Вінницький національний технічний університет
(повне найменування вищого навчального закладу)
Факультет Інформаційних електронних систем
(повне найменування інституту, назва факультету (відділення))
Кафедра Інформаційних радіоелектронних технологій і систем
(повна назва кафедри (предметної, циклової комісії))

ПОЯСНЮВАЛЬНА ЗАПИСКА
до бакалаврської дипломної роботи на тему:

«РОЗУМНИЙ IoT БУДИЛЬНИК НА ARDUINO»

Виконав: студент 2 (4)-го курсу, групи ТКР-22мс,
спеціальності 172 – Телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)
Гладкий М.О.
(прізвище та ініціали)
Керівник: к.т.н., доц., доцент каф. ІРТС
Воловик А.Ю.
(прізвище та ініціали)
«12» 06 2024 р.

Рецензент: д.т.н., доц., професор каф. ІКСТ
Михалевський Д.В.
(прізвище та ініціали)
«12» 06 2024 р.

Допущено до захисту
Завідувач кафедри ІРТС
д.т.н., проф. Осадчук О.В.
(прізвище та ініціали)
«13» 06 2024 р.

Вінниця ВНТУ - 2024 рік

Вінницький національний технічний університет
Факультет Інформаційних електронних систем
Кафедра Інформаційних радіоелектронних технологій і систем
Рівень вищої освіти перший (бакалаврський)
Галузь знань – 17 Електроніка та телекомунікації
Спеціальність – 172 – Телекомунікації та радіотехніка
Освітньо-професійна програма – Радіотехніка

ЗАТВЕРДЖУЮ
Завідувач кафедри ІРТС
Олександр ОСАДЧУК
15 березня 2024 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ
Гладкому Мирославу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи. «Розумний IoT будильник на Arduino»
керівник роботи Воловик Андрій Юрійович, к.т.н., доцент каф. ІРТС
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "11"03 2024 року № 80
2. Строк подання студентом роботи 10 06 2024 року

3. Вихідні дані до роботи: Wi-Fi 802.1 lb/g/n до 150 Мб/с, напруга живлення: 5 В, робоча температура -30°С~ 70°С

4. Зміст текстової частини: Вступ. Аналіз сучасного стану розвитку науки та техніки у галізу інтернету речей. архітектура та апаратура IoT будильника. Експериментальна частина. Охорона праці. Висновки. Список використаних джерел. Додатки..

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень): Структурна схема IP камери відеонагляду на модулі ESP32-CAM
Схема електрична принципова та перелік елементів
Кресленик друкованої плати
Складальний кресленик

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	виконання прийняв
Основна частина	к.т.н., доцент, доцент каф. ІРТС Воловик А.Ю.		
Охорона праці	професор кафедри БЖДПБ, професор, д.п.н., Дембіцька С.В.		

7. Дата видачі завдання 17.03. 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1.	Вибір, узгодження та затвердження теми БДР	14.02.2024-28.02.2024	
2.	Огляд та аналіз літературних джерел.	01.03.2024-10.03.2024	
3.	Затвердження теми. Розробка завдання на БДР.	11.03.2024-31.03.2024	
4.	Попередня розробка основних розділів. Аналіз вирішення поставленої задачі. Розробка структурної схеми та технічних рішень.	01.04.2024-06.05.2024	
5.	Математичне моделювання та електричні розрахунки . Експериментальне дослідження.	07.05.2024-18.05.2024	
6.	Розробка графічної частини БДР	19.05.2024-22.05.2024	
7.	Охорона праці (ОП)	23.05.2024-28.05.2024	
8	Оформлення пояснювальної записки та графічної частини.	29.05.2024-05.06.2024	
9.	Нормоконтроль	06.06.2024-07.06.2024	
10.	Попередній захист БДР, доопрацювання, рецензування БДР	08.06.2024-10.06.2024	
11.	Захист БДР ЕК	11.06.2024-17.06.2024	

Студент _____ Гладкий М.О.
(підпис)

Керівник роботи _____ Воловик А.Ю.
(підпис)

АНОТАЦІЯ

УДК 621.396

Гладкий М.О. Розумний IoT будильник на ARDUINO. Бакалаврська дипломна робота. – Вінниця: ВНТУ, 2024. – 95 с. Українською мовою. Бібліогр.: 54. назв; Рис.: 40.

Розумні пристрої стали невід'ємною частиною таких архітектур, як Інтернет речей (IoT), Кіберфізичні системи (CPS) та Інтернет всього (IoE). Навпаки, ці архітектури становлять систему для реалізації концепції розумних міст і, зрештою, розумної планети. Застосування цих інтелектуальних пристроїв поширюється на різні кіберфізичні системи в архітектурі розумного міста, тобто розумні будинки, розумну охорону здоров'я, розумний транспорт, розумну мережу, розумне сільське господарство тощо. Край мережі з'єднує ці розумні пристрої (сенсори, агрегатори). , і приводи), які можуть працювати у фізичному середовищі та збирають дані, які надалі використовуються для прийняття обґрунтованого рішення через приведення в дію. Тут безпека цих пристроїв надзвичайно важлива, зокрема з точки зору автентифікації, оскільки у випадку неавтентифікованих/зловмисних активів під загрозою буде вся інфраструктура. Ми пропонуємо оновлений огляд механізмів автентифікації за категоріями централізованих і розподілених архітектур. Ми обговорюємо питання безпеки щодо автентифікації цих розумних пристроїв із підтримкою Інтернету речей. Ми оцінюємо та аналізуємо дослідження запропонованих літературних схем, які створюють проблеми автентифікації з точки зору обчислювальних витрат, накладних витрат на зв'язок і моделей, застосованих для досягнення надійності.

Ключові слова: IoT, будильник, годинник, розумний дім

ABSTRACT

Smooth M.O. Smart IoT alarm clock on ARDUINO. Bachelor thesis. – Vinnytsia: VNTU, 2024. – 95 p. In ukrainian. Bibliography: 54 titles; Fig.: 40.

Smart devices have become an integral part of architectures such as the Internet of Things (IoT), Cyber-Physical Systems (CPS), and the Internet of Everything (IoE). Rather, these architectures constitute a system for realizing the concept of smart cities and, ultimately, a smart planet. The application of these intelligent devices extends to various cyber-physical systems in smart city architecture, i.e. smart homes, smart healthcare, smart transportation, smart grid, smart agriculture, etc. The edge of the network connects these smart devices (sensors, aggregators). , and actuators) that can operate in a physical environment and collect data that is further used to make an informed decision through actuation. Here, the security of these devices is extremely important, particularly in terms of authentication, as the entire infrastructure will be at risk in case of unauthenticated/malicious assets. We offer an updated overview of authentication mechanisms categorized by centralized and distributed architectures. We discuss the security issues around authentication of these IoT-enabled smart devices. We evaluate and analyze studies of proposed literature schemes that pose authentication challenges in terms of computational cost, communication overhead, and models applied to achieve trustworthiness.

Keywords: IoT, alarm clock, clock, smart home

ЗМІСТ

ВСТУП

Виконуючи свою основну функцію, годинники часто є художніми та ювелірними виробами, що мають значну цінність завдяки унікальному дизайну.

Сучасні годинники, механічні, електронні або атомні, використовують для вимірювання часу періодичні процеси — автоколивання. Принципова будова всіх типів годинників однакова: вони мають у своєму складі коливну систему, контрольний механізм, джерело енергії та індикатор. Контрольний механізм забезпечує надходження енергії від джерела до коливної системи порціями, що компенсують дисипацію енергії в ній. Індикатор служить для того, щоб відображати інформацію про час на циферблаті зі стрілками або електронному дисплеї.

Механічні годинники використовують гармонічні коливання маятника або пружини, компенсуючи втрату енергії на тертя контрольованим поступанням енергії від джерела. Контроль за отриманням енергії здійснюється завдяки анкерному механізму.

Маятниковий годинник має довгий стрижень із вантажем на кінці, який вільно гойдається у обидва боки. Маятник завжди гойдається з постійною швидкістю, завдяки чому маятниковий годинник відлічує час із великою точністю. Джерелом енергії у маятниковому годиннику є гиря, піднята на певну висоту. Вона повільно опускається з кожним поворотом анкера, віддаючи свою енергію маятнику.

У наручних механічних годинниках замість маятника використовуються обертальні коливання балансира, а джерелом енергії служить скручена пружина.

У електронних годинниках використовуються коливання п'єзоелектричного кристалу кварцу, роль контрольного механізму відіграє електронна схема, а джерелом енергії є батарейка.

Найточнішими є атомні годинники, принцип дії яких полягає у вимірюванні частоти випромінювання окремих атомів. Сучасний еталон секунди визначається, як 9,192,631,770 періодів випромінювання атома

цезію-133 при переході між двома надтонкими рівнями основного стану, розщепленими у магнітному полі ядра, при сталій довжині хвилі, нульовій температурі й відсутності зовнішнього магнітного поля.

Тема дипломної роботи є актуальною для легкого відображення точного часу, а також відображення місцевої погоди.

Точний час і реальна температура навколишнього середовища - це інформаційні продукти, які завжди є актуальними і необхідними для людей. На дисплей, крім відображення часу і температури, можуть також виводиться число, номер місяця і року, атмосферний тиск, радіаційний фон і т.д.

Метою роботи є дослідження IoT будильника з метою покращення її ефективності та підвищення надійності.

Основними задачами дослідження **є:**

- Дослідження можливостей модуля Wemos D1 mini та його використання у IoT будильнику;
- розробка програмного забезпечення для виведення поточного часу та погоди на світлодіодну адресну матрицю;
- тестування розробленого програмного забезпечення та його оцінка.

Об'єктом дослідження є розумний IoT будильник на Arduino

Предметом дослідження є параметри та характеристики розумного IoT будильника на Arduino.

1 АНАЛІЗ СУЧАСНОГО СТАНУ РОЗВИТКУ НАУКИ ТА ТЕХНІКИ У ГАЛУЗІ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Тенденції зростання кількості користувачів Інтернету речей

Експоненціальна кількість інтелектуальних пристроїв, які щодня підключаються до Інтернету, призводить до створення мережі малопотужних пристроїв, які спілкуються між собою. Зв'язок із/без майнера чи сервера дає змогу створити мережу «пристрій-пристрій» (D2D) або «машина-машина» (M2M) [1]. З іншого боку, Інтернет став глобальною ареною для підключення цих розумних пристроїв, але спостерігається експоненціальне зростання кількості підключених розумних пристроїв. Згідно з нещодавнім річним звітом Cisco про Інтернет (2018–2023), майже дві третини населення планети матимуть доступ до Інтернету до 2023 року, що означає, що в майбутньому до Інтернету може бути підключено більше пристроїв. У звіті прогнозується приблизно 5,3 мільярда користувачів Інтернету, тобто 66 відсотків населення світу, до 2023 року. Згідно з оцінками, у 2018 році населення світу збільшиться на 51 відсоток [1], як показано на рисунку 1.1.

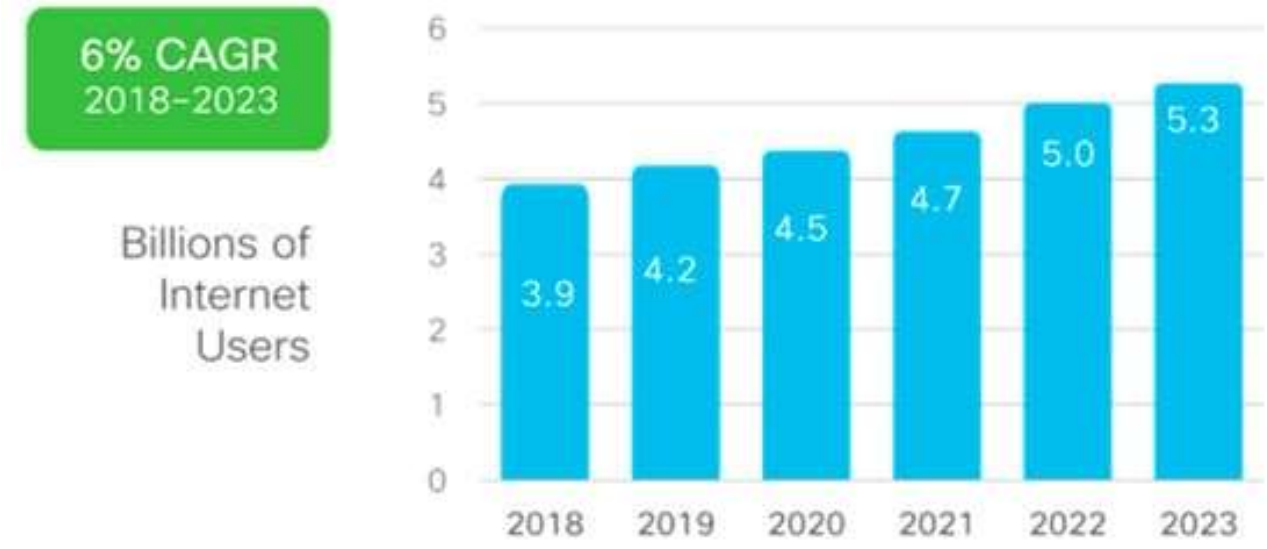


Рисунок 1.1 – Графік зростання кількості користувачів Інтернету з 2018 по 2023 рр.

Ці об’єкти та процеси, пов’язані з Інтернетом речей, були розроблені на основі традиційного протоколу керування передачею/протоколу Інтернету (TCP/IP) на основі стеку Інтернету. Вони не розраховані на таку величезну кількість підключених пристроїв. Він вимагає надійних рішень, які можуть стати основою для його впровадження та інтеграції. Завдяки мережевим моделям, що лежать в основі, все більша кількість інтелектуальних пристроїв успадковує проблеми конфіденційності та безпеки підключених інтелектуальних пристроїв і самої мережі [2]. Ці пристрої відіграють важливу роль у кожному домені, оскільки вони являють собою межу мережі, де збирання даних у реальному часі здійснюється в кібернетичному та фізичному просторі. Широке впровадження цих розумних пристроїв призвело до концепції розумних міст, де багато розумних пристроїв працюють у різних мережах IoT. Він підтримував реалізацію інших кіберфізичних систем, таких як розумні будинки, розумні паркування, розумні будівлі, розумна охорона здоров’я, розумна роздрібна торгівля, розумний транспорт, розумне управління відходами, розумна мережа, розумне сільське господарство тощо, як показано на рисунку 1.2 [3].

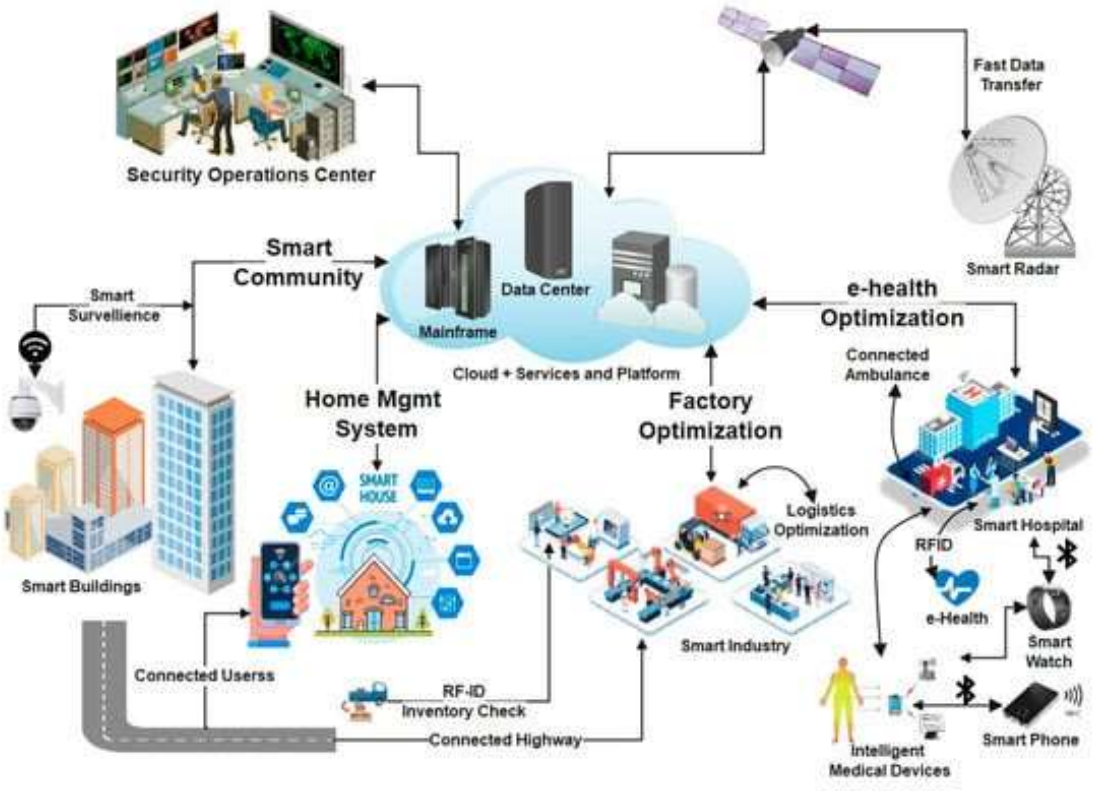


Рисунок 1.2 – Узагальнена архітектура розумного міста

Ці розумні пристрої з підтримкою Інтернету речей, що працюють у відповідних доменах, зрештою призведуть до концепції розумної планети, де всі системи будуть сумісні та взаємопов'язані. Край мережі з'єднує ці інтелектуальні пристрої, такі як датчики, агрегатори та виконавчі механізми, які можуть працювати у фізичному середовищі та збирати дані, які надалі використовуються для прийняття обґрунтованих рішень за допомогою активації. Оскільки ці пристрої працюють на граничному рівні, їх називають граничними вузлами, вони зазвичай малопотужні та відповідають за надсилання певної інформації. Граничні вузли, які працюють в інфраструктурі IoT, є пристроями IoT [4].

1.2 Вдосконалюючі технології

Ці інтелектуальні пристрої використовують відповідні технології на основі типу мереж, тобто бездротові сенсорні мережі (WSN), технології п'ятого/шостого покоління (5G/6G), хмарні обчислення, туманні обчислення тощо [4]. Підключення, яке забезпечується традиційними мережевими технологіями, такими як Wireless Fidelity (Wi-Fi), радіочастотна ідентифікація (RFID), Bluetooth (BT), Near Field Communication (NFC) тощо, підтримує збір і передачу даних, як показано на рисунку 2. Оскільки архітектура розумного міста також покладається на звичайний Інтернет, який підтримується технологіями зв'язку та передачі даних, відповідно, очевидно, що вона може успадкувати проблеми безпеки та конфіденційності.

Тут безпека цих пристроїв надзвичайно важлива, зокрема з точки зору автентифікації, оскільки у випадку неавтентифікованих/зловмисних активів під загрозою буде вся інфраструктура. Багато дослідників в наукових колах і промисловості запропонували різні методи захисту цих інтелектуальних пристроїв і даних, створених ними. Розглядаючи ці проблеми, ми переглянемо літературу, присвячену механізмам автентифікації для інтелектуальних пристроїв із підтримкою Інтернету речей у розумних містах.

1.3 Пов’язані опитування

Кілька опитувань обговорюють проблеми безпеки, пов’язані з розумними активами з підтримкою Інтернету речей у контексті розумного міста. Автори обговорюють питання автентифікації IoT у [5], надаючи широкий спектр протоколів автентифікації, запропонованих у літературі. Використовуючи багатокритеріальну класифікацію, вони порівнюють і оцінюють запропоновані протоколи автентифікації, показуючи їхні сильні та слабкі сторони в багатьох CPS і визначаючи кілька вимог. Відкриті питання можуть бути розглянуті під час розробки нових схем автентифікації для мереж і додатків IoT. Автори в [6] визначають кілька ключових технічних проблем і вимог до комунікаційних систем IoT, заснованих на конфіденційності, безпеці, інтелектуальній конструкції датчиків/приводів, низькій вартості та складності, універсальній конструкції антени та зручному розумному дизайні кіберфізичної системи для її розгортання. . Нарешті, автори представляють проблеми з розгортанням кіберфізичної системи зв’язку та пов’язані з цим проблеми впровадження ефективної та дієвої системи зв’язку IoT. У [7] було представлено всеосяжне дослідження кіберфізичних систем (CPS), що стосується додатків, технологій, стандартів і відповідних вразливостей безпеки, загроз і атак. Далі це веде до визначення ключових проблем і викликів у цій сфері

Крім того, були обговорені та оцінені існуючі заходи безпеки для подальшого посилення визначення обмежень. Різноманітні аспекти безпеки, послуги та найкращі практики забезпечують стійкість і безпеку систем CPS. Опитування зосереджено на CPS, які стикаються з проблемами щодо послуг безпеки, автентифікації та авторизації з пропозиціями та рекомендаціями.

Еволюція технології блокчейн (BC) з урахуванням складових технологій, консенсусних алгоритмів і платформ блокчейну була представлена в [8]. Автори обговорюють питання безпеки для розумних міст і критично оцінюють різні інтелектуальні програми, що підтримуються рішеннями з підтримкою блокчейну. Реалізація на основі реального сценарію блокчейну була

представлена як практичний приклад для подальшого посилення огляду. Огляд представляє ключові потреби для інтеграції ВС у розумні міста та дослідницькі прогалини з точки зору вдосконалення. Систематичний огляд розумних міст на основі Інтернету речей (IoT) і блокчейну (ВС) був представлений зі статистичним аналізом у [9]. Автори обговорюють розподілену природу ВС, яка була прийнята багатьма підприємствами, що створює проблеми для розумних міст на основі IoT. Оскільки Інтернет речей вплинув на сучасне суспільство та індустрію, він створює деякі проблеми з безпекою та конфіденційністю. Автори представляють системний підхід до визначення значущих механізмів та досліджень щодо безпеки в IoT та ВС у розумних містах. Аналіз показує, що інтеграція ВС забезпечує надійну конфіденційність, безпеку, розподілене зберігання, прозорість і довіру, що є гострою потребою для розумних міст на основі Інтернету речей.

Огляд у [10] присвячений блокчейну як потенційній технології, яка може забезпечити надійний механізм безпеки для розумних міст. Автори представляють найсучаснішу технологію блокчейн для вирішення проблем безпеки розумних міст. Це пов’язано з такими основними властивостями, як здатність до аудиту, прозорість, незмінність і децентралізація. Автори пропонують запровадити блокчейн у різних розумних спільнотах, таких як охорона здоров’я, транспорт, розумна мережа, управління ланцюгами поставок, фінансові системи тощо, що представляє майбутні напрямки дослідження опитування. Автори в [11] наголошують на необхідності впровадження механізмів безпеки, які можуть вирішувати зростаючі проблеми безпеки, з якими зіткнеться спільнота ІКТ під час переходу від традиційного способу життя до взаємопов’язаного світу розумних міст.

Огляд моделей блокчейну було запропоновано як взаємодію блокчейну зі смарт-контрактами, і їх застосування в електронному урядуванні сприятиме досягненню надійної безпеки та конфіденційності. Огляд пропонує вдосконалення та додавання нових сценаріїв, які могли б допомогти у подальшому вдосконаленні цього складного та надто амбітного підприємства. В

огляді в [12] представлено огляд багаторівневих архітектур IoT і пов’язаних з ними атак. Було обговорено механізми, які забезпечують вирішення проблем безпеки, з обмеженнями, які висуваються в тому ж напрямку. Опитування розглядає існуючі механізми безпеки для захисту інфраструктури IoT, а також обмеження та правила поточних методів безпеки. Для кращого розуміння також було обговорено декілька відкритих дослідницьких проблем, пов’язаних із технологією IoT. Огляд літератури в [13] визначає компоненти розумного міста для реалізації концепції. Обговорюються реальні впровадження та статистичний аналіз з огляду на контекст розумних міст. Оскільки розумні міста стикаються з серйозними викликами та проблемами через величезні вимоги до обробки даних і неоднорідність розумних активів, було визначено огляд цих майбутніх дослідницьких проблем із описом можливостей для вдосконалення.

Автори в [14] представляють поточні проблеми IoT і блокчейну, а також аналізують потенційні переваги обох. Огляд доступних блокчейн-платформ і руйнівних додатків у цій галузі було виділено для вирішення цих проблем. Автори в [15] обговорюють характеристики технології блокчейн, зосереджуючись на інтеграції технології розподіленої книги в розумні міста. Концептуальна архітектура, заснована на блокчейні, пояснює безпеку на прикладі можливого використання. Крім того, практичне дослідження розумного міста на основі блокчейну обговорювало кілька важливих проблем дослідження.

Концептуальна модель додатків IoT для підприємств була представлена в [16] шляхом визначення додатків IoT для моніторингу та контролю, великих даних і бізнес-аналітики, а також для обміну інформацією та співпраці. Опитування зосереджено на інвестиційних можливостях та оцінці за допомогою NPV і реальних опціонів. Обговорювалися проблеми розгортання додатків IoT для підприємств.

Огляд вищезазначених пов’язаних опитувань розширено до кількох доменів. Однак інтелектуальні пристрої з підтримкою IoT стали важливою частиною таких архітектур, як Інтернет речей (IoT), кіберфізичні системи (CPS),

Інтернет кіберфізичних речей (IoCPT) та Інтернет усього (IoE).). Навпаки, ці архітектури становлять систему для реалізації концепції розумних міст і, зрештою, розумної планети. Було проведено огляд літератури, враховуючи всі вищезазначені архітектурні домени. Конфіденційність, цілісність і доступність служб безпеки (CIA), включаючи автентифікацію, авторизацію та аудит (AAA), є надзвичайно важливими для захисту цих розумних активів; отже, ми взяли на себе ініціативу в наданні оновленого огляду механізмів автентифікації. Цей комплексний огляд є продовженням оглядової статті [17], в якій обговорювалися нещодавно запропоновані рішення на основі блокчейну для автентифікації інтелектуальних пристроїв з підтримкою IoT. Однак у цій статті було прийнято категоричний та описовий підхід шляхом класифікації централізованих і розподілених архітектур. У цьому огляді порівнюються механізми, обговорюючи проблеми безпеки під час автентифікації та ідентифікації інтелектуальних пристроїв із підтримкою IoT. Окрім рішень на основі блокчейну, інші рішення на основі штучного інтелекту та криптосистеми також обговорювалися в майбутніх напрямках досліджень. Огляд запропонованих схем було оцінено на основі точок надійності та слабкості, що зрештою допоможе усунути неоднозначності для вдосконалення в майбутньому. Однак конвергентні схеми автентифікації, засновані на централізованих і розподілених архітектурах, викликають нові проблеми. Основні внески статті представлені нижче.

- Ми досліджуємо та обговорюємо багатошарову архітектуру розумного міста для використання схем автентифікації в різних сценаріях розумного міста.
- Ми розглядаємо та аналізуємо існуючі служби безпеки та пов’язані з ними проблеми та проблеми в розумних містах.
- Ми надаємо глибокі огляди та обговорюємо раннє впровадження традиційних найсучасніших схем автентифікації для розумних активів із підтримкою Інтернету речей, щоб розкрити весь їхній потенціал у розумних містах.

- Ми представляємо вичерпну класифікацію та детальні огляди останніх схем автентифікації для розумних активів із підтримкою Інтернету речей у розумних містах.
- Крім того, ми ретельно переглянули, оцінили та проаналізували схеми автентифікації з підтримкою Інтернету речей на основі централізованих і розподілених архітектур розумних міст із підтримкою блокчейну.
- Ми представляємо та розробляємо нову концепцію Blockchain-as-a-Service в результаті перегляду існуючих рішень та обговорення відповідних проблем і проблем у розумних містах.
- Ми визначили та обговорили плюси та мінуси існуючих схем автентифікації в архітектурі розумних міст.
- Нарешті, ми надаємо останні досягнення та майбутні рекомендації щодо схем автентифікації з підтримкою Інтернету речей у розумних містах і завершуємо статтю в останньому розділі.

1.4 Рівнева архітектура розумного міста

Архітектуру розумного міста можна класифікувати на рівні на основі активів, що працюють у фізичному кіберпросторовому середовищі, яке забезпечує підключення до мережі для потоку даних, наприклад Інтернету. Дані, отримані фізичними активами, тобто датчиками, агрегаторами та виконавчими механізмами, обробляються на фізичному рівні, який називається сенсорним рівнем. Командно-контрольна робота на прикладному рівні визначає програми для поведінки активу на фізичному рівні. Мережа забезпечує підключення за допомогою технологій зв’язку та передачі на рівні передачі. Хоча різні дослідники мають різні думки [18], архітектуру розумного міста можна в основному розділити на трирівневу архітектуру, як показано на рисунку 1.3. Функції, проблеми та слабкі сторони рівнів детальніше досліджуються та обговорюються нижче в цьому розділі.

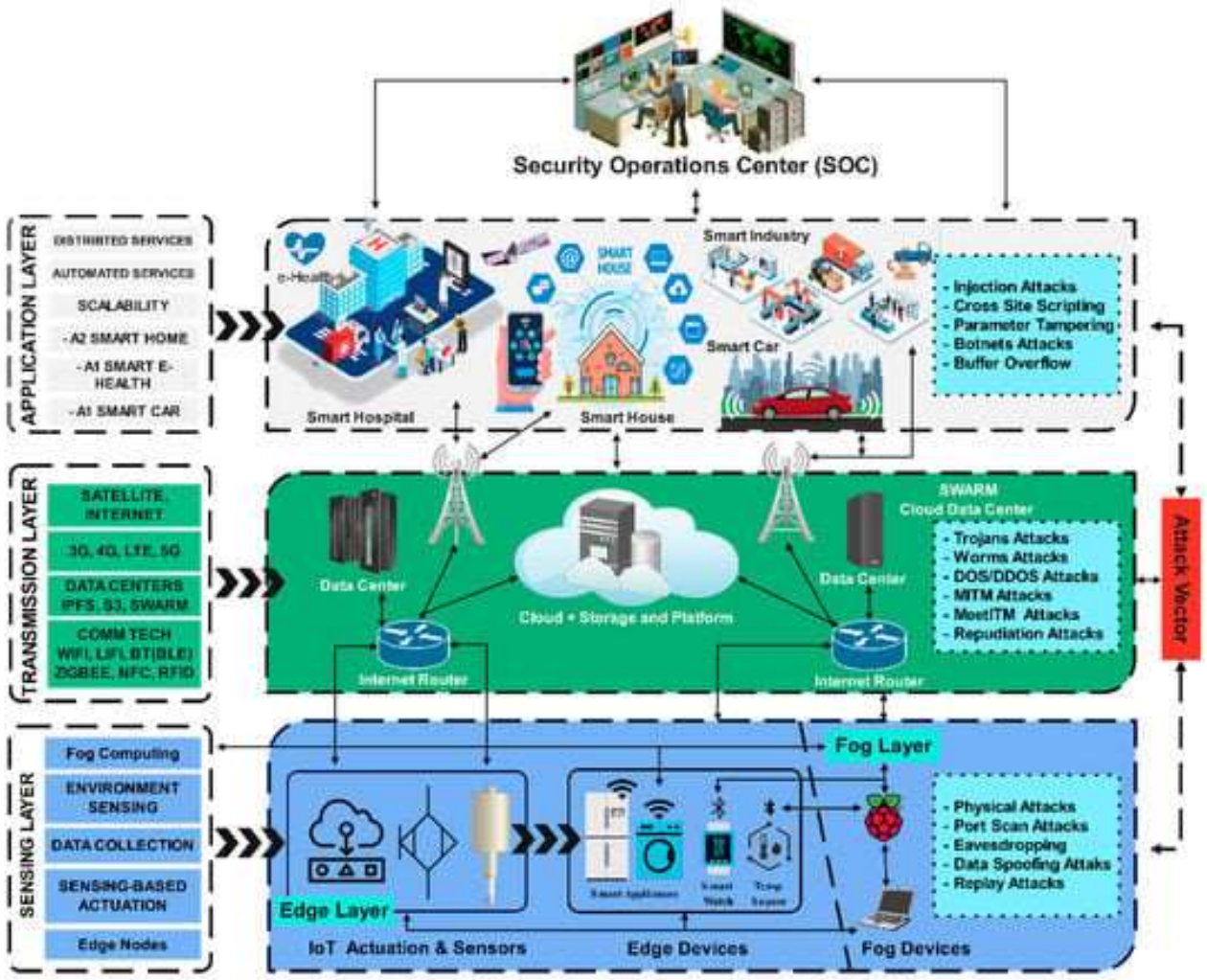


Рисунок 1.3 – Узагальнена багаторівнева архітектура Smart City

1.4.1 Рівень програми

Прикладний рівень відіграє важливу роль у додатках, визначених різними функціями для відповідних CPS, таких як розгортання додатків для розумних будинків, розумних лікарень або розумних автомобілів. Як показано на рисунок 1.3, цей рівень забезпечує шлях для взаємодії з використанням отриманої інформації від рівня передачі. Команди виконуються на основі даних, отриманих від пристроїв на сенсорному рівні [12, 19]. Розгортання здійснюється в центрі безпеки розумного міста (SOC). Це центральна точка для постачальників послуг в архітектурі розумного міста для комунальних компаній, підключених до кількох програм, розташованих у різних місцях. Автоматизовані послуги, що

надаються на цьому рівні, можуть бути централізованими або розподіленими залежно від характеру та вимог CPS до його застосування та масштабованості.

1.4.2 Рівень передачі

Як показано на рисунок 1.3, дані з прикладного рівня передаються через цей рівень. Він відповідає за зв'язок між пристроями між верхнім і нижнім шарами. Ці пристрої підключаються за допомогою традиційних мережевих технологій, які вже використовуються для передачі зібраних даних, наприклад, Wireless Fidelity (Wi-Fi), радіочастотної ідентифікації (RFID), Bluetooth (BT), Near Field Communication (NFC) тощо. Технології передачі, такі як 3G, 4G, LTE, 5G, Інтернет або супутник, відіграють важливу роль у передачі даних і діють як магістраль для зв’язку [4]. Пристрої маршрутизації, такі як маршрутизатори та комутатори, використовують технології зв’язку та передачі для маршрутизації даних. Навпаки, платформи хмарних обчислень, інтернет-шлюзи, брандмауери, системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) забезпечують плавну та безпечну передачу даних. Центри обробки даних веб-серверів, таких як Facebook, Google тощо, також функціонують на цьому рівні, який може бути централізованим або розподіленим за своєю природою, як у випадку міжпланетної файлової системи (IPFS), Swarm, S3 тощо.

1.4.3 Сенсорний рівень

Поруч з передавальним шаром знаходиться чутливий рівень. Він містить крайовий і туманний шар і розгортає крайові та туманні пристрої, такі як датчики, агрегатори, приводи та малинові Pi/сервери для досягнення обробки даних у реальному часі. Пізніше зібрані дані можна використовувати для прийняття обґрунтованих рішень на основі вимог CPS у розумному місті, як показано на рисунок 1.3. Наприклад, увімкнення/вимкнення світла, запис відео кожного разу, коли виявляється будь-який рухомий об’єкт, або ввімкнення/вимкнення будь-якого інтелектуального пристрою під час виявлення

теплових сигнатур запускає зондування навколишнього середовища, яке можна використовувати, щоб надати SOC для подальших дій, тощо.

1.5 Архітектури автентифікації смарт-пристроїв із підтримкою Інтернету речей у розумних містах

Як обговорювалося раніше, проблеми в розумному місті також можна віднести до основних категорій характеристик безпеки, тобто автентифікації, авторизації та аудиту (AAA). Він далі класифікує служби безпеки на конфіденційність, цілісність і доступність (CIA), тоді як конфіденційність користувача та аспекти автентифікації були досліджені. Для будь-якої CPS в інфраструктурі розумного міста основними проблемами є автентичність користувачів і клієнтського обладнання (CPE), тобто датчиків і виконавчих механізмів. Зі швидким зростанням використання та низькою концентрацією на деталях безпеки та конфіденційності пристроїв виявилися очевидними проблеми, які підштовхнули потребу в рішеннях, які могли б вирішити ці проблеми безпеки.

Оскільки ця стаття зосереджена на схемах автентифікації інтелектуальних пристроїв із підтримкою Інтернету речей у розумному місті, у наступному розділі обговорюється огляд традиційних найсучасніших механізмів автентифікації, які вже розгорнуті, а потім запропоновані нові механізми автентифікації. Було обрано категоричний підхід для обговорення сучасного огляду звичайних і нещодавно запропонованих схем автентифікації на основі централізованих і розподілених архітектур.

1.5.1 Сучасні моделі автентифікації

Автентифікація CPE є такою ж важливою, як і інші ознаки ЦРУ. Схеми змусять законних користувачів отримати доступ до ресурсів; інакше на кону опинилася б уся система. Як показано на рисунку 1.4, сучасна модель автентифікації базується на архітектурі автентифікації з двома основними

категоріями, тобто централізованою/нерозподіленою та нецентралізованою/розподіленою моделями автентифікації. Традиційні механізми автентифікації були розроблені на основі переважно централізованої архітектури, де ресурсні машини відіграють важливу роль у наданні послуг автентифікації. Вектор атаки завжди знаходить способи втрутитися в протоколи безпеки. Саме тут стають у пригоді додаткові протоколи автентифікації, такі як OpenID [20], Security Assertion Markups Language (SAML 1.1/2), Fast Identity Online (FIDO) або Open Authorization (OAuth) [21, 22, 23]. У той же час впровадження покладається на надійні сторонні рішення (TTP). OAuth є найбільш прийнятним рішенням, оскільки це одне з найпотужніших рішень відкритої авторизації, доступних розробникам API сьогодні. Його потужні функції можна використовувати для захисту величезного Інтернету речей. Хоча він забезпечує надійний механізм автентифікації єдиного входу (SSO), він також створює загрозу для його централізованої архітектури [24]. Централізовані/нерозподілені механізми, як показано на рисунок 1.4 , включають наступні механізми автентифікації, які традиційно використовувалися та обговорювалися нижче.

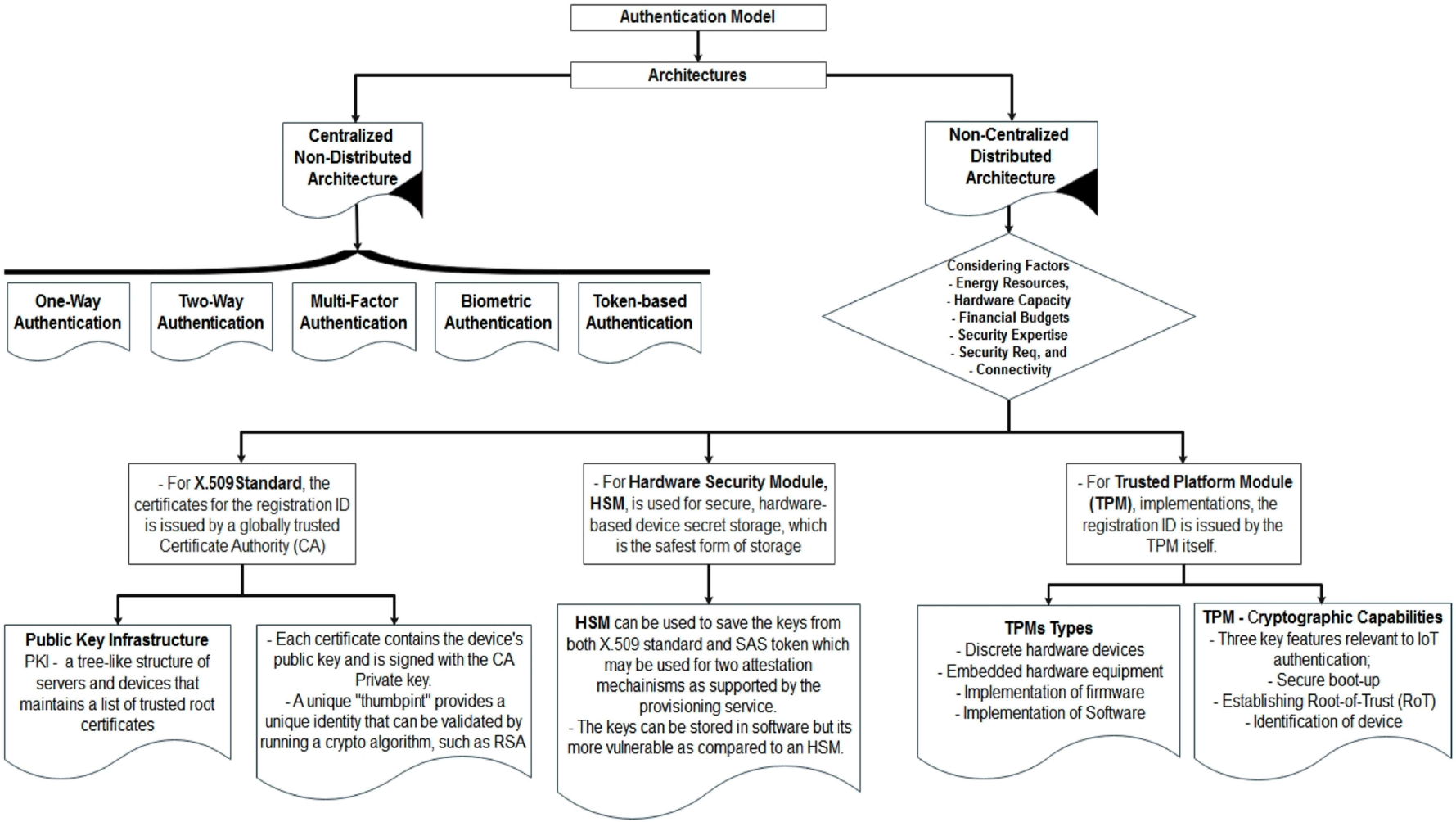


Рисунок 1.4 - Модель автентифікації.

1.5.2 Однофакторна автентифікація (SFA)

SFA, яка називається односторонньою автентифікацією, забезпечує первинну автентифікацію, наприклад пароль, безпечний PIN-код, картку PIV тощо.

1.5.3 Двофакторна автентифікація (2FA)

2FA, яка називається двосторонньою автентифікацією, забезпечує одноразову автентифікацію, наприклад одноразовий пароль, безпечний PIN-код, зареєстрований пристрій тощо [25, 26, 27].

1.5.4 Багатофакторна автентифікація (MFA)

MFA залежить від двох-трьох факторів, які забезпечують автентифікацію, таких як пароль, безпечний PIN-код, надсилання одноразових паролів на номери телефонів користувачів і чарівні посилання, надіслані через SMS або електронні листи, інформація про місцезнаходження тощо. У всіх середовищах, захищених паролем, такі протоколи, як Використовуються PAP і CHAP, що забезпечує достатню зручність використання механізму автентифікації.

1.5.5 Біометрія

Біометрія включає біологічні ознаки, такі як ідентифікатор відбитків пальців і форми обличчя для автентифікації користувача. У 2011 році сканер відбитків пальців був представлений на Android-смартфоні Motorola ATRIX, і з тих пір він широко використовується для автентифікації користувачів для реєстрації пристрою або завершення цифрових покупок [28].

1.5.6 Автентифікація на основі маркерів

Це протокол, який використовується для автентифікації користувачів для підтвердження їх особи на основі унікального маркера, отриманого після перевірки облікових даних. Потім ці маркери використовуються для доступу до веб-сайтів, програм або будь-якого захищеного ресурсу, зменшуючи клопоти,

пов’язані з повторним введенням облікових даних. Автентифікація на основі токенів знижує ризик викрадення факторів автентифікації, оскільки токени захищені від зловживання. Він не використовує потужність обробки системи, як механізм на основі пароля [29].

В інфраструктурі розумного міста автентифікація розумних пристроїв із підтримкою Інтернету речей у кіберфізичній системі є величезною. Незважаючи на те, що вибір відповідної моделі для автентифікації є важливим, але важким рішенням, на кону будуть фактори, що впливають на загальну продуктивність мережі. Продуктивність впливає на енергетичні ресурси, апаратні обмеження, бюджети, знання безпеки, потреби в безпеці та підключення.

Як показано на рисунок 1.4 , розподілена модель безпеки працює на автентифікації на основі сертифікатів, автентифікації на основі апаратного забезпечення з секретним зберіганням і рішеннях автентифікації на основі довіреної платформи [30].

1.5.7 Автентифікація на основі сертифіката

Цей механізм автентифікації використовує стандарт X.509, один із найбільш реалізованих і бажаних варіантів, які покладаються на сертифікати для автентифікації та авторизації. Ці сертифікати використовуються для реєстрації ідентифікатора, виданого всесвітньо довіреним центром сертифікації (CA). Це називається інфраструктурою відкритих ключів (PKI), яка складається з деревоподібної структури серверів і пристроїв, які підтримують список надійних кореневих сертифікатів. Сертифікати містять відкритий ключ пристрою та підписані закритим ключем ЦС. Унікальний «відбиток великого пальця» забезпечує унікальну ідентичність, яку можна підтвердити за допомогою криптоалгоритму, такого як RSA [31].

1.5.8 Апаратний модуль безпеки

Як показано на рисуноку 1.4, інший тип автентифікації забезпечується апаратними пристроями. Він пропонує апаратний модуль безпеки (HSM), який

захищає секретне сховище апаратного пристрою та вважається однією з найбезпечніших форм секретного сховища. HSM може зберігати ключі від стандарту X.509 і токена SAS, які можна використовувати для двох механізмів атестації, які підтримуються службою забезпечення. Ключі можуть зберігатися в програмному забезпеченні, але воно більш вразливе, ніж HSM [32].

1.5.9 Модуль надійної платформи

Реалізації Trusted Platform Module (TPM) включають реєстраційний ідентифікатор, виданий апаратним забезпеченням. Модулі TPM мають кілька форм, наприклад дискретні апаратні пристрої, вбудоване апаратне обладнання, мікропрограми, реалізація програмного забезпечення тощо. TPM має кілька криптографічних можливостей, тоді як кілька ключових функцій можуть бути досить актуальними для автентифікації IoT, наприклад безпечне завантаження, встановлення кореня довіри (RoT) та ідентифікація пристрою [33]. Вищезазначені схеми автентифікації традиційно використовуються; проте були запропоновані нові механізми автентифікації.

Дотримуючись категоричного підходу, оновлений огляд нещодавно запропонованих схем автентифікації на основі централізованих і розподілених архітектур обговорює проблеми безпеки під час автентифікації інтелектуальних пристроїв з підтримкою Інтернету речей. Огляд запропонованих методів було оцінено на основі точки зору надійності та слабкості, що зрештою допоможе усунути неоднозначності для вдосконалення в майбутньому.

1.6 Схеми автентифікації на основі централізованих архітектур у розумних містах

Ресурси розподіляються через взаємопов’язану мережу в централізованих або нерозподілених системах автентифікації та авторизації. Тим не менш, рішення централізовано контролюються машиною майнера, такою як сервер у випадку клієнт-серверних обчислень. Тут будь-яка служба, яка потребує

авторизації для виконання певного завдання, направляється на центральний сервер, який схвалює, якщо всі ключі рішення відповідають критеріям, або відхиляє в іншому випадку. Більшість систем у всьому світі реалізували централізовані механізми як запобіжний захід. Сервер повинен схвалити кожен запит на припинення нелегітимного використання системи. Схеми автентифікації, засновані на централізованій архітектурі, були представлені в цьому розділі, а також аналіз проблем безпеки, пов’язаних із цими механізмами для цілей майбутніх досліджень.

1.6.1 Розумні офіси та розумні будинки

Концепція розумних офісів обговорювалася в, оскільки ефективність, продуктивність і зручності є ключовими факторами для вдосконалення та ефективної роботи. Однак активи IoT та інші пристрої в розумному офісному середовищі створюють проблеми кібербезпеки в концепції розумних міст. Серед викликів кібербезпеці безперервні та неінвазивні механізми автентифікації для всіх цих активів мають величезне значення; отже, автори запропонували розробити та розгорнути безперервну та інтелектуальну архітектуру автентифікації, орієнтовану на Smart Offices. Архітектура орієнтована на парадигму хмарних обчислень і використовує методи машинного навчання (ML) з використанням алгоритму класифікації, наприклад Random Forest, для автентифікації користувачів відповідно до їхньої поведінки. Для оцінки результатів використовувалися такі показники, як точність, запам’ятовування та оцінка F1. Оцінка класифікації персональних комп’ютерів показує середню точність 96,32%, середнє запам’ятовування 90,00% і середній бал F1 92,70%. Навпаки, оцінка класифікації мобільних пристроїв була відзначена із середньою точністю 97,43%, середнім запам’ятовуванням 96,20% і середнім F1-Score 96,76%. Результати оцінювання вважаються хорошими, що стосується ідентифікації пристроїв і розрізнення користувачів.

Автори в запропонували методологію для аналізу проблем безпеки для вбудованих активів IoT, які зазвичай використовуються в розумних будинках.

Методологія передбачає централізовану архітектуру, засновану на хмарних обчисленнях, що використовують кінцеві точки для зв'язку, зберігання та безпеки активів IoT, таких як неправильна конфігурація активів IoT, слабка автентифікація, оновлення постачальників через оновлення пристроїв тощо. Запропонована методологія використовує літературу для домашнього використання. IoT має вміння пом'якшувати методи атак, засоби пом'якшення та зацікавлені сторони. Автори проаналізували 45 пристроїв, щоб виявити забуті області досліджень і обговорити властивості безпеки, тобто вектори атак, засоби пом'якшення та зацікавлені сторони. Оцінку проводили за допомогою сканера Nessus для доступу до пристроїв і хмарних кінцевих точок, Kryptowire, MobSF і Qark для оцінки мобільних програм, а також Nessus Monitor, ntopng, sslsplit і Wireshark для оцінки протоколів зв'язку мережевого рівня. Для тестування використовувався Yahoo Cloud Services Benchmark Test (YCSB), який змінює модуль робочого навантаження YCSB і рівень інтерфейсу даних. Спільнота створила загальнодоступний портал для обміну незалежними висновками, використовуючи дані оцінки.

Кінцевої мети повсюдних обчислень можна досягти, якщо активи IoT використовуватимуться шляхом їх вбудовування в середовище, надаючи користувачеві активи, які будуть працювати в Інтернеті та будуть достатньо розумними, щоб приймати обґрунтовані рішення. Автори в представляють систему «Розумний дім» (SHS), яка містить усілякі розумні об'єкти, необхідні вдома. Автори представили вбудований чіп, тобто SoC (System on Chip) під назвою iVision. Він використовувався для взаємодії з активами IoT, такими як Smart Wall і Smart TV на основі профілю пристрою для веб-служб (DPWS); однак аналіз показує проблеми з продуктивністю та затримкою. Набір вбудованих плат S3C6410 імітує мережу для досягнення реалістичних результатів у домашніх умовах. Справжні веб-сервіси були розгорнуті для роботи на інтелектуальних пристроях, таких як кондиціонер, холодильник, мікрохвильова піч тощо. Багато тестових повідомлень викликали дивну поведінку мережі, у той час як вирішення виявлених драйверів займає ще три секунди на пристрій, а тестування десяти чи

більше пристроїв без зовнішніх шумів буде потрібно 1300 мс. Крім того, була запропонована архітектура, керована контекстом у CPS, щоб покращити якість обслуговування в системі Smart Home. Це досить висока затримка для ідентифікації пристрою в критичних за часом кіберфізичних системах у контексті розумного міста.

1.6.2 Вбудовані ресурси IoT

Щоб пом’якшити використання інтелектуальних активів від фізичних атак, активи Інтернету речей із вбудованими фізичними властивостями були використані для виявлення та усунення фізичних атак на пристрій (таких як атаки з уособленням і атаки на бокових каналах). Автори в запропонували легкий двофакторний механізм автентифікації, який автентифікує пристрій IoT і включає фізичні властивості пристрою. Запропонований механізм використовує визначену функцію на інтегрованих чіпах (IC) під назвою Physically Unclonable Functions (PUF), що передбачає фактори в механізмі автентифікації. Крім того, концепція зворотного нечіткого екстрактора була використана для вирішення проблеми шуму під час роботи PUF. Механізм передбачає централізований сервер, що робить цю архітектуру більш центральною, оскільки механізм залежить від центрального органу (тобто центрального сервера) для зберігання даних автентифікації.

Крім того, механізм вимагає п'яти обмінів повідомленнями між пристроєм і сервером. Вартість обчислень була розрахована за допомогою серії симуляцій криптографічних операцій з використанням віртуальної машини Ubuntu, що працює як сервер. Одноядерний ЦП 798 МГц із 256 МБ оперативної пам’яті (RAM) використовувався як пристрій IoT. Витрати на обчислення для пристроїв IoT становили 2,92 мс для виконання 5NH + NFE. Операції Gen + 2NPUF, тоді як серверу потрібно 3,39 мс для обчислення 5NH + NFE, що становить 6,31 мс як загальна вартість обчислення запропонованої схеми. Обчислювальна вартість виявилася значно нижчою, ніж у попередніх схемах автентифікації.

Як згадувалося раніше в , подібний підхід, але не залежний від сервера для зберігання автентифікованих даних, автори в описують легкий механізм автентифікації, який не потребує зберігання секретних ключів у безпечному централізованому майнері, тобто сервер. Цей механізм також визначає механізми автентифікації на основі фізично неклонованих функцій (PUF), які описують фізичні властивості пристроїв. Ця властивість допомагає пристроям підвищити захист від фізичного насильства з боку зловмисників. Автори представляють протоколи для двох сценаріїв: один, який встановлює зв'язок між пристроєм IoT і сервером, і інший для зв'язку D2D, коли два пристрої IoT хочуть встановити сеанс. Запропонований механізм також вимагав щонайменше п'яти обмінів повідомленнями автентифікації та був оцінений з точки зору обчислювальної складності, накладних витрат на зв'язок і вимог до пам'яті. Обчислювальна складність була нижчою, оскільки складність інтелектуальних пристроїв і серверів із підтримкою IoT була однаковою, тобто O (n + M(l)k). Довжина керування доступом до середовища (MAC) у 32 біти використовувалася для обчислення накладних витрат зв'язку, які були відзначені як 42 байти для повідомлення 2 у протоколі 1, тоді як повідомлення 3 у протоколі 2 становило 120 байт. Для порівняння, протокол 1 виявився набагато ефективнішим, ніж ті, що згадуються в літературі, оскільки його найдовше повідомлення становить приблизно 68 байт. Вимоги до зберігання для запропонованих протоколів взаємної автентифікації не передбачають зберігання змінних, які вважаються необхідними для автентифікації пристрою, а зберігають важливі дані, такі як пара CRP (C i , R i) і відповідний ID i на сервері; тому вимоги до зберігання дуже низькі.

1.6.3 Схеми автентифікації IoT на основі криптосистеми

Автори в мають на увазі проект пошуку мінімальних специфікацій, необхідних для реалізації безпечних алгоритмів автентифікації для різних специфікацій мережі. Вони реалізують один із найвідоміших алгоритмів асиметричної криптосистеми, тобто алгоритм RSA для інтелектуальних

пристроїв з підтримкою IoT. Основна увага була приділена пристроям із продуктивністю одноядерного процесора 100 МГц або нижче, тобто пристроям Інтернету речей, таким як WSN та RFID. Для оцінки експерименти проводилися на Pi як серверній машині; однак ЦП було обмежено 100 МГц одним ядром і 1024 МБ оперативної пам'яті, щоб імітувати властивості пристрою з обмеженням ресурсів. Алгоритм автентифікації на основі RSA PKCS ініціює спочатку підписання, потім перевірку повідомлення для автентифікації сервера, а потім перевірку підпису клієнта. Продуктивність алгоритму RSA вимірювалася, оскільки пристрої могли автентифікувати близько 37 пристроїв на хвилину. Сценарій вимагає, щоб шлюз обробляв 50 спроб автентифікації RSA за хвилину, але із середньою частотою 12,3 МГц, тоді як процес автентифікації потребує 1,6 с для обробки одного запиту. Це обмежує пристрій до 37 автентифікацій на хвилину. Надсилання й очікування перевірки клієнта займає час, а відповідь клієнта не враховується під час тестування. Обчислювальні витрати збільшаться зі зменшенням обчислювальної потужності, як у випадку з інтелектуальними пристроями, що може спричинити проблеми з автентифікацією пристрою.

Автори в обговорюють розроблений механізм автентифікації на основі криптоалгоритму, тобто RSA, для розумного середовища IoT через повітряну мережу з використанням найсучасніших галузевих стандартів. Механізм забезпечує послуги безпеки CIA (такі як конфіденційність, цілісність і доступність), включаючи сертифікат X.509, інфраструктуру відкритих ключів (PKI) на основі RSA та протоколи викликів/відповідей за допомогою постачальника послуг безпеки, викликаного проксі. Вони описують інноваційну модель системи, дизайн протоколу, архітектуру системи та оцінку проти відомих загроз. Крім того, реалізоване рішення розроблено як додатковий сервіс для багатьох інших конфіденційних програм (програми для розумного міста, кіберфізичні системи тощо). Йому потрібна підтримка сертифіката X.509 на основі жорстких маркерів для заповнення інших служб безпеки, включаючи конфіденційність, цілісність, незаперечність, конфіденційність та анонімність ідентифікаторів. Схему автентифікації було оцінено на основі обчислення та

порівняння вартості зв’язку з використанням 64-біт. Криптографічна одностороння хеш-функція та унікальне випадкове число були 128-бітними. Параметри RSA становили 1024 біти, тобто 1024 біти кожен для відкритого/приватного ключа RSA. Вартість зв’язку запропонованої фази входу в систему склала 1024 + 128 + 64 = 1216 біт. Довжина повідомлень на етапі автентифікації спостерігалася як 320 біт. Таким чином, спостережувана загальна вартість становила 1216 + 320 = 1536 біт, що було набагато ефективніше, ніж інші схеми. Вимоги до пам’яті спостерігалися на рівні 2432 біт, що значно нижче, ніж у порівнюваних схемах. Запропоновану схему також було оцінено щодо відомих уразливостей, і надано детальні порівняння з популярними відомими схемами автентифікації.

Було запропоновано нову легку автентифікацію користувача на основі токенів (TBLUA) для інтелектуальних пристроїв Інтернету речей. Він заснований на техніці маркерів для підвищення надійності автентифікації. Схема автентифікації користувача на основі маркерів була б більш безпечною, оскільки автентифікація користувачів на основі механізму пароля неможлива в додатках розумного міста, таких як розумні готелі та офіси. Оцінка безпеки показує безпеку токенів, Perfect Forward Secrecy (PFS) тощо як надійні механізми та залишається сильним конкурентом серед існуючих для автентифікації користувачів у середовищах IoT. Схему автентифікації було оцінено на основі порівняння витрат на обчислення, що спостерігалося за 8 мс для користувача, 18,2 мс для вузла GW і 3,5 мс для інтелектуального пристрою на етапі входу та автентифікації. Розглянуто порівняння вартості зв’язку для схем на основі еліптичної криптографії (ECC) з рівнем безпеки 160 біт. Спостережувана вартість зв’язку становила 84 байти для користувача, 156 байтів для вузла GW і 44 байти для інтелектуального пристрою, вартістю 284 байти. Результати моделювання були багатообіцяючими та ефективними порівняно.

1.6.4 Електронне урядування в розумному місті

Новий протокол віддаленої автентифікації користувача на основі смарт-картки для додатків електронного урядування було запропоновано в під час транзакцій електронного урядування типу громадянин-уряд (C2G). Автори обговорюють фактор ризику передачі даних і проблеми безпеки пристроїв в електронному урядуванні в сценарії розумного міста. Автори пропонують легкий, надійний протокол віддаленої автентифікації користувача та узгодження ключів, заснований на протоколі динамічної ідентифікації на відміну від протоколу статичної ідентифікації, який легко пропускає інформацію. Ідентичність користувача є унікальною для кожного входу; таким чином, навіть якщо зловмисник записує поточне спілкування та відтворює повідомлення, йому не вдається ввійти як законний користувач. Він використовує мітки часу, щоб запобігти атакам відтворення. Протокол відповідає всім атрибутам безпеки та стійкий до всіх відомих атак. Протокол було запропоновано для збереження генерації відкритих і приватних ключів із сервера та зберігання на смарт-картці (SC), яка в подальшому може використовуватися для реєстрації, входу та цілей автентифікації, таких як перевірка користувача та сервер. Запропонований протокол був змодельований за допомогою On-the-fly Model-Checker (OFMC). Обчислювальна вартість запропонованого механізму була представлена нотаціями (тобто TE, TH, TM і TS). TE позначає часову складність для обчислення експоненти, TH позначає хеш, TM позначає множення/ділення, а TS позначає симетричні функції дешифрування та шифрування. Витрати на обчислення для етапу реєстрації були зазначені в $3\ T_H$, етап входу та автентифікації були відзначені в $10\ T_H + 3\ T_E$, а зміна пароля була відзначена в $2\ T_H$ із загальною вартістю $15\ T_H + 3\ T_E$. . Запропонований протокол є легким, оскільки він використовує XOR та односторонню хеш-операцію та вимагає мінімальних витрат, тобто незначних, порівняно з іншими операціями. AVISPA (Автоматизована перевірка протоколів безпеки Інтернету та додатків), інструмент аналізу безпеки, використовувався для перевірки безпеки протоколу в Інтернеті, позначаючи безпеку протоколу як БЕЗПЕЧНИЙ.

Подібний підхід у для програм інтелектуального електронного урядування в розумних містах був запропонований у , тоді як автор розглядає проблеми противників. Навпаки, зв’язок між додатками та розумним містом здійснюється, і для вирішення цієї проблеми запропоновано розширену багатофакторну схему автентифікації користувача. Зареєстровані користувачі отримують дійсну смарт-картку, накопичену з деякими параметрами як конфіденційними значеннями, необхідними для входу в систему та зв’язку із зареєстрованим хмарним сервером, щоб скористатися послугами. Автор стверджує, що природа схеми є легкою та стійкою до багатьох мережевих атак. Механізм є централізованим і в основному залежить від центрального реєстраційного центру (ЦЦ), який надає параметри учасникам на етапі реєстрації. Після реєстрації користувача накопичується дійсна смарт-карта з деякими параметрами як конфіденційними значеннями, необхідними для входу в систему та зв’язку із зареєстрованим хмарним сервером, щоб скористатися послугами. Хмарні сервери (CS) зберігають секретні значення для автентифікації один одного (CS і користувача), надаючи параметри, встановлені для автентифікації. Після реєстрації користувачеві не потрібно повторно реєструватися через RC, оскільки обидва суб’єкти (CS і Користувач) встановлюють секретний ключ сеансу для доступу до необхідних послуг із CS у разі потреби. Запропонована схема в основному розділена на п'ять етапів, як, a. Реєстраційна, б. Вхід і автентифікація, c. Зміна пароля, d. Відкликання користувача, e. Динамічне додавання CSP.

Формальний аналіз було проведено для запропонованої схеми на основі моделі ROR. Було проведено оцінку продуктивності, яка показує низькі обчислювальні витрати та доводить, що схема є ефективною та застосовною до програм електронного урядування в розумному місті. Вартість зв’язку порівняно з попередніми запропонованими схемами (вартість обчислення ≈ 29,2121 мс, ≈13,3767 мс, ≈7,7447 мс, ≈2,2743 мс, ≈11,5891 мс) була набагато меншою, тобто ≈2,2628 мс, що показує, що результати запропонованої схеми ефективніші . Що стосується вимог до пам’яті, пам’ять, необхідна для смарт-картки,

спостерігалася на рівні 960 біт, а вартість 1056 біт з точки зору зв’язку вважалася ефективною серед раніше запропонованих схем. Формальна перевірка за допомогою інструменту AVISPA підтверджує безпеку запропонованої схеми.

2 АРХІТЕКТУРА ТА АПАРАТУРА ІОТ БУДИЛЬНИКА

Internet of Things, IoT, Інтернет речей – система фізичних об’єктів («речей»), взаємопов’язаних між собою за допомогою вбудованих датчиків, програмного забезпечення та/або інших технологій. Рішення на базі IoT – технологій зараз стають все більш затребуваними саме тому, що дають постачальникам розумних рішень можливість отримувати додатковий прибуток. Завдяки «інтелектуалізації» техніка може стати «розумною» за допомогою оснащення системи пристроями збору інформації, її обробки й прийняття рішень. Також поведінка системи стає «розумною» коли вона взаємодіє з іншими системами.

Internet of Things (IoT) це галузь, до якої відносяться такі технології, як «Розумний будинок», «Розумне місто», «Віртуальний маркетинг», «Навігаційна техніка», «Віртуальні інженерні виробництва». Такі технології вже охоплюють практично кожний сегмент у сфері промисловості, бізнесу, охорони здоров’я та споживчих товарів.

Не так часто трапляються нові пристрої відображення інформації. Пристрої, що використовують світлодіоди, виготовляють по одній з основних технологій: LCD, OLED, LED такі пристрої зазвичай застосовують в рекламі для виведення зображень і невеликої текстової інформації.

У дипломному проекті розробляється розумний IoT будильник, який представлений на рисунку 2.1, в основі якого лежить технологія адресних світлодіодів та технологія IoT. Власний хмарний сервіс використовуються для змінення налаштувань годинника та виведення на нього різних текстів.

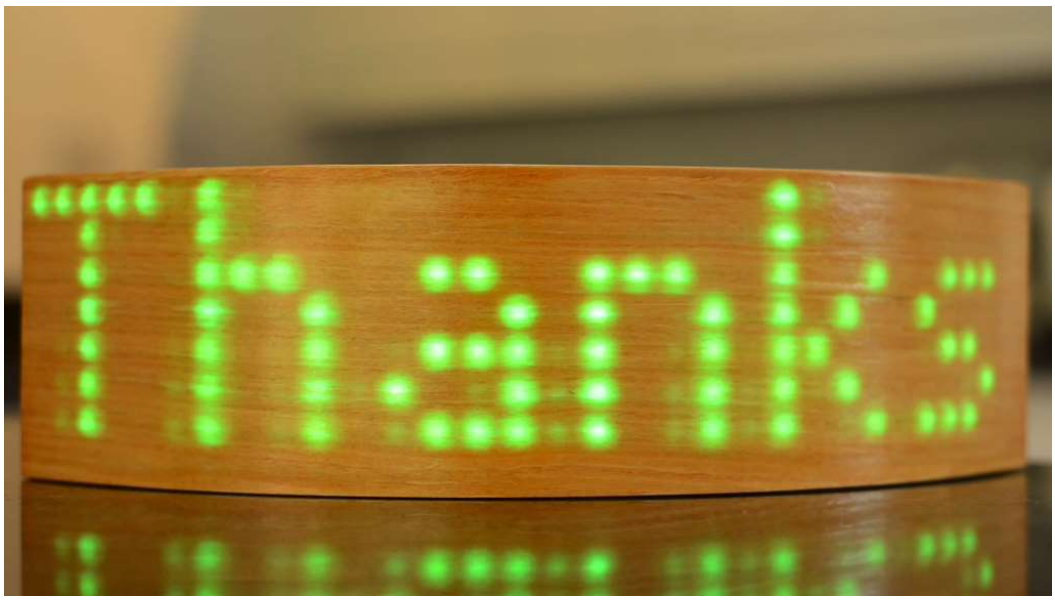


Рисунок 2.1 – Розумний IoT будильник на Arduino

2.1 Вибір та обґрунтування схеми пристрою

Метою цього розділу є забезпечення оптимального вибору схеми, яка задовольняє потреби пристрою і забезпечує його ефективну роботу з урахуванням обґрунтованих вибіркових критеріїв.

2.1.1 Розробка структурної схеми

Технічне завдання передбачає розробку будильника, який буде працювати з технологією IoT, тому має підключатись до мережі Wi-Fi, показувати час та погоду у вибраному регіоні, мати функції будильника та мати можливість настройки через Web – інтерфейс з мобільного телефону, планшету або персонального комп’ютера.

2.1.2 Розробка структурної схеми

Для вдоволення даних вимог буде використовуватись мікроконтролер Wemos D1 minімає зовнішній вигляд відповідно до рисунка 2.2. [34] Його переваги в тому що він побудований на основі Wi-Fi модулю ESP8266EX[35], що дозволяє скороти витрати на придбання додаткових модулів для Arduino, його характеристики наведені в таблиці 2.1.

Таблиця 2.1 - Технічні характеристики модуля WeMos D1

Параметр	Значення
1	2
Підтримка Wi-Fi стандартів	802.11b/g/n
Частота	160МГц
Підтримка режимів	STA/AP/STA+AP
Влаштований стек протоколів	TCP/IP
Живлення	5В
Струм споживання	Макс. 200мА
Струм на виходах	15мА
Підтримка інтерфейсів передачі даних	UART/GP/0
Швидкість передачі даних	до 460800 б/сек
Перепрограмування через хмарний сервер	Присутнє
Програмування через USB	Присутнє
Діапазон робочих температур	–40 +125Cº
Розміри	58х32мм

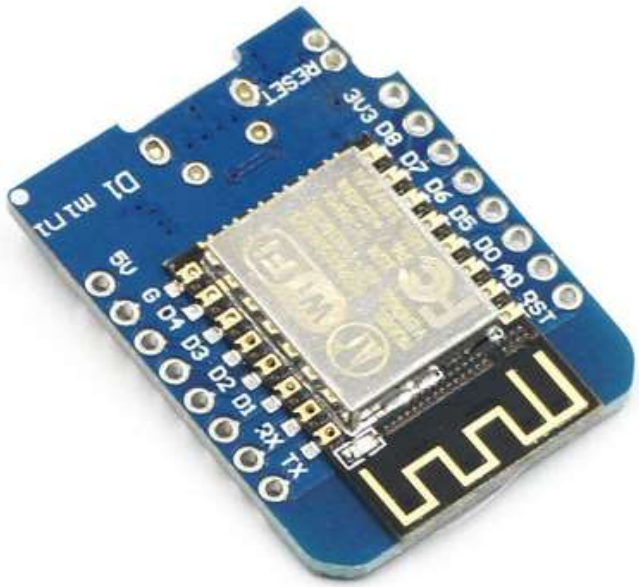


Рисунок 2.2 – Зовнішній вигляд плати Wemos D1 mini

Розподіл портів модуля WeMos D1 mini приведено на рисунку 2.3.

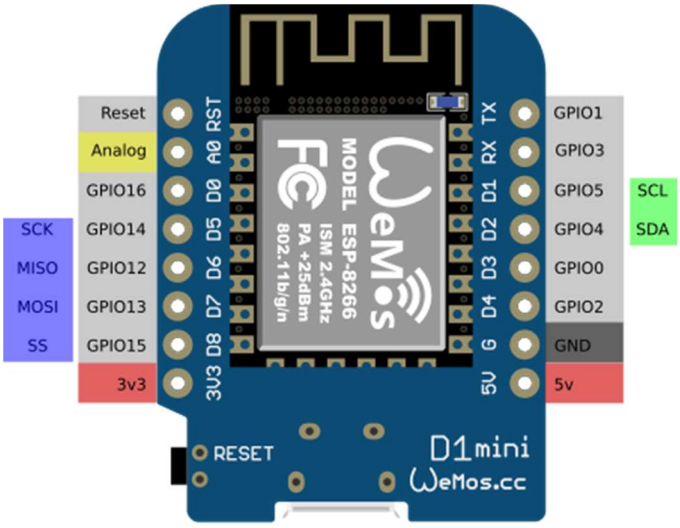


Рисунок 2.3 – Розподіл портів модуля WeMos D1 mini

Структурна схема розумного IoT будильника забражена на рисунку 2.4

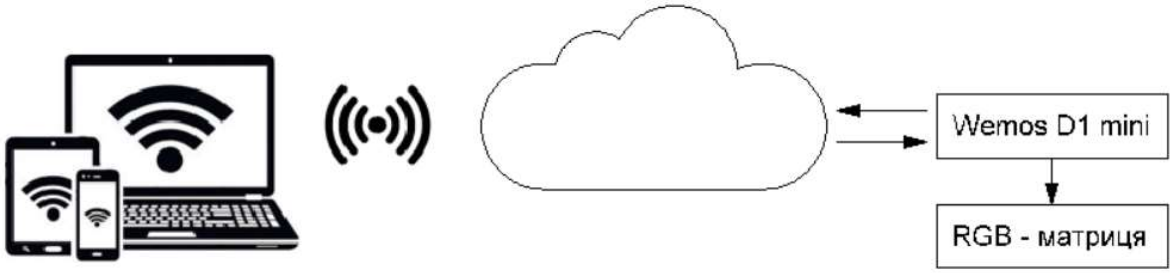


Рисунок 2.4 – Структурна схема розумного IoT будильника

В результаті було розроблено принципову схему та на її основі створено складальне креслення та креслення друкованої плати, що зображено в ілюстративних матеріалах (Додаток Б).

2.1.3 Вибір світлодіодної матриці

Для індикації буде використовуватися адресна світлодіодна матриця 8x32 на адресних світлодіодах WS2812. Алгоритм передачі даних на прикладі кльору, RGB–код якого: 160, 50, 222, представлений нижче. [36]

Передача ведеться «пакетами» по 24 біта, спочатку передається «пакет» для першого світлодіода. Біти передаються в такому порядку: спочатку зелений, потім червоний, потім синій. Порядок побітної передачі даних вказано на рисунку 2.5.

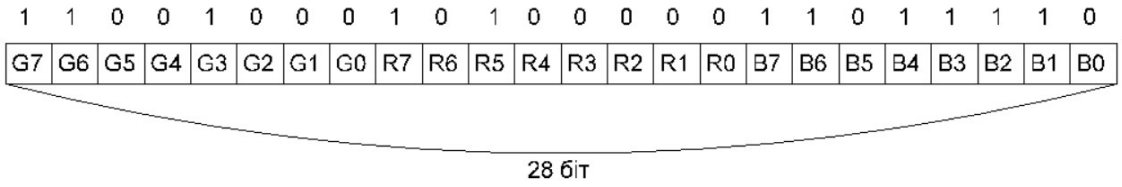


Рисунок 2.5 – Порядок побітної передачі даних

Кожен біт відправляється за 1,25 мкс. При передачі “0” відправляються логічні рівні вказані на рисунку 2.6.

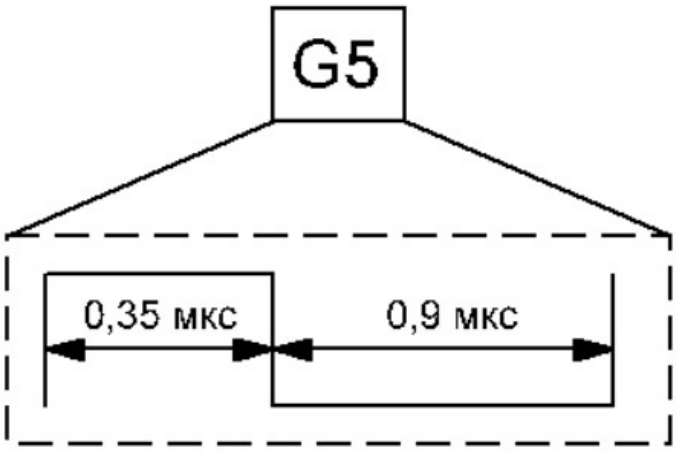


Рисунок 2.6 – Відправка “0” на логічному рівні

При передачі “1” відправляються логічні рівні вказані на рисунку 2.7

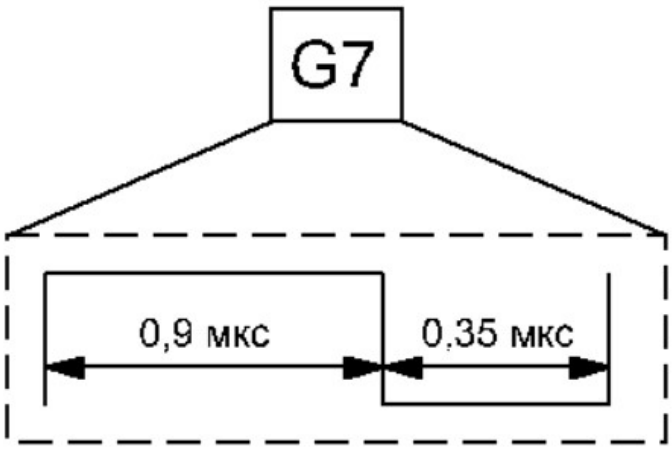


Рисунок 2.7 – Відправка “1” на логічному рівні

Функціональну схему вказано на рисунку 2.8

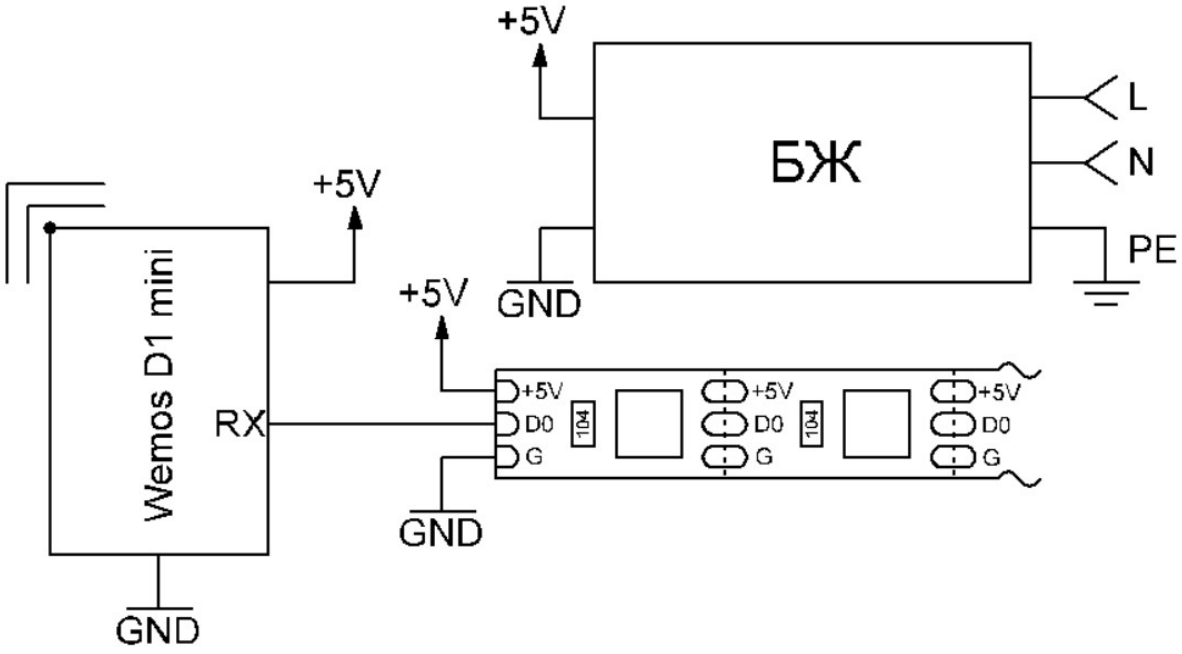


Рисунок 2.8 – Функціонально схема

2.1.4 Система живлення

Вимоги до імпульсного блоку живлення:

– вхідна напруга мережі: 160-255В AC;

– вихідна напруга 5В DC;

- вихідний струм: 12А
- гальванічна розв'язка входу із виходом;
- захист від КЗ у вторинному ланцюзі;
- косинус фі: не менше 0,9;
- час спрацьовування захисту за струмом: не більше 1 мс;
- стабільність вихідної напруги: не гірша 0.1%;
- загальний ККД пристрою: не менше 90%;

Світлодіодна матриця живляться напругою 5В та має номінальну потужність 76 Вт. За формулою (2.1) можна розрахувати струм споживання всієї матриці.

$$I_m = \frac{W}{V} \tag{2.1}$$

$$I_m = \frac{76}{5} = 15.2A$$

де I_m – споживаний струм всією матрицею;

V – номінальна напруга.

W – номінальну потужність;

Приймаючи до уваги що більшу частину робочого часу на годинник буде виводитися поточний час, який відображається кількістю світлодіодів візуально займаючу менше половини матриці рисунок 2.9 та розраховану за формулою (2.2), тобто 7,6А.

$$I = \frac{I_m}{2} \tag{2.2}$$

$$I = \frac{15.2}{2} = 7.6A$$

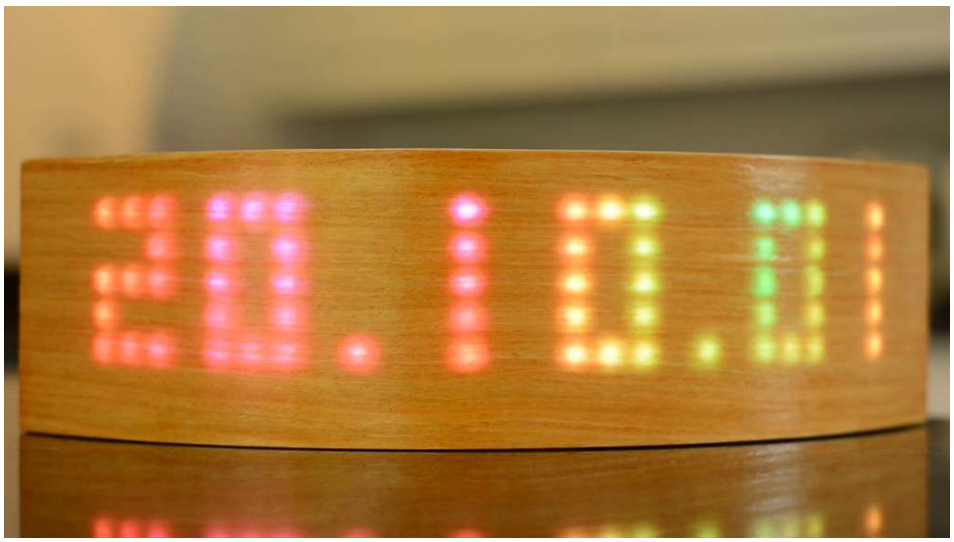


Рисунок 2.9 – Відображення часу на годиннику

Було вибрано блок живлення з номінальним струмом 12А та напругою 5В VST-60-5 [37]. Основні характеристики модуля VST-60-5: вхідна напруга – 100 - 240В (AC); вихідна напруга – 5В (DC); вихідний струм – 12А; Номінальна потужність - 60 Вт;

2.2 Розробка програмного забезпечення

Метою цього розділу є забезпечення ефективної та надійної роботи пристрою шляхом розробки якісного програмного забезпечення, що буде відповідати вимогам функціональності та стандартам якості. Це потрібно, для того, щоб мікроконтролер виконував поставлене завдання.

2.2.1 Розробка Web – інтерфейсу

Для налаштування будильника через інтернет необхідно використати Веб – сторінку яка зображена на рисунку 2.10.

Для курування будильником буде використовуватись Web - інтерфейс за адресую “http://arclock.local/” або по IP – адресом вказаному при включенні.

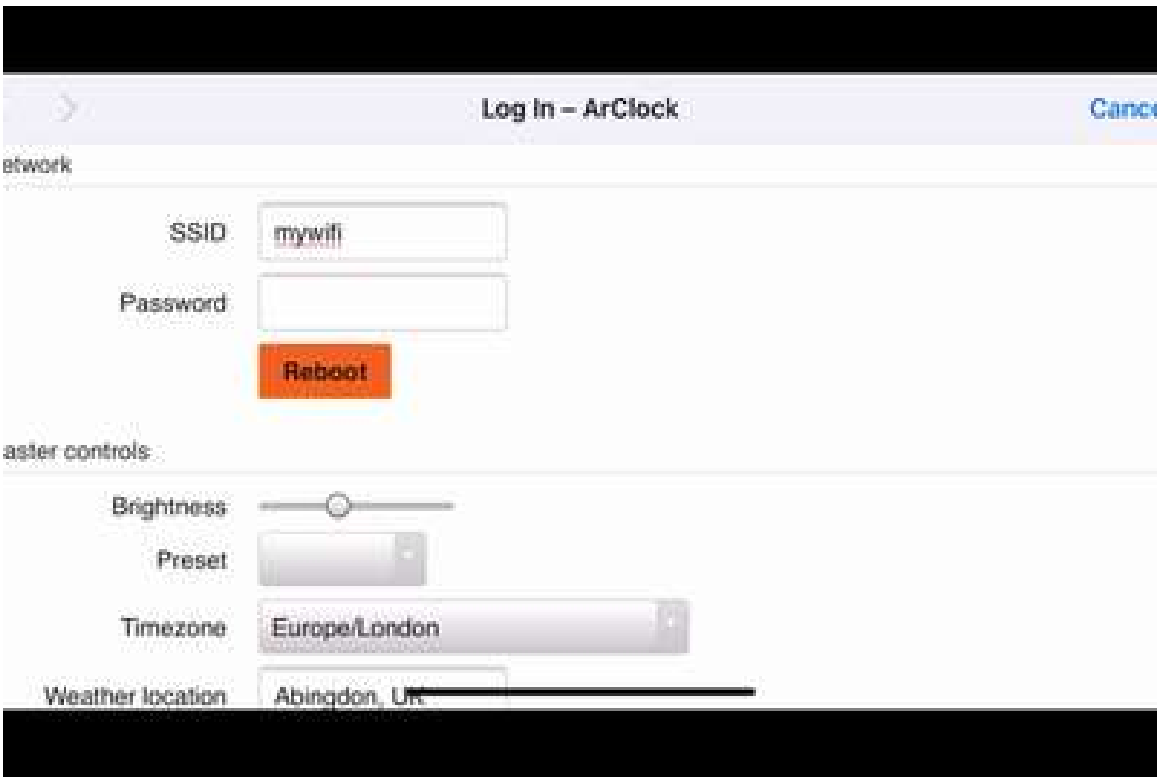


Рисунок 2.10 – Веб – сторінка годинника

2.2.2 Розробка програмного забезпечення ESP8266

Як засіб розробки програмного забезпечення для мікроконтролера ESP8266 вибираємо середовище розробки Arduino IDE [38]. Почнемо з додавання менеджера плати ESP8266 в налаштування Arduino IDE, для цього потрібно зробити наступні дії:

1) У меню програми Arduino IDE вибрати закладку Файл -> Настройки як вказано на рисунку 2.11.

2) У вкладці «Настройки», в пункті «Дополнительные ссылки для менеджера плат», натиснувши на кнопку вибору, у спадному діалоговому вікні, що зображено на рисунку 2.12.

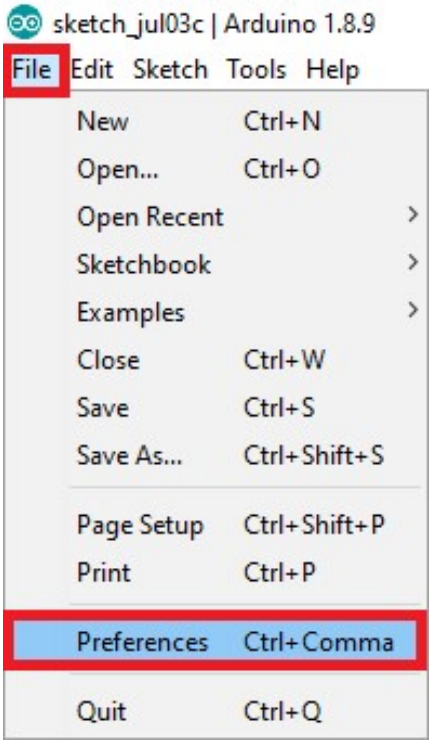


Рисунок 2.11 – Arduino IDE. Вибір закладки Файл -> Настройки

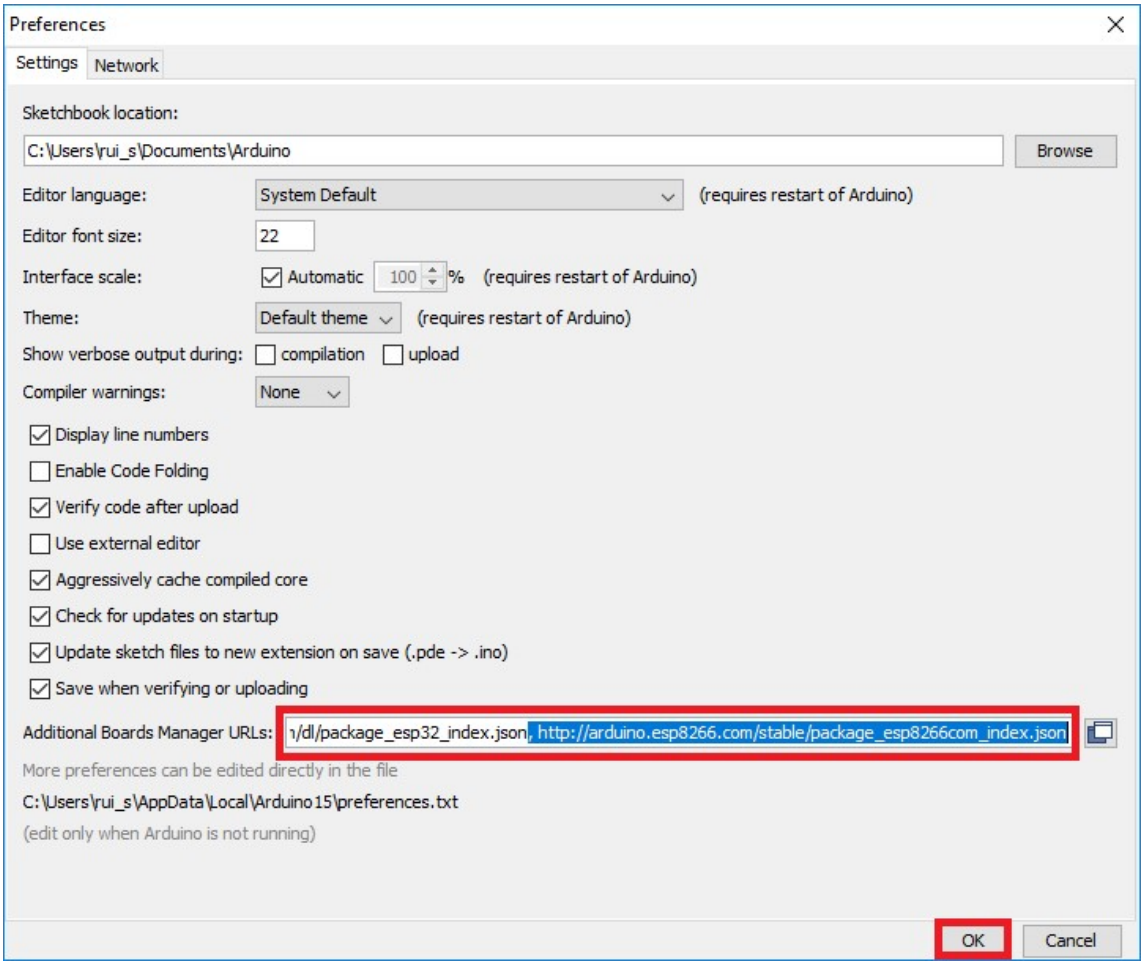


Рисунок 2.12 – Налаштування Arduino IDE для роботи з ESP8266

Наступним кроком є підключення бібліотек та інструментарію ESP8266. В меню Arduino IDE вибираємо Инструменты -> Платы: -> Менеджер плат як зображено на рисунку 2.13.

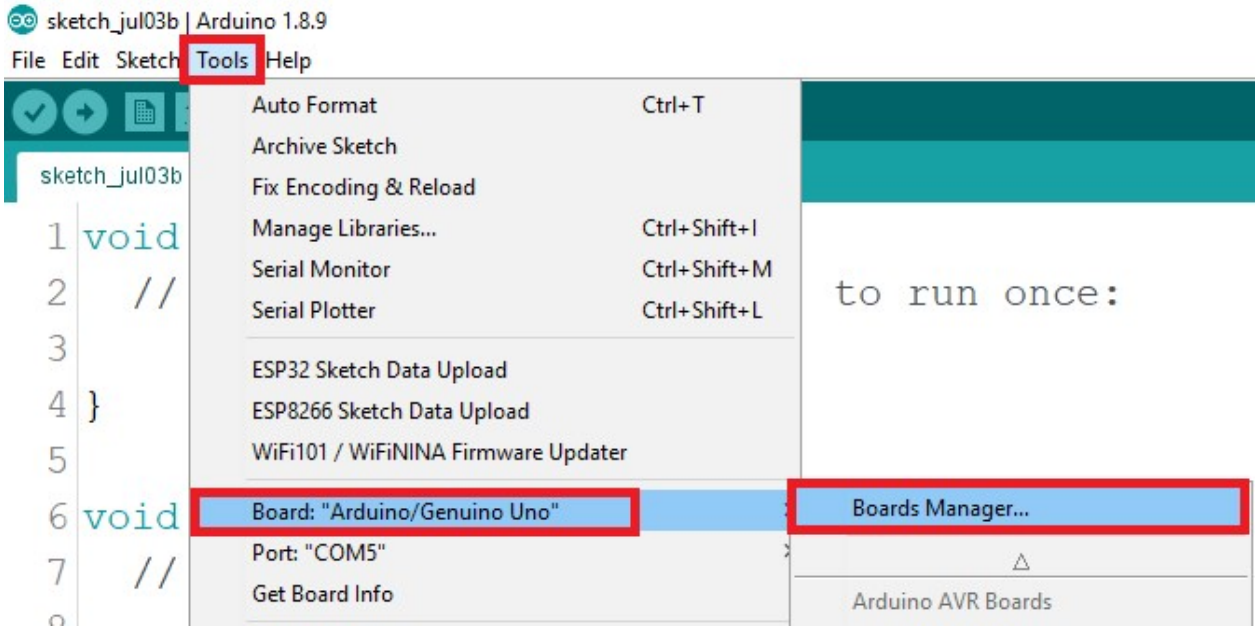


Рисунок 2.13 – Підключення бібліотек та інструментарію ESP8266

У текстовому полі пошуку «Менеджера плат» наберіть ESP, потім виберіть esp8266 by ESP8266 Community та натисніть кнопку «Установка», що зображена на рисунку 2.14.

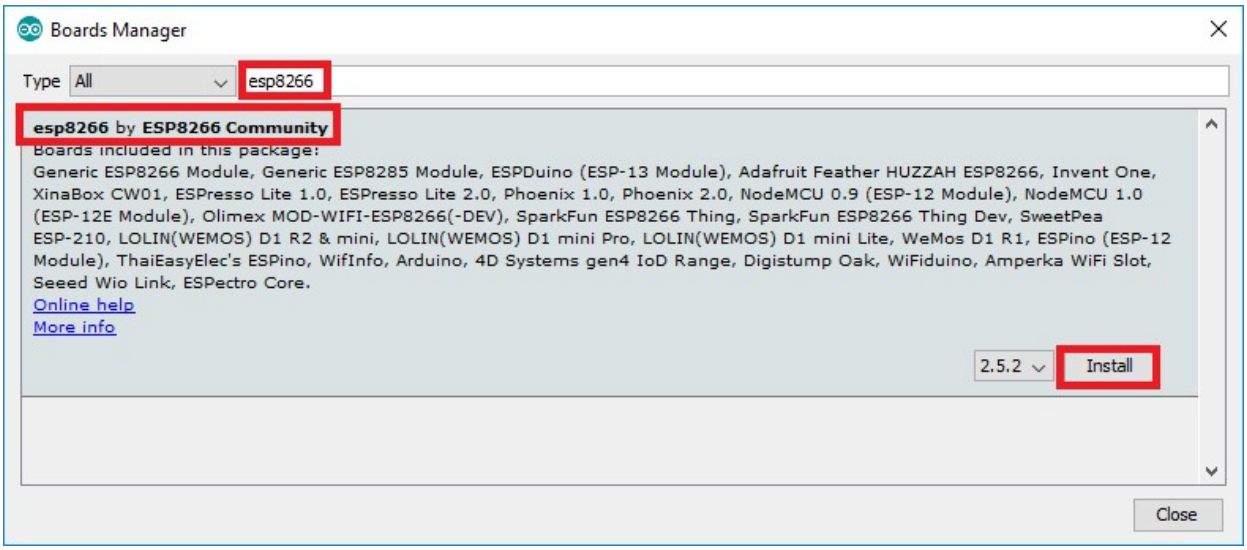


Рисунок 2.14 – Встановлення бібліотек та інструментарію ESP8266

Перейдемо до створення програмної частини проекту. Для роботи з ESP8266 використовуються бібліотека <ESP8266-ping.h>. Дана бібліотека призначена для перевірки затримки між сервером до якого звертається WiFi – модуль та самим модулем.

Також потрібно встановити бібліотеки для роботи із адресними світлодіодами: <NeoPixelBus.h> від Makuna, <Adafruit_GFX.h>, <FastLED.h>.

Далі потрібно скомпілювати прошивку, для цього обрати у списку, що випадає: Скетч>Перевірити/Компілювати, в разі вдалої компіляції побачимо, що написано «Компіляція завершена» та відповідну інформацію про це у вікні Arduino IDE, яке зображено на рисунку 2.15.

Рисунок 2.15 – Вікно з завершеною компіляцією

Після завершення компіляції, під'єднуємось до нової мережі Wi-Fi за допомогою комп’ютера або смартфона та вводимо у пошуковій стрічці браузера адресу 192.168.0.7, у Web – інтерфейсі що відкриється вписуємо логін та пароль нашої мережі. Лістінг програми наведений в додатку В.

2.3 Розрахунок блока живлення

Зворотно-ходові ІБЖ найчастіше використовують як мало та середньо потужні (до 150 Вт), тому що вони дешеві та містять малу кількість компонентів.

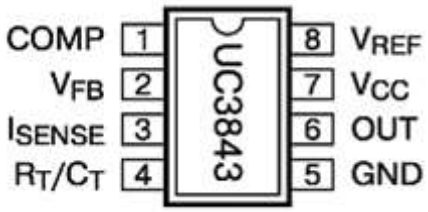


Рисунок 2.16 – Умовне позначення та призначення виводів мікросхеми UC3843

Мікросхема UC3843[39] призначена для побудови на її основі стабілізованих імпульсних блоків живлення з широтно-імпульсною модуляцією (PWM), зображена на рисунку 2.16. Оскільки потужність вихідного каскаду мікросхеми (ІМС) порівняно невелика, а амплітуда вихідного сигналу може досягати напруги живлення мікросхеми, то як ключ спільно з мікросхемою застосовується n-канальний МОН транзистор. Схема проектованого блока живлення вказана на рисунку 2.17.

Параметри імпульсного блока живлення:

– вхідна напруга: 180 – 260В;
– вихідна напруга: 4 – 6В;
– вихідний струм: 12А;
– наявність синфазного фільтра;
– гальванічна розв'язка входу із виходом;
– стабільність вихідної напруги: не менше 0.1%;
– температура силових елементів пристрою: не більше 60 градусів при 100% навантаженні;
– загальний ККД пристрою: не менше 90%.

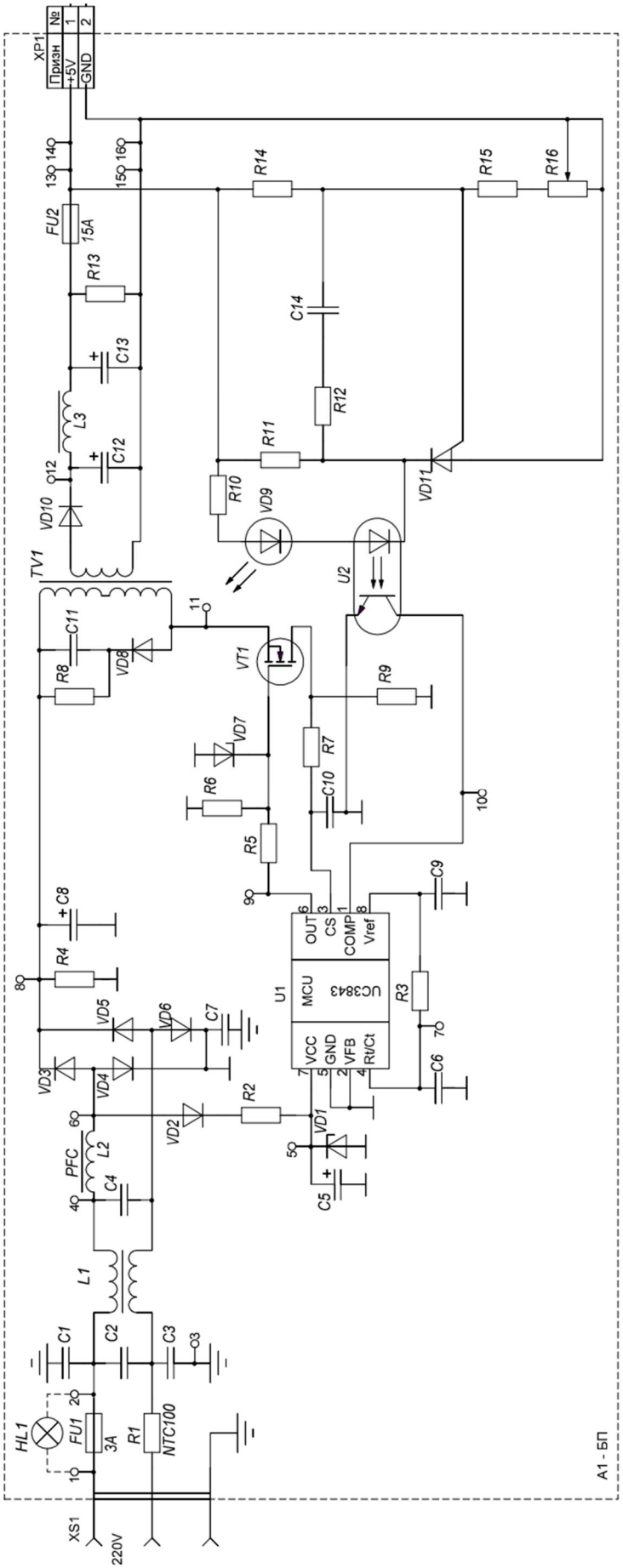


Рисунок 2.17 – Схема імпульсного блока живлення

2.3.1 Розрахунок вихідної частоти UC3843

У мікросхеми UC3843 внутрішній генератор реалізований так. Спочатку конденсатор С повільно заряджається через резистор R від опорного напруги, а потім швидко розряджається внутрішнім ключем з фіксованим струмом розряду (8,3 mA). Час розряду конденсатора через внутрішній ключ визначає «мертвий» час - коли силовий ключ завжди закритий. Відповідно, змінюючи величини R та С можна не тільки задавати частоту перетворення, а й максимальне значення робочого ходу. Рекомендується отримати якомога менший «мертвий» час, що б максимально наблизити коефіцієнт заповнення D до 50%. Частота перетворення розраховується за формулою (2.3).

$$f = \frac{1{,}72}{C \cdot R} \qquad (2.3)$$

2.3.2 Діодний міст

Блок живлення по потужності не буде перевищувати 60 Вт, тому діодний міст може бути виконаний на кремнієвих діодах HER508[40].

Характеристики діодів HER508:

- максимальна зворотня постійна напруга: 1000В;
- максимальний прямий струм: 5А;
- час відновлення: 75нс;
- корпус: DO-201AD.

2.3.3 Подавлення завад

Імпульсні блоки живлення, незалежно від типу PWM, повинні мати схеми подавлення вхідної несиметричної та вхідної симетричної завади.

Несиметрична завада

Несиметрична завада це напруга завади між фазою та нулем. Ефективне подавлення несиметричної завади здійснюється конденсаторами типу X – типу (С2, С4), які мають високу якість та малий ESR. Крім того ці конденсатори

повинні витримувати максимально допустимі в мережі сплески, не загорятися при виході з ладу та не підтримувати горіння. Будуть використовуватися конденсатори X1 MKP GLC 0.68uF 300V.

Симетрична завада

Симетрична завада подавлюється за допомогою котушки індуктивності L1 з двома обмотками, що мають однакове число витків. Вона має високий опір для симетричного струму та практично нульовий для несиметричного. Буде використовуватися дросель з двома обмотками на 13 витків.

Високочастотні імпульси

Високочастотні імпульси проникають зі стоку транзистора на вторинну обмотку через паразитну ємність. Таким чином, на виході блоку живлення присутні пульсації з частотою блоку живлення відносно заземлення та обох мережних проводів. Для подавлення власних імпульсних завад в схему вводиться конденсатор С7. Конденсатор С7 зв’язує мережу з виходом блоку живлення, що небезпечно. Тому він є типу Y (призначений для роботи там, де вихід їх з ладу загрожує життю людей). Буде використовуватися конденсатор DCF103M.

2.3.4 Розрахунок силового трансформатора для зворотно – ходового перетворювача напруги

В схемі на рисунку 2.2 як ключовий елемент використовується польовий транзистор, який працює на частоті 108,3 кГц. Щільність струму обирається не більше 8А/мм^2, якщо буде більше намотувальні вироби будуть нагріватися.

Трансформатор буде намотаний на магнітопровід EI 33.1/24.0/12.8/9.7 PC40. Характеристики EI 33.1/24.0/12.8/9.7 PC40 наведені у таблиці 2.2

Таблиця 2.2 – Технічні характеристики EI 33.1/24.0/12.8/9.7 PC40

Параметр	Значення
Матеріал	N95
Робоча частота	108,3 кГц
Вихідна напруга	5В
Вихідний струм	12А

Для розрахунку трансформатора використовується программа Flyback-Lite.

2.3.5 Розрахунок Flyback Converter

Форми кривих струму та напруги розраховуються за законом Фарадея. Вони не є інкрементованими симуляцією. Прямі напруги діодів розраховувалися при прямому падінні напруги V_F = 0,7, а транзистори інтерпретувалися як ідеальні ключі. Типова схема зворотно-ходового перетворювача зображена на рисунку 2.18.

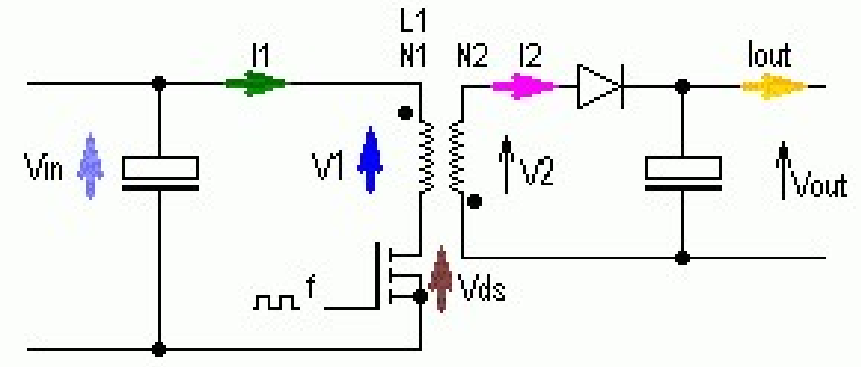


Рисунок 2.18 – Типова схема зворотно-ходового перетворювача

– Якщо поле введення залишається порожнім, вибирається значення за замовчуванням. Це значення відображається після виходу з поля введення.

– Програмі потрібні вихідні значення V_{out} і I_{out}.

– Імпульсне джерело живлення працює в межах певного вхідного діапазону, тобто між V_{in_min} та V_{in_max}.

– Частота перемикання f є робочою частотою транзистора.

– Значення V_{in} є значенням для розрахунку діаграм струму та напруги. V_{in} має лежати між V_{in_min} та V_{in_max} .

Розрахунки зроблено для ККД, що дорівнює 1. Фактично це нереалістично для зворотно-ходового перетворювача. ККД визначається в основному зв'язком первинної та вторинної обмотки. Якщо число витків N1 і N2 сильно різниться (як правило, при низькій вихідній напрузі), то зв'язок між первинною та вторинною обмотками буде поганим, і це призведе до низького ККД порядку 65-70 %. Якщо кількість витків N1 і N2 приблизно дорівнює, то буде досягнуто хорошого зв'язку і ККД може бути > 90%.

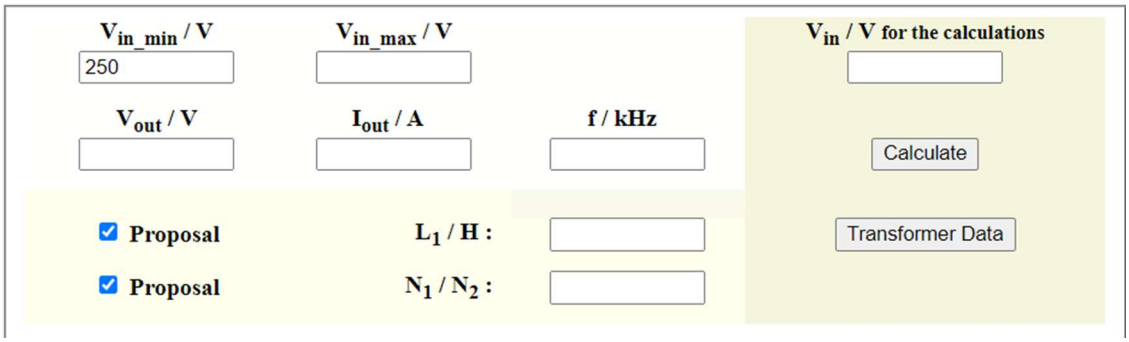


Рисунок 2.19 – Поля для введення даних даних з таблиці

Вводимо значення з таблиці 2.3 в онлайн калькулятор Flyback Converter що вказаний на рисунку 2.19.

Таблиця 2.3 – Вхідні значення

Рядок	Значення
V_{in_min}	250
V_{in_max}	360
V_{in}	305
V_{out}	5
I_{out}	12
f	108.5

Вводимо ці данні у відповідні поля та натискаємо “Calculate”. Результати розрахунку вказані на рисунку 2.20. Вихідні графіки вказані на рисунку 2.21.

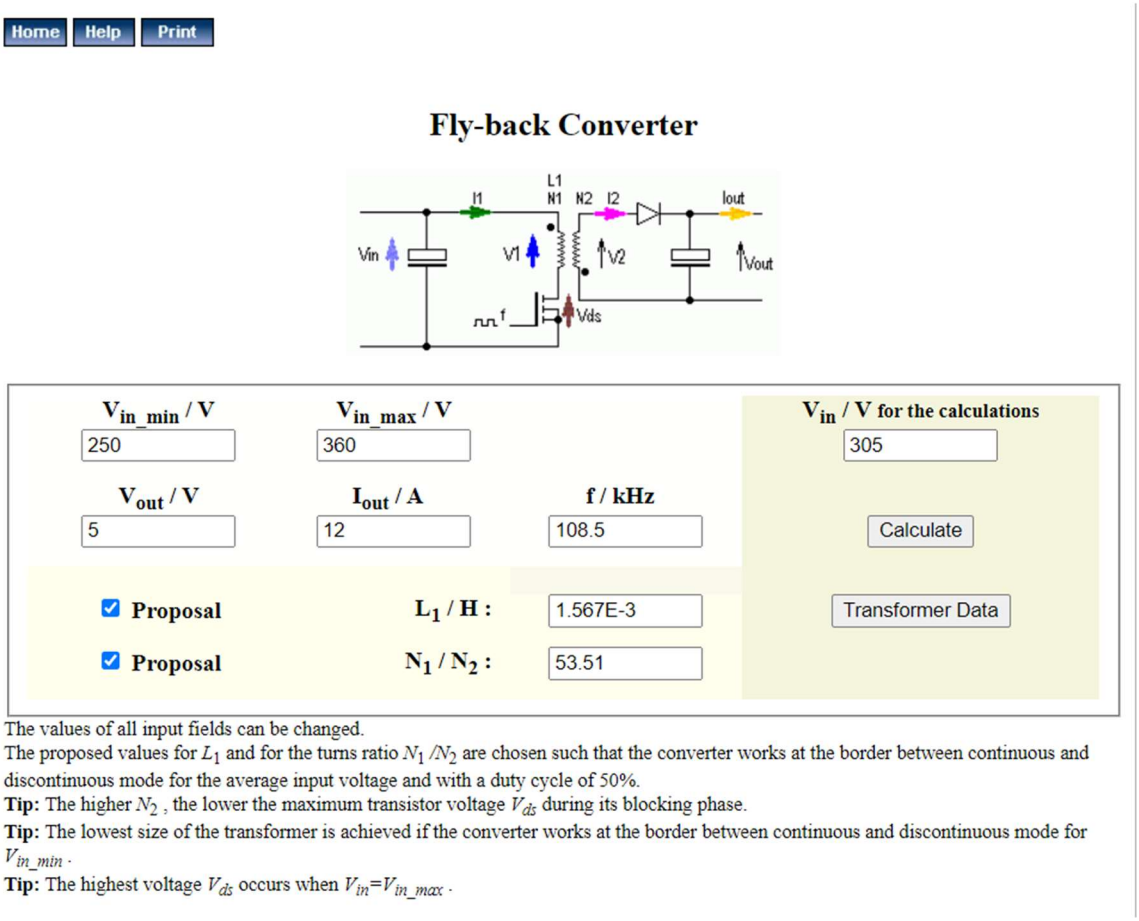


Рисунок 2.20 – Розрахунок у онлайн калькуляторі Flyback Converter

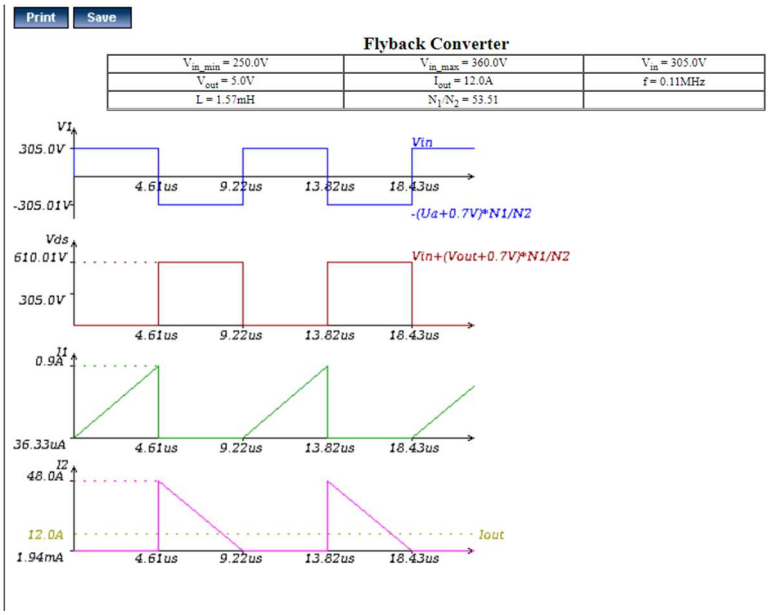


Рисунок 2.21 – Данні отримані після розрахунку

Вибір ключового транзистора VT, у якості якого рекомендується застосовувати MOSFET з n-каналом, здійснюється по величині максимального струму індуктивного елемента. Вибираємо транзистор 77N65 з параметрами: максимальна напруга стік-витік $U_{св}$ = 650В; максимальний струм стік-витік при 25C^{O} $I_{св\ макс.}$=69А; опір каналу у відкритому стані Rds = 0,038Ом; максимальна напруга затвор-витік $U_{зв\ макс.}$= 25В; максимальна потужність, що розсіюється $P_{св.макс.}$ = 400Вт; час спадання імпульсу tf = 20нс; час наростання імпульсу tr = 22нс.

Тепловий режим транзистора розраховується за формулою (2.4)

$$Pn = \left(\frac{i_{out}}{1-D}\right)^2 \cdot Rds(on) \cdot D + \frac{1}{2} \cdot Uout \cdot \left(\frac{i_{out}}{1-D}\right)^2 \cdot (t_r + t_f) \cdot f \quad (2.4)$$

$$P_n = \left(\frac{12}{1-0.5}\right)^2 \cdot 0{,}038 \cdot 0{,}5 + \frac{1}{2} \cdot 5 \cdot \left(\frac{12}{1-0{,}5}\right)^2 \cdot (22 \cdot 10^{-9} + 20 \cdot 10^{-9}) \cdot 108{,}5 \cdot 10^3 == 6{,}6 \text{ Вт}$$

Перший доданок цієї формули являє собою статичні втрати на опорі «стік-витік» відкритого транзистора, а другий – динамічні втрати при його перемиканні. При розрахунку по формулі потрібно підставляти максимальний коефіцієнт заповнення D, що забезпечується схемою перетворювача.

Вибраний транзистор за потужністю розсіювання та максимальним струмом індуктивного елемента відповідає зазначеним вимогам і може використовуватись у перетворювачі напруги.

Як діод VD, якщо дозволяє величина максимальної зворотної напруги, краще використовувати діоди з бар'єром Шотткі[41]. Ці діоди мають невелике падіння напруги в прямому напрямку, високу швидкодією й тим самим підвищують загальний коефіцієнт корисної дії перетворювача. Необхідно вибрати діод, що підходить по величині прямого струму, зворотної напруги й конструктивному виконанню корпуса. Вибираємо діод SBL1640 з параметрами: $U_{звмах}$ = 40В, $I_{прмах}$ = 16А, $U_{пр}$ = 0,57В, $C_{вив}$ = 500пФ.

Теплові втрати діода перетворювача розраховуються за формулою (2.5)

$$P_{CON} = U_f \cdot i_{out} \quad (2.5)$$

$$P_{CON} = 0.57 \cdot 12 = 6.84 \text{ Вт}$$

де Uf – прямий спад напруги на діоді;

I_{out} – Вихідний струм.

Динамічними втратами при розрахунку схеми перетворювача знехтують, тому що їхній внесок у цьому випадку невеликий.

2.3.6 Вибір дроселя PFC

При відсутності PFC-дроселя струм споживання ІБЖ явно не відповідає нормам стандарту EN61000-3-2. Справа в тому, що величина третьої гармоніки I3, як правило, є найбільш критичною щодо верхньої ліміту. Відповідний ліміт стандарту відзначений на рисунку 2.22 лінією червоного кольору. Вимоги стандарту EN61000-3-2 щодо гармонік струму можна забезпечити PFC-дроселем з L ≥ 36 мГн або декількома PFC-дроселями з великим значенням індуктивності рисунку 2.22 б. У практичних схемах EPCOS рекомендує використовувати PFC-дроселі з L ≥ 40 мГн. Рівень гармонік струму для цього випадку ілюструє рисунку 2.22 в.

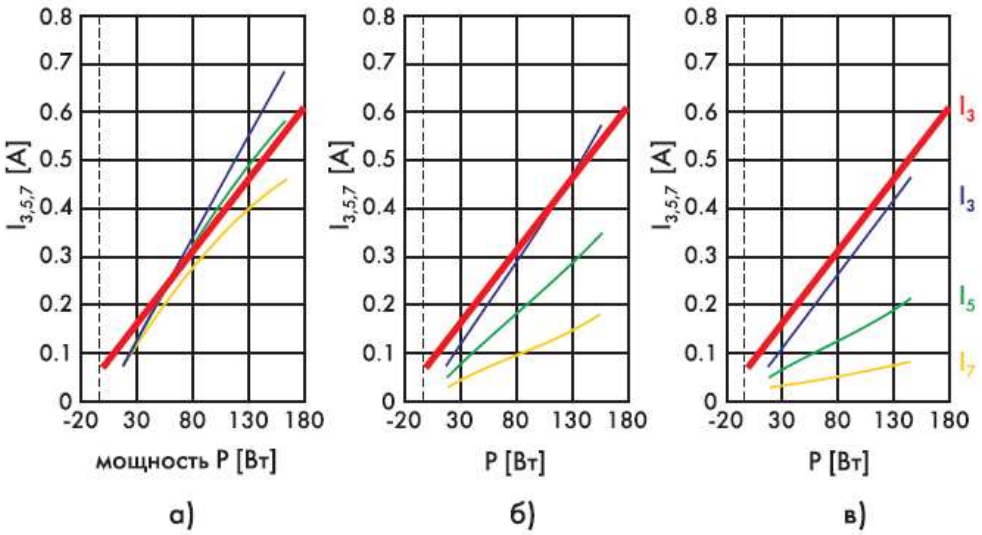


Рисунок 2.22 – Рівень гармонік струму (I3, I5, и I7), що споживає ІБЖ при С = 100мкФ: а) без PFC-дроселя, б) з PFC-дроселем при L = 18 мГн, в) з PFC-дроселем при L = 40 мГн

2.3.7 Розрахунок намотувальних параметрів вихідного дроселя

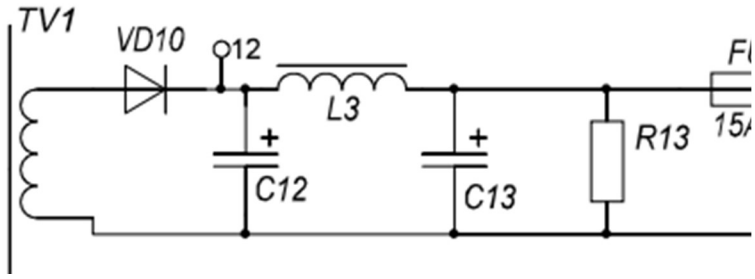


Рисунок 2.23 – Частина схеми що розраховується

Таблиця 2.4 – Вхідні данні для розрахунку вихідного дроселя L3 що зображений на рисунок 2.23

Параметр	Значення
Індуктивність дроселя	1,9 мкГн
Номінальний струм	12А
Амплітуда перед дроселем	7,7В
Амплітуда після дроселя	5В

Частота обирається така як на трансформаторі, в нашому випадку 108,5 кГц. Щільність струму також береться така як трансформаторі, 5А/мм^2. Розрахунок проведений у програмі DrosselRing рисунку 2.24.

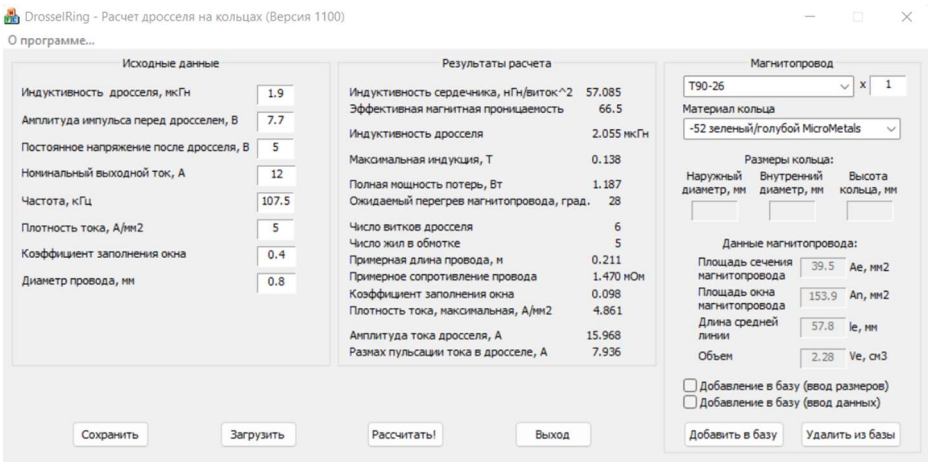


Рисунок 2.24 – Розрахунок у програмі DrosselRing

2.4 Розрахунок надійності

Надійність – це властивості приладів зберігати свої параметри в певних експлуатаційних умовах. Розрахунок надійності заключається у визначенні показників надійності виробу через характеристики складових компонентів що записані у таблиці 2.4 і відомими умовами експлуатації. Основними показниками надійності вважають: імовірність безвідмовної роботи P(t), інтенсивність відмов $\lambda(t)$, середній час безвідмовної роботи T_{CP}.

Данні про надійність беруться з програми mtbf калькулятор[42].

Імовірність безвідмовної роботи – це вірогідність того, що в певному інтервалі часу або в заданих межах напрацювання не відбудеться жодної відмови.

Розрахунок імовірності безвідмовної роботи визначається за формулою (2.6).

$$P(t) = e^{-\lambda * t}, \quad (2.6)$$

де λ – це сумарна інтенсивність відмов;

t – час, необхідної безвідмовної роботи (10000 ч).

Інтенсивність відмов показує, яка частина елементів, відносно загальної кількості працюючих елементів в середньому виходить з ладу за одиницю часу. Визначається за формулою (2.7)

$$\lambda_0 = \Sigma \lambda_{ie} N_i, \quad (2.7)$$

де λ_{ie} - інтенсивність відмов елемента і;

N_i – кількість елементів.

Напрацювання на відмову T_0 – це середній час роботи виробу між суміжними відмовами, розраховується за формулою (2.8).

$$T_0 = 1 / \lambda_0. \quad (2.8)$$

Таблиця 2.5 – Попередній розрахунок надійності

Типи елементів	Середньо групові значення інтенсивності відказів	К-сть елементів	Інтенсивність відмов
Мікросхеми інтегральні напівпровідникові цифрові	0,21	5	1,05
Діоди випрямні	0.85	6	5.1
Транзистори польові	0.3	1	0.3
Транзисторні оптопари	0,29	1	0,29
Резистори металодіелектричні	0,22	18	3,96

Продовження таблиці 2.5

Типи елементів	Середньо групові значення інтенсивності відказів	К-сть елементів	Інтенсивність відмов
Резистори змінні плівкові	0,01	1	0,01
Терморезистори	0,0013	1	0,0013
Конденсатори керамічні	0,03	12	0,36
Конденсатори метало паперові	0,01	5	0,05
Кнопки	0,16	1	0,16
Запобіжники	0,2	1	0,2
Трансформатор імпульсний	1	1	1
Дроселі	0,033	2	0,066
Індикатори одиночні	0,13	256	33,28
Ручна пайка з друкованим монтажем	0,0006	512	0.3072
$(\Sigma N_C \lambda_C)$			46,2445

IoT будильника відноситься до класу GB (наземне стаціонарне обладнання), для якого поправочний коефіцієнт $\pi E = 0,5$. Підставляємо це значення у формулу (2.9) для отримання імовірності відмов.

$$FR = \lambda (1+0,2\ \pi E) \qquad (2.9)$$

Підставивши значення у формулу (2.9) отримуємо:

$$FR = 50{,}41 \times 10^{-6}\ 1/\text{год}.$$

Побудуємо графік ймовірності безвідмовної роботи IoT будильника що зображений на рисунку 2.26 за формулою:

Таблиця 2.6 – Залежність $P(t) = e^{-FR \times t}$

T,тис. год	0	10	20	30	40	50	60	70	80	90	100
P(t)	1,00	0,60	0,36	0,22	0,13	0,08	0,05	0,03	0,02	0,01	0,01

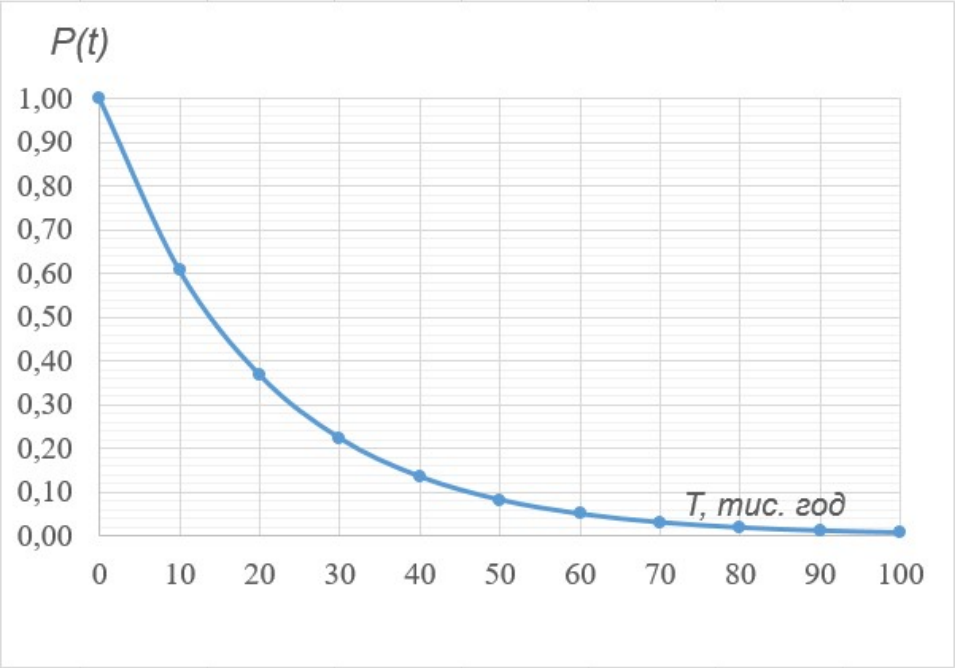


Рисунок 2.26 – Графік ймовірності безвідмовної роботи IoT будильника побудований за таблицею 2.6

3 ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

Для проведення досліджень використовується ноутбук, мобільний телефон, мультиметр.

Схема дослідження струму споживання зображена на рисунку 3.1.

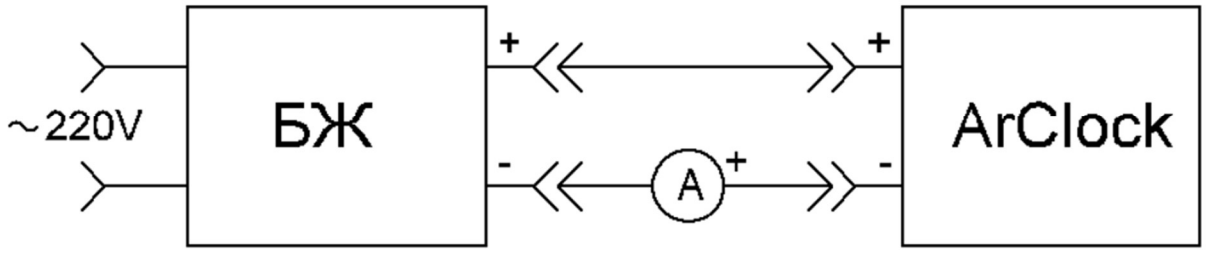
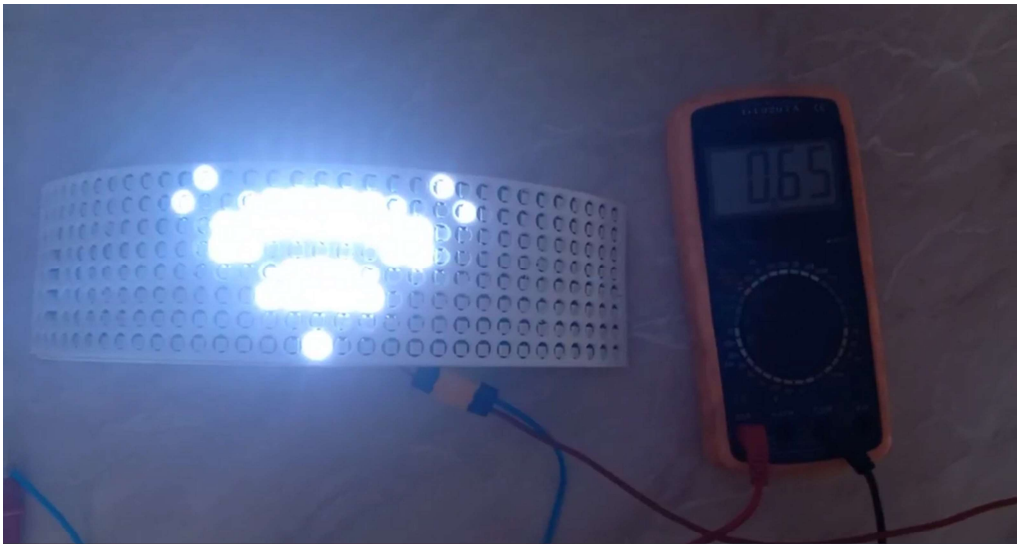


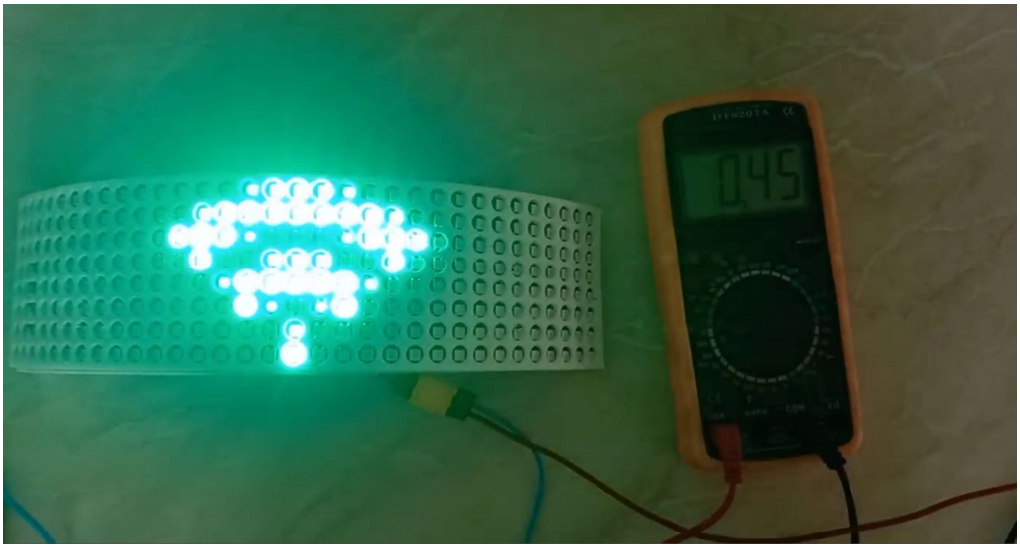
Рисунок 3.1 – Схема дослідження струму споживання

3.1 Дослідження споживання при різних режимах роботи

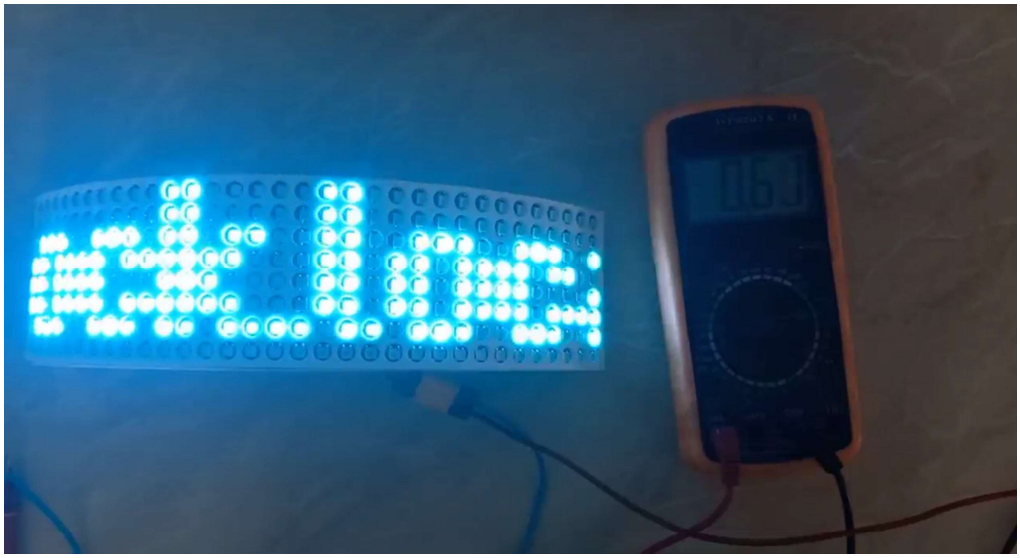
Годинник запускається з налаштуваннями за замовчуванням, з максимальною яскравістю, тому він споживає 6,5А що зображено на рисунку 3.2а.



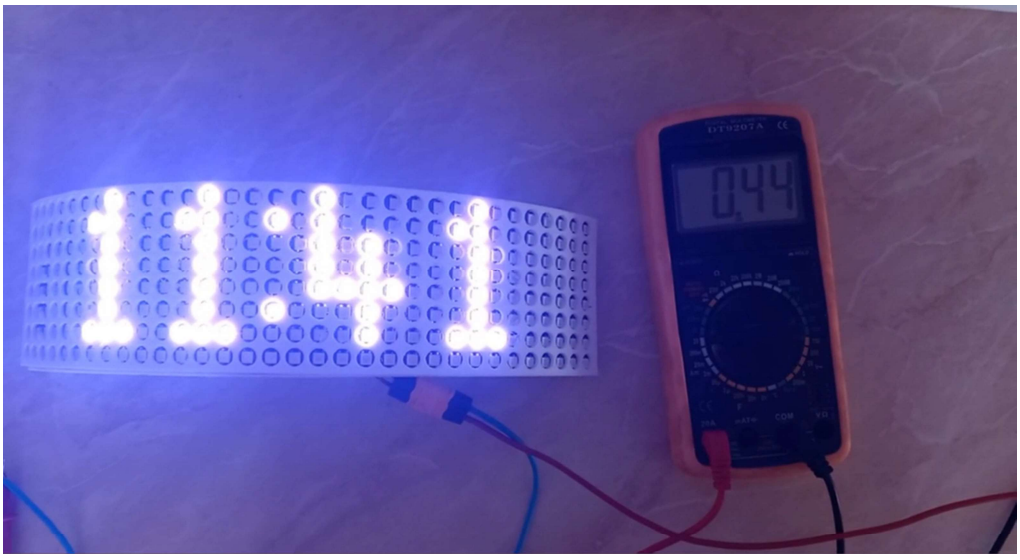
а)



б)



в)



г)

Рисунок 3.2 – Споживання при різних режимах

Після підключення до мережі Wi-Fi, годинник завантажує тимчасові налаштування що виставлені у програмі керування споживання зменшується до 4,5А що зображено на рисунку 3.2б. У режимі відображення тексту годинник споживає 5,4 – 6,9А, зображено на рисунку 3.2в. У режимі відображення часу годинник споживає 4,4А, зображено на рисунку 3.2г.

3.2 Дослідження інтернет з’єднання

Для дослідження інтернет з`єднання буде використовуватися командна стрічка на комп’ютері.

У меню “ Виконати” вводимо “CMD” рисунок 3.3.

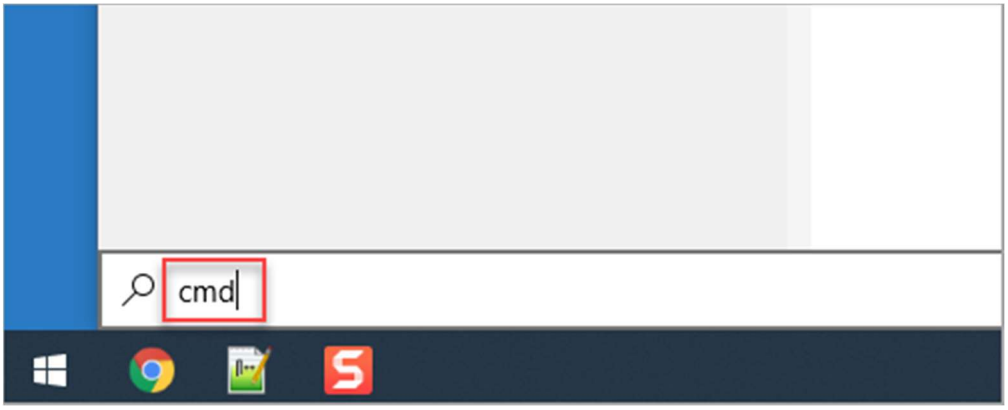


Рисунок 3.3 – Меню “Виконати”

У командну рядок вводимо команду “PING IP-адрес” та натискаємо Enter рисунок 3.4.

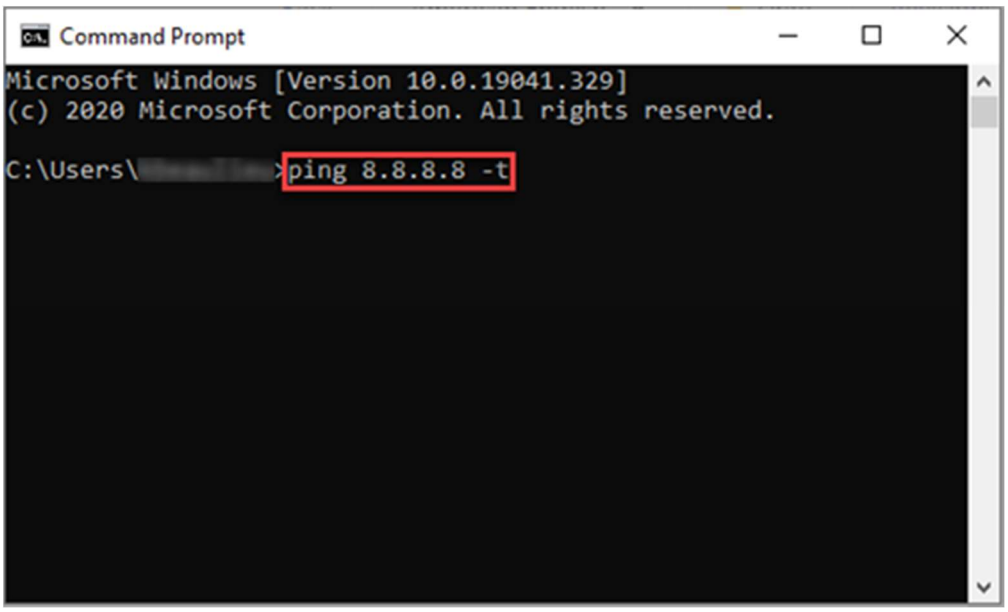


Рисунок 3.4 – Командна рядок

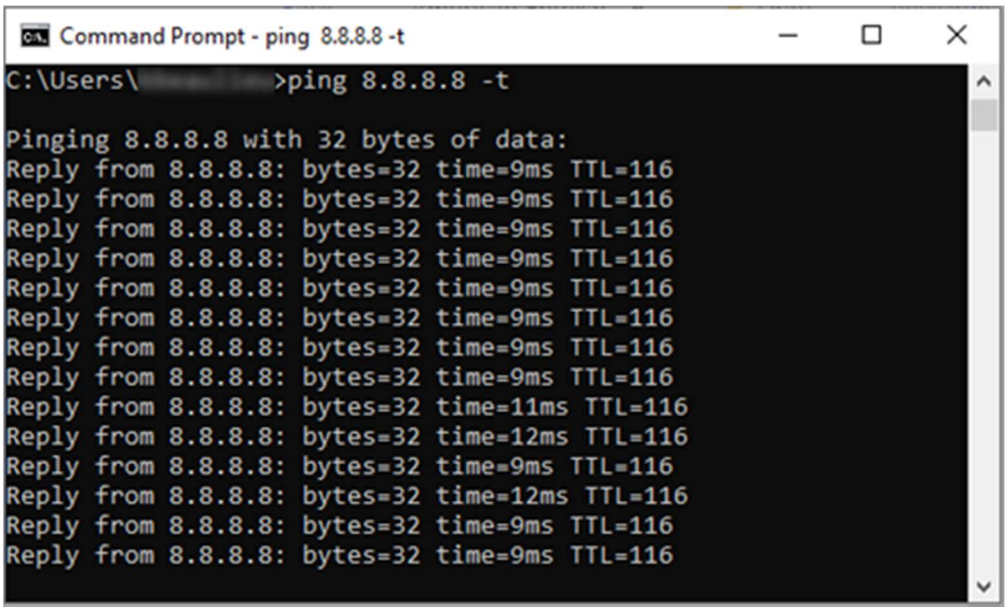


Рисунок 3.5 – Результат перевірки пінгу

З рисунку 3.5 видно що середній пінг знаходиться в районі 28мс, максимальний підіймається до 60мс, при обміні пакетами втрат не відбулося.

Інтерфейс програми керування зображений на рисунку 3.6.

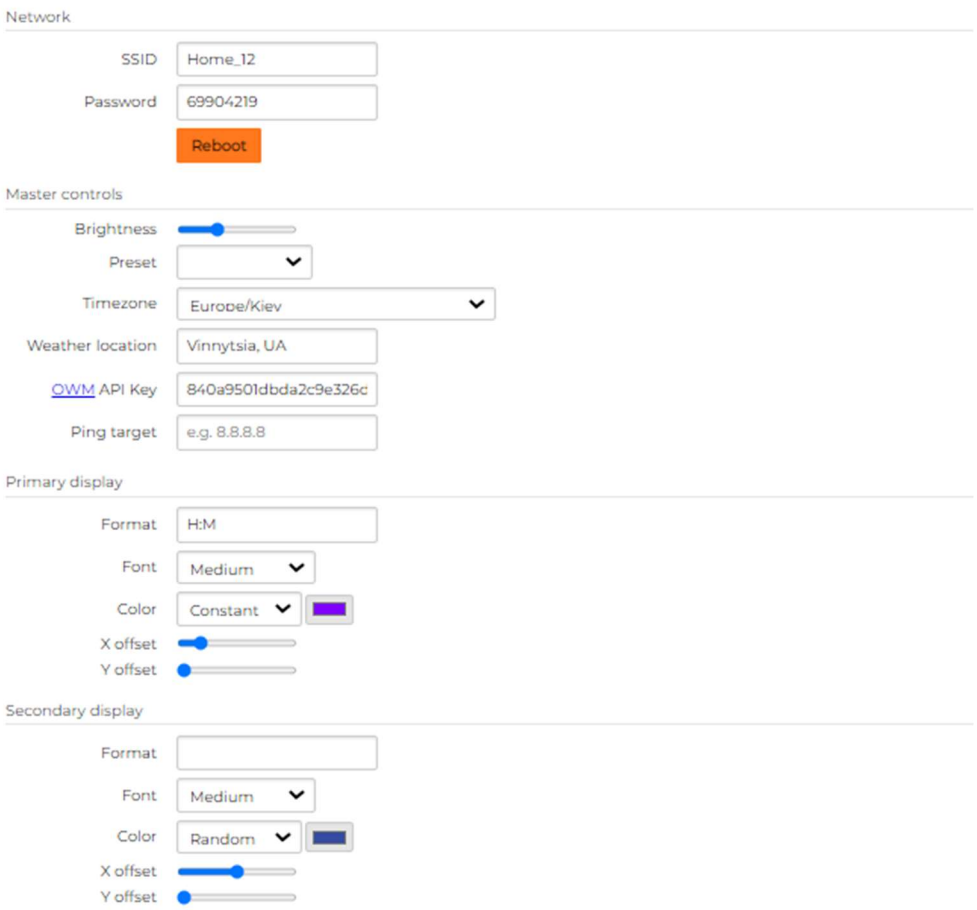


Рисунок 3.6 – Інтерфейс програми керування, що запускається на мобільному телефоні за IP – адресом

4 ОХОРОНА ПРАЦІ

Під час дослідження розумного IoT будильника на Arduino на працівника, впливають такі небезпечні та шкідливі виробничі фактори [43]: підвищена запиленість та загазованість повітря робочої зони; підвищена та понижена температура повітря робочої зони; підвищений рівень шуму; підвищений рівень статичної електрики; підвищена напруженість електричного поля; недостатня освітленість повітря робочої зони; фізичні перевантаження (статичні); нервово - психічні перевантаження (перенапруга аналізаторів).

Відповідно до визначених факторів формуємо рекомендації щодо покращення умов праці на робочому місці.

4.1 Технічні рішення щодо безпечного виконання роботи

На робочому місці дослідника розумного IoT будильника на Arduino виникають небезпечні та шкідливі фактори: підвищений рівень шуму, несприятливі мікрокліматичні умови, недостатній рівень освітленості, шкідливі речовини, підвищений рівень електромагнітних випромінювань радіочастот, висока напруга електричної мережі, статична електрика та інші. Робота з ПК супроводжується також підвищеним ступенем напруженості трудового процесу. При систематичному впливі виробничих факторів, які не відповідають нормативним показникам, зростає рівень професійно зумовленої захворюваності працюючих та можуть виникнути професійні захворювання органів зору, руху, нервової системи.

Проектування робочих місць, забезпечених ПК, відноситься до числа важливих проблем ергономічного проектування в області обчислювальної техніки.

Робоче місце і взаємне розташування всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи. Зокрема, при організації робочого місця

проектувальника повинні бути дотримані наступні основні умови: оптимальне розміщення устаткування, що входить до складу робочого місця і достатній робочий простір, що дозволяє здійснювати всі необхідні рухи і переміщення [44].

Головними елементами робочого місця проектувальника є стіл і крісло. Основним робочим положенням є положення сидячи. Робоча поза сидячи викликає мінімальне стомлення працівника. Раціональне планування робочого місця передбачає чіткий порядок і постійність розміщення предметів, засобів праці і документації. Те, що потрібне для виконання робіт частіше, розташоване в зоні легкої досяжності робочого простору.

Висота робочої поверхні столу для користувачів повинна регулюватися в межах 680-800 мм, при відсутності такої можливості висота робочої поверхні столу повинна бути 725 мм. Модульними розмірами робочої поверхні столу для ПК, на підставі яких повинні розраховуватися конструктивні розміри, слід вважати: ширину 800, 1200, 1400 мм, глибину 800 і 1000 мм при нерегульованої висоті, що дорівнює 725 мм. Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною – не менше 500 мм, глибиною на рівні колін - не менше 450 мм і на рівні простягнутої ноги – не менше 650 мм. Робочий стілець (крісло) повинен бути підйомно-поворотним і регульованим по висоті і кутам нахилу сидіння і спинки, а також - відстані спинки до переднього краю сидіння. Робоче місце необхідно обладнати підставкою для ніг, має ширину не менше 300 мм, глибину не менше 400 мм, регулювання по висоті в межах до 150 мм і по куту нахилу опорної поверхні підставки до 20 градусів. Підставка повинна мати рифлену поверхню і бортик по передньому краю заввишки 10 мм. Клавіатуру слід розташовувати на поверхні столу на відстані 100-300 мм від краю, зверненого до користувача, або на спеціальній регульованій по висоті робочої поверхні, відокремленої від основної стільниці.

Електричний струм – являє собою прихований тип небезпеки, бо його важко визначити в токо- та неструмоведучих частинах устаткування, які є хорошими провідниками електрики. Смертельно небезпечним для життя людини

вважають струм, величина якого перевищує 0,05 А, струм менше 0,05 А - безпечний (до 1000 В). З метою попередження уражень електричним струмом до роботи повинні допускатися тільки особи, що добре вивчили основні правила з безпеки виконання роботи.

Приміщення, де експлуатуються ПК, належать до приміщень без підвищеної небезпеки ураження людини електричним струмом. Вимоги електробезпеки і пожежної безпеки у приміщеннях, де встановлені ПК і все устаткування для обслуговування, ремонту та налагодження роботи їх, електропроводи і кабелі мають відповідати електробезпеці зони та мати апаратуру захисту від струму короткого замикання.

Лінії електромережі ПК, у приміщенні виконана як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників (заземлення або занулення), причому площі перерізу нульового робочого і нульового захисного провідника повинні бути не менші за площу перерізу фазового провідника.

Відповідно до правил електробезпеки в службовому приміщенні повинен здійснюватись постійний контроль стану електропроводки, запобіжних щитів, шнурів, за допомогою яких включаються в електромережу комп'ютери, освітлювальні прилади, інші електроприлади. Електричні установки, до яких відноситься практично все обладнання ПК, представляють для людини велику потенційну небезпеку, тому що в процесі експлуатації або проведенні профілактичних робіт людина може торкнутися частин, що знаходяться під напругою. Специфічна небезпека електроустановок - струмоведучі провідники, корпуси стійок ПК і іншого устаткування, яка під напругою в результаті пошкодження (пробою) ізоляції, не подають будь-яких сигналів, які попереджають людину про небезпеку. Реакція людини на електричний струм виникає лише при протіканні останнього через тіло людини. Виключно важливе значення для запобігання електротравматизму має правильна організація обслуговування діючих електроустановок ВЦ, проведення ремонтних, монтажних і профілактичних робіт.

Оскільки в приміщенні використовується понад п’ять ПК, тому на помітному місці встановлено аварійний резервний вимикач, який в разі небезпеки повністю знеструмлює електричну мережу (крім освітлення). В такому випадку при використанні трипровідникового захищеного проводу або кабелю в оболонці з негорючого або важкогорючого матеріалу дозволено прокладати їх без металевих труб та гнучких металевих рукавів, що ми і спостерігаємо у приміщенні.

4.2 Технічні рішення з гігієни праці та виробничої санітарії

4.2.1 Мікроклімат

Мікроклімат виробничих приміщень нормується в залежності від теплових характеристик виробничого приміщення, категорії робіт по важкості і періоду року. Категорія виконуваних робіт під час дослідження розумного IoT будильника на Arduino - 1а [47] (табл.4.2.1).

Таблиця 4.2.1 – Параметри мікроклімату

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні Відносна вологість Швидкість руху повітря	21 ... 25 ° С 40 ... 60% до 0,1 м / с
Теплий	Температура повітря в приміщенні Відносна вологість Швидкість руху повітря	22 ... 28 ° С 40 ... 60% 0,1 ... 0,2 м / с

Для підтримання у виробничих приміщеннях метеорологічних умов, які задовольняють нормативні вимоги використовують систему вентиляції. Приміщення обладнано системою загально обмінної припливно-витяжної вентиляції. На кожну вентиляційну установку складений паспорт з технічною характеристикою та схемою установки.

Крім того, для підтримання температури в холодний період року використовують загальну систему опалення.

4.2.2 Склад повітря робочої зони

ГДК шкідливих речовин, які знаходяться в досліджуваному приміщені, наведені в таблиці 4.2.2.

Таблиця 4.2.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Оксид азоту	0,085	0,085	2
Вуглекислий газ	3	1	4
Пил нетоксичний	0,5	0,15	4
Озон	0,16	0,03	1

Під час роботи на ПК важливо, щоб повітря мало певний іонний склад. Рівні позитивних і негативних іонів у повітрі приміщень з ПК мають відповідати санітарно-гігієнічним нормам (табл.4.2.3).

Таблиця 4.2.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 см^3	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально необхідні	50000	50000

Забезпечення складу повітря робочої зони здійснюється за допомогою системи кондиціювання, регулярного провітрювання, та вологого прибирання.

4.2.3 Виробниче освітлення

Природне освітлення на робочому місці проектувальника є бічне одностороннє.

Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні (характеристика зорової роботи – дуже високої точності) зазначені у таблиці 4.2.4:

Таблиця 4.2.4 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, $e_н$,%			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє	Бокове	Верхнє або верхнє і бокове	Бокове
Дуже високої точності	Від 0,15 до 0,3	II	г	великий	світлий	1000	300	7	2,5	4,2	1,5

Для максимального використання природного освітлення в приміщенні слід систематично очищувати вікна від пилу та встановити жалюзі. Віконні прорізи не затемнюються іншими будівлями.

Як джерела світла для штучного освітлення в приміщенні застосовуються люмінесцентні лампи типу ЛБ. Допускається застосування ламп розжарювання у світильниках місцевого освітлення

4.2.4 Виробничий шум

Рівні шуму на робочих місцях визначаються за ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку» [48] (табл.4.2.5).

Таблиця 4.2.5 Допустимі рівні звуку, еквівалентні рівні звуку і рівні звукового тиску в октавних смугах частот

Вид трудової діяльності, робочі місця	Рівні звукового тиску в дБ в октавних смугах із середньогеометричними частотами, Гц									Рівні звуку, еквівалентні рівні звуку, дБА/дБАекв.
	31,5	63	125	250	500	1000	2000	4000	8000	
Творча діяльність, обробка даних,	86	71	61	54	49	45	42	40	38	60

Рівень шуму на робочих місцях не має перевищувати 60 дБА, що досягається застосуванням малошумного обладнання, використанням спеціальних матеріалів для обшивки приміщень, а також різноманітними звукопоглинальними пристроями (перегородки, кожухи, прокладки тощо).

4.2.5 Виробничі випромінювання

Значення напруженості електростатичного поля на робочих місцях із ПК (як у зоні екрана дисплея, так і на поверхнях обладнання, клавіатури, друкувального пристрою) мають не перевищувати гранично допустимих [49] (табл.4.2.6).

Таблиця 4.2.6 – Допустимі параметри електромагнітних випромінювань

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні відеомонітору	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні відеомонітору	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати:	для дорослих користувачів 20кВ/м для дітей 15кВ/м

Інтенсивність потоків інфрачервоного випромінювання має не перевищувати допустимих значень [46].

Потужність експозиційної дози рентгенівського випромінювання на відстані 0,05 м від екрана та корпуса відео термінала при будь-яких положеннях регулювальних пристроїв не повинна перевищувати ОД бер/год (100 мкР/год).

Для забезпечення захисту і досягнення нормованих рівнів комп'ютерних випромінювань необхідно застосовувати при екранні фільтри, локальні світлофільтри (засоби індивідуального захисту очей) та інші засоби захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат (згідно Директиви № 90/270/ЕЄС [50]).

4.3 Пожежна безпека

Пожежна безпека – стан об'єкта, при якому виключається можливість пожежі, а в разі його виникнення запобігається вплив на людей небезпечних факторів пожежі і забезпечується захист матеріальних цінностей. Пожежна безпека забезпечується системою запобігання пожежі і системою пожежного захисту.

Пожежна безпека приміщення повинна відповідати вимогам Кодексу цивільного захисту України [51] та «Правила пожежної безпеки в Україні» [52].

За вибуховою і пожежною небезпекою приміщення належить до категорії Д, згідно з нормами технологічного проектування «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою» [53]. У приміщенні знаходяться ПК та інша оргтехніка, що можуть спричинити пожежу.

Згідно даних наведених у таблиці 3.1 будівля, в якій знаходиться приміщення, має II ступінь вогнестійкості [54] приміщення можна віднести до категорії вибухопожежонебезпеки В (табл.4.3.1).

Таблиця 4.3.1. – Визначення ступеня вогнестійкості будівельних конструкцій

Ступінь вогнестійкості будинків	Мінімальні межі вогнестійкості будівельних конструкцій (у хвилинах) та максимальні межі поширення вогню по них (см)								
	стіни				колони	сходові площадки, косоури, сходи, балки, марші сходових клітків	перекриття міжповерхові (у т. ч. горищні та над підвалами)	елементи суміщених покриттів	
	несучі та сходових клітків	самонесучі	зовнішні ненесучі	внутрішні ненесучі (перегородки)				плити, настили, прогони	балки, ферми, арки, рами
III	REI 120 M0	REI 60 M0	E15, M0 E30, M1	EI 15 M1	R 120 M0	R 60 M0	REI 45 M1	Не нормуються	

Клас приміщення і зон з вибухо- і пожежонебезпеки П-IIа (приміщення, у якому знаходяться тверді горючі речовини та матеріали.)

4.3.1 Технічні рішення системи запобігання пожежі

Для запобігання виникнення пожежі в приміщенні застосовують такі заходи:

– щорічне проведення повторних протипожежних інструктажів та занять за програмою пожежно-технічного мінімуму з особами, що відповідальні за пожежну безпеку;

– утримання в справному стані засобів протипожежного захисту;

– своєчасне інформування про несправність пожежної техніки, систем протипожежного захисту, водопостачання тощо.

Електромережі, електроприлади і апаратура експлуатується тільки у справному стані з урахуванням вказівок та рекомендацій підприємств-

виготовлювачів. У разі виявлення пошкоджень електромереж, вимикачів, розеток та інших електровиробів слід негайно вимкнути їх та вжити необхідних заходів щодо приведення в пожежобезпечний стан.

4.3.2 Технічні рішення системи протипожежного захисту

Протипожежний захист – це комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, запобігання пожежі, обмеження її розповсюдження, а також на створення умов для успішного гасіння пожежі.

У всіх службових приміщеннях обов'язково повинен бути «План евакуації людей при пожежі», що регламентує дії персоналу у разі виникнення вогнища загоряння і в якому зазначено місця розташування пожежної техніки. Як відомо пожежа може виникнути при взаємодії горючих речовин, окислення і джерел запалювання. У робочому приміщенні присутні всі три основні чинника, необхідні для виникнення пожежі. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, двері, підлоги, ізоляція кабелів і ін

Джерелами запалювання у ВЦ можуть бути електронні схеми від ПК, прилади, застосовувані для технічного обслуговування, пристрої електроживлення, кондиціонування повітря, де внаслідок різних порушень утворюються перегріті елементи, електричні іскри та дуги, здатні викликати загоряння горючих матеріалів. У сучасних ПК дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються сполучні дроти, кабелі. При протіканні по них електричного струму виділяється значна кількість теплоти. При цьому можливо оплавлення ізоляції. Для відведення надлишкової теплоти від ЕОМ служать системи вентиляції та кондиціонування повітря. При постійному дії ці системи представляють собою додаткову пожежну небезпеку.

При проведенні обслуговуючих, ремонтних і профілактичних робіт використовуються різні мастильні речовини, легкозаймисті рідини,

прокладаються тимчасові електропровідниками, ведуть пайку та чистку окремих вузлів. Виникає додаткова пожежна небезпека, яка потребує додаткових заходів пожежного захисту. Зокрема, при роботі з паяльником слід використовувати неспалену підставку з нескладними пристроями для зменшення споживаної потужності в неробочому стані.

Однією з найбільш важливих завдань пожежної захисту є захист будівельних приміщень від руйнувань та забезпечення їх достатньої міцності в умовах впливу високих температур при пожежі. З огляду на високу вартість електронного устаткування приміщення, а також категорію його пожежної небезпеки, будинки для ВЦ і частини будинку іншого призначення, в яких передбачено розміщення ПК повинні бути 1 і 2 ступеня вогнестійкості.

Для виготовлення будівельних конструкцій використовуються, як правило, цегла, залізобетон, скло, метал та інші негорючі матеріали. Застосування дерева повинна бути обмежено, а в разі використання необхідно просочувати його вогнезахисними складами.

До засобів гасіння пожежі, призначених для локалізації невеликих загорянь, відносяться внутрішні пожежні водопроводи, вогнегасники, сухий пісок, азбестові ковдри і т. д. Застосування води в машинних залах ПК, сховищах носіїв інформації, приміщеннях контрольно-вимірювальних приладів, зважаючи на небезпеку пошкодження або повного виходу з ладу дорогого устаткування можливо у виняткових випадках, коли пожежа приймає загрозливо великі розміри. При цьому кількість води повинна бути мінімальною, а пристрої ПК необхідно захистити від попадання води, накриваючи їх брезентом або полотном.

Для гасіння пожеж на початкових стадіях широко застосовуються вогнегасники. У приміщенні застосовуються головним чином вуглекислотні вогнегасники, перевагами якого є висока ефективність гасіння пожежі, схоронність електронного устаткування, діелектричні властивості вуглекислого газу, що дозволяє використовувати ці вогнегасники навіть у тому випадку, коли не вдається знеструмити електроустановку відразу.

ВИСНОВКИ

У бакалаврській дипломній роботі було розроблено мікроелектронний пристрій, який контролює тип дизельного палива.

Було проведено порівняльну характеристику приладу з іншими приладами, які вже існують, вказані переваги та недоліки.

Запропонована електрична принципова схема пристрою, на основі якої було проведено трасування та встановлені розміри плати виробу 50х100 мм і розрахована маса 34,28 г.

За матеріал для друкованої плати обрано склотекстоліт фольгований односторонній марки СФ-1-35-1,5, який має товщину фольги 35 мкм., товщина матеріалу з фольгою – 1,5 мм.

Даний аналіз роботи показав переваги пристрою:

- здешевлена вартість, щодо лабораторного обладнання;
- простота у застосуванні;
- точність одержуваної інформації
- схемо технічна частота
- висока температурна стабільність.

Усі ці фактори, які дають привід задуматися про придбання приладу, як організаціям так і фізичним особам які мають необхідність, бажання контролювати якість використовуваної продукції.

При розрахунку на удар бачимо що спосіб кріплення та товщина плати забезпечують найменшу частоту власних коливань, найбільше віброзміщення при дії вібрації і найменше ударне прискорення при дії ударів.

Згідно розрахунків, можна сказати, що даний пристрій задовольняє усі техніко-технологічні характеристики та може бути введений в експлуатацію

Отож, завданням даної роботи було провести аналіз пристрою, контролю типу дизельного палива, що в результаті і було досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco. Cisco: 2020 CISO Benchmark Report; Cisco: San Jose, CA, USA, 2020; Volume 2020. [Google Scholar]

2. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Commun. Surv. Tutor. 2019, 21, 2671–2701. [Google Scholar] [CrossRef]

3. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Commun. Surv. Tutor. 2020, 22, 1686–1721. [Google Scholar] [CrossRef] [Green Version]

4. Farooq, M.U.; Waseem, M.; Mazhar, S.; Khairi, A.; Kamal, T. A Review on Internet of Things (IoT). Int. J. Comput. Appl. 2015, 113, 1–7. [Google Scholar] [CrossRef]

5. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. Sensors 2019, 19, 1141. [Google Scholar] [CrossRef] [PubMed] [Green Version]

6. Rana, M.M.; Bo, R. IoT-based cyber-physical communication architecture: Challenges and research directions. IET Cyber-Phys. Syst. Theory Appl. 2020, 5, 25–30. [Google Scholar] [CrossRef]

7. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. Microprocess. Microsyst. 2020, 77, 103201. [Google Scholar] [CrossRef] [PubMed]

8. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.M.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. J. Netw. Comput. Appl. 2021, 181, 103007. [Google Scholar] [CrossRef]

9. Yu, Z.; Song, L.; Jiang, L.; Khold Sharafi, O. Systematic literature review on the security challenges of blockchain in IoT-based smart cities. Kybernetes 2022, 51, 323–347. [Google Scholar] [CrossRef]

10. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustain. Cities Soc. 2020, 61, 102360. [Google Scholar] [CrossRef]

11. Theodorou, S.; Sklavos, N. Blockchain-based security and privacy in smart cities. In Smart Cities Cybersecurity and Privacy; Elsevier: Amsterdam, The Netherlands, 2018; pp. 21–37. ISBN 9780128150320. [Google Scholar]

12. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT elements, layered architectures and security issues: A comprehensive survey. Sensors 2018, 18, 2796. [Google Scholar] [CrossRef] [Green Version]

13. Silva, B.N.; Khan, M.; Han, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustain. Cities Soc. 2018, 38, 697–713. [Google Scholar] [CrossRef]

14. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. 2018, 88, 173–190. [Google Scholar] [CrossRef]

15. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. IEEE Netw. 2020, 34, 8–14. [Google Scholar] [CrossRef]

16. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus. Horiz. 2015, 58, 431–440. [Google Scholar] [CrossRef]

17. Khalil, S.H.U.; Mueen-Uddin; Malik, O.A.; Hong, O.W. A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-art, Advancement, Challenges and Future Research Directions. IEEE Access 2022, 1–20. [Google Scholar] [CrossRef]

18. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Sensing as a service model for smart cities supported by Internet of Things. Trans. Emerg. Telecommun. Technol. 2014, 25, 81–93. [Google Scholar] [CrossRef] [Green Version]

19. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. 2013, 29, 1645–1660. [Google Scholar] [CrossRef] [Green Version]

20. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-based authentication and authorization for smart city applications. Inf. Process. Manag. 2021, 58, 102468. [Google Scholar] [CrossRef]

21. Fotiou, N.; Pittaras, I.; Siris, V.A.; Voulgaris, S.; Polyzos, G.C. OAuth 2.0 Authorization using Blockchain-based Tokens. arXiv 2021, arXiv:2001.10461. [Google Scholar] [CrossRef]

22. Raible, M. What the Heck is OAuth?|Okta Developer. Available online: https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth (accessed on 27 May 2021).

23. Shepherd, J. The Ultimate Authentication Playbook. 2019. Available online: https://www.okta.com/blog/2019/02/the-ultimate-authentication-playbook/ (accessed on 1 June 2021).

24. Tahir, M.; Sardaraz, M.; Muhammad, S.; Khan, M.S. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability 2020, 12, 6960. [Google Scholar] [CrossRef]

25. Ferreira, C.M.S.; Garrocho, C.T.B.; Oliveira, R.A.R.; Silva, J.S.á.; da Cavalcanti, C.F.M.C. IoT registration and authentication in smart city applications with blockchain. Sensors 2021, 21, 1323. [Google Scholar] [CrossRef]

26. Punia, A.; Gupta, D.; Jaiswal, S. A perspective on available security techniques in IoT. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017; pp. 1553–1559. [Google Scholar] [CrossRef]

27. Kaaniche, N.; Laurent, M. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Comput. Commun. 2017, 111, 120–141. [Google Scholar] [CrossRef]

28. Hriez, S.; Obeid, N.; Awajan, A. User authentication on smartphones using keystroke dynamics. In Proceedings of the Pervasive Health: Pervasive

Computing Technologies for Healthcare, Trento, Italy, 20–23 May 2019; pp. 2–5. [Google Scholar]

29. What Is Token-Based Authentication? 2021. Available online: https://www.okta.com/identity-101/what-is-token-based-authentication/

30. WorkOS A Developer's History of Authentication. 2020. Available online: https://workos.com/blog/a-developers-history-of-authentication

31. Mumtaz, M.; Akram, J.; Ping, L. An RSA based authentication system for smart IoT environment. In Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10–12 August 2019; pp. 758–765. [Google Scholar] [CrossRef]

32. Arcenegui, J.; Arjona, R.; Román, R.; Baturone, I. Secure combination of iot and blockchain by physically binding iot devices to smart non-fungible tokens using pufs. Sensors 2021, 21, 3119. [Google Scholar] [CrossRef]

33. Siddiqui, A.S.; Gui, Y.; Lawrence, D.; Laval, S.; Plusquellic, J.; Manjrekar, M.; Chowdhury, B.; Saqib, F. Hardware assisted security architecture for smart grid. In Proceedings of the IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 2890–2895. [Google Scholar] [CrossRef]

34. WeMos D1 Wi-Fi UNO (ESP8266 ESP-12E). URL: https://radioprog.ru/shop/merch/57

35. Офіційна документація на мікроконтролер ESP8266EX. URL: http://surl.li/alxhy

36. STM Урок 119. WS2812B. Лента на умных светодиодах RGB. Часть 1. URL: https://narodstream.ru/stm-urok-119-ws2812b-lenta-na-umnyx-svetodiodax-rgb-chast-1/

37. Блок питания Venom 5В 60Вт Standart IP20 (VST-60-5). URL: http://surl.li/azinl

38. Arduino IDE. URL: https://www.arduino.cc/en/software

39. UC3843 даташит (PDF) - Texas Instruments. URL: https://www.alldatasheetru.com/datasheet-pdf/pdf/101216/TI/UC3843.html

40. HER508 датащи (PDF) - DIOTEC Electronics Corporation. URL: https://www.alldatasheetru.com/datasheet-pdf/pdf/486856/DEC/HER508.html

41. Діоди шотткі. URL: https://radiostore.com.ua/ua/g5210269-diody-shottki

42. mtbf калькулятор. URL: https://reliability-software.ru/Reliability-Software/free-mtbf-calculator.html

43. ДСТУ OHSAS 18002:2015. Системи управління гігієною та безпекою праці. Основні принципи виконання вимог OHSAS 18001:2007 (OHSAS 18002:2008, IDT). К. : ГП «УкрНИУЦ», 2016. 21 с

44. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. URL: http://sop.zp.ua/norm_npaop _0 _ 00-7_ 15-18_01_ua.php

45. ДБНВ.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд. К. : Мінбуд України, 2006. 154 с

46. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. - [Електронний ресурс] - Режим доступу: http://mozdocs.kiev.ua/view.php?id=1972

47. Гігієнічна класифікація праці (за показниками шкідливості і небезпеки факторів виробничого середовища від 12.08.1986 № 4137-86. - [Електронний ресурс] - Режим доступу: http://zakon4.rada.gov.ua/laws/show/v4137400-86

48. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. - [Електронний ресурс] - Режим доступу: http://document.ua/ sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html

49. ДСНіП3.3.6.096-2002. Державні санітарні норми і правила при роботі з джерелами електромагнітних полів. URL: http://zakon2.rada.gov.ua/laws/show/ z0203-03

50. Директива № 90/270/ЕЄС «Про мінімум вимог безпеки і гігієни праці

при роботі з екранними пристроями - [Електронний ресурс] - Режим доступу: https://osha.europa.eu/en/legislation/directives/provisions-on-workload-ergonomical-and-psychosocial-risks/osh-directives/5

51. Кодекс цивільного захисту України від 02.10.2012 № 5403-VI

52. НАПБА.01.001-14. Правила пожежної безпеки в Україні. К. : МВС України, 2014. 47 с.

53. ДСТУ Б В.1.1-36:2016 Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпек. URL: https://dbn.co.ua/load/normativy/dstu/dstu_b_v_1_1_36/5-1-0-1759.

54. ДБН В.1.1-7:2016 Пожежна безпека об`єктів будівництва. Загальні вимоги. URL: http://www.poliplast.ua/doc/dbn _v.1.1-7-200

Додаток А
(обов`язковий)

ІЛЮСТРАТИВНИЙ МАТЕРІАЛ

РОЗУМНИЙ IoT БУДИЛЬНИК НА ARDUINO

Виконав: студент 2 (4)-го курсу, групи ТКР-22мс
спеціальності 172 – Телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)
_____ Гладкий М.О.
(прізвище та ініціали)
Керівник: к.т.н., доц., доцент каф. ІРТС
_____ Воловик А.Ю.
(прізвище та ініціали)
«12» 06 2024 р.

Вінниця ВНТУ - 2024 рік

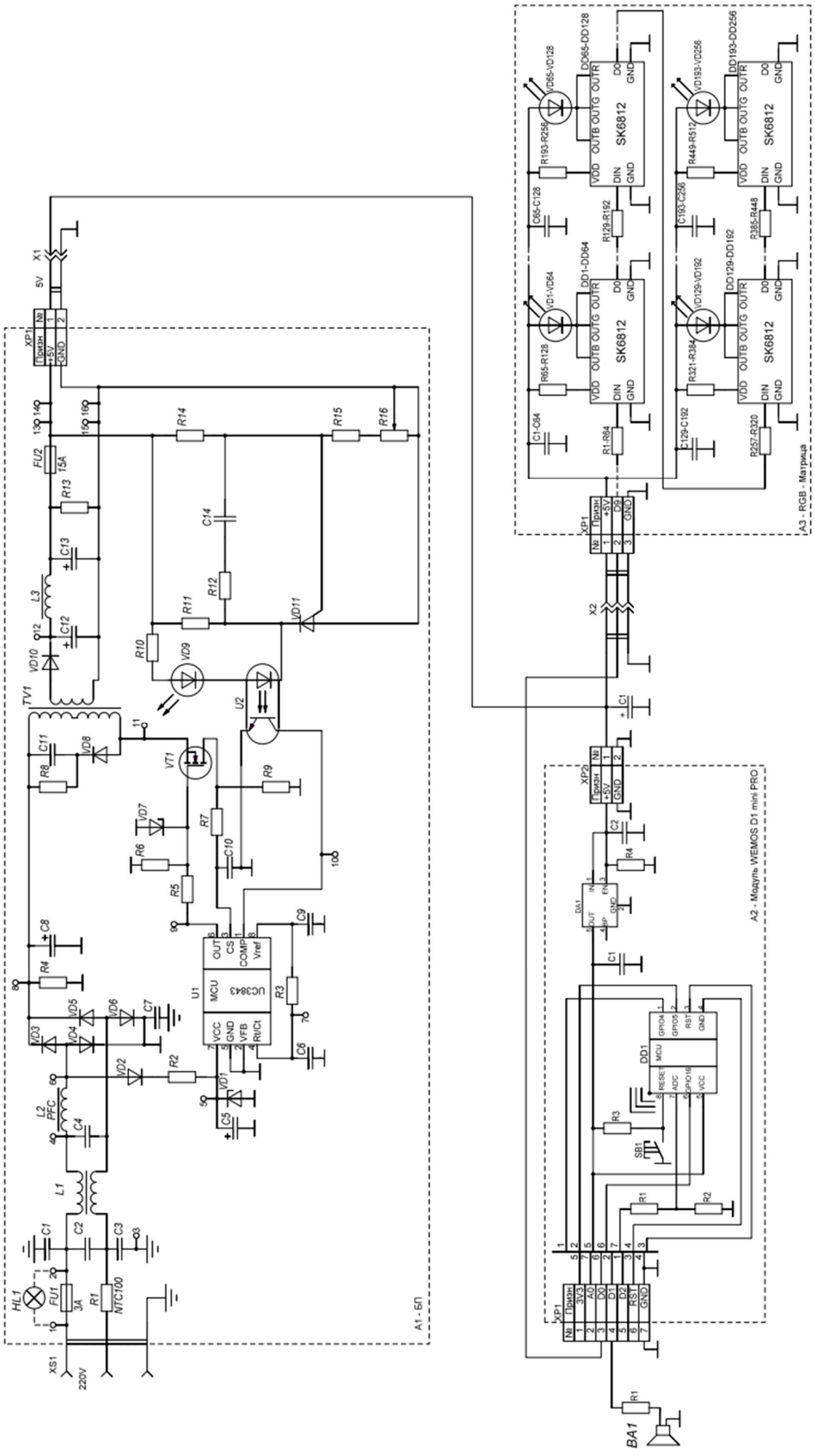
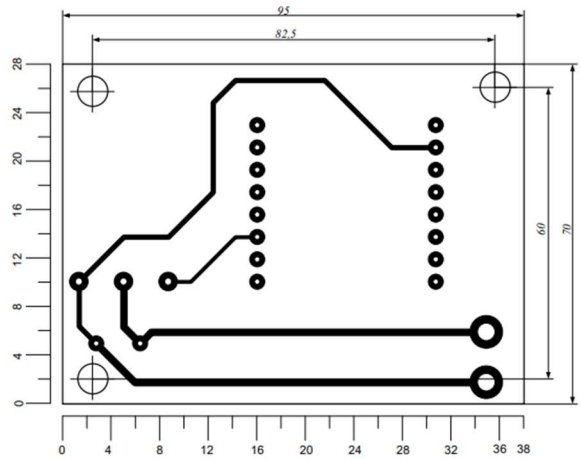


Рисунок 1 – Схема електрична принципова



1.* Розмір для довідок.

2. Плату виготовити негативним методом.

3. Крок координатної сітки 2,5мм. Лінії сітки умовно нанесені через одну.

4. Конфігурацію провідників витримати по координатній сітці.

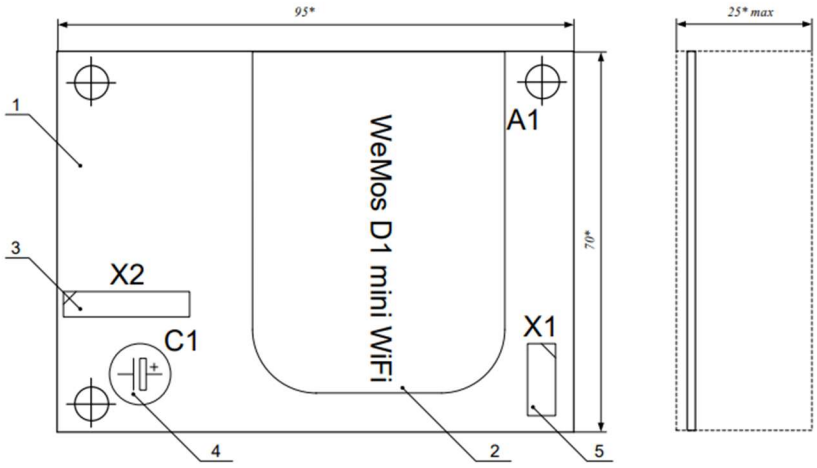
5. Провідники умовно позначені суцільними лініями виконати шириною 0,4±0,1 мм.

6. Відстань між провідниками не меньше 0,8мм, в вузьких місцях - 0,4мм.

7. Плата повинна відповідати ГОСТ23752-79.

Умовне позначення отвору	Діаметр отвору, мм	Наявність металізації в отворі	Діаметр контактної площадки, мм	Кількість отворів
	1,1	немає	2,2	3
	0,9	немає	1,8	18
	3,5	немає	-	3
	2,3	немає	3,8	2

Рисунок 2 – Друкована плата



1.* Розмір для довідок.
2. Паяти: припой ПОС61 ГОСТ 21931-79.
3. Встановку елементів проводити за ГОСТ 4ГО. 010.030-81.
4. ** Розмір встановлюється робочим інструментом.
5. Плату після зборки покрити емаллю ЕЛ-572, колір білий ТУ-10-1539-76

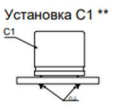


Рисунок 3 – Складальне креслення

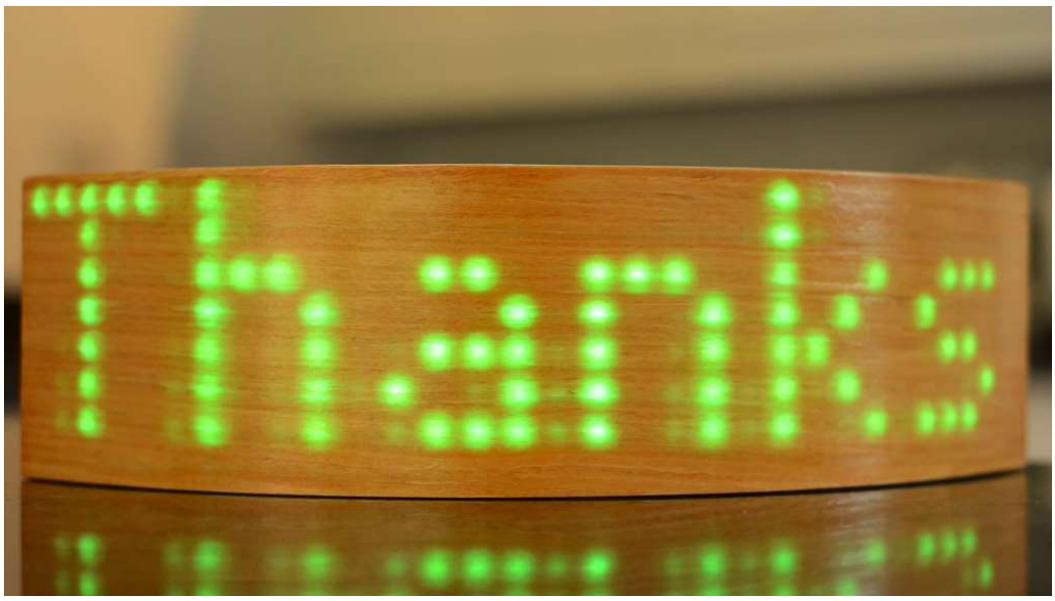


Рисунок 4 – Загальний вигляд розумного IoT будильника

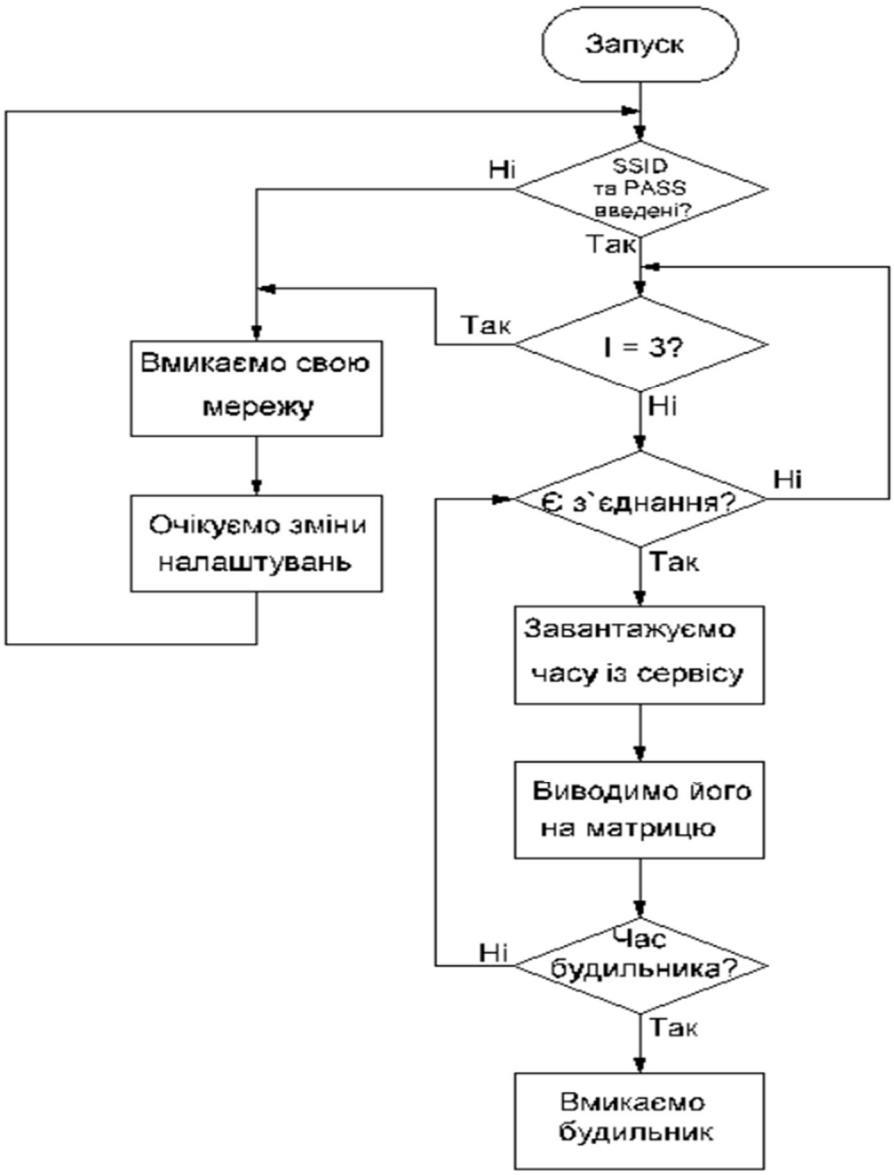


Рисунок 5 – Алгоритм роботи розумного IoT будильника

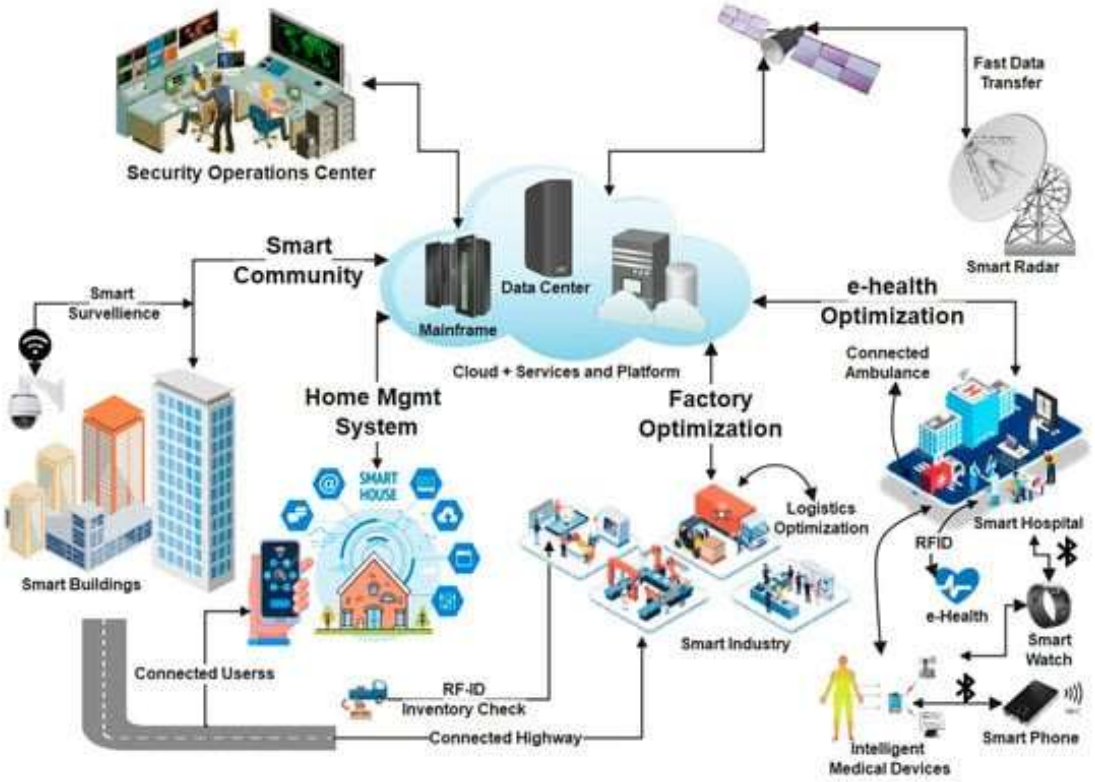


Рисунок 6 – Узагальнена архітектура розумного міста

Додаток Б

(обов`язковий)

ПРОТОКОЛ ПЕРЕВІРКИ РОБОТИ

РОЗУМНИЙ IoT БУДИЛЬНИК НА ARDUINO

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: **«Розумний IoT будильник на Arduino»**

Тип роботи: БДР
(БДР, МКР)

Підрозділ IPTC, IEC
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 90,7% Схожість 9,3%

Аналіз звіту подібності (відмітити потрібне):

☑ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Олександр ЗВЯГІН
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Мирослав ГЛАДКИЙ
(підпис) (прізвище, ініціали)

Керівник роботи _____ Андрій ВОЛОВИК
(підпис) (прізвище, ініціали)

Додаток В

(довідниковий)

Лістинг програми для розумного IoT будильника на Arduino

```
#pragma once
#include <sstream>

using Settings = std::map<String, String>;

Settings settings;

//Default settings

const char default_settings[] PROGMEM =
R""(OWMAPIKey=
effect=None
effectColor=#ff0022
effectColorMode=Varying
effectDecay=0
effectSpeed=50
masterBrightness=32
messageColor=#1ab500
messageRepeat=
password=69904219
pingTarget=8.8.8.8
primaryColor=#408080
primaryColorMode=Constant
primaryFont=Medium
primaryFormat=H:M
primaryX=6
primaryY=0
secondaryColor=#364ca0
secondaryColorMode=Constant
secondaryFont=Small
secondaryFormat=
secondaryX=23
secondaryY=1
ssid=Home_12
timezone=Etc/UTC
weatherLocation=
)"";
```

```
//Standard presets

const char *preset_names[] PROGMEM =
{
  "",
  "Vanilla",
  "Minimalist",
  "Utility",
  "Perpetual",
  "Pride",
  "Ping",
  "1990s"
};

const char null_preset[] PROGMEM = "";

const char vanilla_preset[] PROGMEM =
R""(effect=None
primaryColor=#505030
primaryColorMode=Constant
primaryFont=Medium
primaryFormat=H:M
primaryX=6
primaryY=0
secondaryFormat=
)"";

const char minimalist_preset[] PROGMEM =
R""(effect=None
primaryColor=#184640
primaryColorMode=Varing
primaryFont=Small
primaryFormat=H:M
primaryX=14
primaryY=2
secondaryFormat=
)"";

const char utility_preset[] PROGMEM =
 R""(effect=None
primaryColor=#20440f
primaryColorMode=Constant
primaryFont=Medium
primaryFormat=H:M
primaryX=0
```

```
primaryY=0
secondaryColor=#364ca0
secondaryColorMode=Constant
secondaryFont=Small
secondaryFormat=C*
secondaryX=23
secondaryY=2
)"";

const char perpetual_preset[] PROGMEM =
R""(effect=None
primaryColor=#204284
primaryColorMode=Plasma
primaryFont=Small
primaryFormat=y.m.d
primaryX=3
primaryY=1
secondaryFormat=
)"";

const char pride_preset[] PROGMEM =
R""(effect=None
primaryColor=#82166c
primaryColorMode=Rainbow
primaryFont=Extra large
primaryFormat=H:M
primaryX=1
primaryY=0
secondaryFormat=
)"";

const char ping_preset[] PROGMEM =
R""(effect=Ping graph
effectColor=#320000
effectColorMode=Constant
effectDecay=58
effectSpeed=500
pingTarget=8.8.8.8
primaryColor=#6b6b6b
primaryColorMode=Constant
primaryFont=Small
primaryFormat=p
primaryX=10
primaryY=1
secondaryFormat=
```

```
)"";

const char nineties_preset[] PROGMEM =
R""(effect=Rain
effectColor=#00e000
effectColorMode=Constant
effectDecay=0
effectSpeed=305
primaryColor=#600000
primaryColorMode=Constant
primaryFont=7-segment
primaryFormat=H:M
primaryX=3
primaryY=1
secondaryFormat=
)"";

const char *presets[] PROGMEM =
{
  null_preset,
  vanilla_preset,
  minimalist_preset,
  utility_preset,
  perpetual_preset,
  pride_preset,
  ping_preset,
  nineties_preset,
};

void parse_settings (const char *data)
{

//TODO: Arduino-ise this

  std::string string (data);
  std::istringstream iss (string);
  while (!iss.eof ())
  {
    std::string key, value;
    std::getline (iss, key, '=');
    std::getline (iss, value, '\n');
    if (!key.empty ())
    {
      settings[key.c_str ()] = value.c_str ();
    }
```

```
  }
}

void load_settings ()
{

//Load fall-back defaults

  parse_settings (String (FPSTR (default_settings)).c_str ());

  //Read from flash

  LittleFS.begin ();
  auto file = LittleFS.open (F("arclock_settings"), "r");
  auto bytes = file.size ();
  auto buffer = reinterpret_cast<char *> (malloc (bytes + 1));
  file.read (reinterpret_cast<uint8_t *> (buffer), bytes);
  buffer[bytes] = '\0';
  file.close ();

//Load them

  parse_settings (buffer);
  free (buffer);
}

void save_settings ()
{

//Create settings string

  String str;
  for (const auto &key_value : settings)
  {
    str += key_value.first;
    str += '=';
    str += key_value.second;
    str += '\n';
  }

//Save changes to flash

  auto file = LittleFS.open (F("arclock_settings"), "w");
  file.write (str.c_str (), str.length ());
  file.close ();
```

```
}

void load_preset (const String &name)
{
  for (ssize_t i = 0; i != std::end (preset_names) - std::begin (preset_names); ++i)
  {
    if (name == preset_names[i])
    {
      parse_settings (String (FPSTR (presets[i])).c_str ());
    }
  }
}
```