддаленого перегляду користувачів системи та недоліків шляхом комбінації та з'єднання фізичних та програмних компонентів, розробкою надійних заходів безпеки, створенням ергономічного інтерфейсу для користувачів системи.

Покращуючи відомі рішення, кваліфікаційна робота прагне зробити свій внесок у покращення технології контролю доступу в приміщення, в кінцевому підсумку підвищуючи рівень захищеності, зручність та надійність для власників будинків та підприємств в цілому.

2 ЕЛЕМЕНТНА БАЗА КІБЕРФІЗИЧНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ПІДПРИЄМСТВА НА ОСНОВІ ESP8266

2.1 Кіберфізична система контролю доступу до підприємства на основі мікроконтролера ESP8266 та елементна база

Продовжуючи дослідження та проектування системи контролю доступу на основі мікроконтролера та RFID-модуля, вибір елементів для створення системи і є однією з базових частин проекту. Для проектування та створення кіберфізичної системи контролю доступу до підприємства на основі Esp8266 будуть використовуватися такі компоненти:

1. ESP8266(NodeMCU).
2. Сервопривід.
3. RFID-модуля RC522.
4. Символьний дисплей 1602A LCD.
5. Кабель живлення MicroUSB/Type A.
6. Модуль звуку зумер з динаміком.
7. I2c.
8. Макетна плата разом з джемперними дротами.

Мікроконтролер ESP8266 є компактним і функціональним рішенням китайського виробництва, яке отримало широке застосування завдяки наявності вбудованого Wi-Fi-модуля. Його інтеграція в систему дозволяє реалізовувати бездротове з'єднання без необхідності підключення додаткових периферійних модулів, як це зазвичай потрібно у випадку з класичними Arduino-платами. Крім бездротового інтерфейсу, ESP8266 також підтримує SPI, що забезпечує можливість використання зовнішньої пам’яті для зберігання та виконання програмного коду.

Популярність ESP8266 почала стрімко зростати з 2014 року, коли на ринку з’явилися перші рішення на його базі, що мали суттєву перевагу в ціні порівняно з аналогами. У 2016 році було представлено нову версію ESP8285, яка поєднує всі

функції ESP8266 із вбудованою флеш-пам’яттю обсягом 1 мегабайт, що розширило сферу її застосування.

Однією з особливостей мікроконтролера ESP8266 є відсутність енергонезалежної пам’яті на самому кристалі. Увесь програмний код виконується зі зовнішньої SPI-пам’яті, яка завантажується в кеш інструкцій у міру необхідності. Завантаження здійснюється апаратним шляхом і відбувається прозоро для користувача. Контролер підтримує до 16 мегабайт зовнішньої пам’яті, що забезпечує достатній обсяг для зберігання складного програмного забезпечення. Також реалізована підтримка режимів SPI: стандартного, подвійного або квадро.

Офіційна документація від виробника не розкриває детальної інформації про внутрішню архітектуру та периферійні модулі мікроконтролера. Замість цього пропонується використовувати офіційний набір бібліотек і API для взаємодії з апаратною частиною. У зв’язку з цим у відкритому доступі відсутні точні дані щодо обсягу оперативної пам’яті: зазначено лише приблизний обсяг, що залишається після ініціалізації бібліотек, близько 50 кілобайт. На основі досліджень користувачів, які активно працюють із цією платформою, було встановлено, що контролер містить 32 кілобайти кешу інструкцій і 80 кілобайт оперативної пам’яті для обробки даних.

NodeMCU це плата розробки на основі мікросхеми ESP8266 у версії ESP-12E, яка поєднує UART та Wi-Fi-модуль із низьким енергоспоживанням. Чіп призначений для проєктування пристроїв у сфері інтернету речей, а сама плата оптимізована для швидкої розробки та прототипування. Вона оснащена попередньо встановленим USB-інтерфейсом, стабілізатором живлення та стандартним виводом контактів із кроком 2,54 мм, що дозволяє зручно використовувати її з макетними платами без потреби у паянні. Також не останньою перевагою є наявність прошивки NodeMCU, яка дає можливість програмування на мові Lua або через середовище Arduino IDE, що значно полегшує процес розробки застосунків для різних кіберфізичних систем та пристроїв. Плата мікроконтролера ESP8266 зображена на (рисунку 1.9).

Таблиця 2.1 – Основні характеристики плати ESP8266:

Параметр	Значення
З'єднання	WiFi 802.11 b / g / n.
Режими	Підтримка STA / AP / STA + AP режимів
Протоколи	Вбудований стек протоколів TCP / IP з підтримкою множинних клієнтських підключень
Цифрові піни	Цифрові піни D0-D8, SD1-SD3:
Вихідний струм	15 мА
Напруга живлення	4.5-9В, також можливе живлення від USB
Швидкість передачі даних	110-460800 б/сек.
Інтерфейси передачі даних	UART та GPIO інтерфейси
Відстань між контактами	28мм
Робоча температура	Від -40 до +125 °С
Вага	18 г

Конкурентом плати ESP8266 (рисунок 2.1) є плата ESP32 (рисунок 2.2) яка була створена у 2016 році.

Особливістю цього мікроконтролера є інтегровані контролери Wi-Fi та Bluetooth що забезпечують з'єднання мікроконтролера з багатьма іншими пристроями які мають дані мережеві інтерфейси в своїй системі.

Як і ESP8266 ця плата також є енергоефективною та має компактний дизайн і розміри. У серії ESP32 використовується мікропроцесор Tensilica Xtensa LX6 в двоядерних та одноядерних варіаціях та обєднує в собі вбудовані антенні перемикачі, радіочастотний балун, підсилювач потужності, приймач з низьким рівнем шумів, фільтри та модулі керування живленням. ESP32 створений та розроблений компанією Espressif Systems, це китайська компанія яка розташована

у місті Шанхай, а самим виготовленням займається інша компанія, яка має назву TSMC.

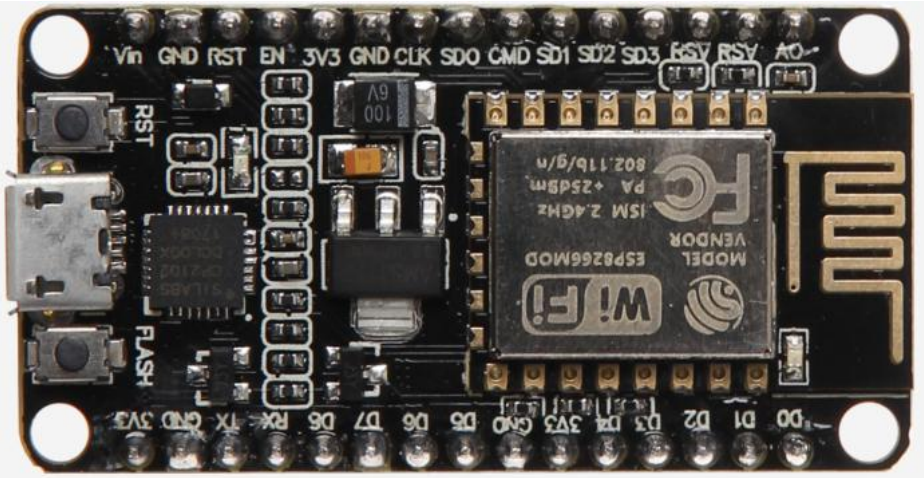


Рисунок 2.1 – ESP8266 [9]

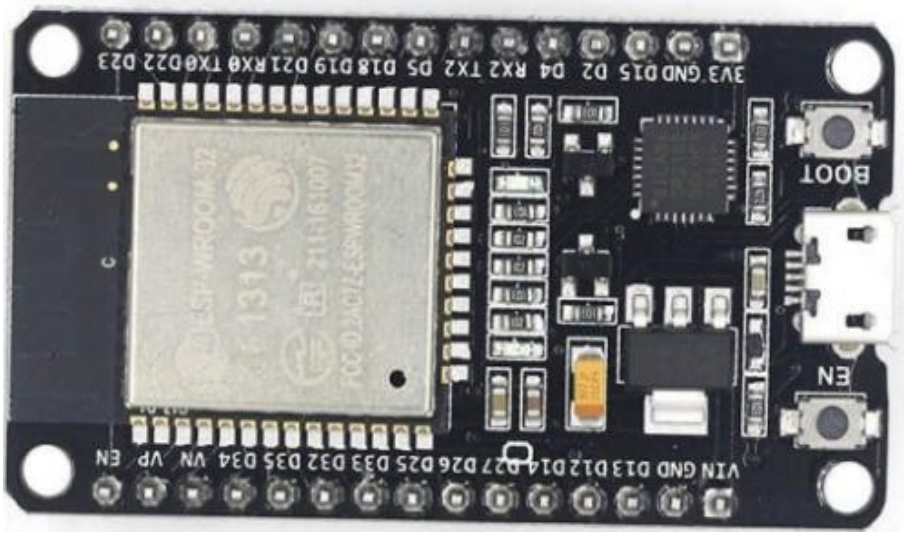


Рисунок 2.2 – плата ESP-WROOM-32 ESP32 [10]

В таблиці (таблиця 2.2) яка наведена нижче зроблено порівняння цих двох плат щоб детальніше розглянути їх характеристики та основні відмінності, а також переваги та недоліки кожної плати і визначитись яка з цих двох плат підходить для виконання того чи іншого завдання, та обрати ідеальне рішення для створення кіберфізичної системи контролю доступу до підприємства чи інших будівель та установ.

Таблиця 2.2 – Порівняльна характеристика плат

Характеристика	ESP8266	ESP32
Кількість ядер CPU	1 ядро, Tensilica L106	2 ядра, Tensilica Xtensa LX6
Тактова частота, МГц	80-160МГц	200-260МГц
ОЗП, Кб	50 Кб	520 Кб
Пам’ять модуля	512 Кб-16 Мб	16 Мб
Наявність Wi-Fi	802.11 b/g/n	802.11 b/g/n
Наявність Bluetooth	Відсутній	BLE + Bluetooth Classic
GPIO контакти	11	30-36
Аналогово Цифровий Перетворювач (АЦП)	1 канал	12 каналів
Цифро Аналоговий Перетворювач (ЦАП)	Немає	2 канали
Широтно-імпульсна модуляція(PWM)	Доступна	Доступна
Слот для підключення microSD карти	Немає	Підтримується формат карти SDIO
Споживання енергії	Низьке	Низьке
Підтримка інтерфейсів SPI / I²C / UART	Наявна але є певні обмеження	Є можливість підключати кілька інтерфейсів
Ціна	2-3 $	4-8$
Вага	8 г	12 г

Мікроконтролер ESP8266 був вибраний через його можливості такі як, Wi-Fi модуль який вбудовано в нього, досить невелику вартість на теперішній час, а також через сумісність з Arduino IDE для досить швидкого та ефективного програмування. Для даного проекту цілком достатньо його характеристик, хоча як

бачимо з порівняльної таблиці (таблиця 2.2) мікроконтролер ESP32 має більшу ефективність, але для проекту цілком підходить ESP8266, для керування RFID зчитувачем та числовим дисплеєм йому вистачає пам’яті та швидкості процесора.

Мікроконтролер ESP8266 є центром усієї кіберфізичної системи, за допомогою мікроконтролера відбувається зчитування данних ключ-карт через RFID-модуль, також він виводить інформацію про доступ на дисплей та вмикає звук буззера якщо сталась помилка чи доступ відхилено, також він обробляє інформацію яку зчитує, підключається до точки доступу Wi-Fi та через MQTT протокол відправляє запити до Google Sheets на внесення даних у таблицю.

Живиться ESP8266 від USB або від 3.3-5 В яке можна подати з батареї, також від плати буде живитися сам зчитувач RFID-RC522 (рисунок 2.3). Для живлення ESP8266 можна використати дешеві та дуже поширені LI-Ion акумулятори 18650, для прикладу аккумулятор SAMSUNG INR 18650 (рисунок 2.4) в якого місткість 2900 мА/год, з номінальною напругою 3.7 В та з максимальним струмомо заряду 8.25 А, вага такого акумулятора всього 48 г

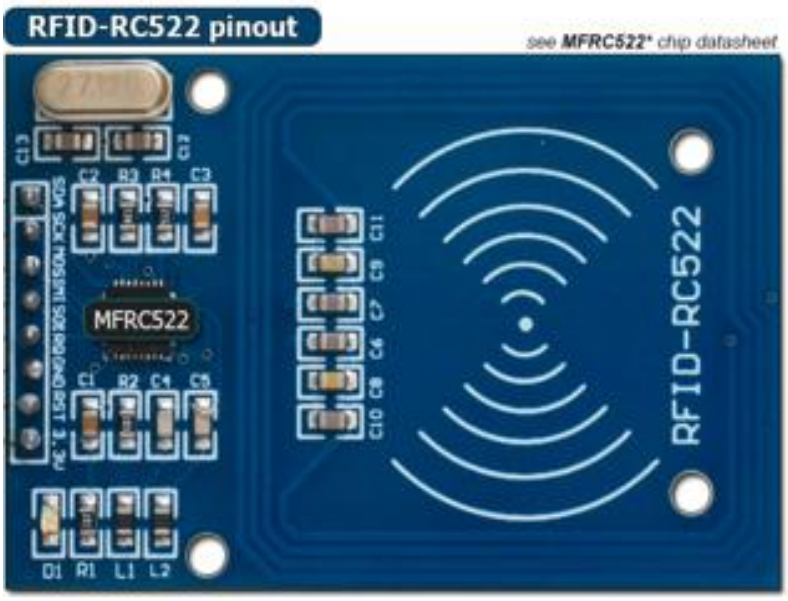


Рисунок 2.3 – Зчитувач RC522 [4]

Рисунок 2.4 – Samsung INR18650 29E 2900 mAh E7[11]

Даний акумулятор, вироблений у Південній Кореї, вирізняється серед аналогів того ж форм-фактора підвищеною реальною ємністю та здатністю віддавати великі струми, що робить його придатним для широкого спектра застосувань. Його активно використовують у сфері перепакування акумуляторів ноутбуків, у шуруповертах та подібних портативних електропристроях. Останнім часом популярність елемента суттєво зросла через активне використання в акумуляторних збірках для безпілотних літальних апаратів, зокрема дронів. Завдяки своїм характеристикам цей акумулятор також ідеально підходить для живлення сервоприводів, які приводять у дію механізм відкривання дверей та виконують контроль доступу. Після ідентифікації користувача сервопривід автоматично зачиняє двері через декілька секунд, запобігаючи несанкціонованому проникненню сторонніх осіб.

У межах створення кіберфізичної системи, яка була реалізована в ході цієї кваліфікаційної роботи, було використано символьний LCD-дисплей 1602A.

Основними критеріями вибору стали доступна вартість, надійність та простота інтеграції з мікроконтролером. Для роботи з дисплеєм необхідно лише підключити відповідні виводи до контролера та забезпечити його живлення. В середовищі розробки Arduino IDE передбачено стандартну бібліотеку “LiquidCrystal”, яка суттєво спрощує виведення інформації на дисплей. Освоїти принципи роботи з цим компонентом не становить труднощів, оскільки Arduino IDE також містить приклади застосування.

У рамках проєкту дисплей буде використовуватись для відображення поточного стану системи: зокрема, індикації її активності, статусу підключення до точки доступу та наявності з’єднання з мережею. Крім того, на екрані відображатимуться дані після зчитування ідентифікатора ключ-карти або RFID-мітки, що дозволить користувачеві оперативно отримувати підтвердження успішного доступу.Базові характеристики LCD дисплея описані в таблиці(таблиця 2.3).

Таблиця 2.3 – Базові характеристики LCD 1602A дисплея

Параметр	Характеристика
Розмір	80×36 мм
Діапазон робочих температур	Від 0 до 50 °C
Підсвітка	Зелена або синя
Колір символів	Чорний
Розмір символів	4.35×2.95 мм
Формат	16×2
Інтерфейс	HD44780
Видима область	64.5 × 13.8 мм
Живлення	5 В
Орієнтовна ціна	2 $

Для зручного підключення LCD дисплея (рисунок 2.5) до мікроконтролера і щоб зробити підключення простішим, підключення в данному проекті буде здійснюватися через так званну послідовну шину для зв’язку інтегральних схем I2c.

Стандартний I2c інтерфейсний модуль базується на мікросхемі PCF8574T для збільшення кількості портів вводу/виводу для контролерів Arduino чи ESP, мікроконтролерів STM8 та STM32 також для мінікомп’ютерів Raspberry Pi, Orange Pi, Banana Pi, Rock64, Arduino Mega. Він може бути використаним як інтерфейсна плата для підключення дисплеїв 1602 і 2004, так і як окремий пристрій. Для

встановлення та налаштування контрастності дисплея в платі є вбудований змінний резистор. Для оптимальної роботи дисплея потрібно відрегулювати його контрастність за допомогою змінного резистора що знаходиться на платі.

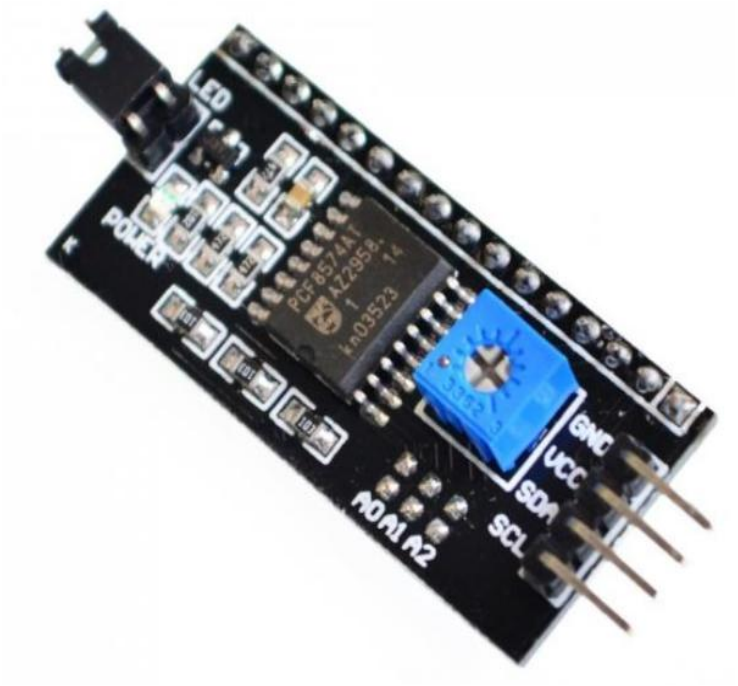


Рисунок 2.5 – I2c модуль розширення виводів Arduino для підключення LCD дисплея [12]

Максимальна кількість модулів одного типу що можуть бути підєднаними до модуля з I2C інтерфейсом становить 8 одиниць, оптимальна робоча напруга живлення для модуля 5 В, цей модуль повністю сумісний з всіма мікроконтролерами типу Arduino та ESP

Контакти цього модуля потрібно запаяти на відповідні контакти дисплея а далі контакти які призначені для живлення та виводу інформації з’єднати з мікроконтролером за допомогою джемперних дротів.

Провода цього розміру ідеально підходять для пайки та з’єднання дрібних компонентів мікроконтролера. Або якщо не потрібно збирати дану систему на довготривалий термін можна використовувати макетну плату та джемперні дроти.

Макетна плата (рисунок 2.6) це основа на якій відбувається розробка прототипів електронних пристроїв до їхньої повної збірки, джемперні дроти створенні для того щоб їх використовували з цією платою для з’єднання компонентів. Макетна плата та джемперні дроти забезпечують надійне з’єднання без використання методу пайки, а також за допомогою них можна корегувати зміни у збірці.

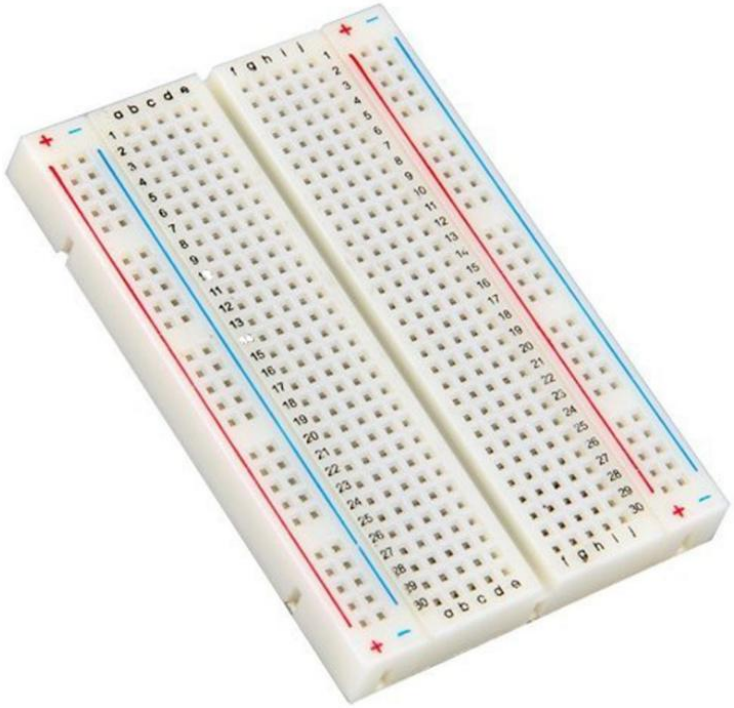


Рисунок 2.6 – Макетна плата для Arduino [13]

Візуальний користувацький інтерфейс не потребує візуалізації за допомогою розробки програми, за основу взято надійне програмне забезпечення від Google, а саме Google Sheets в якому буде здійснюватися вивід усієї інформації що опрацьовує мікроконтролер.

Інтерфейс користувача дозволяє людям взаємодіяти з системою, робити налаштування безпеки та взаємодіяти з програмою. Одним з варіантів взаємодії з системою є фізичні кнопки чи сенсорна панель які доповняються різного типу дисплеями для візуального відображення інформації про події що відбулись в системі або дані користувача які були введені. Якщо інтегрувати систему в

мобільний пристрій в вигляді веб-додатка чи програми, цим можна покращити зручність користування та віддаленого налаштування. В пропонованій системі сканер RFID зчитує дані з ключа та передає дані на обробку ESP8266 а сам мікроконтролер після обробки використовуємо HTTPSRedirect формуємо запит і робимо публікацію у гугл таблицю у певні колонки.

Якщо користувач піклується про заходи безпеки і остерігаєтесь що систему може бути пошкоджено чи взламано зловмисниками, можете переконатися на практиці що, захист системи відбувається безпосередньо через захист вашого облікового запису гугл, якщо він захищений нема причин для паніки, також важливо щоб ключ доступу до таблиці через який відбувається спілкування мікроконтролера ESP8266 та безпосередньо Google Sheets не був втраченний або переданий сторонім особам.

Google Таблиці це додаток для роботи з онлайн таблицями, його перевага в тому що він є безкоштовним та доступним усім. Google Таблиці доступні з будь якого пристрою який має доступ до інтернету, популярність гугл таблиць в тому що ти можеш редагувати та вносити зміни будь коли навіть не маючи доступу до інтернету, і коли доступ знову з’явиться данні автоматисно і швидко синхронізуються з таблицею.

Google Таблиці (рисунок 2.7) є багатофункціональним інструментом для відстеження та аналізу даних а також в цьому сервісі є багато інструментів для перегляду статистик графіків та відстеження прогресу.

Якщо дані були видалені помилково, Google Sheets зберігає останню історію змін і є можливість легко відновити втраченні дані, також можна переглянути які правки вносили користувачі яким був наданий доступ.

Таблиці Google служать інструментом для спільного багатокористувацького редагування електронних таблиць в режимі реального часу. Також в застосунку є функція чату на бічній панелі що дає змогу користувачам повідомляти та коментувати зміни. Історія змін дає змогу користувачам бачити що нового було внесено в документ, а всі користувачі які вносили зміни відрізняються різними

кольорами. Таблиці які були побудовані в додатку Google Sheets, можна експортувати на комп'ютер користувача у різних форматах.А також пізніше розробити різні фільтри та статистику для моніторингу часу роботи та продуктивності працівників.

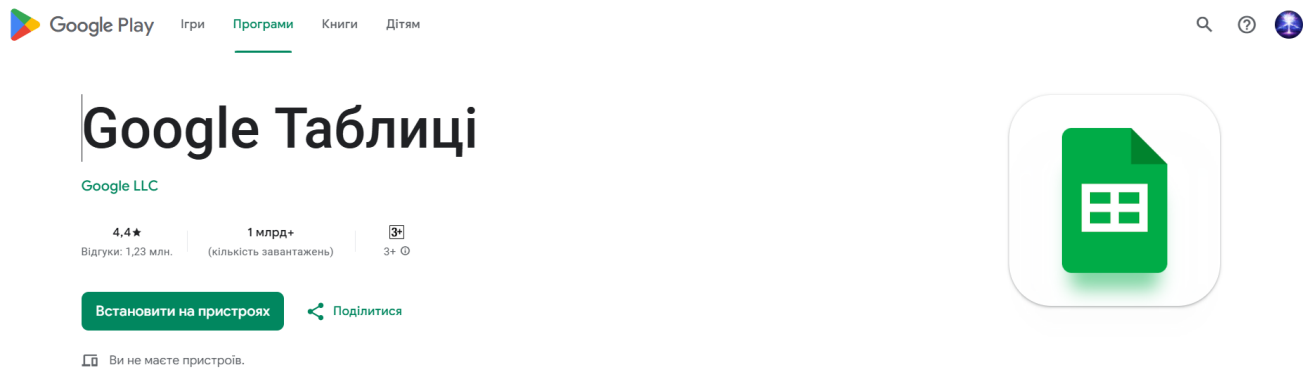


Рисунок 2.7 – Вигляд додатку Google Таблиці у магазині додатків Google Play[14]

При виборі елементної бази потрібно завжди робити баланс та підраховувати вартість системи, користувачів завжди цікавитть економічність системи, але також не потрібно забувати про ефективність системи, наврятчи користувач хоче дешеву систему яка через тиждень почне працювати погано чи зламається взагалі, тому економія економією але компоненти потрібно підбирати якісні, також у вартість системи потрібно при рахунку компонентів враховувати вартість збірки та монтажу, щоб система не була дуже складна в експлуатації та монтажу з налаштуванням.

При правильному підбору якісних комплектуючих та правильній збірці компонентів в один пристрій отримуємо ефективну кіберфізичну систему на основі мікроконтролера ESP8266 та RFID зчитувача.

Для початку розробки великої системи це є гарним стартом і початком розвитку новітньої системи контролю доступу до підприємства і забезпечення виконання вимог працівників та керівників підприємств.

2.2 Принципи функціонування кіберфізичної системи доступу до підприємства на основі мікроконтролера ESP8266

Щоб зрозуміти, як працює створена система, спочатку варто розглянути її склад і основні функції. Система контролю доступу побудована на базі RFID-зчитувача, що працює разом із мікроконтролером ESP8266. Основне завдання цієї системи зчитування інформації з карток або міток, перевірка її достовірності та, у разі успіху, запис даних про візит користувача (зокрема час і дату) до електронної таблиці Google Sheets.

У складі пристрою є кілька основних елементів. Найважливішим серед них є мікроконтролер ESP8266 (NodeMCU), який обробляє дані, керує RFID-зчитувачем, зв'язується з інтернетом і передає інформацію до таблиці. Сам RFID-зчитувач використовується для ідентифікації користувача він зчитує інформацію з картки або RFID-тега, яка є унікальною для кожної особи.

Система не містить фізичного замка, але конструкція дозволяє додати сервопривід, що підключений до плати, вже зараз може відкривати і закривати двері у разі дозволу на вхід. Джерелом живлення може бути як стандартна розетка, так і батарея, яка забезпечує роботу всіх компонентів від зчитувача до дисплея.

LCD-дисплей формату 16x2 виконує роль індикатора, показуючи повідомлення про стан системи: наприклад, чи надано доступ, чи користувач не впізнаний, а також інші супровідні дані (дата, ім'я тощо).

Програмна частина містить спеціальну прошивку для ESP8266, яка керує всім процесом від зчитування тегів до передавання інформації в хмару. Вся логіка поведінки пристрою реалізована у вигляді послідовних кроків, які виконуються автоматично при кожному ввімкненні.

Коли система запускається, мікроконтролер спочатку готує до роботи зчитувач та дисплей, після чого намагається під'єднатися до Wi-Fi мережі. Якщо з'єднання встановлено успішно, пристрій готовий до взаємодії з користувачем. При піднесенні тега до зчитувача відбувається зчитування інформації та її перевірка.

Якщо все збігається з тим, що збережено в системі, на екрані з’являється повідомлення про дозвіл на вхід, двері відкриваються, а в таблицю записується час ідентифікації. Якщо ж дані не розпізнано або тег неправильний користувачу буде відмовлено в доступі, про що він також буде проінформований через дисплей і звуковий сигнал. У майбутньому можна передбачити й автоматичне повідомлення охорони у разі підозрілої активності.

Таким чином, система працює як повноцінний електронний помічник, який забезпечує облік відвідувань та контроль за тим, хто саме отримує доступ до приміщення.

2.3 Огляд систем одноплатних комп'ютерів та HTTPS POST-запитів

Одноплатні комп’ютери активно застосовуються у складі промислових систем, кіберфізичних рішень, апаратно-програмних засобів та пристроїв Інтернету речей (IoT). Згідно з останніми статистичними даними від виробників та дистриб’юторів, значна частина фахівців у галузі електроніки та програмування використовує одноплатні комп’ютери (SBC) у виробах промислового та комерційного призначення. Серед усього різноманіття пристроїв найбільшу популярність отримала плата Raspberry Pi (рис. 2.8), яку обирає близько 44% розробників. На другому місці за популярністю знаходиться плата Arduino, яку використовує понад 28% інженерів. Третю позицію займає платформа BeagleBoard від компанії Texas Instruments з часткою приблизно 6%.

Одноплатний комп’ютер представляє собою електронний пристрій, у якому всі основні апаратні елементи розміщені на одній друкованій платі. Спочатку такі пристрої орієнтувались переважно на промислове застосування, однак із розвитком електронної компонентної бази та зростанням потреб у мініатюризації вони стали використовуватись і в побутових та офісних умовах.

На відміну від класичних настільних ПК, більшість одноплатних комп’ютерів не мають повноцінних інтерфейсів для підключення широкого

спектра периферійного обладнання. Це обмежує їх функціональність у загальному користувацькому середовищі, проте не є критичним для спеціалізованих технічних задач.

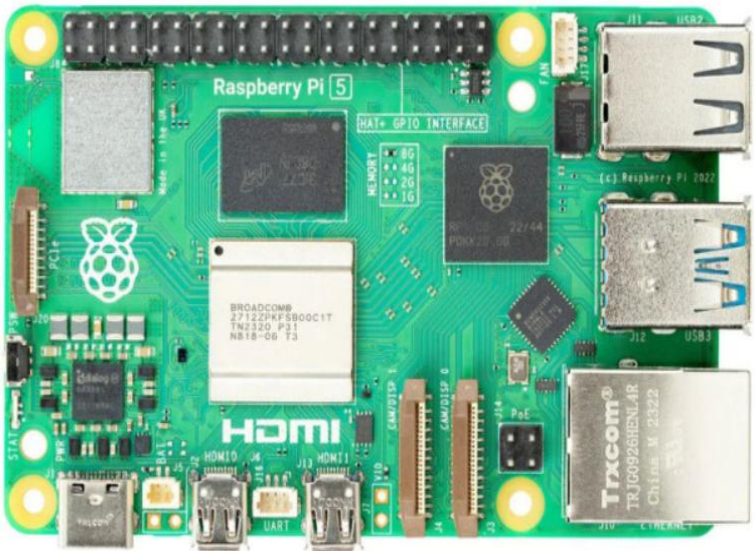


Рисунок 2.8 – Одноплатний комп’ютер Raspberry Pi 5 4Gb [15]

Серед найпоширеніших варіантів одноплатних комп’ютерів виділяють ті, що побудовані на основі стандартизованих форм-факторів, призначених для встановлення в задню частину комп’ютерного корпусу. До таких рішень належать CompactPCI, PXI, VMEbus, VXI та PICMG. Ці стандарти знайшли широке застосування в промислових та спеціалізованих комп’ютерних системах.

Одноплатні комп’ютери створювалися на основі різноманітних апаратних архітектур. Деякі з них побудовані навколо архітектури Intel, інші на базі енергоефективних обчислювальних структур, зокрема RISC та SPARC. Часто використовуються також багатоядерні процесори, що забезпечують можливість паралельної обробки даних. У таких системах типова для архітектури Intel схема передбачає, що основні логічні вузли розташовані на окремих модулях, які підключаються до загальної пасивної шини. У підсумку формується конфігурація, схожа на традиційну материнську плату, але з чітко визначеною топологією слотів.

Однією з найвідоміших і доступних платформ у цій категорії є Raspberry Pi одноплатний комп'ютер, розроблений у 2012 році благодійною організацією Raspberry Pi Foundation у Великій Британії.

Початково проєкт мав на меті популяризувати основи інформатики серед школярів і студентів, зокрема ознайомити їх із базовими принципами роботи комп'ютера та операційної системи. Проте після появи перших моделей Raspberry Pi швидко набув широкого визнання й у професійних галузях, зокрема в медицині, системах автоматизації, кіберфізичних системах, а також в інтелектуальних системах безпеки та контролю доступу.

Через популярність платформи, для неї був згодом розроблений спеціальний дистрибутив операційної системи на базі Debian, Raspbian OS (Raspberry Pi OS). Цей дистрибутив оптимізований для апаратних особливостей плати, має попередньо встановлені прикладні програми, зокрема офісні пакети (KOffice) та веббраузер Iceweasel.

Крім того, було впроваджено спеціалізований магазин застосунків Pi Store, де користувачі можуть завантажувати як безкоштовне, так і комерційне програмне забезпечення. Основною мовою програмування, яка використовується для роботи з Raspberry Pi, є Python одна з найбільш популярних мов у сфері освітніх і прикладних проєктів.

З огляду на широке розповсюдження та активне використання Raspberry Pi в технічних рішеннях, подальший аналіз одноплатних комп'ютерів доцільно проводити на прикладі сучасної моделі цієї платформи Raspberry Pi 5 (рисунок 2.8).Основні характеристики плати та її опис можна переглянути у таблиці (таблиця 2.4).

У таблиці (таблиця 2.5) проведено опис та порівння характеристик двох одноплатних комп'ютерів одного виробника, а саме Raspberry Pi 4 4Gb та Raspberry Pi 5 4Gb які є актуальні на даний час, та широкозастосовуються у розробках систем Інтернету речей (IoT).

Таблиця 2.4 – Основі характеристики плати Raspberry Pi 5

Характеристика	Опис
Процесор	Чотириядерний 64-бітний Arm Cortex-A76, 2.4 ГГц
Графічний процесор	VideoCore VII, 800 МГц, з підтримкою OpenGL ES 3.1
Оперативна пам’ять	4 ГБ
Зберігання данних	Підтримка microSD та SSD (через інтерфейс M.2)
Бездротові інтерфейси	Wi-Fi 802.11ac (2.4/5 ГГц), Bluetooth 5.0
Роз’єми USB	USB 3.0, USB 2.0
Відеовиходи	micro HDMI
Мережевий інтерфейс	Gigabit Ethernet
Системна шина	PCIe 2.0 x1

Після опрацювання даних про представлені одноплатні комп’ютери можна зробити висновки про характеристики плат та підібрати найкращу яка підходить для вибраного проекту.

Таблиця 2.5 – Порівняння одноплатних комп’ютерів

Комплектуючі	Raspberry Pi 4 4Gb	Raspberry Pi 5 4Gb
Процесор	4× Cortex-A72 @ 1.5 ГГц	4× Cortex-A76 @ 2.4 ГГц
Графічний процесор	VideoCore VI @ 500 МГц	VideoCore VII @ 800 МГц
Оперативна пам’ять	LPDDR4 @ 3200 МГц	LPDDR4X @ 4267 МГц
HDMI	micro HDMI (4Kp30)	Micro HDMI(4Kp60)
USB	USB 3.0, USB 2.0	USB 3.0, USB 2.0
Бездротове з’єднання	802.11ac / Bluetooth 5.0	802.11ac / Bluetooth 5.0

Розглянемо принцип дії HTTP POST-запитів, що лежать в основі функціонування розроблюваної системи. Метод POST (рисунок 2.9) є одним із

стандартних методів, підтримуваних протоколом HTTP, який широко застосовується для передачі даних у мережах, зокрема в Інтернеті. Основним призначенням методу POST є ініціювання запиту до вебсервера з одночасною передачею інформації у тілі HTTP-повідомлення. Передані дані, як правило, зберігаються сервером для подальшої обробки.

Метод POST найчастіше використовується у випадках, коли потрібно передати на сервер дані з вебформи або завантажити файли. На відміну від нього, метод GET застосовується для отримання даних із сервера. У GET-запитах частина інформації, така як параметри або умови вибірки, передається безпосередньо в URL-адресі, що може мати обмеження за обсягом переданих даних і впливає на рівень безпеки.

Завдяки можливостям POST-запитів, система, заснована на мікроконтролері ESP8266, зможе передавати зібрані дані (наприклад, ідентифікатори користувачів RFID) у зовнішній вебсервіс або безпосередньо до Google Sheets для подальшого збереження й аналізу.

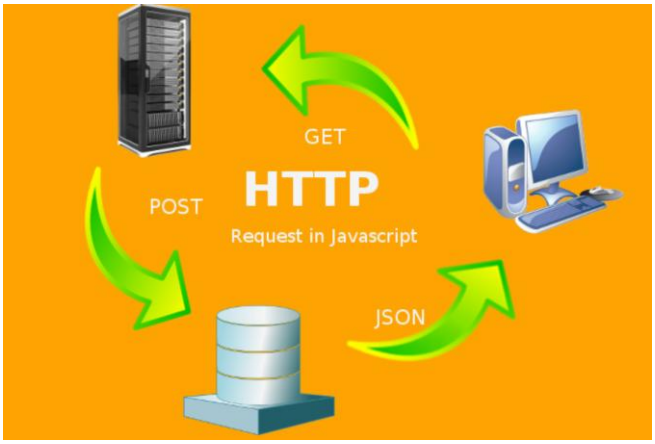


Рисунок 2.9 – Приклад роботи метода POST та GET [16]

Всесвітня павутина Інтернет і протокол HTTP грунтується на різних методах для створення запитів, основні це POST, GET, PUT, DELETE і також багато інших. Інтернет браузери майже завжди користуються методами GET і POST, але REST онлайн-додатки потребують використання багатьох інших. Метод POST

призначений для надсиланя запиту на сервер нової інформації, так що вона зберігатиметься як підресурс для якогось ресурсу. Доприкладу, для URL http://mosquitto.com/admin використовуючи POST запит можна було б записувати та добавляти нових адмінів, в кожного з яких метод містив би прізвище, адресу та інші дані.

2.4 Електричні характеристики пропонованої кіберфізичної системи

Розглядаючи електричні характеристики пропонованої кіберфізичної системи можна визначити основні деталі системи.

Джерелом живлення системи при розробці і тестуванні було використано живлення напряму від кабеля microUSB, живлення USB вистачало для запуску мікроконтролера RFID- модуля та екрана, але при збірці готового пристрою бажано зробити живлення від батареї наприклад 18650 на 4.2В чи крону на 9 В з стабілізатором напруги щоб отримати на виході 5 В. При підключенні на вихід мікроконтролера завжди існує небезпека під час підключення механічних/магнітних пристроїв таких як мотори чи реле в одному колі з мікроконтролерами/логічними вентилями. Силові пристрої є шумними та видають зворотний зв'язок, який потрібно фільтрувати використовуючи фільтри чи конденсатори, щоб не відбулося виведення з ладу електроніки. Силові пристрої також є досить енергоспоживаючими, що може призвести до падіння напруги під час ввімкнення. Дані падіння можуть призвести до помилок та навіть скидання налаштувань в електроніці на логічному рівні.

Підключення мікроконтролера ESP8266 до компонентів: контакт VCC ESP8266 підключений до шини яка видає 3.3 В на макетній платі. Контакт GND ESP8266 підключений до шини заземлення яка є спільною для всіх компонентів. Контакти GPIO ESP8266 підключені до керуючих контактів динаміка та символьного LCD дисплея.

Модуль зчитування RFID RC522: контакт VCC підключений до 3.3 В. Контакт GND підключений до заземлення. SPI контакти (SDA, SCK, MOSI, MISO, RST, IRQ) підключені до відповідних контактів на мікроконтролері ESP8266.

Модуль звуку зумер з динаміком: Пін керування підключений до шини GPIO. Пін GND підключений до землі.

LCD символьний (I2C) Контакт VCC підключений до контакту VIN на платі ESP8266. Пін GND підключений до шини землі. Піни SDA та SCL підключені до відповідних GPIO виходів на ESP8266 для I2C-зєднання.

Сервопривід підключений на відповідні контакти GND VCC та сигнальний контакти по якому безпосередньо відбувається передача сигналу для відкриття та закриття дверей щоб забезпечити вхід та вихід персоналу з підприємства в обідній та робочий час, а саме обід чи відлучення по поважній причині яка була обговорена з керівництвом.

У наведеній таблиці наочно продемонстровано схему підключення компонентів системи, що дозволяє легко орієнтуватися у з'єднанні елементів.

Таблиця 2.5 – Підключення компонентів системи

Компонент	Контакти з'єднаня	Вимоги до напруги споживання	Значення в системі
Батарея	V+ та GND	3.3-5 В	Використовується для живлення всієї системи.
ESP8266	VCC: 3.3 В, GND: GND, Контакти GPIO: Підключені до відповідних контактів RFID, LCD та модуля звуку.	3.3 В	Перетворює за необхідності вхідні 5 В до 3.3 В для нормальної роботи компонентів системи.

Закінчення Таблиці 2.5 – Підключення компонентів системи

Модуль звуку зумер з динаміком	GND: GND, PIN2: GPIO контакт на платі ESP8266.	3.3 В	Призначений для звукового сигналізування стану системи, відіграє роль сигналізації.
LCD символьний дисплей з I2C	VCC: VIN, GND: GND, SDA, SCL: підключені до GPIO контактів ESP8266	5 В	Відображає стан системи та інформацію про користувача.
Сервопривід	VCC,GND та сигнальний контакт який підключений до ESP8266	3.3 В	Займається відкриванням та закриттям вхідних дверей.
RFID-зчитувач RC522	VCC: 3.3В шина, GND: GND, SDA,SCK,MOSL,MIDO,RST ,IRQ: Підключені до ESP8266	3.3 В	Живиться від мікроконтролера який видає 3.3 В. Призначиний для ідентифікації в системі.

2.5 Висновки

В результаті проведених досліджень у розділі 2, проаналізувавши компоненти та спосіб функціонування кіберфізичної системи контролю доступу до підприємства яка базується на мікроконтролері ESP8266 та RFID-модулі, можна зробити такі висновки.

Пропонована кіберфізична система має свої позитивні якості і відрізняється від уже існуючих своїм функціоналом та реалізацією.

Розроблена система базується на мікроконтролері ESP8266, який виконує роль центрального керуючого елементу всієї кіберфізичної платформи. Саме завдяки йому реалізується взаємодія між усіма модулями та забезпечується загальна логіка роботи. RFID-зчитувач RC522 виступає в ролі електронного замка: він ідентифікує RFID-мітки або ключ-карти та передає отримані дані на обробку мікроконтролеру. Після обробки інформації дані виводяться на символьний дисплей LCD, що дозволяє користувачеві системи візуально спостерігати за станом доступу.

Мікроконтролер виконує функції логічного аналізу на основі отриманої інформації приймається рішення про надання чи відмову у доступі, а також за необхідності активується звукове сповіщення про успішне зчитування або несанкціоновану спробу доступу. Особливістю запропонованої системи є не лише можливість контролю входу, але й збереження інформації про всі спроби авторизації незалежно від їх результату. Це стало можливим завдяки підключенню мікроконтролера до Wi-Fi-мережі та Інтернету, через які за допомогою HTTP-запитів типу POST здійснюється передача відповідних даних у Google Sheets для подальшого збереження та аналізу.

3 РЕАЛІЗАЦІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ПІДПРИЄМСТВА НА ОСНОВІ МІКРОКОНТРОЛЕРА ESP8266

3.1 Підготовка середовища розробки

Для розробки програмного забезпечення мікроконтролера ESP8266 у даній системі було обрано середовище Arduino IDE. Це середовище програмування стало оптимальним вибором, оскільки підтримує створення програм для широкого кола мікроконтролерів, зокрема платформ Arduino та ESP-сумісних пристроїв. Arduino IDE поєднує в собі функціональний текстовий редактор, що дозволяє зручно створювати та редагувати програмний код, вікно для виведення повідомлень про компіляцію, помилки й поточний стан процесу, а також консоль, яка дає змогу виконувати необхідні дії під час налаштування та завантаження прошивки. Крім того, середовище містить меню з основними інструментами, що полегшують керування процесом розробки, а також підтримує підключення додаткових бібліотек для розширення функціоналу системи.

За допомогою інтегрованого середовища розробки відбувається підключення до апаратного забезпечення плати для завантаження прошивки та спілкування один з одним, в свою чергу плата ESP8266 в своїй будові має недорогий, маленький Wi-Fi мікрочіп з стеком TCP/IP та зберігає усі можливості звичайного мікроконтролера. Проаналізувавши це можемо зробити висновок що він може підключатися та спілкуватися з різними пристроями та мати доступ до інтернету через Wi-F, тому через його ціну та легкість в розробці його часто використовують для проектування пристроїв та систем для Інтернету речей.

Платформа Arduino IDE забезпечує простий та функціональний інтерфейс для розробки програмного забезпечення, компіляції коду та завантаження прошивки на мікроконтролер. У межах цієї кваліфікаційної роботи Arduino IDE застосовується для написання програмного коду та його завантаження на мікроконтролер ESP8266. Окрім цього, середовище використовується для обробки

даних, отриманих від RFID-зчитувача, та керування активацією звукового модуля, що виконує функцію сигналізації.

Мікроконтролер ESP8266 виступає основним елементом системи, відповідаючи за реалізацію функцій контролю доступу на основі RFID-технології. Завдяки інтегрованому Wi-Fi-модулю, пристрій здатен забезпечити зв'язок з мережею Інтернет, що дозволяє передавати та зберігати інформацію про користувачів у хмарному середовищі. Компактність, універсальність та доступна вартість роблять ESP8266 оптимальним варіантом для реалізації систем управління доступом у складі кіберфізичних пристроїв. Переходячи до етапу налаштування середовища для розробки програмного забезпечення, слід зосередитися на встановленні Arduino IDE.

Для того щоб розпочати роботу з цим середовищем і перейти безпосередньо до написання коду, необхідно попередньо завантажити програму з офіційного вебсайту розробників або через магазин додатків Microsoft Store [17].

Розглянемо процес встановлення та налаштування середовища для розробки програмного забезпечення для кіберфізичної системи контролю доступу до підприємства.

Початковим кроком буде завантаження середовища розробки Arduino IDE з магазину Microsoft Store (рисунок 3.1).

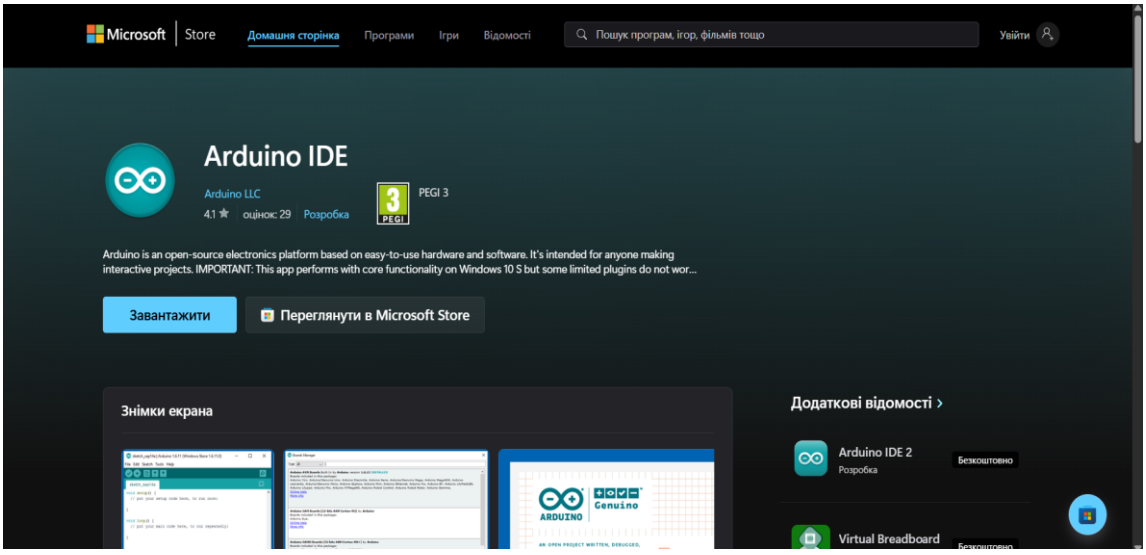


Рисунок 3.1 – Крок 1

Наступним кроком буде створення файлу і перехід до налаштувань середовища для написання коду програмного забезпечення мікроконтролера ESP8266 (рисунок 3.2).

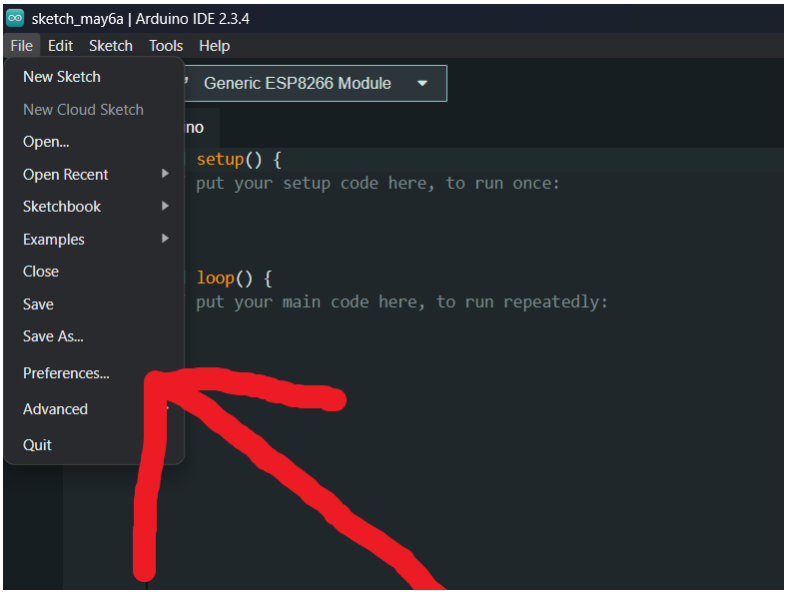


Рисунок 3.2 – Крок 2

Після базових налаштувань (рисунок 3.3) потрібно додати потрібну плату. Для цього необхідно додати у поле“Additional Board Manager URL” посилання на плату[18].

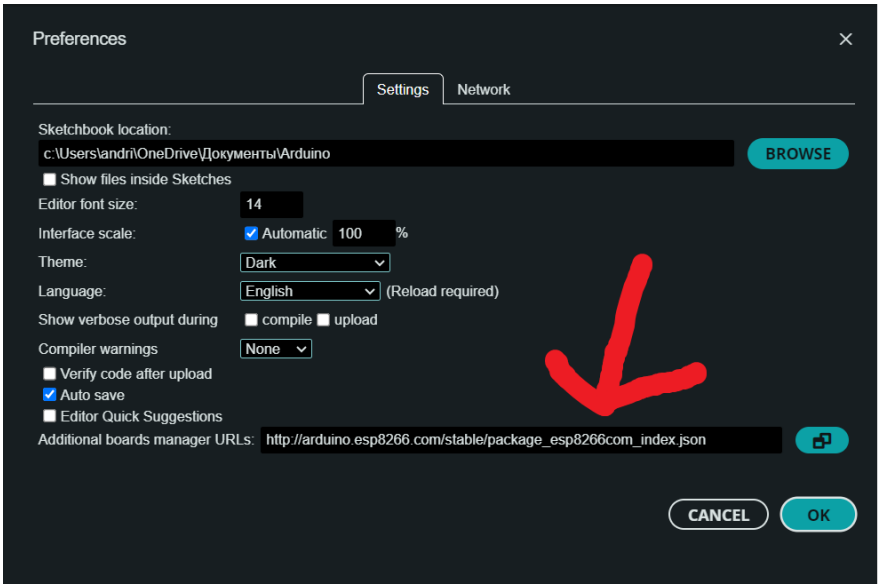


Рисунок 3.3 – Крок 3

Після успішного додавання бібліотеки для використання плати необхідно перейти до вкладки Інструменти > Плата > Диспетчер плат (рисунок 3.4).

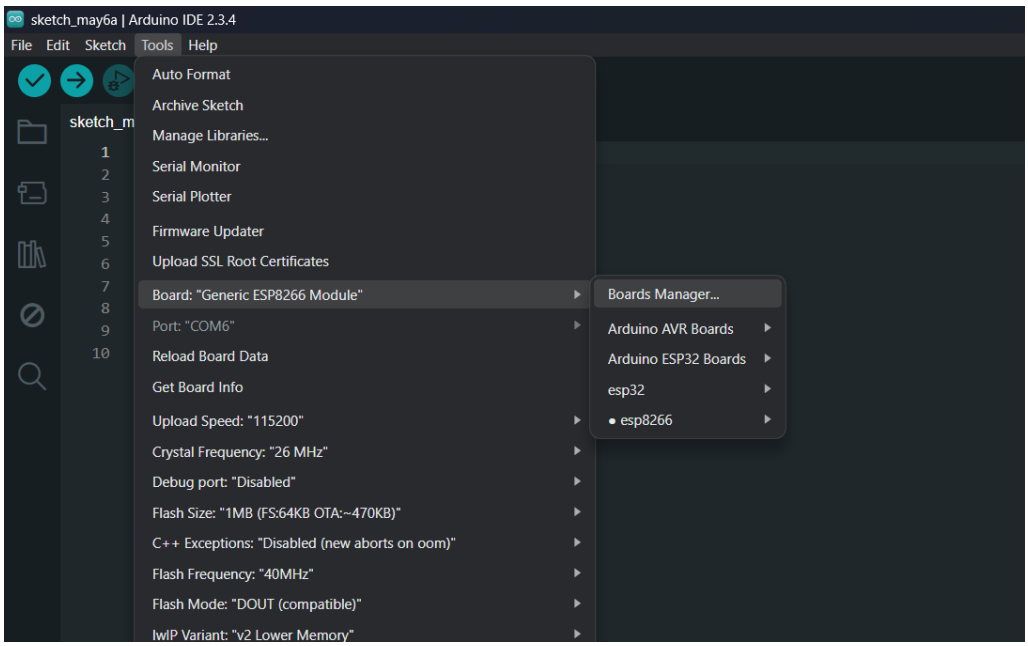


Рисунок 3.4 – Крок 4

Відкривши диспетчер плат необхідно знайти у пошуковому рядку “ESP8266”, та обрати пакет "esp8266 by ESP8266 Community" і натиснути кнопку "Встановити" (рисунок3.5).

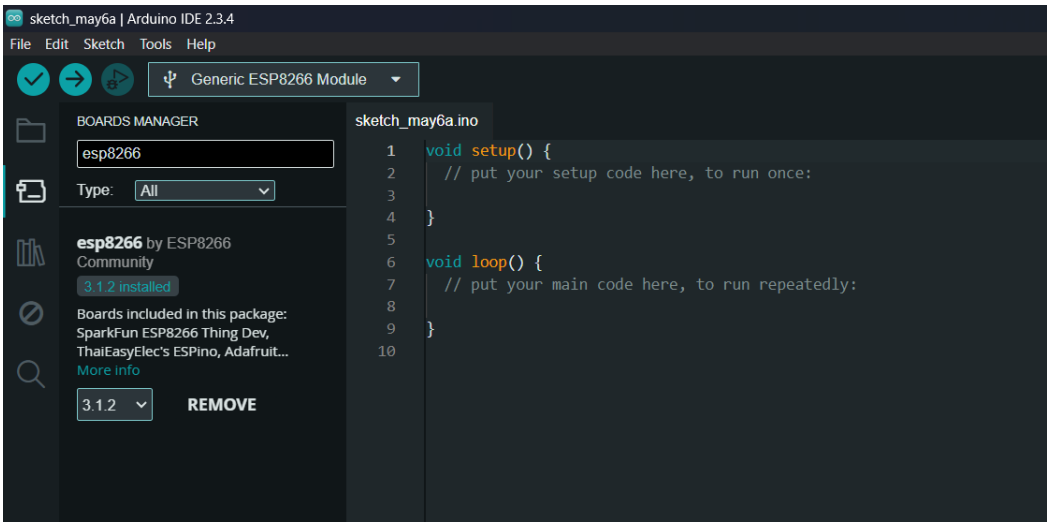


Рисунок 3.5 – Крок 5

Завершальним кроком є підтвердження встановлення бібліотеки мікроконтролера ESP8266 (рисунок 3.6).

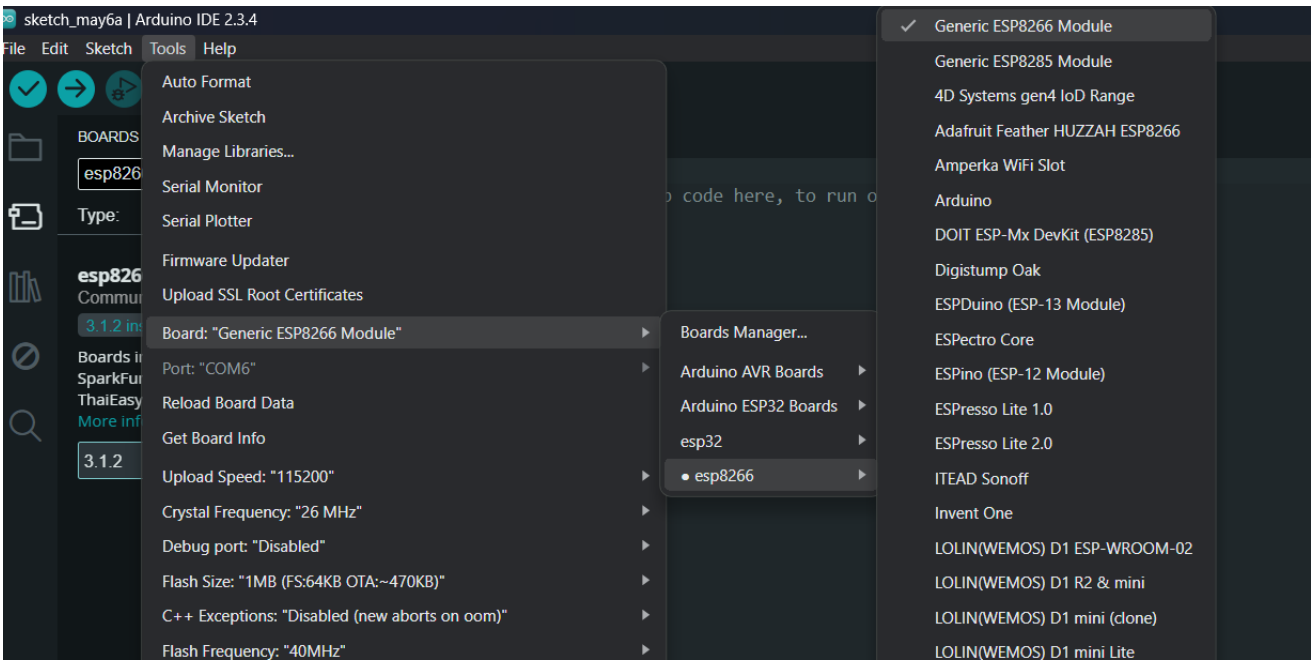


Рисунок 3.6 – Крок 6

Після завершення налаштування середовища розробки можна переходити до написання програмного коду для реалізації функціоналу кіберфізичної системи.

3.2 Підключення елементів кіберфізичної системи до макетної плати та монтажна схема

Для моделювання, підключення та схематичного з’єднання компонентів у проєкті застосовується програмне забезпечення Fritzing.

Fritzing є ефективним та простим у використанні інструментом, призначеним як для початківців, так і для досвідчених розробників. Програма дає змогу створювати електронні схеми, макети друкованих плат (PCB), а також прототипи з використанням графічного середовища без необхідності у глибоких технічних знаннях.

Інтерфейс користувача є інтуїтивно зрозумілим. Компоненти легко розміщуються та з’єднуються за принципом "перетягування", що дозволяє швидко

формувати схему на віртуальній макетній платі. Fritzing забезпечує зручне проєктування схем з подальшою можливістю симуляції й верифікації перед виготовленням, що дає змогу зменшити ризик помилок та оптимізувати використання ресурсів.

Окрім основних функцій, програма підтримує збереження та обмін проєктами у форматах файлів, зображень та PDF, що полегшує командну роботу, спільне тестування та вдосконалення розробок.

У межах даного проєкту, що стосується створення кіберфізичної системи контролю доступу з використанням мікроконтролера ESP8266 та модуля RFID, Fritzing було використано для візуального представлення структури системи. Розроблені у програмі схеми демонструють зв’язки між основними елементами: ESP8266, RFID-зчитувачем, LCD-дисплеєм та іншими складовими.

Програма дозволяє задокументувати апаратну конфігурацію, що спрощує аналіз функціонування системи й забезпечує можливість відтворення проєкту в майбутньому. Використання візуалізаційних інструментів особливо корисне при поясненні роботи системи користувачам без технічної підготовки.

3.3 Фізична схема кіберфізичної системи контролю доступу до підприємства на основі мікроконтролера ESP8266

Почнімо розгляд фізичої схеми програмного та технічного управління кіберфізичної системи побудованої на платі ESP8266. Підключення компонентів системи таких як LCD чисельний дисплей та звуковий динамік з модулем зчитування RFID показаний на (рисунок 3.8) та (рисуно 3.9).

У центрі розробленої схеми знаходиться мікроконтролер ESP8266 (NodeMCU), який було обрано завдяки його зручності у підключенні до мережі Wi-Fi. Обраний мікроконтролер забезпечує чіткий та стабільний зв'язок з мережею, що є ключовою умовою для роботи кіберфізичної системи контролю доступу.

Зчитувач RFID-тегів, ще його називають модулем радіочастотної ідентифікації користувачав використаний в цій системі для зчитування унікальних даних користувачів та відвідувачів підприємств які записані в ключ-картах. Дана модель модуля може взаємодіяти з мікроконтролером за допомогою досить розповсюджених інтерфейсів SPI та UART.

Разом з модулем RFID RC522 в комплекті ідуть теги (рисунок 3.7), які можна програмно за допомогою Arduino та самого модуля прошити під свої потреби та дані. RFID-теги це маленькі пристрої в яких міститься чіп памяті за допомогою якого відбувається збереження інформації про користувача яка записуємться в нього.

Кожна мітка має унікальні данні як і кожна людина свою структуру ДНК, в пропонованій системі ці мітки використовуються для ідентифікації користувачів в системі для подальшого аналізу даних і прийнятті результату.

Також в пропонованій системі замість механізму замка як в більшості систем я використав звуковий динамік для сигналізації, його при збірці схеми можна замінити на реле та електронний замок але в пропонованій мною схемі використаний він щоб давати звуковий сигнал користувачу що ідентифікація успішна чи вмикати сигнал тривоги якщо данні не розпізнанні чи не збігаються з данними які ьули отриманні попередньо.

Рисунок 3.7 – Приклад RFID-мітки

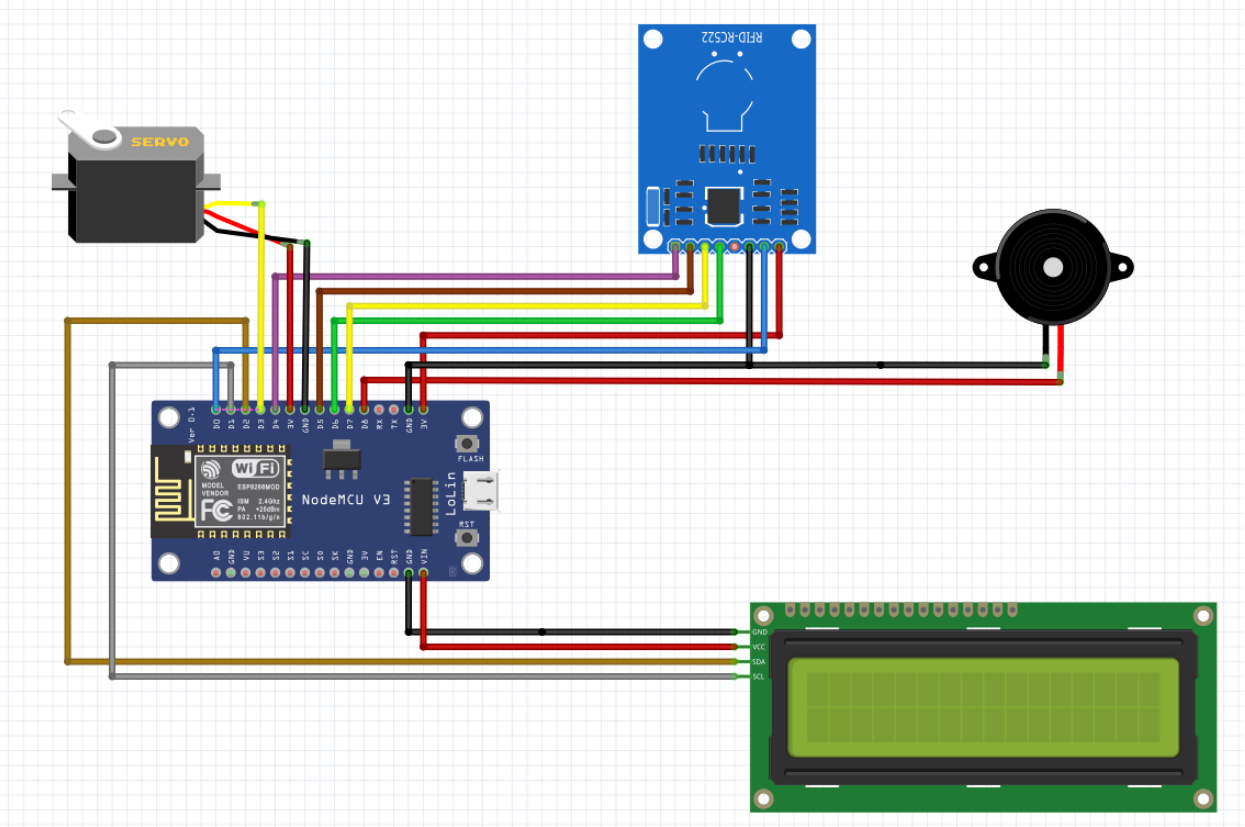


Рисунок 3.8 – Схема підключення компонентів системи

За допомогою програмного забезпечення та функціоналу Fritzing було створено електричну схему (рисунок 3.9).

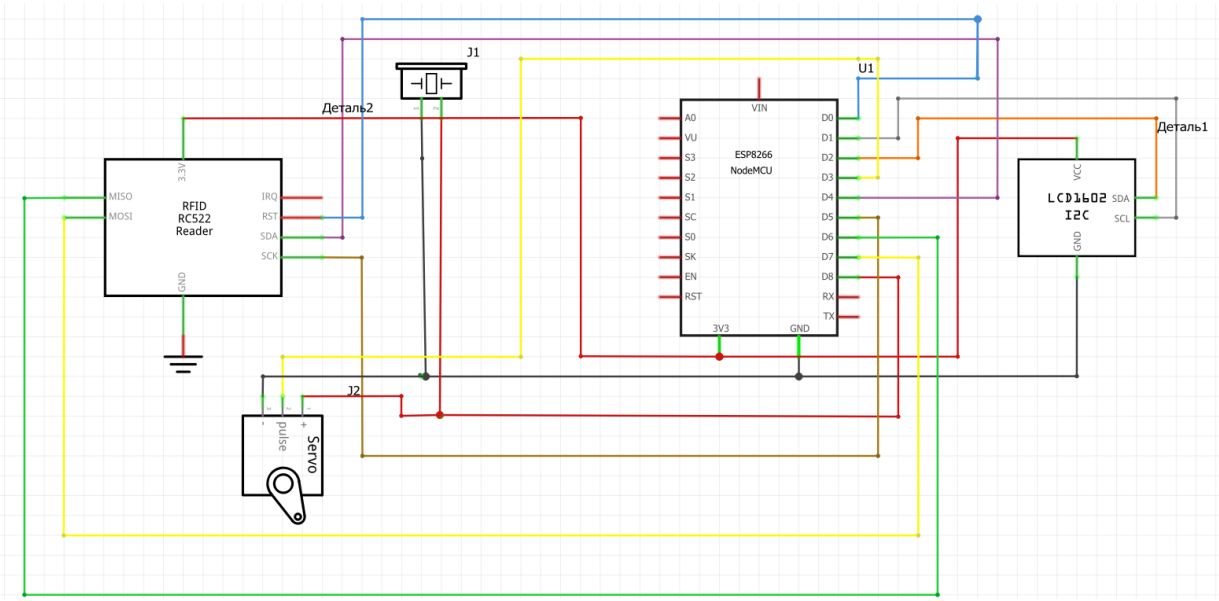


Рисунок 3.9 – Електрична схема кіберфізичної системи контролю доступу до підприємства

Також за допомогою програмного забезпечення Fritzing можна створити макет друкованої плати (рисунок 3.10), який у подальшому можна використати для виготовлення фізичної плати. Програма дозволяє виконувати автоматичну або ручну розводку доріжок, орієнтуючись на попередньо складену схему з'єднання компонентів.

У даній схемі живлення плати реалізується через роз'єм microUSB. Альтернативно допускається живлення від зовнішнього джерела, наприклад, батареї номіналом 9 В. У такому випадку для забезпечення роботи компонентів, що потребують 5 В, необхідне використання понижувального перетворювача напруги.

Модуль NodeMCU на базі ESP8266 функціонує при напрузі 3.3 В. Проте можливе його живлення і від 5 В, якщо джерело підключене до контактів VIN та GND. У такій конфігурації вбудований стабілізатор здійснює зниження напруги до необхідного рівня.

На схемі також застосовуються перемички, які виконують роль допоміжних електричних з'єднань між елементами на макетній платі. Їх використання дозволяє уникнути прокладання окремих дротів до кожного контакту, наприклад, GND. Перемички можуть відрізнятися за довжиною, формою та кольором залежно від потреб монтажу.

Макетна плата використана в даній роботі як інструмент розробки і створення прототипів щоб не просто скласти систему а потім переробляти якщо виникнуть якісь незручності чи будуть виявлені недоліки а просто і швидко замінити чи змінити підключення компонентів між собою чи додати ще елементи на плату для більшої функціональності системи.

USB-кабель був використаний для з'єднання мікроконтролерної плати з комп'ютером та завантаження програмного забезпечення кіберфізичної системи, а також як живлення системи для тестування.USB-кабель забезпечує живлення системи на етапі тестування а також зворотній зв'язок між мікроконтролером та ПК при програмування чи виконанні програми.

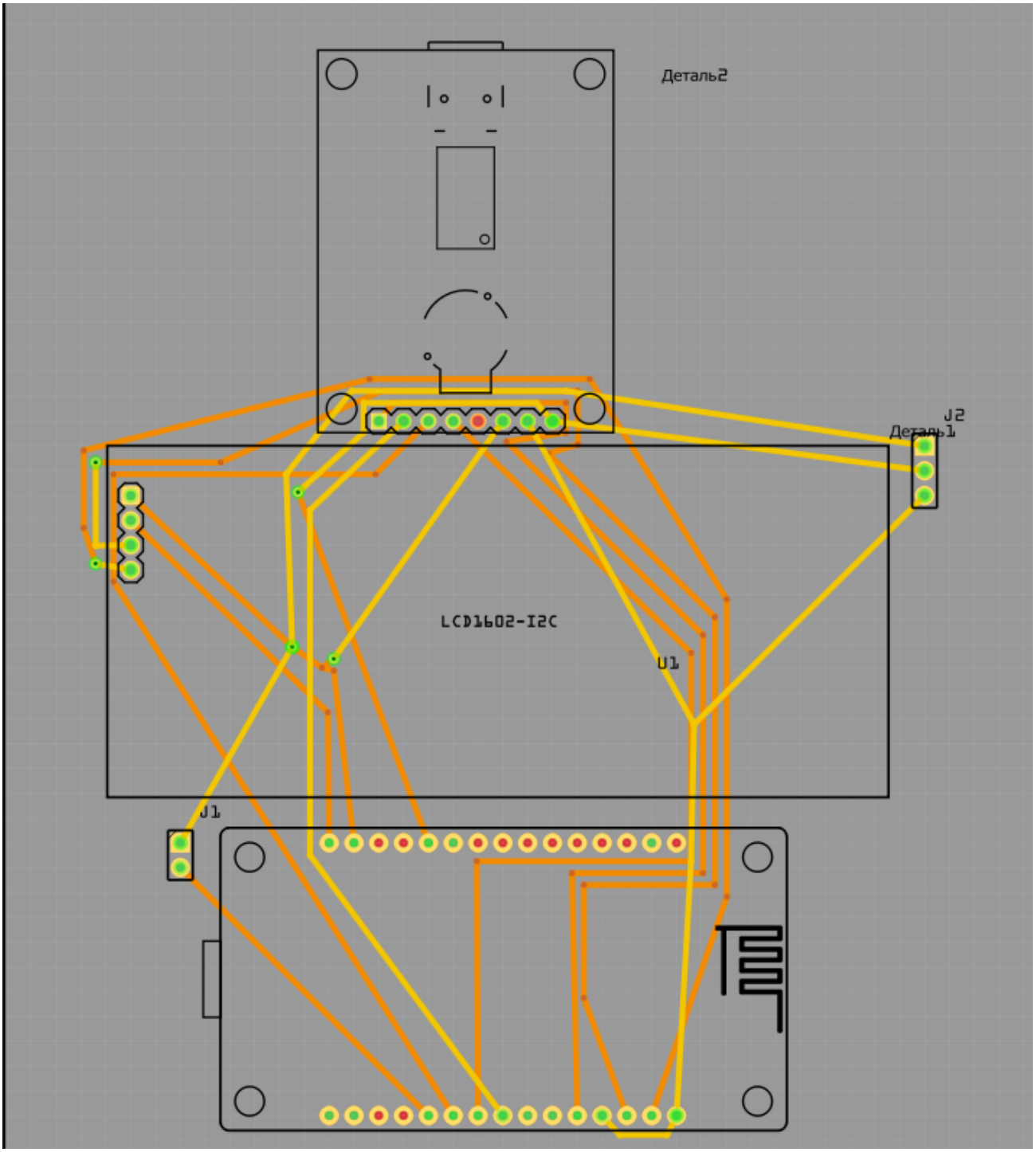


Рисунок 3.10 – Вигляд діаграми друкованої плати кіберфізичної системи розведенної за допомогою інструментів Fritzing

Для наочного пояснення принципу роботи кіберфізичної системи контролю доступу до підприємства, побудованої на базі мікроконтролера ESP8266, розроблено спрощену блок-схему функціонування системи (рисунок 3.11).

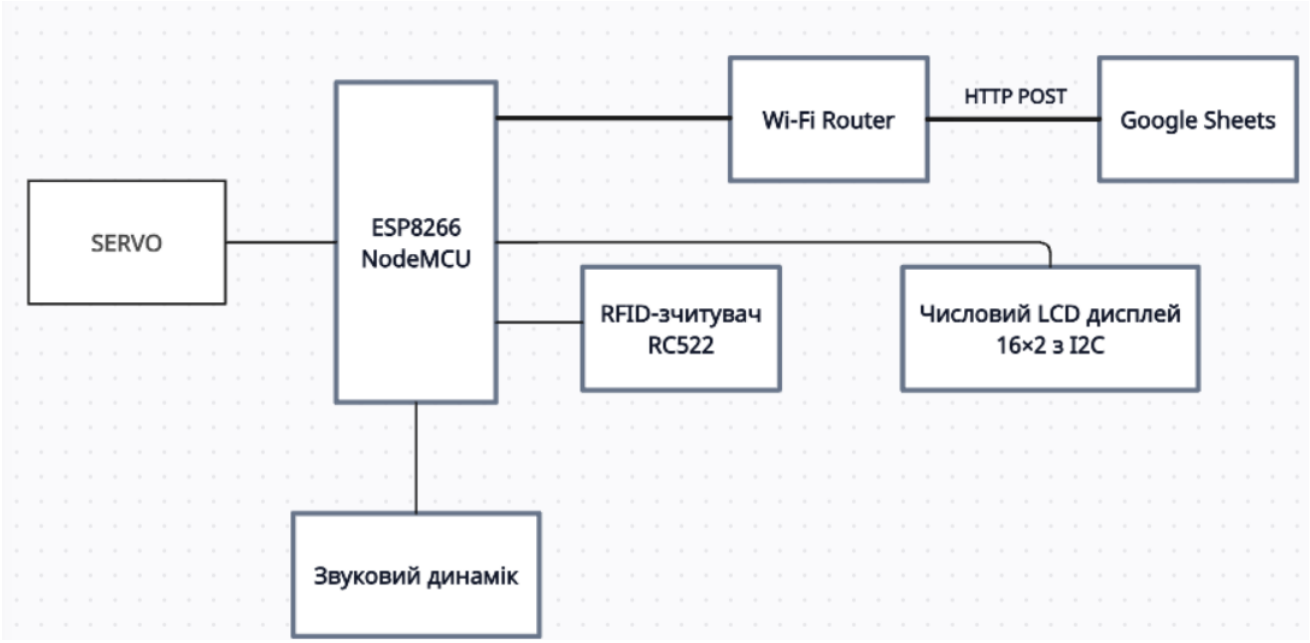


Рисунок 3.11 – Структурна схема кіберфізичної системи

RFID-модуль зчитує інформацію з RFID-мітки або ключа під час контакту, після чого передає отримані дані мікроконтролеру для подальшої обробки. Мікроконтролер ESP8266 виступає основним обчислювальним елементом системи, приймає дані від RFID-зчитувача, виконує їх обробку та формує HTTP POST-запит для надсилання інформації до таблиці Google Sheets, яка виконує функцію бази даних користувачів.

Після обробки мікроконтролер передає сигнал на звуковий модуль, що генерує відповідне звукове сповіщення про результат перевірки доступу (успішний або відхилений). Одночасно, на символьному LCD-дисплеї виводиться службова інформація, що підтверджує ідентифікацію користувача. У разі позитивної відповіді, мікроконтролер активує сервопривід, який забезпечує відкриття дверей на визначений інтервал часу (приблизно 3 секунди), що дозволяє користувачеві увійти до приміщення. Стабільна робота системи потребує наявності доступу до бездротової мережі Wi-Fi для передачі даних в онлайн-базу. Підключення до мережі відображено в блок-схемі через Wi-Fi-роутер. Живлення елементів здійснюється від блоку живлення або акумулятора, що забезпечує тривалу автономну або стаціонарну роботу пристрою.

3.4 Створення програмного забезпечення для кіберфізичної системи контролю доступу до підприємства на основі Esp8266

В попередніх розділах було проведено розробку та аналіз фізичної частини кіберфізичної системи контролю доступу до підприємства на основі Esp8266, а також завантажено та налаштовано середовище для розробки програмного забезпечення.

Розпочнемо розгляд процесу підключення та налаштування Google Sheets для роботи з нашим мікроконтролером Esp8266.

Для початку відкриємо в браузері онлайн версію звичного Microsoft Excel а саме Google Sheets (рисунок 3.12).

Після переходу за посиланням натисніть кнопку створити нову таблицю або кнопку з символом додати таблицю. Для коректної роботи онлайн версії додатку обов'язково потрібно мати доступ до мережі інтернет через Wi-Fi чи мобільний інтернет.

Після успішного створення потрібно надати таблиці та аркушу назву, це є дуже важливим оскільки в подальшому це буде використовуватися для написання коду програми. До прикладу для формування повідомлення яке буде надходити в таблицю в програмі для Esp8266 пишемо наступний код:

```
String payload_base = "{\"command\": \"insert_row\", \"sheet_name\": \"Table\", \"values\": ";
```

Даний фрагмент коду допомагає мікроконтролеру під час роботи і підключення до мережі інтернет через Wi-Fi обмінюватися з електронною таблицею данними а якщо простіше додовати в таблицю з такою назвою в такий рядок та стовпець данні які потрібні для авторизації користувачів в системі після успішного зчитування RFID-міток чи ключ карт які мають бути зроблені та виданні усім робітникам на підприємстві.

Наступним кроком буде створення та налаштування назви аркуша таблиці а також відкриття редактора коду для написання скриптів. Для цього потрібно перейти у меню інструментів на вкладку Розширення та далі App Script.

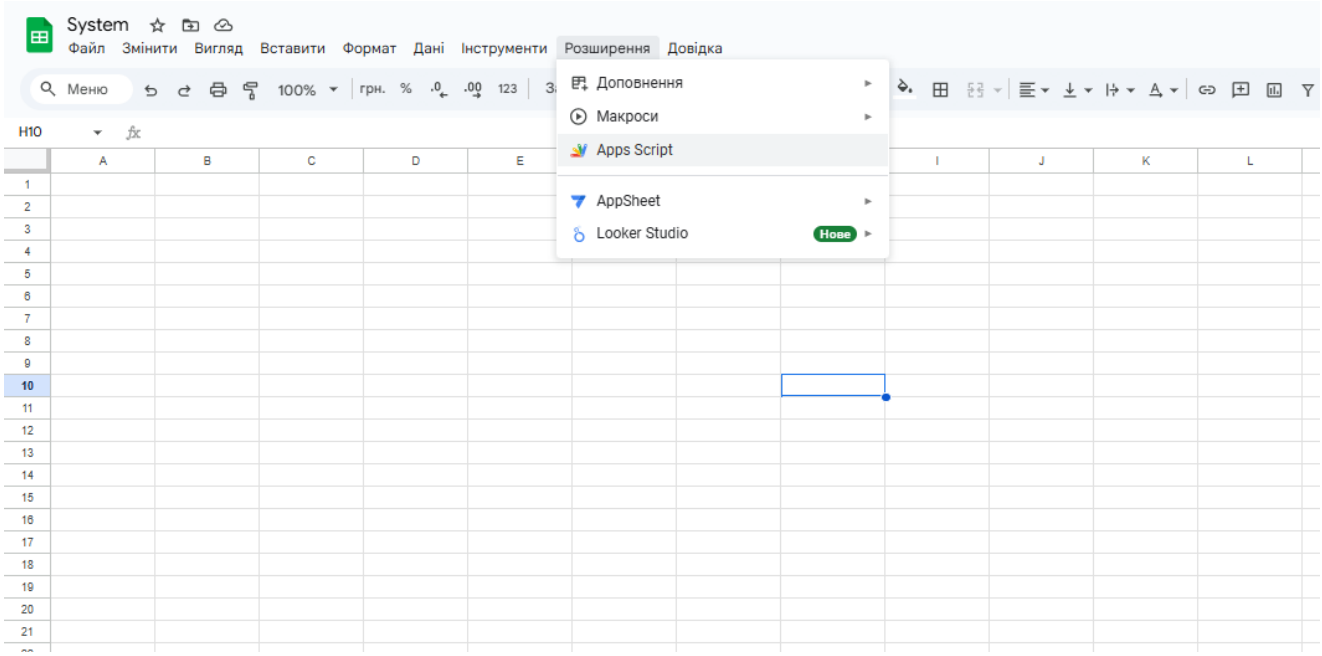


Рисунок 3.12 – Відкриття редактора коду

У межах реалізації програмної частини кіберфізичної системи контролю доступу буде використано платформу Google App Script, яка надає можливість створення серверної логіки для обробки запитів. У даному випадку за допомогою App Script буде створено спеціалізований скрипт, який відповідатиме за приймання HTTP POST-запитів, що надходять від мікроконтролера ESP8266.

Отримані зчитувачем RFID-дані, після обробки скриптом, автоматично зберігатимуться в таблиці Google Sheets, яка виконує функцію бази даних користувачів. Такий підхід дозволяє зручно вести облік подій доступу, забезпечує централізоване зберігання інформації та дозволяє здійснювати її подальший аналіз. Скрипт також може бути доповнений механізмами фільтрації, перевірки автентичності запитів або сортування інформації за часовими мітками.

Виконавши попередній етап, а саме створення скрипта, скрипт потрібно запустити, тому потрібно натиснути кнопку “Ввести в дію” та вибрати з випадаючого меню “Нове введення в дію”.

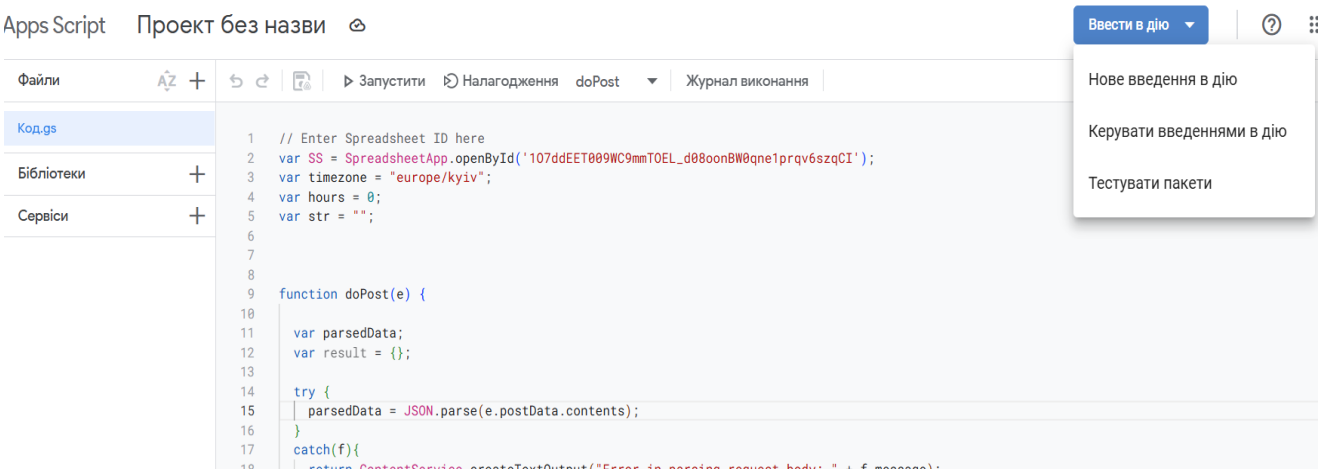


Рисунок 3.13 – Введення в дію скрипта

Після натискання кнопки відкриється вікно з налаштуванням де буде потрібно вказати опис що це за веб-додаток та налаштувати доступ до таблиці.

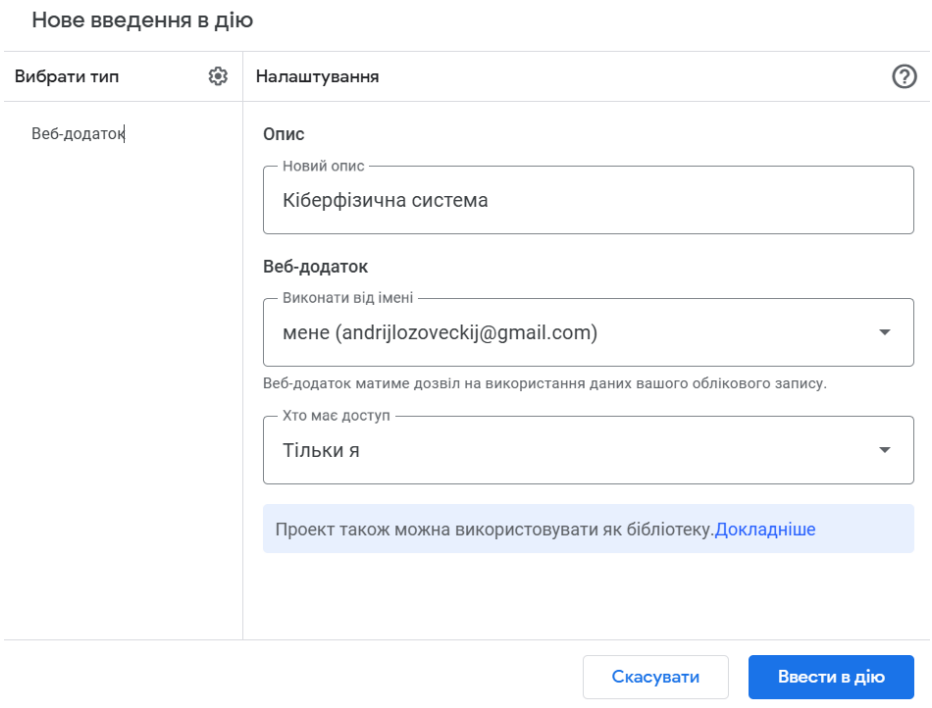


Рисунок 3.14 – Налаштування веб-додатку

Виконавши та підтвердивши попередні налаштуваня натискаємо на кнопку “Ввести в дію” та підтверджуємо виконання процесу. Після успішного введення в дію вам буде доступно посилання на веб-додаток та ідентифікатор введення в дію який далі буде використовуватися в коді додатку.

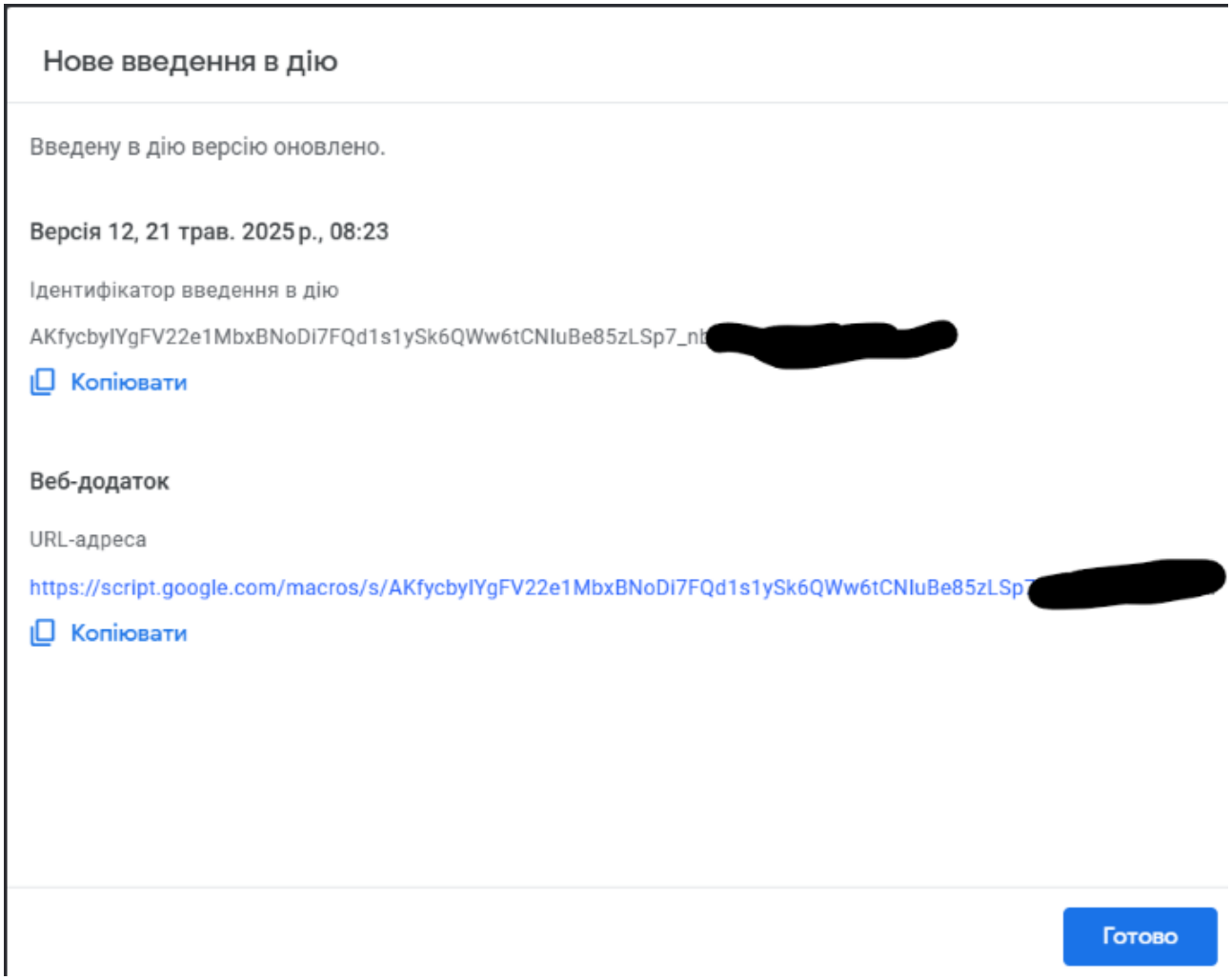


Рисунок 3.15 – Успішне введення в дію

Для розробки та написання коду для мікроконтролера Esp8266 як раніше було вказано будемо використовувати Arduino IDE та бібліотеки які потрібно для взаємодії компонентів системи з мікроконтролером для забезпечення нормального функціонування системи без помилок та збоїв при роботі з мережею.

Для додавання бібліотек можна знайти їх у вкладці бібліотеки або скачати з інтернету та додати вручну (рисунок 3.16)

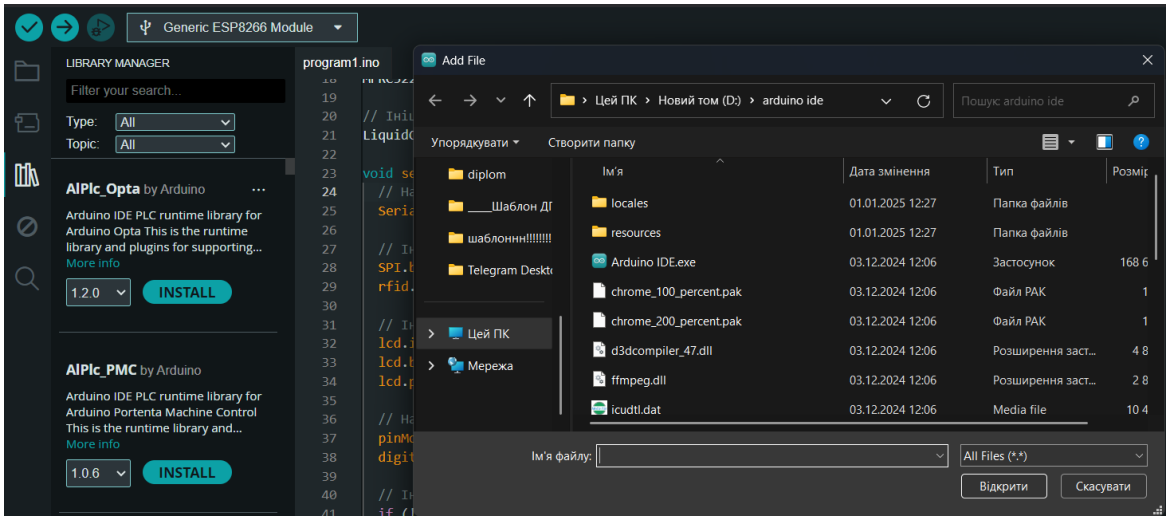


Рисунок 3.16 – Додавання бібліотек

Під час створення програмного забезпечення для кіберфізичної системи будемо використовувати такі бібліотеки:

– Arduino.h.
– ESP8266WiFi.h.
– SPI.h.
– MFRC522.h.
– Servo.h.
– HTTPSRedirect.h.
– Wire.h.
– LiquidCrystal_I2C.h.

Бібліотека Arduino.h це бібліотека яка повинна бути використана оскільки вона надає основні функції та типи даних для написання коду. Прикладом використання цієї бібліотеки є функції digitalWrite(), analogRead(), pinMode() та інші функції які допомагають працювати з зчитуванням даних та обробкою.

Бібліотека ESP8266WiFi.h базова бібліотека для роботи з мікроконтролером Esp8266 та його основними можливостями які включають Wi-Fi, створення та підключення до різних точок доступу та з'єднання з інтернетом. Основний функціонал бібліотеки це підключення до мережі Wi-Fi, створення клієнтів та розгортання серверів, а також робота з різними IP-адресами. В даній роботі вона

використовується для взаємодії мікроконтролера з Wi-Fi та надсиланням POST-запитів до електронної таблиці.

Бібліотека SPI.h це одна з найпотрібніших бібліотек для даного проекту створення кіберфізичної системи контролю доступу, оскільки використовуємо RFID-зчитувач для контролю доступу до підприємства і саме для нього була використана ця бібліотека. Вона використовується для обміну даних з мікроконтролером та пристороями типу дистплеїв чи RFID-модулів.

Бібліотека MFRC522.h це вже бібліотека для роботи з RFID-зчитувачем який використано для розробки кіберфізичної системи. Призначення бібліотеки це зчитування RFID-міток та карт доступу, читання та запис данних у пам’ять мітки.

Бібліотека Servo.h це досить проста бібліотека яка використовується для звичайного керування сервоприводом та привязкою його до піна. В даному проекті використовується як механізм відкриття дверей при успішній перевірці ключа доступу.

Бібліотека HTTPSRedirect.h використана при розробці програмного забезпечення для відправлення HTTPS-запитів таких як POST для запису даних у електронну таблицю гугл та робота з гугл через App Script.

Wire.h бібліотека використовується для роботи з I2c інтерфейсом а він в свою чергу використовується для зв’язку та взаємодію між мікроконтролером та LCD дисплеєм та передачей байтів інформації між ними.

Бібліотека LiquidCrystal_I2C.h використовується безпосередньо для роботою та нормальним функціонуванням LCD дисплея у зв’язці з мікроконтролером Arduino або ESP8266. В кваліфікаційній роботі використовується для виведення тексту на LCD дисплей та керування різними функціями дисплея.

Всі ці бібліотеки критично важливі і необхідні для нормального функціонування кіберфізичної системи, тому що без них система буде не цілісна і не буде мати функції які роблять її унікальною та особливою, і через які зручність користування нею є на високому рівні в порівнянні з іншими схожими системами які на даний час використовуються.

3.5 Алгоритм роботи кіберфізичної системи

Кіберфізична система має свої алгоритми роботи які розділені щоб краще функціонувати, в системі є кілька ключових алгоритмів які і відповідають за роботу системи. До таких алгоритмів відносяться алгоритми які:

- вмикають систему;
- алгоритми підключення та аутентифікації точки доступу;
- алгоритм з’єднання з мережею;
- алгоритм запису даних в таблицю;
- алгоритм зчитування RFID-мітки;
- алгоритм виведення даних на LCD дисплей;
- алгоритм подання звукового сигналу;
- алгоритм відкривання дверей.

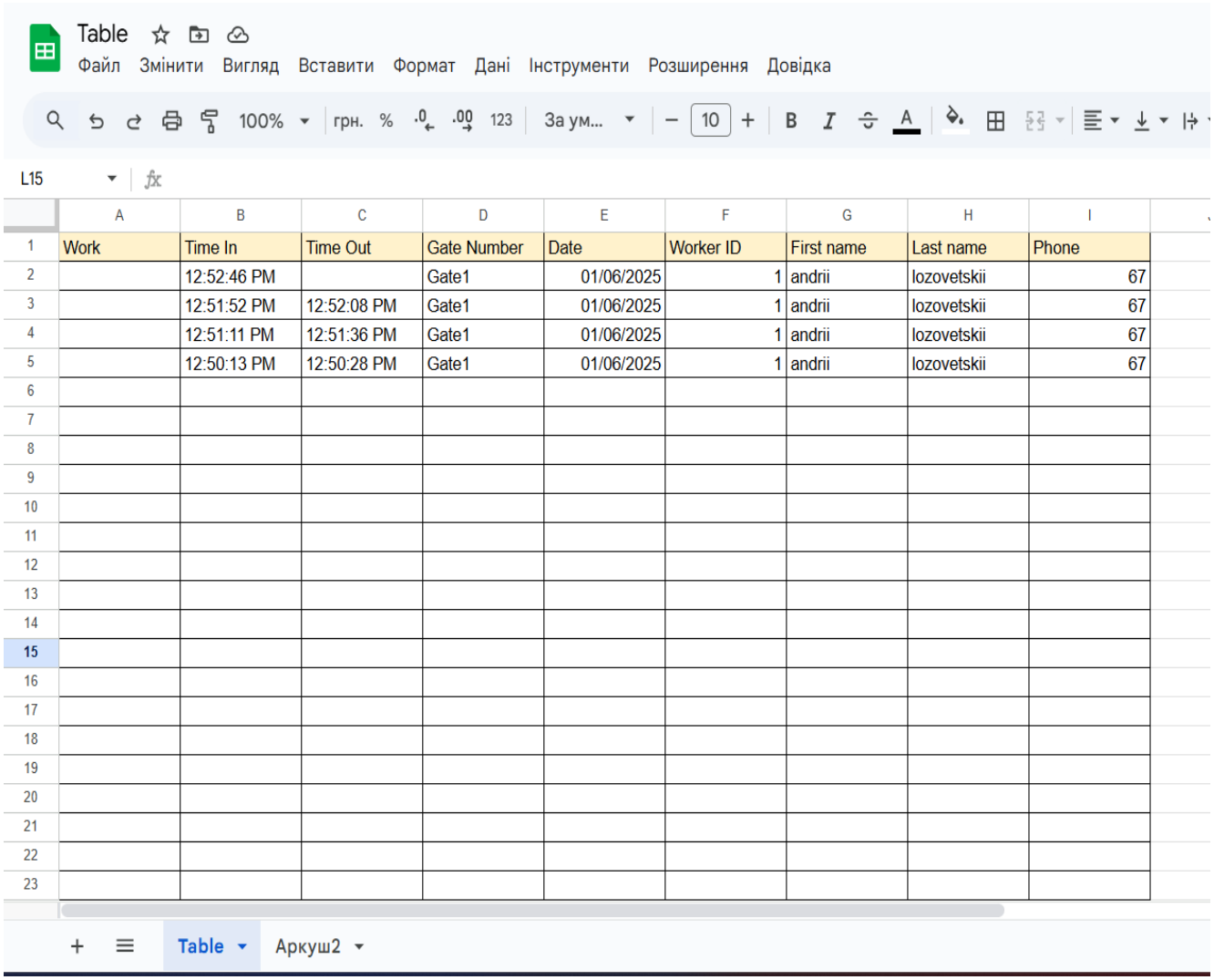
Розглянемо коротко основні алгоритми та їх функціонал.

Алгоритм вмикання системи та підключення пристроїв до мікроконтролера являє собою алгоритм який є базовим при ввімкнені системи. В його основу входить підключення та ініціалізація всіх пристроїв в системі та початок роботи з ними, він розпочинає свою роботу при ввімкнені системи та подачі живлення на неї.

Алгоритм підключення та аутентифікації точки доступу працює наступним чином. Після ввімкнення системи мікроконтролер за допомогою програмного забезпечення та бібліотеки вмикає модуль Wi-Fi і розпочинає пошук точки доступу яка була вказана в коді програми, якщо він її знаходить відбувається підключення до неї і на дисплеї буде здійснений вивід інформації про підключення. Якщо підключення не вдалося то виведеться інформація про це. Даний алгоритм критично необхідний оскільки без нього кіберфізична система не буде взаємодіяти з Google Sheetsh та не буде здійснено запис даних в таблицю.

Алгоритм запису в таблицю даних включає в себе приймання POST-запитів від мікроконтролера обробку за допомогою Apps Script коду та запис даних про

користувачів в базу даних яка являє собою Електрону таблицю з відповідними колонками(рисунок 3.19).



	A	B	C	D	E	F	G	H	I
1	Work	Time In	Time Out	Gate Number	Date	Worker ID	First name	Last name	Phone
2		12:52:46 PM		Gate1	01/06/2025	1	andrii	lozovetskii	67
3		12:51:52 PM	12:52:08 PM	Gate1	01/06/2025	1	andrii	lozovetskii	67
4		12:51:11 PM	12:51:36 PM	Gate1	01/06/2025	1	andrii	lozovetskii	67
5		12:50:13 PM	12:50:28 PM	Gate1	01/06/2025	1	andrii	lozovetskii	67
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									

Рисунок 3.17 – Вигляд таблиці для запису інформації про працівників підприємства

В таблиці присутні ключові стовпці по яких зручно перевіряти інформацію про працівників і графік відвідування працівниками підприємства. До ключових стовпців відносяться:

1. Work-стовпчик в якій можна вказати назву підприємства чи окрему робочу ланку.
2. Time In-тут записуються дані про час входу працівника до підприємства.

3. Time Out-відповідно як Time In вносяться дані про те коли працівник покинув робочу зону підприємства.

4. Gate Number-номер входу, якщо на підприємстві є кілька дверей для входу або кілька кімнат.

5. Date-дата коли працівник ввійшов на підприємство.

6. Worker ID-унікальний номер працівника по якому можна давати та забороняти доступ на відповідні частини підприємства якщо такі є.

7. First name-і’мя працівника

8. Last Name-прізвище працівника

9. Phone-Номер телефону працівника

Алгоритм зчитування RFID-мітки це алгоритм який вмикає режим зчитування на RFID-модулі для того щоб при прикладані мітки чи карти відбувалась процедура зчитування, цей алгоритм зчитує дані з мітки і передає їх мікроконтролеру для подальшого опрацювання.

Алгоритм виведення даних на дисплей включає в себе виведення даних про користувачів, про стан системи та її статус на LCD дисплей який підключений до мікроконтролера через шину I2c.

Алгоритм подання звукового сигналу найпростіший алгоритм в якого два сценарія це або тиша або подання звуку при аутентифікації користувача коли він прикладає мітку або подання звуку що сталась помилка.

Алгоритм відкривання дверей має два режими, двері закрито та двері відкрито, двері закрито весь час коли користувач приклав мітку та дані були опрацьовані та внесені в базу то двері відмикаються на 3 секунти і працівник може потрапити до приміщення.

Всі вище описані алгоритми і я'вляють собою програмну частину кіберфізичної системи контролю доступу до підприємства на основі мікроконтролера Esp8266. Без програмної частичи чи без хочаб одного алгоритму дана кіберфізична система буде неповноцінною та малоефективною і користувачі не будуть отримувати належної безпеки, комфорту та задоволення при використані

даної кіберфізичної системи на підприємствах, навчальних закладах і навіть в житлових будинках.

3.6 Висновки

Кіберфізична система контролю доступу до підприємства це високотехнологічна та сучасна система яка потрібно багатьом підприємствам для різного типу задач, відслідковування часу роботи працівників і чи вони працюють належним чином і не запізнюються на роботу. Система є унікальною і розроблена для повсякденного користування, в розробці та налаштуванні є не надто складною але потребує вимог до встановлення, основною вимогою є наявність постійного джерела живлення та доступу до мережі щоб взаємодіяти з таблицею.

Система збирається з деталей які були описані в даній роботі, всі деталі можна вмістити в невеликий корпус який можна змоделювати самому та надрукувати при можливості на 3D принтері або замовити щоб розробили модель під розміри компонентів і саомтійно все туди вмонтувати.

Система працює за допомогою ключових алгоритмів які допомагають їй функціонувати правильно та ефективно. Дані алгоритми допомагають виявляти RFID-мітки перевіряти і записувати інформацію про користувачів та дозволяти чи забороняти доступ до підприємства на основі даних, а для зручності все це виводиться на дисплей щоб користувач мав можливість переглядати статус.

ВИСНОВКИ

За результатами виконаної роботи та проведення теоретичних та практичних досліджень під час розробки кіберфізичної системи було спроектовано та створено працюючу кіберфізичну системи для контролю доступу до підприємства на основі мікроконтролера Esp8266, з використанням RFID-модуля.

Для початку у першому розділі було зроблено аналіз та коротко описано що таке взагалі кіберфізична система з яких елементів вона може складатися, які функції виконувати та багато чого іншого. Також було наведено приклад мікроконтролера та його схему функціонування. У першому розділі також було наведено різні компоненти системи з яких вона може складатися та їх аналоги.

У другому розділі проведено дослідження та вибір деталей для створення працюючої кіберфізичної системи контролю доступу до підприємства на основі мікроконтролера Esp8266. Було проаналізовано різні компоненти та аналоги а також слабкі та сильні сторони цих деталів, їхні особливості та приклади як вони можуть використовуватися та підключатися і здійснювати обмін інформацією та взаємодіяти з мікроконтролером.

У третьому розділі було описано процес встановлення та налаштування середовища розробки для створення прошивки розробленої кіберфізичної системи та детально покроково описано як налаштувати середовище розробки Arduino IDE та як створити і відкрити Google Sheets та після цього налаштувати Apps Script для запису в таблицю даних які надсилає мікроконтролер після обробки. Також наведено схему для збірки кіберфізичної системи, зроблено розведення друкованої плати та створено схему електричну принципову. Під час створення прошивки було використанобагато бібліотек які були детально описані у розділі навіщо вони та для чого вони використовуються.

Основна мета кваліфікаційної роботи, а саме розробка кіберфізичної системи контролю доступу до підприємства на сонові Esp8266 була повною мірою успішно виконана.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Мікроконтролер AT89C2051-24SI. URL: https://www.amazon.in/embsys-89C2051-Microcontroller-SMD/dp/B01B2NGE8A (дата звернення 20.05.2025).
2. Блок схема мікроконтролера i8081. URL: https://www.automatika.rs/baza-znanja/mikrokontroleri/opis-strukture-mikrokontrolera-8051.html (дата звернення 20.05.2025).
3. Arduino UNO URL: https://ims.dp.ua/?product=arduino-nano-v3-0-ch340g-atmega328-ch340 (дата звернення 20.05.2025).
4. RFID модуль RC522. URL: https://arduino.ua/prod649-rfid-modyl-rc522-s-kartochkoi-dostypa-dlya-arduino?srsltid=AfmBOopRLukeGDgN_dKcc-YHLmU1YDs1Cir93FB875K4pw_ADvm-vJrf (дата звернення 20.05.2025).
5. RFID модуль RDM6300. URL: https://electropeak.com/learn/interfacing-rdm6300-125khz-rfid-reader-module-with-arduino/ (дата звернення 20.05.2025).
6. Розумний дверний біометричний замок SEVEN LOCK SL-7740BF URL: https://seven-systems.com.ua/ua/p2269577508-umnyj-dvernoj-biometricheskij.html (дата звернення 20.05.2025).
7. Розумний дверний замок. URL: https://surl.li/qkotod (дата звернення 20.05.2025).
8. PES Alabay розумний замок із вбудованим відеодомофоном URL: https://surl.lu/pllcyb (дата звернення 20.05.2025).
9. Мікроконтролер ESP8266. URL: https://joy-it.net/en/products/SBC-NodeMCU (дата звернення 20.05.2025).
10. Плата розробника ESP-WROOM-32 ESP32 30 Pin URL: https://ardushop.in.ua/arduino/developer-board-esp-wroom-32-esp-32-wi-fi-bluetooth (дата звернення 20.05.2025).
11. Акумулятор 18650 Samsung INR 18650 29E 7 2900 mAh Li-ion 3.7B URL: https://bestbattery.com.ua/ua/li_ion_1850_ua/li_ion_18650_ua/18650_not_protected_ua/samsung_inr18650_29e_ua (дата звернення 20.05.2025).

12. I2C модуль розширення виводів Arduino для підключення дисплея URL: https://arduino.ua/prod1790-iici2cinterfeis-lcd1602-2004?srsltid=AfmBOopKXIqPe4vumYwo_JcLREXkonRTkz8oTr9Nq-a_lZjo1L0OBuuW (дата звернення 20.05.2025).

13. Макетна плата URL: https://miniboard.com.ua/maketni-plati/39-maketnaya-plata-400-points.html (дата звернення 20.05.2025).

14. Додаток Google Sheets URL: https://play.google.com/store/apps/details?id=com.google.android.apps.docs.editors.sheets&hl=ua (дата звернення 20.05.2025).

15. Одноплатний комп'ютер Raspberry Pi 5 4Gb URL: https://surli.cc/qoyqky (дата звернення 20.05.2025).

16. Приклад роботи метода POST URL: https://www.freecodecamp.org/ukrainian/news/naypopulyarnishi-sposoby-zrobyty-zapyt-http-u-javascript/ (дата звернення 20.05.2025).

17. Додаток для розробки програмного забезпечення Arduino IDE URL: https://apps.microsoft.com/detail/9nblggh4rsd8?hl=uk-UA&gl=UA (дата звернення 20.05.2025).

18. Бібліотека для використання плати ESP8266 у середовищі Arduion IDE URL: http://arduino.esp8266.com/stable/package_esp8266com_index.json (дата звернення 20.05.2025).

19. Liu C. C., Bedoya J. C., Sahani N., Stefanov A., Appiah-Kubi J., Sun C. C., et al. Cyber-physical system security of distribution systems. *Foundations and Trends in Electric Energy Systems.* 2021. Vol.4(4). P. 346-410.

20. Macheso P., Chisale S., Daka C., Dzupire N., Mlatho J., Mukanyirigira D. Design of standalone asynchronous ESP32 web-server for temperature and humidity monitoring. *IEEE.* 2021. Vol.7th Int. Conf. on Advanced Computing and Communication Systems. P. 635-638.

21. Lal R., Singh B., Wassay M. A. IoT in Smart Irrigation and Node MCU ESP 8266 Wi-Fi Module. *IEEE.* 2022. Vol.Int. Conf. on Computational Modelling, Simulation and Optimization. P. 296-300.

22. Bourennane A., Tanougast C., Diou C., Gorse J. Accurate Multi-Channel QCM Sensor Measurement Enabled by FPGA-Based Embedded System Using GPS. *Electronics.* 2023. Vol.12(12). P. Art. 2666.

23. Bureneva O., Mironov S. Fast FPGA-based multipliers by constant for digital signal processing systems. *Electronics.* 2023. Vol.12(3). P. Art. 605.

24. Rizqulloh S. R., Hadikusuma R. S., Aulia N., Hidayat R. Automatic Sluice Monitoring Based On The Water Ph In a Brackish Water Pool Using a Web Server. *Jurnal Elektro Teknik.* 2022. Vol.1(1). P. 22-29.

25. Paguay J. A. C., Brito G. A. H., Rojas D. L. H., Calva J. J. C. Secure home automation system based on ESP-NOW mesh network, MQTT and Home Assistant platform. *IEEE Latin America Transactions.* 2023. Vol.21(7). P. 829-838.

26. Puranik S., Barve M., Rodi S., Patrikar R. Acceleration of Trading System Back End with FPGAs Using High-Level Synthesis Flow. *Electronics.* 2023. Vol.12(3). P. Art. 520.

27. Puranik S., Barve M., Rodi S., Patrikar R. Acceleration of Trading System Back End with FPGAs Using High-Level Synthesis Flow. *Electronics.* 2023. Vol.12. P. Art. 520.

28. Tibaldi M., Pilato C. A Survey of FPGA Optimization Methods for Data Center Energy Efficiency. *IEEE Transactions on Sustainable Computing.* 2023.

29. Chakraborty S., Aithal P. S. IoT-Based Switch Board for Kids Using ESP Module And AWS. *International Journal of Case Studies in Business, IT, and Education (IJCSBE).* 2023. Vol.7(3). P. 248-254.

30. Kumar Y., Subba B. Stacking ensemble-based HIDS framework for detecting anomalous system processes in windows based operating systems using multiple word embedding. *Computers & Security.* 2023. Vol.125. P. Art. 102961.

31. Shukla A., Diwan R. IoT based load automation with remote access surveillance using ESP 32 Camand ESP 8266 module. *Annals of the Romanian Society for Cell Biology.* 2021. Vol.25(3). P. 6904-6914.

32. Arunyagool D., Chamnongthai K., Khawparisuth D. Monitoring and Energy Control Inside Home Using Google Sheets with Line Notification. *IEEE.* 2021. Vol.Int. Conf. on Power, Energy and Innovations (ICPEI). P. 99-102.

33. Mohammad A., Das R., Islam M. A., Mahjabeen F. Real-time Operating Systems (RTOS) for Embedded Systems. *Asian Journal of Mechatronics and Electrical Engineering.* 2023. Vol.2(2). P. 95-104.

34. Uddin N., Hermawan H., Darajat T. M., Marwanto S. Internet-based temperature monitoring system for hydroponic. *IOP Conference Series: Earth and Environmental Science.* 2021. Vol.922(1). P. Art. 012017.

35. Mitu N. S., Vassilev V., Tabany M. R. Low cost, easy-to-use, IoT and cloud-based real-time environment monitoring system using ESP8266 microcontroller. *International Journal of Internet of Things and Web Services.* 2021. Vol.6. P. 30-44.

36. Mitu N. S., Vassilev V., Tabany M. R. Low cost, easy-to-use, IoT and cloud-based real-time environment monitoring system using ESP8266 microcontroller. *International Journal of Internet of Things and Web Services.* 2021. Vol.6. P. 30-44.

37. Suryana T. Implementasi Komunikasi Web Server Nodemcu Esp8266 Dan Web Server Apache Mysql Untuk Otomatisasi Dan Kontrol Peralatan Elektronik Jarak Jauh Via Internet. 2021.

38. Chakraborty S., Aithal P. S. Communication Channels Review For ESP Module Using Arduino IDE And NodeMCU. *International Journal of Applied Engineering and Management Letters.* 2024. Vol.8(1). P. 1-14.

39. Szpyrka M., Suszalski P., Obara S., Nalepa G. J. Email campaign evaluation based on user and mail server response. *Applied Sciences.* 2023. Vol.13(3). P. Art. 1630.

40. Wang J., Wang Y., Zhang N. Secure and timely gpu execution in cyber-physical systems. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security.* 2023. P. 2591-2605.

41. Kossifos K. M., Georgiou J., Antoniades M. A. ASIC Enabled Programmable Metasurfaces-Part 2: Performance and Synthesis. *IEEE Transactions on Antennas and Propagation.* 2024.

42. Alassaf A. S. Linux OS Versus Windows OS Security. *International Journal of Multidisciplinary Innovation and Research Methodology.* 2023. Vol.2(3). P. 1-7.

43. Balasingam S., Zapiee M. K., Mohana D. Smart home automation system using IoT. *International Journal of Recent Technology and Applied Science (IJORTAS).* 2022. Vol.4(1). P. 44-53.

44. Gunawan A. A. S. The development of a smart door decision system, based on pir sensor, embedded face recognition and server request using ttgo esp 32. 2021.

45. Balasingam S., Zapiee M. K., Mohana D. Smart home automation system using IoT. *International Journal of Recent Technology and Applied Science (IJORTAS).* 2022. Vol.4(1). P. 44-53.

46. Pradisthi A. S., Aryanto J. Monitoring and automation system for bird feeding and drinking based on internet of things using ESP32. *Advance Sustainable Science, Engineering and Technology.* 2023. Vol.5(3). P. Art. 0230308.

47. Erwan A. N. M., Alfian M. N. H. M., Adenan M. S. M. Smart door lock. *International Journal of Recent Technology and Applied Science (IJORTAS).* 2021. Vol.3(1). P. 1-15.

48. Adenan M. S. M., Erwan A. N. M., Alfian M. N. H. M. Smart Smoke Detector. *International Journal of Recent Technology and Applied Science (IJORTAS).* 2021. Vol.3(1). P. 16-31.

49. McCalpin J. D. Bandwidth Limits in the Intel Xeon Max (Sapphire Rapids with HBM) Processors. *International Conference on High Performance Computing.* 2023. P. 403-413.

50. Nooyimsai S., Thaloy J., Jansengrat P., Janratchakool W., Krohkaew J., Crisnapati P. N., Thwe Y. Enhancing Breeding Control: The IoT-Driven Automated System for Budgie Farming. *IEEE.* 2023. Vol.11th International Conference on Cyber and IT Service Management (CITSM). P. 1-6.

51. Suryana T. Automation and Remote Control of Electronic Equipment Using the Internet with NODEMCU ESP8266 Interface and Apache MYSQL Web Server. 2021.

52. Msekh Z. A., Msekh A. A. Design and implementation wireless sensor node with security algorithm based on microcontroller esp8266. *Springer Nature Singapore.* 2021. Vol.Int. Conf. on Micro-Electronics and Telecommunication Engineering. P. 363-371.

53. Salikhov R. B., Abdrakhmanov V. K., Safargalin I. N. Internet of things (IoT) security alarms on ESP32-CAM. *Journal of Physics: Conference Series.* 2021. Vol.2096(1). P. Art. 012109.

54. Habibullah H. Sistem keamanan pintu rumah menggunakan solenoid dan keypad berbasis internet of things (IoT) dengan modul nodemcu esp8266. *Universitas Islam Negeri Maulana Malik Ibrahim.* 2021. P. Doctoral dissertation.

55. Swayamsiddha S., Mukherjee D., Ramavath S. Home automation using ESP8266 of IOT module. *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020.* 2021. Vol.1. P. 409–417.

56. Spandana N. N. N. Smart home automation through ESP8266. *Juni Khyat.* 2021. Vol.11(1). P. 301-305.

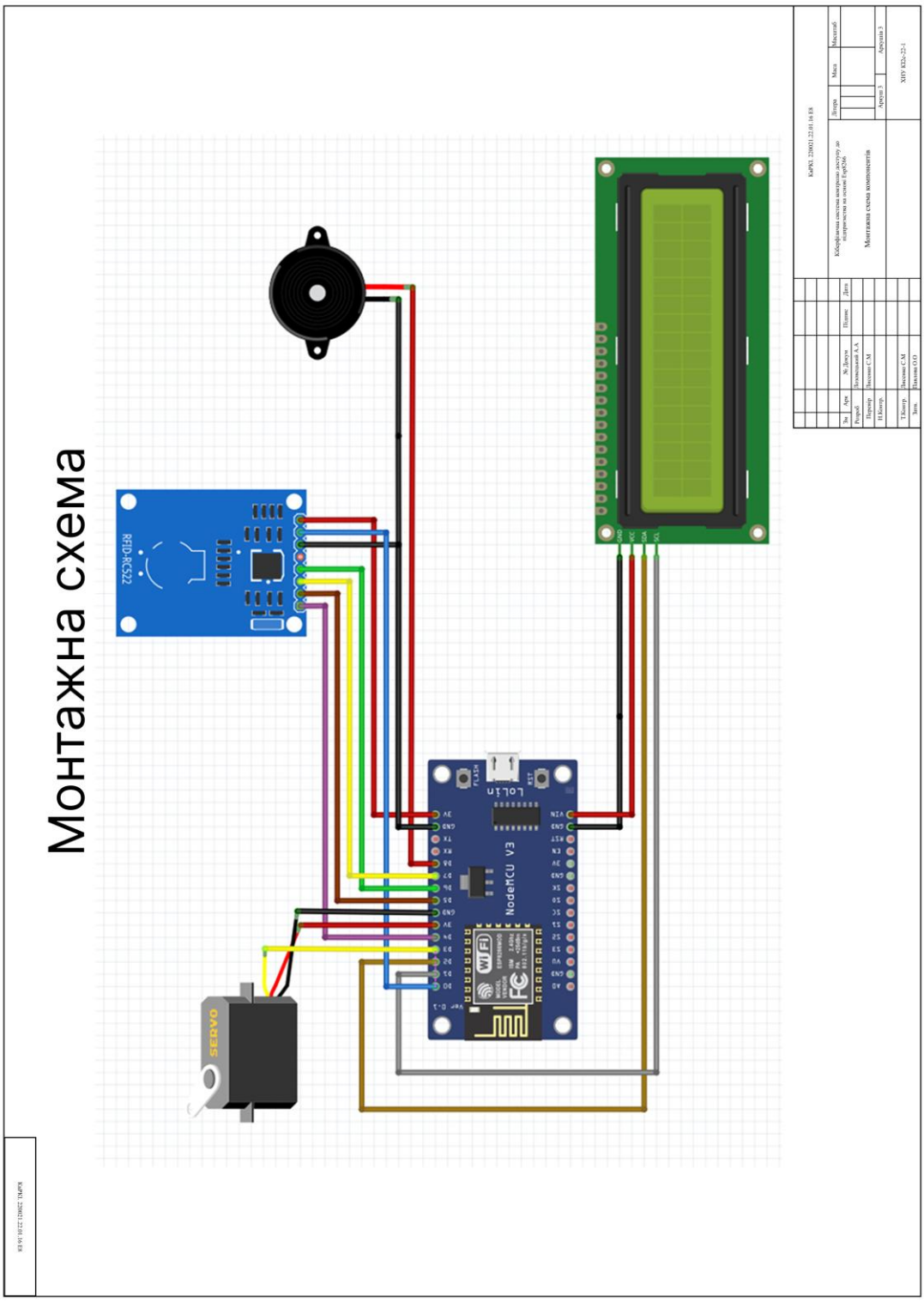
57. Chen C. Y., Wu S. H., Huang B. W., Huang C. H., Yang C. F. Web-based Internet of Things on environmental and lighting control and monitoring system using node-RED, MQTT and Modbus communications within embedded Linux platform. *Internet of Things.* 2024. Vol.27. P. Art. 101305.

58. Hasbullah M. Z., Mohamad H., Sabillah A. H. F., Mahamod U., Ariffin K. N. Z., Rahman S. A. IoT Based Indoor Air and Water Quality Monitoring System Using Node-RED. *IEEE.* 2023. Vol.9th International Conference on Computer and Communication Engineering (ICCCE). P. 161-166.

Додаток А

(обов’язковий)

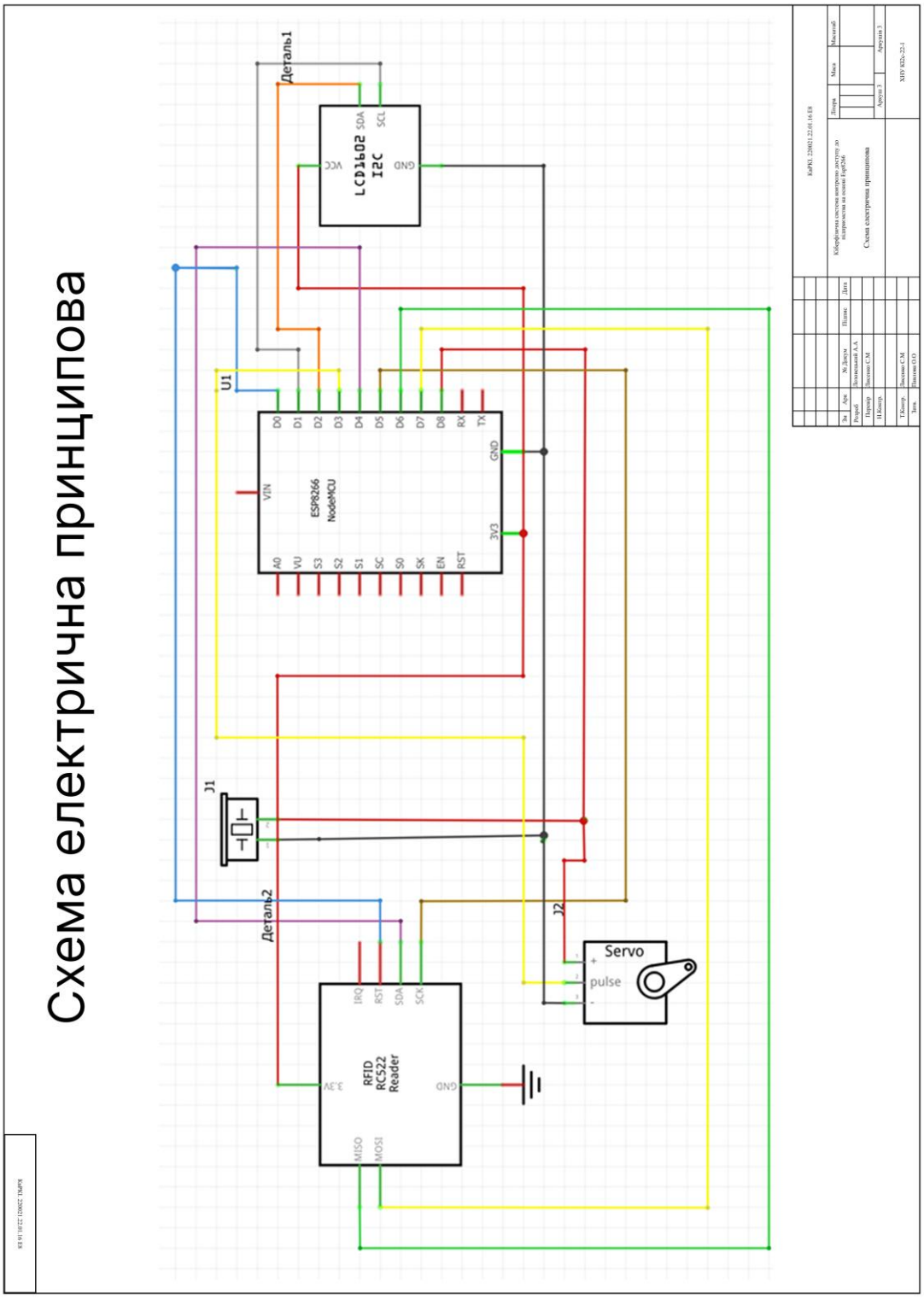
КОПІЯ КРЕСЛЕННЯ «МОНТАЖНА СХЕМА»



Додаток Б

(обов’язковий)

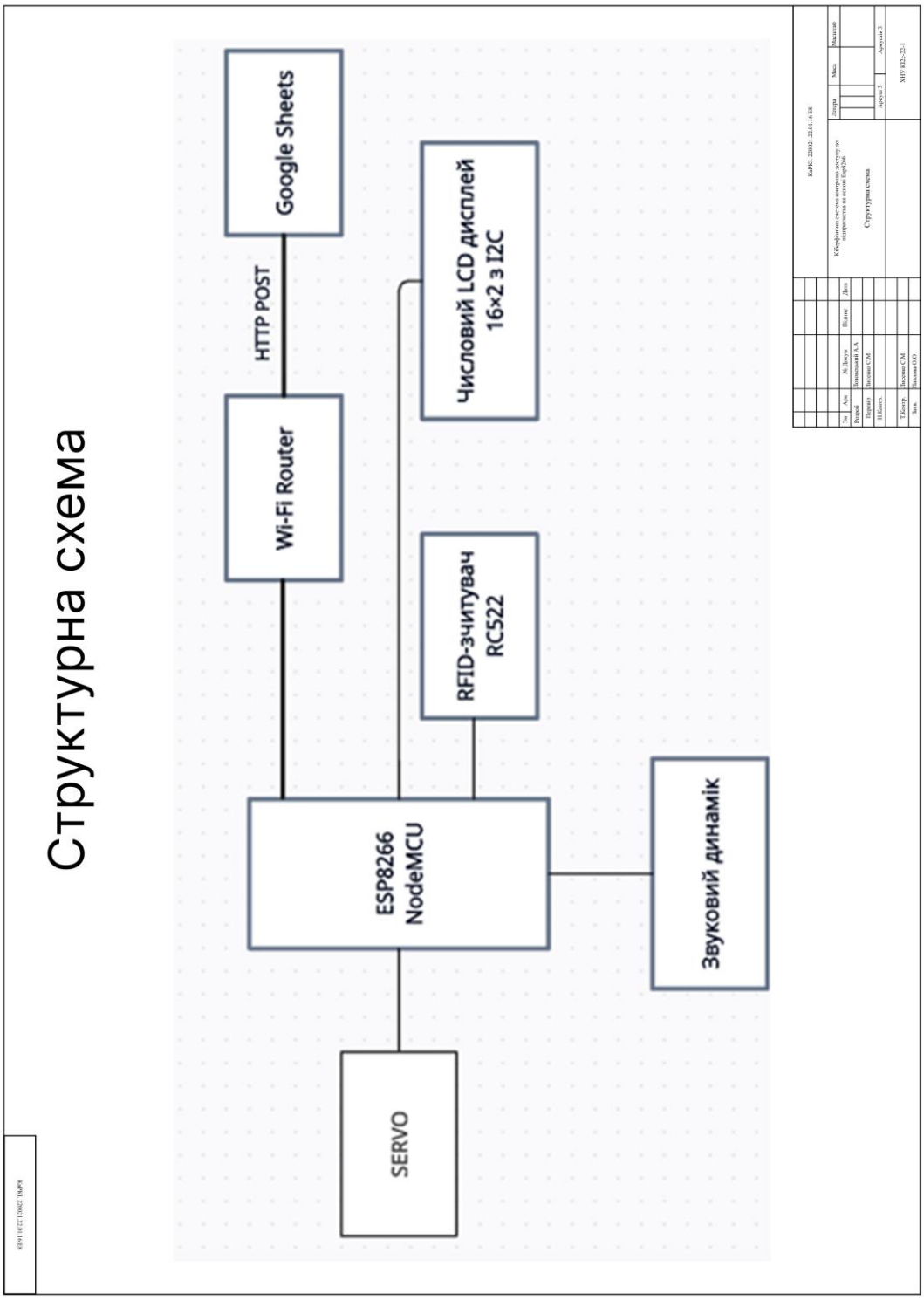
КОПІЯ КРЕСЛЕННЯ «СХЕМА ЕЛЕКТРИЧНА ПРИНЦИПОВА»



Додаток В

(обов’язковий)

КОПІЯ КРЕСЛЕННЯ «СТРУКТУРНА СХЕМА»



Додаток Г

(обов'язковий)

КОД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МІКРОКОНТРОЛЕРА ESP8266

```
    #include <Arduino.h>
    #include <ESP8266WiFi.h>
    #include <SPI.h>
    #include <MFRC522.h>
    #include <Servo.h>
    #include <HTTPSRedirect.h>
    #include <Wire.h>
    #include <LiquidCrystal_I2C.h>
    LiquidCrystal_I2C lcd(0x27, 16, 2);
    Servo doorServo;
    const char *GScriptId = "ID_Google";
    String gate_number = "Gate1";
    const char* ssid = "Tenda_DAC2B0";
    const char* password = "12344321";
    String payload_base = "{\"command\": \"insert_row\",
\"sheet_name\": \"Table\", \"values\": ";
    String payload = "";
    const char* host = "script.google.com";
    const int httpsPort = 443;
    String url = String("/macros/s/") + GScriptId + "/exec";
    HTTPSRedirect* client = nullptr;
    #define SS_PIN 2
    #define RST_PIN 16
    #define BUZZER 4
```

```
#define SERVO_PIN 0
MFRC522 mfrc522(SS_PIN, RST_PIN);
MFRC522::MIFARE_Key key;
MFRC522::StatusCode status;
int blocks[] = {4, 5, 6, 8, 9};
#define total_blocks (sizeof(blocks) / sizeof(blocks[0]))
int blockNum = 2;
byte bufferLen = 18;
byte readBlockData[18];
String student_id;
void setup() {
Serial.begin(9600);
SPI.begin();
lcd.init();
lcd.backlight();
lcd.setCursor(0, 0);
lcd.print("Connecting to");
lcd.setCursor(0, 1);
lcd.print("WiFi...");
WiFi.begin(ssid, password);
while (WiFi.status() != WL_CONNECTED) {
delay(1000);}
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("Connecting to");
lcd.setCursor(0, 1);
lcd.print("Google...");
delay(5000);
client = new HTTPSRedirect(httpsPort);
```

```
client->setInsecure();
client->setPrintResponseBody(true);
client->setContentTypeHeader("application/json");
for (int i = 0; i < 5; i++) {
if (client->connect(host, httpsPort)) {
lcd.clear();
lcd.print("Connected. OK");
delay(2000);
break;
}}
delete client;
client = nullptr;
mfrc522.PCD_Init();
doorServo.attach(SERVO_PIN);
doorServo.write(0);
}
void loop() {
static bool flag = false;
if (!flag) {
client = new HTTPSRedirect(httpsPort);
client->setInsecure();
client->setPrintResponseBody(true);
client->setContentTypeHeader("application/json");
flag = true;
}
if (client && !client->connected()) {
if (!client->connect(host, httpsPort)) {
lcd.clear();
lcd.print("Disconnected.");
```

```
lcd.setCursor(0, 1);
lcd.print("Retrying...");
return;
}}
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("Scan your Tag");
if (!mfrc522.PICC_IsNewCardPresent()) return;
if (!mfrc522.PICC_ReadCardSerial()) return;
String values = "", data;
for (byte i = 0; i < total_blocks; i++) {
ReadDataFromBlock(blocks[i], readBlockData);
data = String((char*)readBlockData);
data.trim();
if (i == 0) {
student_id = data;
values = "\"" + data + ",";
} else {
values += data + ",";
}}
values += gate_number + "\"}";
payload = payload_base + values;
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("Publishing Data");
if (client->POST(url, host, payload)) {
lcd.clear();
lcd.print("Access granted");
doorServo.write(90);
```

```
    delay(3000);
    doorServo.write(0);
    } else {
    lcd.clear();
    lcd.print("Failed.");
    lcd.setCursor(0, 1);
    lcd.print("Try Again");
    }
    delay(5000);}
    void ReadDataFromBlock(int blockNum, byte readBlockData[])
{
    for (byte i = 0; i < 6; i++) {
    key.keyByte[i] = 0xFF;}
    status =
mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A,
blockNum, &key, &(mfrc522.uid));
    if (status != MFRC522::STATUS_OK) {
    Serial.print("Authentication failed: ");
    Serial.println(mfrc522.GetStatusCodeName(status));
    return;}
    status = mfrc522.MIFARE_Read(blockNum, readBlockData,
&bufferLen);
    if (status != MFRC522::STATUS_OK) {
    Serial.print("Reading failed: ");
    Serial.println(mfrc522.GetStatusCodeName(status));
    return;}
    readBlockData[16] = ' ';
    readBlockData[17] = ' ';
    }}
```

Додаток Ґ

(обов'язковий)

КОД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ GOOGLE APPS SCRIPT

```
var SS = SpreadsheetApp.openById('mTOEL_d08oonBW0qne1prqv6szqCI');
var timezone = "europe/kyiv";
var hours = 0;
var str = "";
function doPost(e) {
  var parsedData;
  var result = {};
  try {
    parsedData = JSON.parse(e.postData.contents);
  } catch(f){
    return ContentService.createTextOutput("Error in parsing request body: " + f.message);}
  if (parsedData !== undefined){
    var flag = parsedData.format;
    if (flag === undefined){
      flag = 0;
    }
    var sheet = SS.getSheetByName(parsedData.sheet_name);
    if (sheet == null) {
      return ContentService.createTextOutput("Error: Sheet with the name '" + parsedData.sheet_name + "' not found.");
    }
    var dataArr = parsedData.values.split(",");
```

```
        var Curr_Date = Utilities.formatDate(new Date(),
timezone, "MM/dd/yyyy");
        var Curr_Time = Utilities.formatDate(new Date(),
timezone, "hh:mm:ss a");
        var value0 = dataArr[0];
        var value1 = dataArr[1];
        var value2 = dataArr[2];
        var value3 = dataArr[3];
        var value4 = dataArr[4];
        var value5 = dataArr[5];
        var data = sheet.getDataRange().getValues();
        var row_number = 0;
        var time_out = "";
        for(var i = 0; i < data.length ; i++){
          if(data[i][0] == value0){
            row_number = i+1;
            time_out = data[i][2];
            break;
          }
        }
        if(row_number > 0){
          if(time_out === ""){
            sheet.getRange("C"+row_number).setValue(Curr_Time);
            str = "Success";
            return ContentService.createTextOutput(str);
          }
        }
        switch (parsedData.command) {
          case "insert_row":
```

```
            sheet.insertRows(2);
            sheet.getRange('A2').setValue(value0);
            sheet.getRange('B2').setValue(Curr_Time);
            sheet.getRange('D2').setValue(value5);
            sheet.getRange('E2').setValue(Curr_Date);
            sheet.getRange('F2').setValue(value1);
            sheet.getRange('G2').setValue(value2);
            sheet.getRange('H2').setValue(value3);
            sheet.getRange('I2').setValue(value4);
            str = "Success";
            SpreadsheetApp.flush();
            break;
          case "append_row":
            var publish_array = new Array();
            publish_array[0] = value0;
            publish_array[1] = Curr_Time;
            publish_array[3] = Curr_Date;
            publish_array[4] = value1;
            publish_array[5] = value2;
            sheet.appendRow(publish_array);
            str = "Success";
            SpreadsheetApp.flush();
            break;     }
        return ContentService.createTextOutput(str);
      } else {
        return ContentService.createTextOutput("Error! Request
body empty or in incorrect format.");
      }}
```

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 2.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 14%**

ID: 242675 Title: БКР Кіберфізична система контролю доступу до підприємства на основі Esp8266 Added in a DB: 2025-05-30 Authors: Андрій ЛОЗОВЕЦЬКИЙ Heads: Сергій ЛИСЕНКО Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	80693	565	2316 (3%)	33 (6%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Андрій ЛОЗОВЕЦЬКИЙ

Співавтор:

Назва: Лозовецький_Кіберфізична система контролю доступу до підприємства на основі Esp8266

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:8.7%

Коефіцієнт подібності 2:3.5%

Мікропробіли: 10

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-05-30 20:03:46.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-05-31 Доцент Андрій Нічепорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Лозовецький Андрій Анатолійович

Тема: Кіберфізична система контролю доступу до підприємства на основі Esp8266

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___60___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проектування кіберфізичної системи контролю доступу до підприємства на основі Esp8266.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено дослідження предметної області (проаналізовано мікроконтролери Arduino UNO та ESP8266, виявлено переваги та недоліки кожного з них, а також розглянуто модулі безконтактного зчитування RFID-карток. В другому розділі кваліфікаційної роботи проведено аналіз та підбір компонентів для проектування та розробки кіберфізичної системи контролю доступу до підприємства на основі Esp8266, розглянуто принцип функціонування кіберфізичної системи, проведено дослідження одноплатних комп'ютерів та HTTPS-запитів а також проведено аналіз електричних характеристик компонентів системи а також системи в цілому. В третьому розділі кваліфікаційної роботи виконано програмну та фізичну реалізацію кіберфізичної системи контролю доступу до підприємствана основі Esp8266, розглянуто підготовку середовища для розробки програмного забезпечення, описано схему підключення елементів системи, створено схему електричну принципову, виконано розведення друкованої плати у програмному забезпечені Fritzing, а також зроблено опис необхідних бібліотек для створення

програмного забезпечення та описано алгоритм функціонування кіберфізичної системи.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: не розглянуто процес збереження та запису інформації RFID міток.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: –

9. Оцінка дипломної роботи: Задовільно

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Корнуш Юрій Володимирович

доцент кафедри ІСТ

"2" червня 2025 р. _____(підпис)

Завідувачу кафедри КІІС
д-р. філософії, доц. Ользі ПАВЛОВІЙ

Андрія ЛОЗОВЕЦЬКОГО
ПІБ здобувача вищої освіти

ФІТ, 3 курсу, групи КІ2с-22-1

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 (Strike-Plagiarism 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.

07.06 2025 року

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: Кіберфізична система контролю доступу до підприємства на основі Esp8266

Автор: Андрій ЛОЗОВЕЦЬКИЙ

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Сергій ЛИСЕНКО, 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 розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10 джерелами на один фрагмент речення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 8.7% і адресується до 47 першоджерел; та системою Anti-Plagiarism складає 2.0%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Сергій ЛИСЕНКО

Гарант ОП _____ Андрій НІЧЕПОРУК

Завідувач кафедри КІС _____ Ольга ПАВЛОВА