МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ім. Ю.М. ПОТЕБНІ

Кафедра електроніки, інформаційних систем
та програмного забезпечення
(повна назва кафедри)

Кваліфікаційна робота

другий (магістерський)
(рівень вищої освіти)

на тему Дослідження та розробка систем IoT

Виконав: студент II курсу, групи 8.1713
спеціальності 171 «Електроніка»
(код і назва спеціальності)
освітньої програми Електроніка
(код і назва освітньої програми)

Грідін О.С.
(ініціали та прізвище)

Керівник к.т.н. доц. Шмалій С.П.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Рецензент зast. дир. НВКФ „Екотех"
(посада, вчене звання, науковий ступінь, прізвище та ініціали)
Шершов С.А.

Запоріжжя
2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ім. Ю.М. ПОТЕБНІ

Кафедра електроніки, інформаційних систем та програмного забезпечення
Рівень вищої освіти другий (магістерський)
Спеціальність 171 «Електроніка»
(код і назва)
Освітня програма Електроніка
(код і назва)
Спеціалізація _____

ЗАТВЕРДЖУЮ
Завідувач кафедри Критська Т.В.
"01" 10 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТОВІ (СТУДЕНТЦІ)

Грідіну Олександру Сергійовичу
(прізвище, ім'я, по батькові)

1 Тема роботи (проєкту) Дослідження та розробка систем IoT

керівник **роботи** к.т.н. доц. Шмалій С.Л.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ЗНУ від "28" лютого 2024 року № 361-с

2 Строк подання студентом роботи 3 грудня 2024 року

3 Вихідні дані до роботи Напруга живлення 5В, струм 0,5А доступ до мережі інтернет, Вхідна напруга моніторингу 220В

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Загальні відомості про системи IoT, Етапи розробки IoT систем, Дослідження та розробка прилрою, Конструкторсько-технологічна частина Техніко- економічне обґрунтування

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Постановка завдання (AI), Апаратні платформи Моделювання, Схема електрична структурна Схема електрична принципова, Алгоритми роботи пристрою, Охорона праці

6 Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	К.т.н. доц. Шмалій С.Л.	9.09.24	22.09.24
2	К.т.н. доц. Шмалій С.Л.	25.09.24	28.09.24
3	К.т.н. доц. Шмалій С.Л.	29.09.24	04.10.24.
4	К.т.н. доц. Шмалій С.Л.	05.11.24	11.11.24
5	К.т.н. доц. Шмалій С.Л.	12.11.24	15.11.24

7 Дата видачі завдання 2.09.24

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи магістра	Строк виконання етапів роботи	Примітка
1	Робота над 1 розділом	22.09.24	виконано
2	Робота над 2 розділом	28.09.24	виконано
3	Робота над 3 розділом	04.10.24	виконано
4	Робота над 4 розділом	11.11.24	виконано
5	Робота над 5 розділом	15.11.24	виконано
6	Оформлення пояснювальної записки	25.11.24	вик.
7	Оформлення графічної частини	01.12.24	вик.

Студент _____ Гріднін О.С.
(підпис) (прізвище та ініціали)

Керівник роботи (проекту) _____ Шмалій С.Л.
(підпис) (прізвище та ініціали)

Нормоконтроль пройдено

Нормоконтролер _____ Гуртов К.О.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Дипломний проект містить: 94 стор., 32 рис., 10 табл., 21 джерел

IoT, МІКРОКОНТРОЛЕР, СИСТЕМА МОНІТОРИНГУ, ЗМІННА НАПРУГА, СТРУМ, БЕЗПЕКА, АЛГОРИТМ, ХМАРНІ ОБЧИСЛЕННЯ.

Об’єкт дослідження: інтеграція IoT із хмарними та периферійними обчисленнями.

Предмет дослідження: Методи та алгоритми обробки даних, зібраних IoT-сенсорами, способи підвищення надійності та енергоефективності IoT-пристроїв.

Мета роботи: дослідження використання мікроконтролерів в якості системи управління IoT.

У даній роботі проведено дослідження використання сучасних мікроконтролерів для моніторингу напруги. Показано переваги використання таких контролерів з метою підвищення якості енергопостачання.

Проведено математичне моделювання схеми моніторингу напруги.

ЗМІСТ

Вступ 6
1 Загальні відомості про системи IoT 8
1.1 Архітектури IoT. Загальна архітектура IoT 8
1.1.1. Шар сприйняття 14
1.1.2. Мережевий шар 14
1.1.3 Шар застосунків 14
1.2. Архітектура IoHT 15
1.3. Архітектура IoT із використанням fog computing 16
1.3.1. Хмарні обчислення (Cloud Computing) 18
1.3.2. Рівень туманніх обчислень 18
1.3.3. Датчиковий або фізичний шар 19
1.4. Архітектура IoT для смарт-домів 19
1.5. Архітектура смарт-міста на основі блокчейну 21
1.6. Застосування IoT 23
1.6.1. Розумний дім 24
1.6.2. Розумне сільське господарство 24
1.6.3. Розумні міста 25
1.6.4. Розумне охорона здоров'я 26
1.6.5. Розумні енергомережі 26
1.6.6. Розумна промисловість 28
2 Етапи розробки IoT систем 30
2.1 Основні етапи розробки IoT-систем 30
2.2 Аналіз апаратних платформ для IoT 31
2.2.1 Опис платформи Raspberry Pi 32
2.2.2 Опис платформи ESP32 34
2.3 Платформа BeagleBone AI-64 43
2.4 Проблеми безпеки у світі IoT 45
2.5 Накопичування та аналіз даних 49

2.5.1 Сервіс ThingSpeak 49
2.5.2 Сервіс open-monitoring.online 50
2.5.3 Сервіс beebotte 52
3 Дослідження та розробка пристрою 53
3.1. Аналіз програмної частини для завдань моніторингу напруги 53
3.2 Розробка схеми електричної принципової пристрою 66
4 Конструкторсько-технологічна частина 70
4.1 Конструкція пристрою моніторингу напруги 70
4.2 Програмні продукти для проектування друкованих плат 71
4.3 Заходи з охорони праці 72
4.3.1 Заходи з поліпшення умов праці 77
4.3.2 Виробнича санітарія 78
4.3.3 Пожежна та техногенна безпека 79
4.3.4 Електробезпека 81
4.3.5 Інженерні рішення з охорони праці 82
5 Техніко-економічне обгрунтування 85
5.1 Визначення стадій розробки 85
5.2 Розрахунок заробітної плати 87
5.3 Розрахунок кошторису витрат 88
Висновки 90
Список використаних джерел 92
Додаток А 94

ВСТУП

Інтернет речей (IoT, Internet of Things) найшвидше зростаюча технологічна галузь. У сучасному світі IoT виступає як ключовий драйвер інновацій, що змінює спосіб, у який люди взаємодіють із технологіями, об'єктами та середовищем. IoT об'єднує в єдину мережу мільярди пристроїв, які збирають, обробляють і передають дані через інтернет. Ця концепція грунтується на інтеграції сенсорів, комунікаційних модулів, мікропроцесорів та програмного забезпечення, що дозволяє автоматизувати процеси, підвищувати ефективність і створювати нові можливості для управління даними.

IoT вже сьогодні трансформує звичні процеси в побуті, бізнесі та промисловості, відкриваючи широкі можливості для розвитку технологій. Завдяки постійному вдосконаленню апаратних та програмних рішень Інтернет речей залишається однією з найперспективніших сфер інновацій. Його впровадження дозволяє не лише оптимізувати ресурси, а й підвищувати якість життя та створювати більш комфортний і безпечний світ.

Розвиток IoT все ще перебуває на ранніх етапах, і існує безліч взаємопов'язаних проблем, які необхідно вирішити. IoT — це об'єднуюча ідея вбудовування всього. Інтернет речей пропонує величезні можливості для покращення доступності, цілісності, доступності, масштабованості, конфіденційності та взаємодії в світі. Однак забезпечення безпеки Інтернету речей є складною задачею. IoT прагне з'єднати майже все в рамках єдиної інфраструктури. Це допомагає контролювати пристрої і дозволяє оновлювати їхній статус скрізь і в будь-який час. Для розвитку технологій через IoT було проведено кілька важливих наукових досліджень та запитів. Однак багато проблем і перешкод все ще залишаються для подолання, щоб досягти максимального потенціалу IoT.

Таким чином, аналізуючи отриману інформацію можна сформувати наступні завдання для диплоної роботи.

- Вивчити сучасний стан розвитку Інтернету речей та основні напрями його використання.

- Проаналізувати ключові технології та протоколи зв'язку (Wi-Fi, Bluetooth, Zigbee, LoRaWAN, MQTT тощо).

- Оцінити тенденції розвитку IoT, включаючи впровадження штучного інтелекту, 5G.

- Вибрати сферу дослідження (розумний дім, медицина, сільське господарство, логістика тощо).

- Провести аналіз існуючих рішень і визначити їх недоліки.

- Спроєктувати архітектуру IoT-системи, включаючи апаратну та програмну частини.

- Вибрати апаратні компоненти для прототипу (сенсори, мікроконтролери, мережеві модулі).

- Розглянути програмне забезпечення для управління пристроями та обробки даних.

- Виміряти продуктивність системи, включаючи швидкість передачі даних, енергоспоживання, стабільність роботи.

- Оцінити переваги і недоліки створеного рішення, порівнявши його з аналогами.

- Надати рекомендації щодо подальшого вдосконалення системи.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО СИСТЕМИ IoT

Інтернет речей (IoT) — це концепція, яка підключає фізичні об'єкти до Інтернету, дозволяючи їм збирати, обробляти та передавати дані без потреби у втручанні людини. Мета Інтернету речей полягає в створенні кращого середовища для людей, у якому предмети (фізичні об'єкти; терміни, як-от об'єкт, гаджет, сутність і річ, є взаємозамінними) навколо нас можуть розуміти наші вподобання та діяти відповідно без чітких інструкцій. Експоненціальне зростання Інтернету речей було спричинено значним прогресом у виробництві недорогих сенсорів, протоколів зв’язку, вбудованих систем, виконавчих механізмів та зменшенні розмірів апаратного забезпечення.

Очікується, що загальна кількість підключених IoT-пристроїв у світі зросте в п'ять разів за десятиліття, рахуючи з 2015 року та досягне одного трильйона пристроїв. IoT — це величезна колекція розумних вбудованих пристроїв, які підключені до Інтернету та надають унікальні послуги для задоволення потреб користувачів. IoT представляє перехід від простого підключення пристроїв кінцевого користувача до Інтернету до використання Інтернету для підключення розумних об'єктів (також відомих як IoT-пристрої), щоб дозволити їм взаємодіяти між собою та/або з людьми, включаючи різноманітні додатки та послуги [1].

Платформи IoT зазвичай розгортають велику кількість розумних пристроїв, таких як носимі сенсори, пристрої з радіочастотною ідентифікацією (RFID) і виконавчі механізми, для віддаленого керування різними фізичними, екологічними та фізіологічними параметрами. IoT, який базується на комп’ютерному Інтернеті, фактично створює Інтернет, спираючись на RFID та технологію радіопередачі даних для підключення речей. Отже, RFID є однією з найважливіших фундаментальних технологій IoT. У межах цієї мережі речі можуть спілкуватися одна з одною без необхідності втручання людини. Основою Інтернету речей є автоматична ідентифікація об'єктів, їх взаємозв'язок і обмін інформацією через комп’ютерний Інтернет, заснований

на RFID-технології, яка, по суті, дозволяє об’єктам «розмовляти». RFID-мітки використовуються на етапі IoT для зберігання інформації за допомогою законів і забезпечення сумісності, які автоматично записуються в центральну інформаційну систему через радіосистему передачі даних, що дозволяє ідентифікувати речі та обмінюватися інформацією через відкритий Інтернет.

Для підтримки різноманітних систем віддаленого моніторингу пристрої IoT часто працюють у довготривалому режимі та бездротово взаємодіють один з одним і з центральним вузлом злиття. Віддалені системи спостереження зазвичай живляться від батарей; обмежена потужність батареї впливає на ефективність системи, що призводить до нижчої інтеграції та відповідності споживачів. Щоб вирішити ці обмеження, отримані дані повинні спочатку стискатися перед передачею до центру злиття оптимізованими шляхами, щоб зменшити споживання енергії. Розвинені методи стиснення та передачі даних зазвичай споживають значну кількість енергії на борту; тому обраний метод стиснення має забезпечувати довготривалий надійний моніторинг, водночас знижуючи споживання енергії.

Інтелектуальні додатки вийшли за межі взаємодії лише з людьми і поширилися на об'єкти, які нас оточують, у міру розвитку інформаційних технологій. Мережі сенсорів, Інтернет, мобільний зв'язок, хмарні обчислення, інтелектуальна обробка інформації та інші розвинені мережеві та інформаційні технології є складовими Інтернету речей. Встановлюючи гетерогенний зв’язок між основними та термінальними мережами, Інтернет речей зосереджується на інформаційних послугах, об'єднуючи комп’ютерні системи зі спостереженням фізичного світу, його пізнанням, впливом і контролем. Реальний, цифровий і віртуальний світи, а також людське сприйняття пов’язані між собою.

У результаті, наразі не існує загальноприйнятого поняття Інтернету речей (IoT), а сучасні уявлення про нього залишаються нечіткими. Інтернет речей зосереджений на конвергенції різних стандартів і технологій, що

забезпечують функціональні можливості сенсорики, мереж, зберігання, обчислень та інших аспектів.

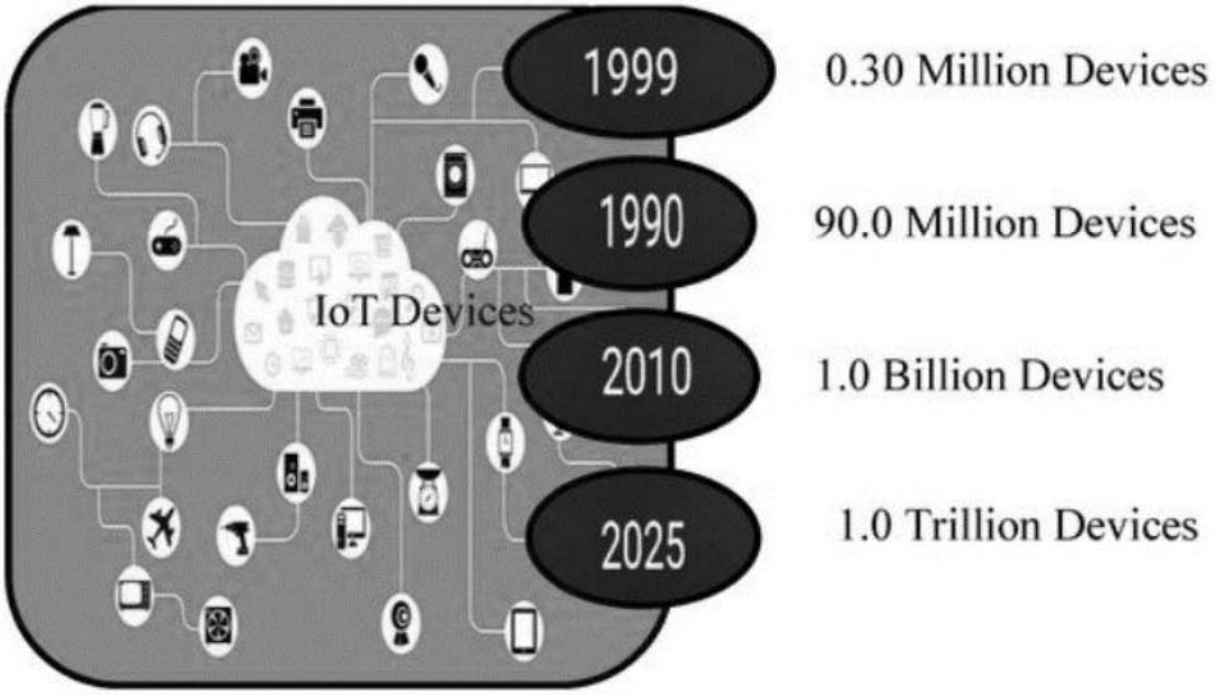


Рисунок 1.1 - Кількість пристроїв IoT до 2025 року

Однак через фрагментацію стандартів і різноманітність впроваджених технологій забезпечення повної взаємодії всіх компонентів є серйозною проблемою. Таким чином, однією з головних перешкод для розвитку IoT є динамічна інтеграція. Багато організацій зі стандартизації, партнерств, науковців і промислових секторів працюють над розвитком, інноваціями та стандартизацією IoT; однак все ще залишається потреба в цілісній системі з інтегрованими стандартами в рамках єдиного бачення IoT [2].

IoT має багато чого запропонувати в різних сферах життя та технологій. Він володіє значним потенціалом як для вдосконалення технологій, так і для полегшення життя людей. Таким чином, IoT є сучасною моделлю, яка поєднує наступне покоління технологічних досягнень із наявними сервісами. Технології IoT практично не мають меж, що дозволяє кіберсвіту легко зливатися з реальним світом. Проте, незважаючи на значні зусилля агентств зі стандартизації, асоціацій, секторів, науковців та інших учасників, для

досягнення повного потенціалу IoT необхідно вирішити низку проблем. Ці проблеми мають розглядатися з різних точок зору, зокрема підтримки технологій, впровадження, ринкових моделей, а також соціальних та екологічних впливів.

Багато з основних проблем, з якими стикається IoT, пов'язані з мережевим трафіком і його різноманітними моделями. Щодня до Інтернету підключається все більше пристроїв, які стають головними виробниками та споживачами трафіку. Це породжує нові вимоги до трафіку та необхідність у нових моделях трафіку, протоколах, мережевих потужностях, засобах захисту тощо. Потрібна спрощена система, а впровадження нової архітектури Інтернет-протоколів (IP) забезпечує плавну роботу мереж і ефективне управління в гетерогенному мережевому середовищі (HetNet).

Інші технологічні питання IoT включають розпізнавання систем, адресацію, інтероперабельність, зручність використання, управління, енергоспоживання, стабільність, конфіденційність, масштабування та інше. Крім того, майбутні впровадження IoT повинні сприяти створенню сталого розумного планети з акцентом на «зелені» IoT-технології, що є ще однією важливою проблемою. З останніми досягненнями у сфері інтернет-технологій IoT поступово впливає на наше повсякденне життя і починає надавати нові цікаві та корисні послуги. Відповідно до ключових бачень IoT і підтримуючих технологій, ця стаття містить звіти про сучасний стан, нові тенденції та відкриті питання.

Блокчейн, або децентралізовані розподілені реєстри, є революційною технологією, яка може допомогти вирішити питання безпеки IoT. Підхід на основі блокчейну в IoT-мережах здатен усунути багато проблем існуючої парадигми, водночас підвищуючи рівень безпеки. Використання блокчейну для забезпечення безпеки IoT дозволяє пристроям обмінюватися інформацією безпосередньо між собою, а не через централізовану мережу, що зменшує вразливість IoT до кібератак. Згідно зі звітом Gartner, у США найбільші темпи впровадження блокчейну серед компаній, які використовують IoT,

спостерігаються в галузях охорони здоров'я, транспорту та енергетики. Таким чином, ця стаття надає читачам корисні рекомендації для розуміння парадигми IoT, пов'язаних відкритих питань, а також потенційних можливостей для досліджень та розробок.

1.1 Архітектури IoT. Загальна архітектура IoT.

У світі немає єдиної загальновизнаної архітектури IoT. Різні дослідники пропонують різні архітектури, такі як архітектура для охорони здоров'я, архітектура для розумних будинків, архітектура на основі туманних обчислень (FC-based architecture) тощо.

Сфера IoT включає широкий спектр технологій, заснованих на різних архітектурах. Тому неможливо використовувати одну референтну архітектуру як основу для всіх можливих реалізацій. Хоча існує певний базовий підхід, інші схожі моделі співіснуватимуть в інтернеті. У цьому контексті архітектура визначається як структура для опису фізичних компонентів, функціонального розташування, мережевих аспектів, принципів роботи, процедур та форматів даних, які використовуються в її функціонуванні.

Дизайн IoT із запатентованими протоколами є надзвичайно масштабованим і здатний підтримувати кілька різних мережевих реалізацій, як показано на рис. 1. Для інтеграції з інтернет-середовищем даних необхідно включити певне проміжне програмне забезпечення (middleware), що забезпечує масштабованість, стабільність і семантику [2].

IoT-структура включає різноманітні фізичні об'єкти, пристрої, мережі додатків, інженерів, активатори, мережеві канали, клієнтів, ринкові ціни та протоколи IoT. Архітектура рівнів IoT представлена на рис. 2 і головним чином працює на трьох рівнях. Функції кожного рівня описані нижче.

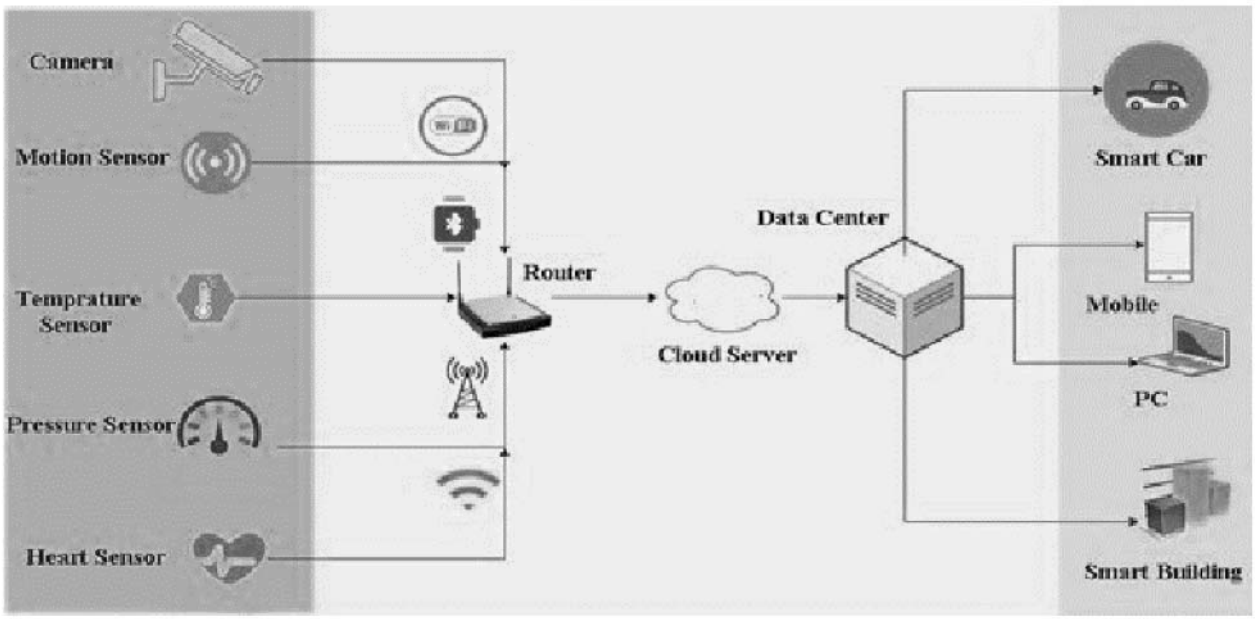


Рисунок 1.1 - Архітектура IoT

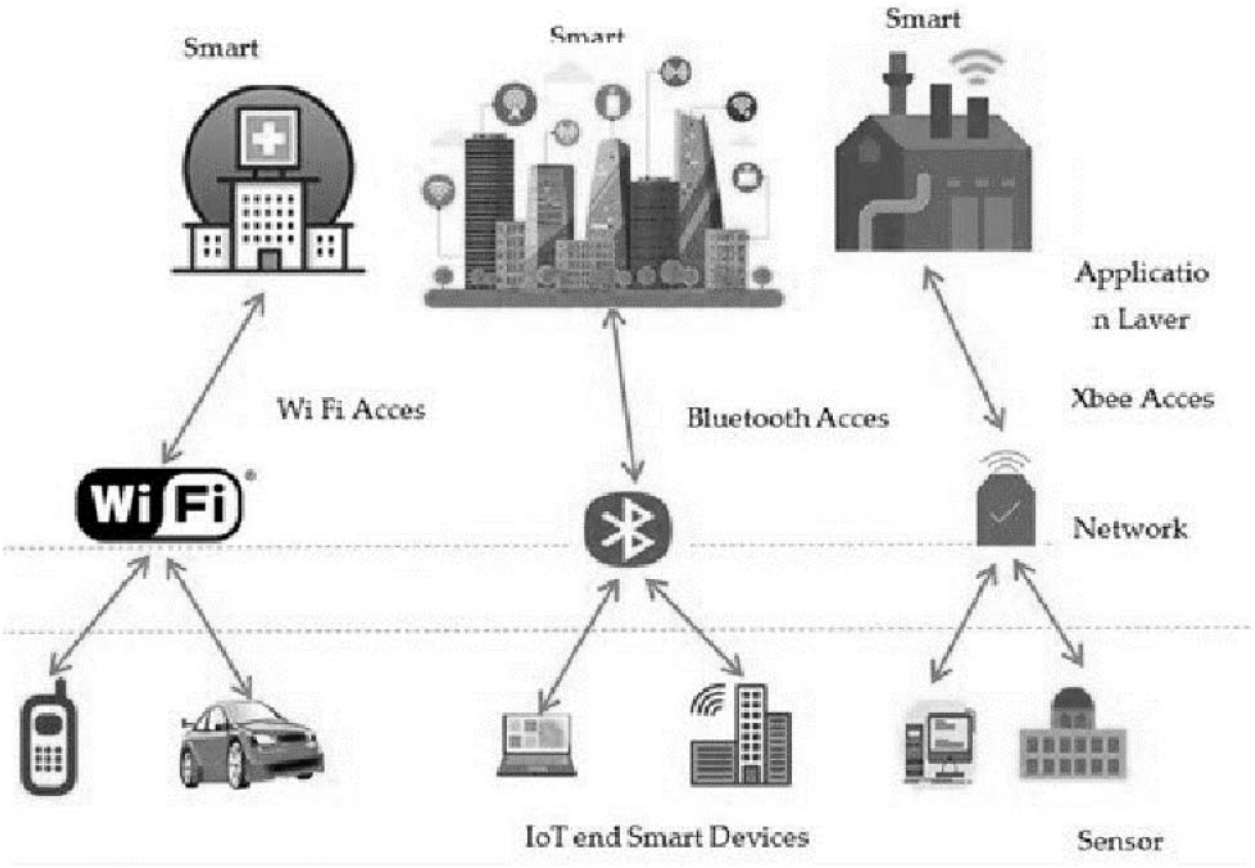


Рисунок 1.2 - Архітектура рівня IoT

1.1.1 Шар сприйняття

Шар сприйняття, також відомий як фізичний шар структури, безпосередньо працює із сенсорами IoT. Особливість сенсорів полягає в їхній здатності інтерпретувати інформацію, отриману з навколишнього середовища. Іншими словами, для інтеграції сенсорів у тришарову систему IoT необхідно отримати дані у форматі, який може бути оброблений. Унікальна властивість сенсорів полягає в їхній здатності перетворювати отримані дані з фізичного світу в інформацію для аналізу. Цей процес продовжується з використанням виконавчих пристроїв (актуаторів), які взаємодіють із фізичною реальністю, наприклад, вимикають світло або регулюють температуру в кімнаті. Таким чином, етапи сприйняття та виконання охоплюють і змінюють усе необхідне для подальшого вивчення реального середовища.

1.1.2. Мережевий шар

Мережевий шар забезпечує доступ до даних через мережу та виконує роль хмарної інфраструктури. Він зв’язує розумні об’єкти, мережеві пристрої та сервери. Його основна функція — передача даних із сенсорів для подальшого аналізу. На цьому етапі оптимізовані дані передаються до IT-середовища через шари архітектури IoT. Особливо важливу роль тут відіграють крайові IT-системи, які проводять попередній аналіз і обробку даних, зокрема із застосуванням технологій машинного навчання та візуалізації.

Додатковий аналіз може виконуватися в центрі обробки даних. Крім того, цей етап тісно пов’язаний із попередніми фазами архітектури IoT, забезпечуючи розміщення крайових IT-систем поруч із сенсорами та актуаторами. Разом із цим передбачається можливість їх віддаленого розташування, наприклад, далеко від робочого місця.

1.1.3. Шар застосунків

Шар застосунків надає унікальні ресурси для користувачів і визначає

різні застосування IoT, такі як розумні будинки, інтелектуальні громади та системи охорони здоров'я. У цьому останньому етапі архітектури IoT основні процеси відбуваються в дата-центрі або хмарі. Це дозволяє проводити детальну обробку даних і подальший аналіз зворотного зв’язку.

На цьому етапі потрібна експертиза фахівців із інформаційних технологій (IT) та операційних технологій (OT). Це процес, який поєднує високий рівень наукових знань про сучасне середовище та людей. Дані з інших джерел також можуть використовуватися для більш детального аналізу. Проте обсяг інформації, що генерується, стає складно зберігати та обробляти на локальних етапах. Цю проблему вирішує адаптивність хмарних обчислень (CC). Розподілені обчислення надають ресурси за невеликі або зовсім відсутні витрати з боку користувачів [2].

1.2. Архітектура IoHT

Головними викликами для створення ефективної архітектури Інтернету медичних речей (IoHT) у гетерогенному середовищі є масштабованість, модульність, інтероперабельність і гнучкість. Архітектура IoHT має бути розроблена так, щоб відповідати вимогам міждоменної взаємодії та інтеграції багатосистемних рішень, забезпечуючи легке й гнучке управління функціональними зв’язками, обробку та зберігання великих обсягів даних, а також зручні для користувача застосунки.

Програмне забезпечення має підтримувати масштабування функціоналу та включати елементи штучного інтелекту й автоматизації для IoT-систем. Величезний обсяг даних, який генерується при взаємодії між сенсорами та пристроями IoT, створює нові виклики. Тому для роботи з великими потоками даних у межах IoHT потрібна потужна архітектура. Шари сприйняття, мережі та застосунків функціонують на трьох різних рівнях.

На рис. 1.3, заснованому на IoHT, показано потік інформації через ці шари. Через залучення людини кожен із шарів має певні проблеми безпеки, зокрема забезпечення конфіденційності, цілісності та достовірності даних.

Зв'язок із людьми підвищує чутливість системи, тому дані, отримані від людей і пацієнтів, потребують авторизації в системі для отримання доступу. Через проблеми конфіденційності користувачі не завжди можуть повністю використовувати певні пристрої.

Захист медичних даних є критично важливим, тому потрібно забезпечити їхню справжність, достовірність і конфіденційність. Для поточної системи моніторингу стану здоров'я необхідно розробити систему безпеки. У даний час медичні техніки й парамедики використовують різноманітні захисні системи та обладнання.

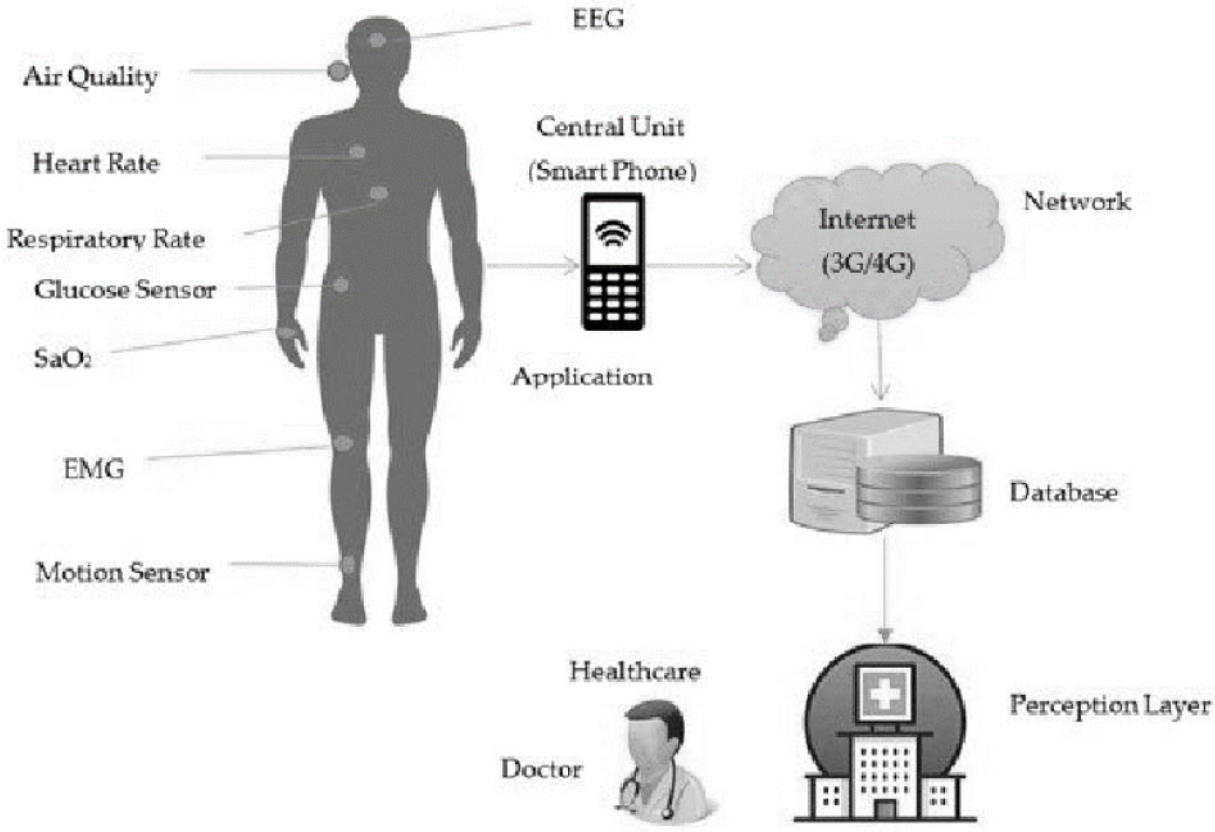


Рисунок 1.3 - Моделі охорони здоров’я IoHT

1.3. Архітектура IoT із використанням fog computing

Дані FC (fog computing, обчислення на периферії) отримуються від сенсорів, підключених до фізичних пристроїв на платформі IoT. Модель FC використовує локальні обчислювальні служби, розташовані на краю мережі, замість хмарних ресурсів. Основними перевагами цієї парадигми є низька

затримка, прийняття рішень у реальному часі та оптимальне використання пропускної здатності.

Архітектура FC дозволяє динамічно переміщати вузли туману (fog nodes), хмари та IoT через обчислювальні, мережеві та сховищні сервіси. Інтерфейси туману забезпечують гнучкий і складний рух пристроїв, зберігання та контрольних функцій між різними організаціями для взаємодії із сервером, іншими вузлами туману, персоналом або користувачами. Це сприяє точному оцінюванню параметрів QoS (якості обслуговування) і успішному їхньому контролю.

FC діє як шлюз між хмарою та кінцевим користувачем, забезпечуючи доступ до даних, сховищ і мережевих ресурсів. Вузли туману — це окремі одиниці, які можуть бути розміщені в будь-якому місці з мережею. На рис. 1.4, заснованому на оптимізації параметрів QoS і запропонованій моделі, показано архітектуру платформи для технологій розумного міста. Функції різних шарів описані нижче.

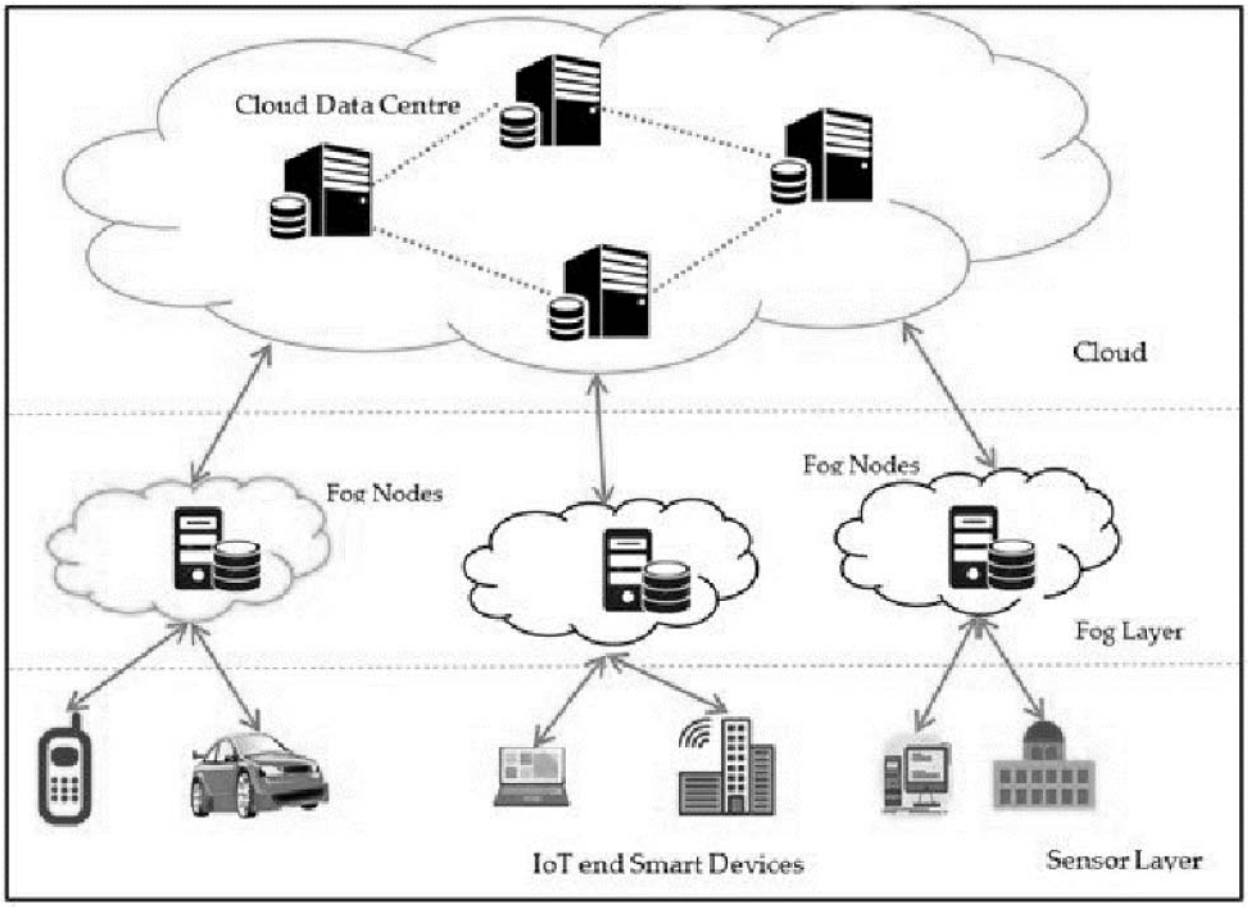


Рисунок 1.4 - Системна архітектура IoT з туманними обчисленнями

1.3.1. Хмарні обчислення (Cloud Computing)

Шар хмарних обчислень відповідає за обробку та виконання інформації, отриманої з інших шарів у гетерогенній IoT-системі. CC, працюючи з різноманітними гетерогенними IoT, здатна негайно обробляти великий обсяг даних певним чином. Це стає можливим завдяки здатності хмарних сервісів відстежувати ієрархічні обчислення.

Окрім можливостей зберігання, провайдери хмарних рішень також можуть приймати рішення на основі отриманих даних. Крім того, використовуючи архітектури, орієнтовані на події надзвичайних ситуацій, хмарні провайдери здатні вживати рішучих дій у певних критичних умовах гетерогенних IoT-середовищ.

1.3.2. Рівень туманніх обчислень

Як було сказано вище, туманні обчислення (Fog Computing) — це технологія, за якої обробка, аналіз і збереження даних відбуваються ближче до джерела їх генерації, у локальній мережі, між кінцевим пристроєм (наприклад, IoT-сенсором) і централізованим дата-центром (ЦОД). Це дозволяє зменшити затримки, знизити навантаження на хмарні ресурси та забезпечити оперативний доступ до даних.

Приклади використання:

Керування розумними містами (трафік, освітлення).

Системи моніторингу здоров'я пацієнтів у реальному часі.

Управління промисловими IoT-пристроями.

Ця технологія важлива для застосунків, де критичною є низька затримка та висока надійність зв’язку.

Концептуальний менеджер туману відповідає за цей шар, який аналізує та категоризує запити залежно від їх складності в момент часу. Обробник туману є критичним компонентом для оптимізації якості обслуговування (QoS) та використання інструментів у шарах туману.

1.3.3. Датчиковий або фізичний шар

Конкретні датчики в фізичному шарі IoT збирають дані з різних місць, які потім передаються в хмарну інфраструктуру для прийняття рішень. Велику кількість датчиків розміщують у певній локації, і для передачі даних розробляється топологія. У стандартній мережі є вузли-мішки, вузли-датчики та контрольні вузли. Вузли туману діють як міст між кінцевим пристроєм і хмарною інфраструктурою. Вузли туману вважаються тимчасовими, а отже, їм не можна довіряти. Кінцевий пристрій (наприклад, користувач або розумний пристрій IoT) повинен бути аутентифікований вузлом туману, перш ніж йому буде надано будь-яку послугу. Ця аутентифікація може включати сервер хмари, що вводить затримку та додаткове навантаження на сервер хмари. Зазвичай аутентифікація та встановлення сесійного ключа між кінцевим пристроєм і вузлами туману ґрунтуються на криптографії з публічними ключами. Однак це досить витратно з точки зору обчислювальних ресурсів. Вузли туману вважаються тимчасовими, можливо, через те, що вони виходять за межі діапазону або виходять з ладу з різних причин. У такому випадку кінцевий користувач повинен буде пройти повторну аутентифікацію з вторинним вузлом туману, який перейме функції попереднього вузла. Основна мета цього дослідження — забезпечити перехідну аутентифікацію без необхідності використання криптографії з публічними ключами. Це можна досягти, якщо вузли туману заздалегідь узгодять певні безпекові токени, які потім надаються кінцевому пристрою після першої аутентифікації. Ці безпекові токени можуть використовуватись для швидкої аутентифікації між кінцевим пристроєм та вторинним вузлом туману. Крім того, незахищена комунікація між кінцевими пристроями та вузлами туману може піддатися різноманітним атакам безпеки, таким як відтворення, підробка особистості, атака "людина посередині" та атаки відмови в обслуговуванні.

1.4. Архітектура IoT для смарт-домів

Датчик створює дані, але сам по собі він мало що додає до домашнього

середовища. Термостат часто не називають "розумним", оскільки власник дому має регулювати температуру, враховуючи зовнішню температуру, вологість та інші фактори. Можна підтримувати стабільну температуру, але це автоматизація, а не "розумність". Лише коли всі екологічні дані колективно аналізуються на основі зібраних патернів і приймаються рішення без втручання споживача, це можна назвати "розумною" екосистемою. Спосіб взаємодії датчиків, як і де обробляється інформація про використання датчиків і обладнання, як ці дані інтерпретуються та виявляються патерни, а також як споживач може взаємодіяти з системами і навпаки — це все визначається інфраструктурою смарт-дому.

Симбіоз численних компонентів, таких як датчики, з'єднання та програми, що формують складну, гетерогенну інфраструктуру для ефективного управління пристроями в домі та надання розширених послуг споживачам, можна описати як смарт-дом. На рис. 1.5 зображена загальна архітектура смарт-дому на основі хмари. Внутрішня мережа складається з термінальних пристроїв, камер, процесорів та актуаторів. Ці пристрої з'єднуються з міжмережевим екраном на краю мережі, що робить підключення внутрішніх мереж до Інтернету ще простішим. Різниця в комунікаціях між кінцевими користувачами, датчиками, програмним забезпеченням і хмарою моститься через шлюзовий комп'ютер.

Між кінцевими користувачами, сенсорами, програмним забезпеченням і хмарою місток створює шлюзовий комп’ютер [3].

Архітектура шлюзу смарт-дому, налаштована з урахуванням прийнятих комунікаційних протоколів, здатна перетворювати гетерогенні дані з датчиків у стандартний формат. Зазвичай шлюз є пристроєм, який підтримує кілька комунікаційних протоколів для взаємодії з кінцевими пристроями, забезпечуючи їх сумісність. Шлюз достатньо ефективний для виконання обчислень на межі мережі перед завантаженням даних у хмару. Крім того, шлюз додає додатковий рівень безпеки до мережі смарт-дому, оскільки він встановлює з'єднання між кінцевими пристроями та зовнішнім світом, тобто

вся комунікація фільтрується перед тим, як інструкції будуть надіслані до кінцевих пристроїв.

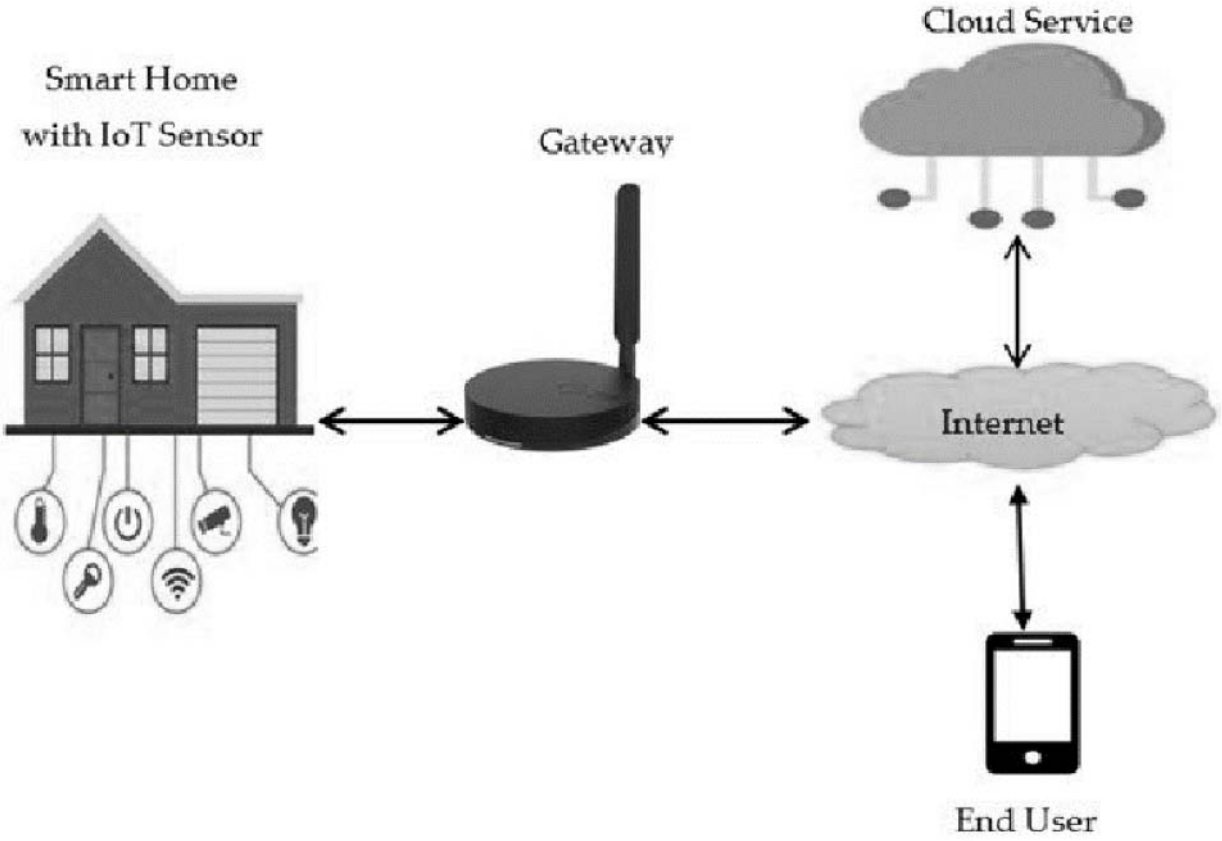


Рисунок 1.5 - Архітектура розумного будинку на основі IoT

Це ефективно включає методи покращення зручності використання, стабільності та безпеки, одночасно використовуючи більшу обчислювальну потужність і масштабовану архітектуру. Хмара також може підключати різноманітні сервіси від сторонніх постачальників, такі як візуалізація даних, управління смарт-продуктами для дому або керування доступом та ролями для споживачів.

1.5. Архітектура смарт-міста на основі блокчейну

Блокчейни — це децентралізовані розподілені реєстри, які є технологією, що змінює гру, і можуть допомогти вирішити проблеми безпеки IoT. Підхід на основі блокчейну до IoT-мереж може вирішити багато проблем існуючої парадигми, одночасно підвищуючи безпеку. Використання блокчейнів у безпеці IoT дозволяє безпосередньо обмінюватися інформацією

між підключеними пристроями, а не через централізовану мережу, що зменшує вразливість IoT до кібератак. За даними звіту Gartner, охорона здоров'я, транспорт і енергетика мають найвищі показники використання блокчейну серед компаній, що використовують IoT в USA.

Коли мова йде про шифрування, технологія, що використовується в системах цифрових реєстрів, є досить передовою. Оскільки блокчейн — це зашифрована база даних, яка є розподіленою, децентралізованою та непроникною, вона привернула увагу молоді сьогоднішнього дня. З моменту свого створення вона була використана для зміни способу ведення бізнесу майже в усіх сферах, охоплюючи уряд, фінанси, охорону здоров'я та розумні міста. Рис. 1.6 зображує архітектуру смарт-міста на основі блокчейну, яка включає різні пристрої IoT та інфраструктурні додатки.

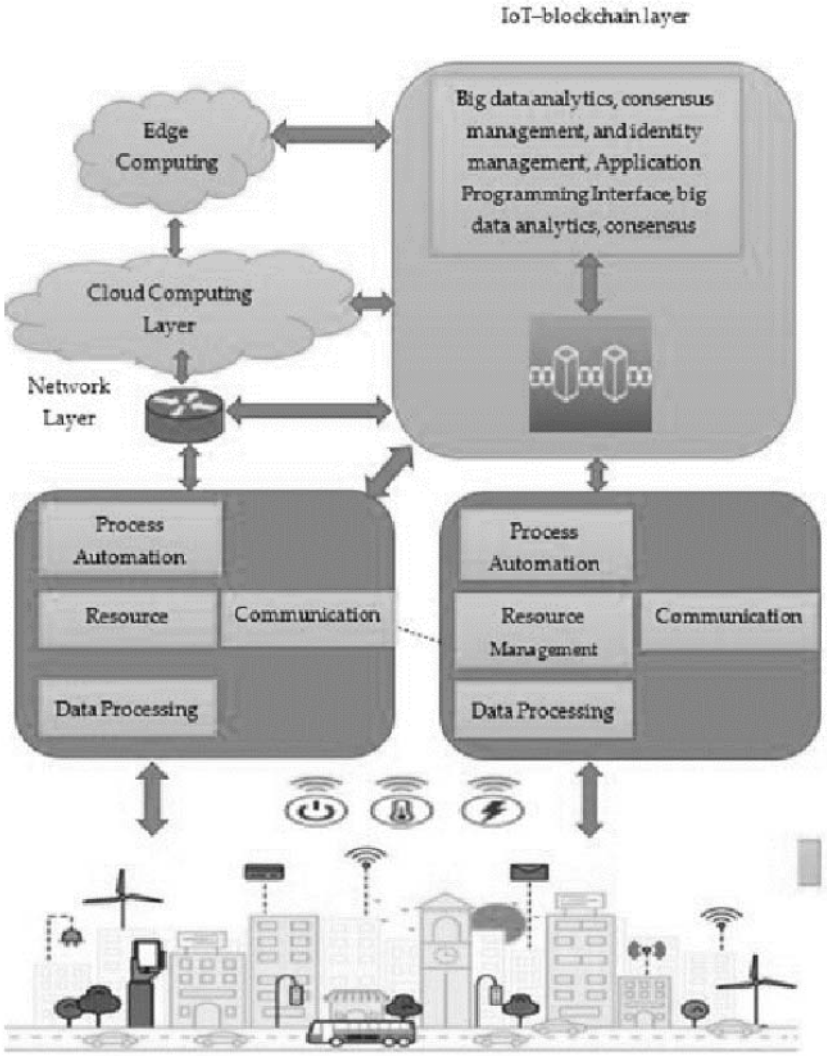


Рисунок 1.6 - Архітектура розумного міста на основі блокчейну

Інтеграція пристроїв IoT включає хмарні системи, обчислення на краю мережі, шлюзи та різні типи IoT-пристроїв, починаючи від базових сенсорів, які можуть спілкуватися лише з сусідніми шлюзами, і до пристроїв з обчислювальними та обробними можливостями. Вражає, як блокчейн і обчислення на краю мережі пов'язані між собою. Блокчейн-вузли можуть використовувати обчислення на краю мережі або розподілені архітектури обчислень для зберігання та валідації транзакцій. З іншого боку, блокчейни можуть створювати повністю відкритий і дистрибуційний хмарний ринок.

1.6. Застосування IoT

Технології IoT мають потенціал значно вплинути на життя людей, відкриваючи нові можливості. Вони можуть стати наступним етапом розвитку, об'єднуючи сучасні мобільні мережі, передові пристрої та інноваційні обчислювальні технології в єдину екосистему. IoT здатний забезпечити зв'язок і обмін даними між трильйонами повсякденних об'єктів. Приклади сфер застосування IoT наведені на рис. 1.7.

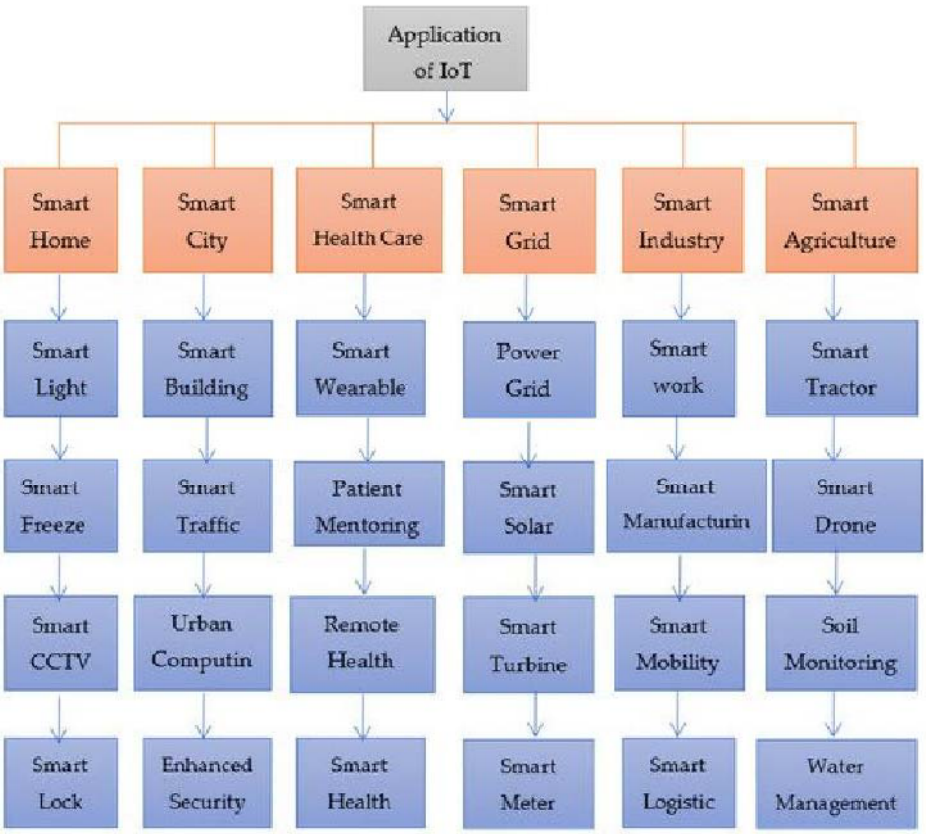


Рисунок 1.7 - Сфери застосування IoT

1.6.1. Розумний дім

Системи розумного дому спрямовані на створення комфортного середовища ще до приходу мешканців. Наприклад, можна заздалегідь активувати перевірку умов у приміщенні, щоб забезпечити комфорт після повернення додому. Їжу, яка готується в духовці чи мультиварці, можна приготувати віддалено, щоб вона була готова до приходу.

Засоби безпеки також стають більш доступними, дозволяючи користувачам дистанційно керувати побутовою технікою, освітленням та активувати смарт-замок для надання доступу гостям навіть без фізичного ключа. Основні функції розумного дому наведені на рис. 1.8 [2].

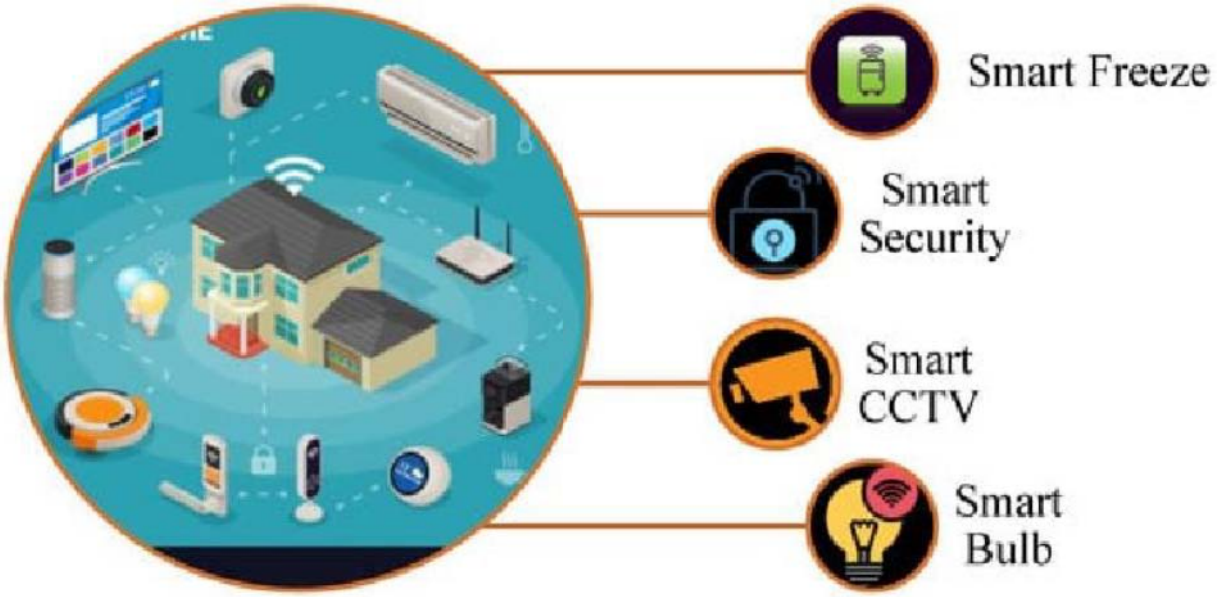


Рисунок 1.8 - Функції розумного дому

1.6.2. Розумне сільське господарство

Застосування IoT у сільському господарстві спрямоване на вдосконалення традиційних методів для задоволення зростаючих потреб та зменшення втрат урожаю. Інтеграція робототехніки, дронів, віддалених датчиків і комп'ютерного зору разом із сучасними інструментами машинного навчання та аналітики дозволяє здійснювати моніторинг полів, огляд ферм і контроль стану посівів. Це надає фермерам цінну інформацію для оптимізації управлінських рішень, економії часу та ресурсів.

У закритих приміщеннях IoT забезпечує ефективний контроль мікроклімату, що сприяє підвищенню врожайності. На відкритих полях датчики IoT дозволяють вимірювати вологість ґрунту, температуру і рівень поживних речовин, забезпечуючи розумне управління системами зрошення та внесення добрив. Наприклад, подача води лише через системи поливу мінімізує втрати ресурсів і підвищує ефективність. Основні функції розумного сільського господарства наведені на рис. 1.9.

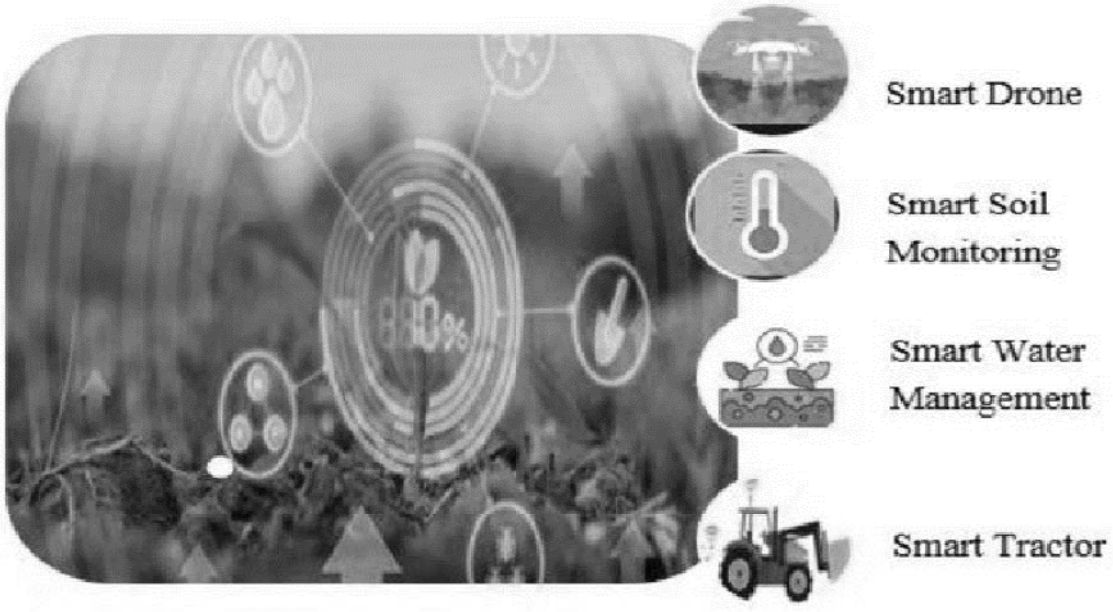


Рисунок 1.9 - Функції розумного сільського господарства

1.6.3. Розумні міста

IoT відкриває можливості для розвитку технологій розумного міста в різних сферах, сприяючи створенню безпечнішого середовища, покращенню громадської безпеки та оптимізації вуличного освітлення. Розумні системи паркування можуть визначати зайнятість місць і вільні зони, використовуючи GPS-дані зі смартфонів водіїв або сенсори на паркувальних майданчиках, що дозволяє створювати ефективні громадські системи.

Розумні міста, як випливає з їхньої концепції, є масштабним досягненням, яке охоплює широкий спектр можливостей: від управління постачанням і контролем водних ресурсів до організації транспортних потоків,

зменшення кількості відходів та захисту навколишнього середовища. Основні функції розумного міста наведено на рис. 1.10.

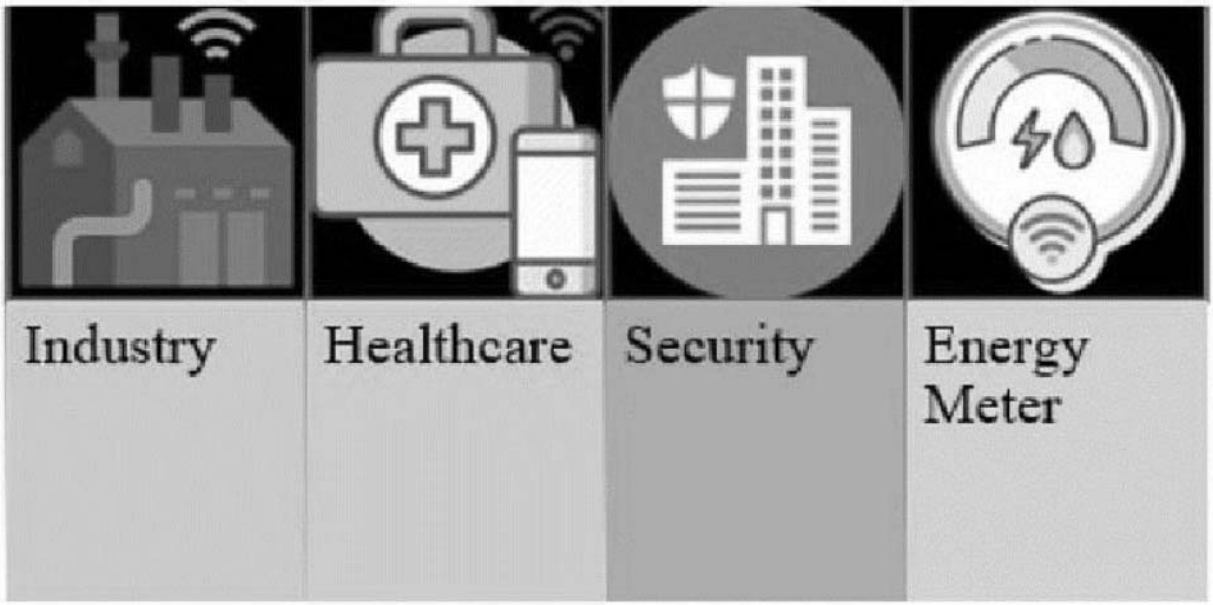


Рисунок 1.10 - Функції розумного міста

1.6.4. Розумне охорона здоров'я

На початковому етапі носимі IoT-технології дозволяють лікарням віддалено моніторити стан пацієнтів вдома, зменшуючи кількість медичних візитів та забезпечуючи доступ до життєво важливої інформації в реальному часі. Розумні ліжка в лікарнях допомагають персоналу контролювати доступність місць, сприяючи більш ефективному використанню ресурсів.

Розміщення IoT-сенсорів на критично важливому медичному обладнанні знижує ризик поломок і підвищує довговічність, що може бути вирішальним у критичних ситуаціях. Реактивні медичні мережі, інтегровані з IoT-технологіями, стають адаптивними системами, орієнтованими на добробут пацієнтів.

Інформація з реального світу, яка є обмеженою в традиційній медичній науці, доповнюється IoT шляхом збору, аналізу та використання даних у реальному часі. Це дозволяє отримувати цінні інсайти через спостереження, оцінювання та проведення медичних тестів у керованих середовищах. IoT також сприяє підвищенню міцності, ефективності та зручності роботи

медичного обладнання, виступаючи не лише як апаратне забезпечення, але і як ключовий елемент побудови інтелектуальних систем. Деякі функції інтелектуальної системи охорони здоров'я наведено на рис. 1.11.

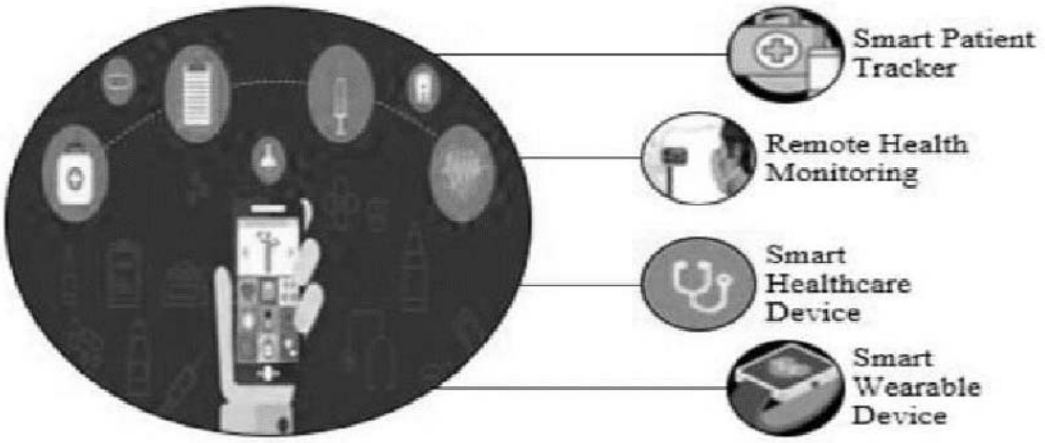


Рисунок 1.11 - Розумне охорона здоров'я

1.6.5. Розумні енергомережі

Однією з перспективних сфер застосування технологій IoT є розумні енергомережі. Їх основна мета — забезпечити безперервний збір даних від споживачів та постачальників енергії для підвищення якості та надійності її доставки. Для цього використовуються IoT-пристрої, які здійснюють моніторинг таких параметрів, як вологість, температура та освітленість. Основні функції розумних енергомереж відображені на рисунку 1.12.

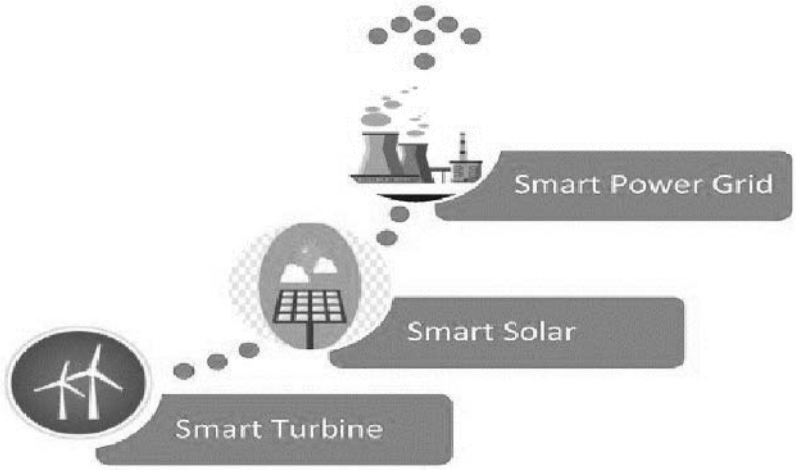


Рисунок 1.12 - Особливості розумної енергомережі

Інформація, отримана з IoT-сенсорів, слугує основою для розробки алгоритмів, які дозволяють автоматично відслідковувати споживання енергії та адаптувати процеси без втручання людини.

1.6.6. Розумна промисловість

Ще один спосіб ознайомлення з Інтернетом речей — це аналіз підключених пристроїв та обладнання у таких галузях, як енергетика, гірничодобувна промисловість, газовий сектор і медичні послуги. У цих сферах непередбачувані збої та несправності можуть створювати серйозні ризики для життя. IoT-пристрої, такі як кардіотрекери чи розумні побутові прилади, можуть допомагати в таких ситуаціях. Хоча ці системи зазвичай прості у використанні, вони часто стикаються з викликами під час надзвичайних ситуацій.

Ще одним важливим напрямком IoT є автомобільна галузь і промислова автоматизація. На виробничих майданчиках від початку до кінця процесу RFID-системи та GPS дозволяють постачальникам відстежувати рух товарів у всьому ланцюгу постачання до кінцевої точки. Сенсори IoT збирають дані про час транспортування, стан обладнання та навколишні умови. Основні особливості розумної промисловості відображено на рисунку 1.13 [2].

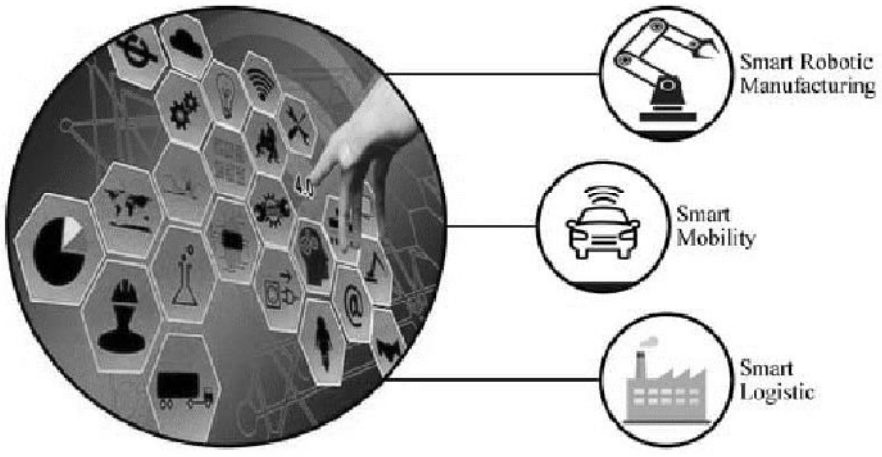


Рисунок 1.13 - Особливості розумної промисловості.

У ході дослідження сучасного стану розвитку IoT було встановлено, що ця технологія стрімко змінює підходи до роботи в різних галузях, включаючи промисловість, транспорт, медицину, сільське господарство, енергетику та побут. Завдяки інтеграції IoT пристроїв із хмарними платформами, аналітичними інструментами та інтелектуальними алгоритмами спостерігається підвищення ефективності, продуктивності та безпеки процесів.

Основними елементами IoT є сенсори, актуатори, пристрої обробки даних і комунікаційні модулі, які взаємодіють через стандартизовані протоколи зв'язку, такі як MQTT, HTTP/HTTPS. Це забезпечує надійну передачу даних, масштабованість мережі та синхронізацію між різними пристроями. IoT сприяє створенню розумних екосистем, де інформація аналізується в реальному часі, що дозволяє автоматизувати процеси, знижувати витрати та приймати точні управлінські рішення.

Перспективи розвитку IoT включають впровадження штучного інтелекту для прогнозного аналізу, розвиток технологій 5G для швидшого обміну даними, а також підвищення кібербезпеки для захисту інформації в інтелектуальних системах.

2 ЕТАПИ РОЗРОБКИ IoT СИСТЕМ

2.1 Основні етапи розробки IoT-систем.

Серед основних вимог на етапі розробці можна навести наступні:

- Аналіз вимог. Розробка IoT-систем починається з визначення потреб користувачів або бізнесу. Важливо оцінити, які дані будуть збиратися, як вони оброблятимуться та які результати очікуються.

- Вибір апаратної платформи. Обираються сенсори, мікроконтролери (наприклад, ESP32, Raspberry Pi), мережеві модулі, які відповідатимуть завданням проєкту. Увага приділяється таким параметрам, як енергоефективність, вартість і масштабованість.

- Розробка програмного забезпечення. Розробники створюють прошивки для пристроїв, серверні додатки, а також інтерфейси для користувачів (мобільні або веб-додатки). Значна увага приділяється забезпеченню безперебійної інтеграції між компонентами системи.

- Тестування системи. IoT-системи повинні пройти ретельне тестування в умовах реального середовища. Перевіряється надійність збору даних, стабільність зв'язку, енергоспоживання, захист від несанкціонованого доступу.

- Масштабування та інтеграція. Після успішного впровадження пілотного проєкту IoT-систему можна масштабувати, додаючи нові пристрої або функції. Також забезпечується інтеграція з іншими системами чи платформами.

Серед перспектив та проблем з використанням IoT можна виділити наступні:

- Висока вартість впровадження: хоча IoT стає доступнішим, початкові витрати на створення масштабованої мережі можуть бути значними.

- Інтероперабельність: різні IoT-пристрої часто працюють за несумісними стандартами, що створює проблеми при інтеграції.

- Майбутнє IoT: очікується, що подальший розвиток IoT зосередиться на квантових обчисленнях, розвитку екологічних технологій, а також на створенні автономних систем, здатних приймати рішення без участі людини.

Таким чином, дослідження та розробка IoT-систем залишаються стратегічним напрямком, що відкриває нові горизонти для науки, бізнесу та суспільства. З огляду на швидкі темпи розвитку технологій, роль IoT у майбутньому лише зростатиме, формуючи основу для інновацій у найрізноманітніших галузях.

2.2 Аналіз апаратних платформ для IoT

Апаратні платформи для Інтернету речей (IoT) відіграють ключову роль у створенні розумних пристроїв і систем, забезпечуючи основу для збору, обробки та передачі даних. Основними критеріями вибору апаратних платформ є їх продуктивність, енергоефективність, підтримка протоколів зв'язку, доступність інтерфейсів вводу/виводу та вартість.

Популярними апаратними платформами для IoT є:

Arduino – проста у використанні платформа для прототипування, яка підходить для невеликих проектів завдяки своїй доступності та підтримці великої кількості модулів.

Raspberry Pi – більш потужна платформа з можливістю запуску операційних систем, яка підходить для проєктів з обробкою великих обсягів даних та підключенням до інтернету.

ESP8266/ESP32 – енергоефективні мікроконтролери з вбудованим Wi-Fi та Bluetooth, які часто використовуються для створення недорогих IoT-пристроїв.

STM32 – платформи на базі ARM-мікроконтролерів, які забезпечують високу продуктивність та широкі можливості для складних IoT-додатків.

BeagleBone – платформа, орієнтована на промислові застосування завдяки своїй надійності та широким можливостям вводу/виводу.

Аналіз також показує, що вибір апаратної платформи залежить від специфіки завдання: для проєктів, орієнтованих на зменшення енергоспоживання, використовують платформи з низьким споживанням енергії (наприклад, ESP32), тоді як для обробки складних алгоритмів краще підходять платформи на базі ARM.

Тенденції розвитку апаратних платформ для IoT включають інтеграцію більш потужних процесорів, поліпшення енергоефективності, збільшення обсягу вбудованої пам'яті та розширення підтримки різних протоколів зв’язку, що забезпечує більшу функціональність і гнучкість у використанні IoT-рішень.

2.2.1 Опис платформи Raspberry Pi

Одноплатний мікрокомп'ютер Raspberry Pi 4 Model B - це новий продукт у популярному ряді мікрокомп'ютерів Raspberry Pi. Плата несе в собі досить багато удосконалень: підвищення швидкості роботи процесора, покращено продуктивність мультимедійного модуля, збільшення кількості та швидкості оперативної пам'яті та оновлені мережеві модулі порівняно з попереднім поколінням Raspberry Pi 3 Model B+, при цьому збережено рівень енергоспоживання та сумісність периферійних модулів. Для кінцевого користувача Raspberry Pi 4 Model B забезпечує продуктивність стаціонарних рішень початкового рівня на X86 архітектурі [4].

Ключовими характеристиками даного продукту є новий, високопродуктивний 64-розрядний чотириядерний процесор, підтримка двох дисплеїв з роздільною здатністю до 4k через пару micro-HDMI портів, апаратне декодування відео в 4Kp60, від 1-го до 4 х Гб оперативної пам'яті (залежно від обраної моделі), дводіапазонна бездротова мережа на 2,4 та 5,0 ГГц, Bluetooth 5.0, Gigabit Ethernet, два порти USB 3.0 та PoE (за допомогою окремого модуля PoE HAT).

Двоканальна бездротова LAN і Bluetooth мають модульну сертифікацію, що дозволяє платі використовуватися в кінцевих продуктах зі значно

спрощеним тестуванням на відповідність стандартам, покращуючи як вартість, так і час виходу на ринок.

Характеристики:

Процесор:

Broadcom BCM2711, 4 core Cortex-A72 (ARM v8) 64-bit SoC@1.5GHz

Оперативна пам'ять:

1GB LPDDR4-2400 SDRAM для Raspberry Pi 4 Model B 1GB

2GB LPDDR4-2400 SDRAM для Raspberry Pi 4 Model B 2GB

4GB LPDDR4-2400 SDRAM для Raspberry Pi 4 Model B 4GB

8GB LPDDR4-2400 SDRAM для Raspberry Pi 4 Model B 8GB

Підключення:

- 2.4 GHz та 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE
- Gigabit Ethernet
- 2 x USB 3.0 ports
- 2 x USB 2.0 ports.

Роз'єм GPIO: Raspberry Pi standard 40 pin GPIO header (fully backwards compatible with previous boards)

Відео та звук:

- 2 × micro-HDMI ports (up to 4kp60 supported)
- 2-lane MIPI DSI display port
- 2-lane MIPI CSI camera port
- 4-pole stereo audio and composite video port

Підтримка мультимедіа:

- H.265 (4kp60 decode)
- H264 (1080p60 decode, 1080p30 encode)
- OpenGL ES 3.0 graphics

Підтримка карток SD:

- Micro-SD card slot для loading operating system and data storage

Живлення:

- 5V DC via USB-C connector (minimum 3A*)

- 5V DC via GPIO header (minimum 3A*)
- Power over Ethernet (PoE) Enabled (Requires separate PoE HAT) [4].



Рисунок 2.1 - Raspberry Pi 4 Model B 8GB

2.2.2 Опис платформи ESP32

Особливе місце у розвитку IoT посідає ESP32 – потужний мікроконтролер із вбудованими модулями Wi-Fi та Bluetooth. Завдяки своїй універсальності, невисокій вартості та низькому енергоспоживанню ESP32 використовується як у побутових пристроях (розумні лампи, термостати, камери спостереження), так і в промислових рішеннях (моніторинг обладнання, автоматизація виробничих процесів, система "розумний склад").

Широкий функціонал, підтримка протоколів зв'язку, а також можливість інтеграції з хмарними сервісами роблять ESP32 ідеальним вибором для розробників IoT-проєктів. Завдяки таким технологіям наше життя стає зручнішим, безпечнішим і технологічно досконалим.

ESP32 — це гнучка платформа для різноманітних проектів, оскільки вона включає двоядерний процесор, з'єднання Wi-Fi та Bluetooth, різні порти введення/виведення та широкий набір периферійних пристроїв. Він використовує мікроархітектуру Xtensa LX6 і працює на тактовій частоті до 240 МГц.

Зараз доступно кілька різних моделей мікросхем, зокрема:

- ESP32-D0WDQ6 (and ESP32D0WD)
- ESP32-D2WD
- ESP32-S0WD
- І система в комплекті (SiP) – ESP32-PICO-D4

Таблиця 2.1 – Порівняння версій модулів ESP32

Версія ESP32	Максимальна частота ЦП	Wi-Fi Internet,	Bluetooth	Піни GPIO	Оперативна пам'ять	флеш-пам'ять	Додаткові можливості
ESP32-S2	До 240 МГц	2.4 ГГц Wi-Fi	Немає Bluetooth	43	320 KB	128 KB	USB OTG, безпечне завантаження, криптографічне апаратне прискорення
ESP32-S3	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	43	512 KB	До 4 МБ	USB OTG, безпечне завантаження, криптографічне апаратне прискорення
ESP32-WROOM-32	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	38	520 KB	4 MB	-
ESP32-WROOM-32D	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	38	520 KB	4 MB	-
ESP32-WROOM-32U	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	38	520 KB	4 MB	Роз'єм U.FL для зовнішньої антени
ESP32-WROVER	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	38	520 KB	4 MB	Підтримка зовнішнього SPI Flash
ESP32-WROVER-B	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	38	520 KB	4 MB	Підтримка зовнішнього SPI Flash
ESP32-PICO-D4	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	20	520 KB	4 MB	Інтегрований SPI Flash, інтегрований кварцевий генератор
ESP32-DevKitC	До 240 МГц	2.4 ГГц Wi-Fi	Bluetooth le	38	520 KB	4 MB	Міст USB-UART, кнопки, світлодіоди, слот для карт MicroSD

Архітектурна блок-схема ESP32, яка відображає кожен функціональний блок ESP32 SoC, показана на рис. 2.2.

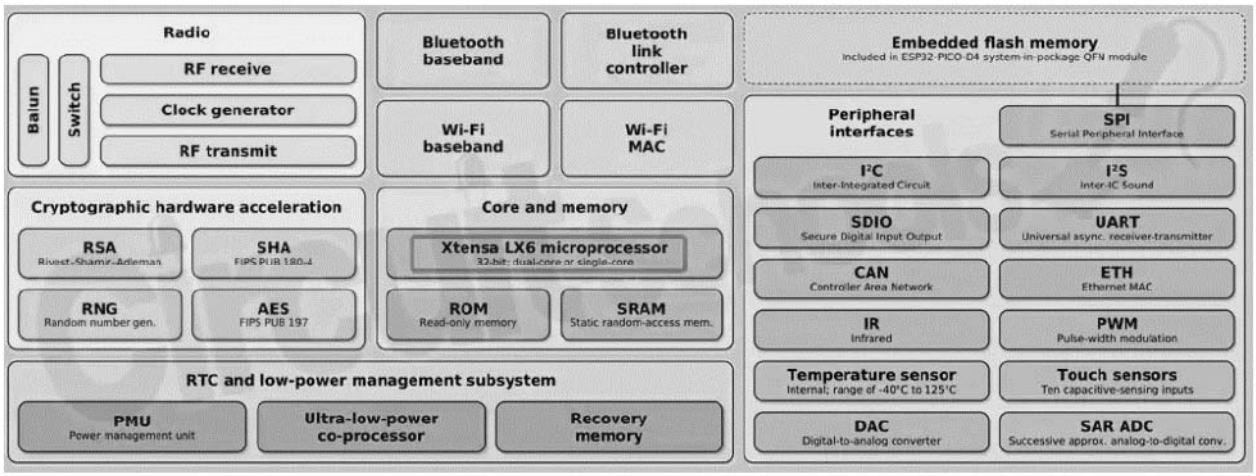


Рисунок 2.2 - Блок-схема ESP32

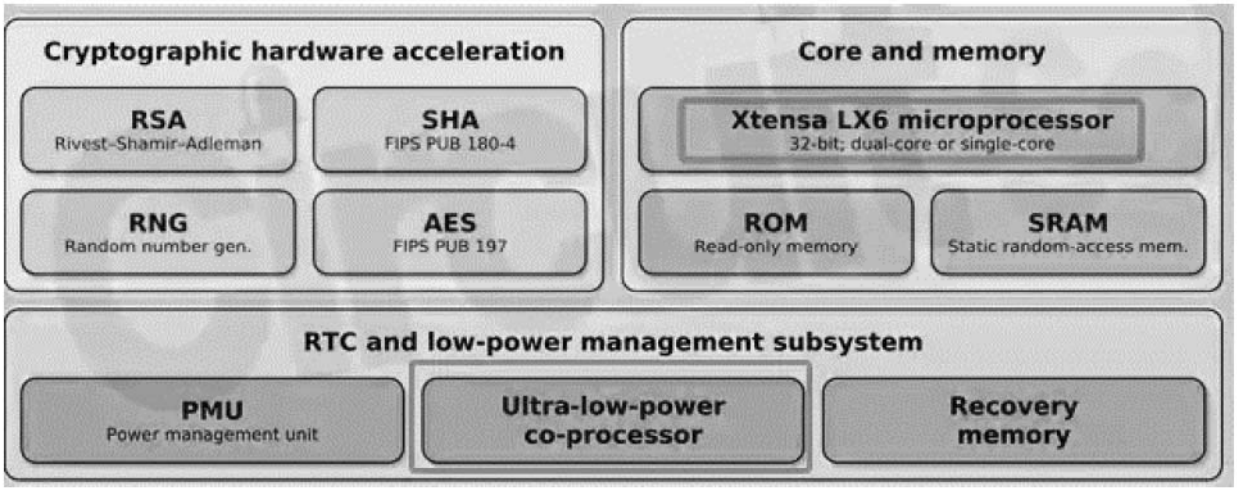


Рисунок 2.3 – Структура двоядерного процесору

ESP32 оснащений двоядерним процесором Tensilica LX6, що забезпечує високу обчислювальну потужність і здатність виконувати кілька завдань одночасно.

Розробка містить наднизький споживаний процесор, як видно на зображенні основного блоку вгорі, який використовується для виконання аналого-цифрових перетворень та інших завдань, коли система працює в режимі глибокого сну з низьким енергоспоживанням. . Це показує, що ESP32 пропонує різні режими енергозбереження та функції для оптимізації енергоефективності, що робить його придатним для додатків із живленням від акумулятора та з низьким енергоспоживанням [5].

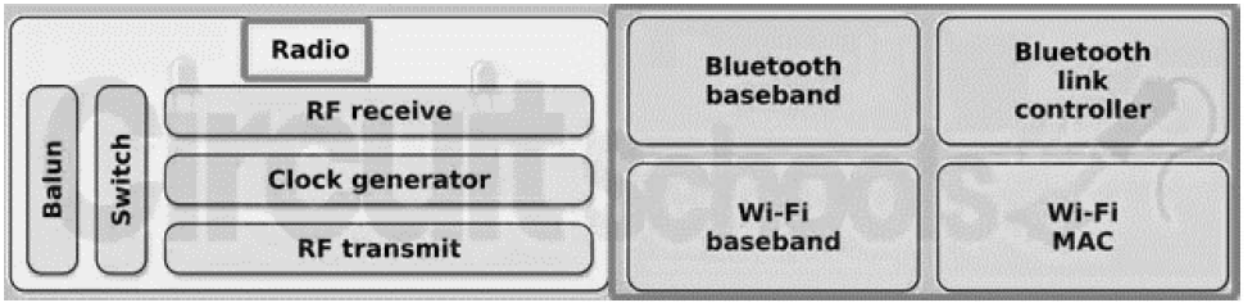


Рисунок 2.4. - Підтримка протоколу IoT

ESP32 підтримує стандарти Wi-Fi 802.11 b/g/n, що дозволяє підключатися до мереж Wi-Fi як клієнт або створювати власну точку доступу. Це забезпечує повну інтеграцію в бездротові мережі та підключення до Інтернету. Він також підтримує протоколи Bluetooth Classic і Bluetooth Low Energy (BLE), що забезпечує зв'язок з іншими пристроями Bluetooth, такими як смартфони, планшети та інші пристрої IoT.

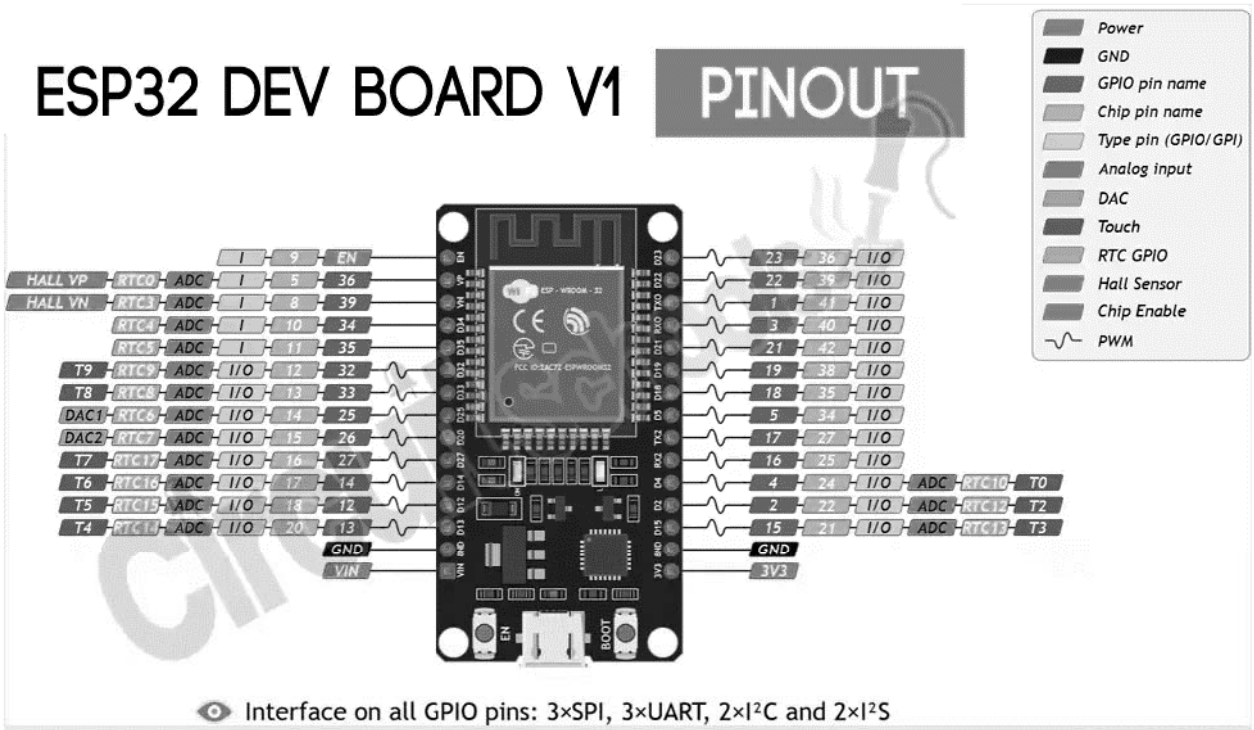


Рисунок 2.5 - Піни GPIO

Всього на ESP34 є 32 цифрові контакти. Ці контакти нагадують цифрові

контакти на платі Arduino і дозволяють нам додавати світлодіодні дисплеї, OLED-дисплеї, датчики, кнопки, зумери та інші компоненти до наших проектів.

Більшість цих штифтів також підтримують статус високого імпедансу, внутрішнє підтягування та опускання. Це робить їх ідеальними для застосування методів управління світлодіодами, а також для підключення кнопок і матричних клавіатур.

ESP32 забезпечує різноманітні периферійні інтерфейси, включаючи UART, SPI, I2C, I2S, SD/MMC, CAN, Ethernet MAC тощо. Ці інтерфейси полегшують зв'язок і передачу даних із широким спектром зовнішніх пристроїв. Також він містить кілька каналів АЦП, що дозволяє зчитувати показання аналогового датчика та вимірювати напругу.

ESP32 містить такі функції безпеки, як безпечне завантаження та флеш-шифрування, щоб гарантувати автентичність і цілісність мікропрограми, а також захистити конфіденційні дані.

ESP32 сумісний з операційною системою FreeRTOS, забезпечуючи багатозадачне середовище для ефективного керування та планування завдань.

ESP-IDF (ESP32 IoT Development Framework), який є офіційним комплектом розробки програмного забезпечення (SDK) для ESP32, надається ESP-IDF. Він містить бібліотеки, приклади та інструменти для полегшення розробки та програмування програм на основі ESP32.

В результаті ESP32 популярний для IoT завдяки своїй низькій вартості, низькому енергоспоживанню, вбудованим можливостям Wi-Fi та Bluetooth, достатній обчислювальній потужності та широкій підтримці спільноти.

Сам чіп просто відомий як ESP32. Виробникам пристроїв і розробникам доступні різні формати, кожен із яких має свої переваги та недоліки.

Espressif робить цей базовий чіп ESP32, саме так він і називається. Він неекранований і вимагає пайки для підключення до модуля або плати. Оскільки це ще більше ускладнить процес виробництва, більшість виробників пристроїв не просто купують мікросхеми [5].

Мікросхема розміщена в цих поверхневих модулях. Перевага придбання модуля полягає в тому, що протягом усього процесу виробництва його можна швидко встановити в MCU. Виробникам пристроїв не потрібно турбуватися про включення додаткових етапів у виробничий процес, щоб відповідати деяким IoT сертифікація пристрою наприклад відповідність вимогам FCC щодо екранування Wi-Fi, оскільки чіп часто ізольований і попередньо схвалений FCC.

Широко доступні плати розробки ESP32 пропонують просту точку входу для IoT-проектів на основі ESP32. Ці плати часто мають вбудований мікроконтролер ESP32 разом із додатковими деталями та можливостями, які роблять Апаратне забезпечення IoT розробка і створювати прототипи легше.

Шлюз ESP32 IoT це шлюз або крайовий пристрій, який містить мікроконтролер ESP32 або модуль на основі ESP32. Він підключає локальні пристрої або датчики IoT до хмари або центрального сервера, спрощуючи обмін даними, регулювання агрегації та контроль. Шлюзи ESP32 знаходять застосування в різноманітних сценаріях IoT, де потрібна локальна обробка даних, мережа та з’єднання пристроїв IoT із хмарними або центральними серверами.

Вони широко поширені в автоматизації розумного будинку, промисловому Інтернеті речей, моніторингу навколишнього середовища, розумному сільському господарстві та багатьох інших реалізаціях Інтернету речей.

Оцініть обчислювальну потужність і можливості пам'яті шлюзу ESP32. Враховуйте складність вашої програми IoT і необхідний обсяг обробки та зберігання даних. Потужніший шлюз може знадобитися для додатків, які передбачають інтенсивну обробку даних або виконання завдань на периферійних обчисленнях.

Мікроконтролер ESP32, який використовується в Dusun шлюз забезпечує високопродуктивні можливості обробки. Він оснащений двоядерним процесором, достатньою кількістю оперативної пам’яті та флеш-

пам’яті, що забезпечує ефективну обробку даних, аналітику в режимі реального часу та завдання периферійних обчислень.

Перевірте можливості шлюзу ESP32 для індивідуальних API або популярних протоколів шлюзу, таких як MQTT і HTTP. Для плавної інтеграції з вашими пристроями IoT і хмарними платформами важливо, щоб обраний вами протокол зв’язку був із ними сумісний. Залежно від конкретних потреб ваших пристроїв та інфраструктури IoT визначте, чи підтримуються вони необхідні бездротові протоколи, такі як Wi-Fi, Bluetooth або LoRa.

Wi-Fi, Bluetooth, BLE і Zigbee – це лише деякі стандарти бездротового зв’язку, які підтримуються Dusun Шлюз ESP32. Цей широкий вибір варіантів підключення забезпечує гнучке та масштабоване розгортання, дозволяючи легку інтеграцію з різними пристроями та датчиками IoT.

Для шлюзу на базі ESP32, який ви розглядаєте, перевірте наявність інструментів розробки, програмних інфраструктур і підтримки спільноти. Створювати й налагоджувати програми IoT може бути простіше, якщо у вас є доступ до інструментів, бібліотек і прикладів із потужного та активного середовища розробки.

Центральний мікроконтролер ESP32 побудовано на апаратному та програмному забезпеченні з відкритим кодом, що дає свободу створювати власне мікропрограмне забезпечення та програми. Ви можете програмувати ESP32 і використовувати його можливості завдяки великій колекції інструментів, бібліотек і прикладів, наданих ESP-IDF.

Ви можете змінити можливості Dusun шлюзу ESP32 Bluetooth WiFi Gateway відповідають потребам вашого конкретного проекту за допомогою ESP-IDF або інших сумісних структур програмування. Створення унікальних протоколів зв’язку, застосування методів обробки даних на практиці, підключення до хмарних платформ тощо підпадають під цю категорію. Bluetooth-шлюз на базі ESP32 підтримує найновішу версію Bluetooth 5.2, що варто виділити.

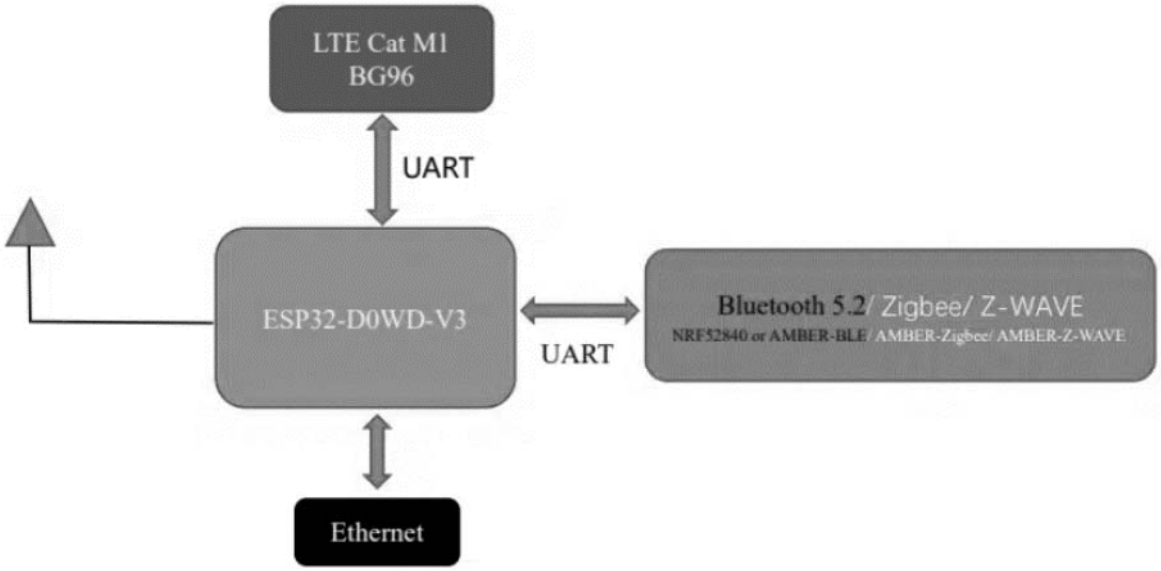


Рисунок 2.6 – Структура звязку модуля

Клієнти можуть керувати розумною побутовою технікою за допомогою платформи Tuya. Виробники розумної побутової техніки можуть безпосередньо використовувати Tuya, оскільки процес досить простий, а не створення хмари та часткової програми для керування продуктом.

Це дозволить скоротити витрати. Виробники та постачальники можуть легко активувати свої продукти для Tuya Smart Life або Tuya Smart, зареєструвавши їх на платформі Tuya.

Крім того, Dusun IoT надає ряд продуктів Tuya, таких як датчики (PIR, датчики диму, газу або витоку води, відкривання дверей або вікон, сирена, вологість/температура та SoS), засоби моніторингу безпеки (камери) та контролери клапанів. Крім того виробник має лінейку сучасних продуктів на базі SoC. Один з них цс системa на модулі на базі Arm® Cortcx®-A55 та Cortcx-M33.

DSOM-170N NXP i.MX93 SOM, заснований на системі на кристалі (SoC) сімейства i.MX 93 i.MX9352 від NXP, забезпечує високу обчислювальну потужність при низькому енергоспоживанні. Розміри всього 48 мм x 33 мм, оснащений Arm® Ethos™-U65 microNPU і заснований на інноваційній архітектурі Energy Flex від NXP, модуль дозволяє розробляти потужні,

економічні та енергоефективні можливості для широкого спектру медичних, промислові, енергетичні та транспортні програми, включаючи Інтернет речей (IoT), автоматизацію, людино-машинний інтерфейс (HMI), моніторинг обладнання, аудіо/голос, периферійні обчислення та машинне навчання (наприклад, виявлення аномалій).

Апаратна частина системи: ЦП: 1,7 ГГц Dual Cortex™-A55 NXP iMX93 процесор із 250 МГц Cortex-M33 співпроцесором реального часу, NPU: 0,5 TOPS Ethos U-65 microNPU для легких застосувань ШІ, Пам'ять: 1 ГБ LPDDR, 8 ГБ eMMC, Інтерфейси: 8 × UART, 2 × Ethernet (з 1 портом із підтримкою TSN), 2 × USB2.0 і 2 × CAN-FD, 1 × 2-смуговий MIPI-CSI, 1 × 4-смуговий MIPI DSI, Розмір: 48 мм × 33 мм × 1,5 мм [6].

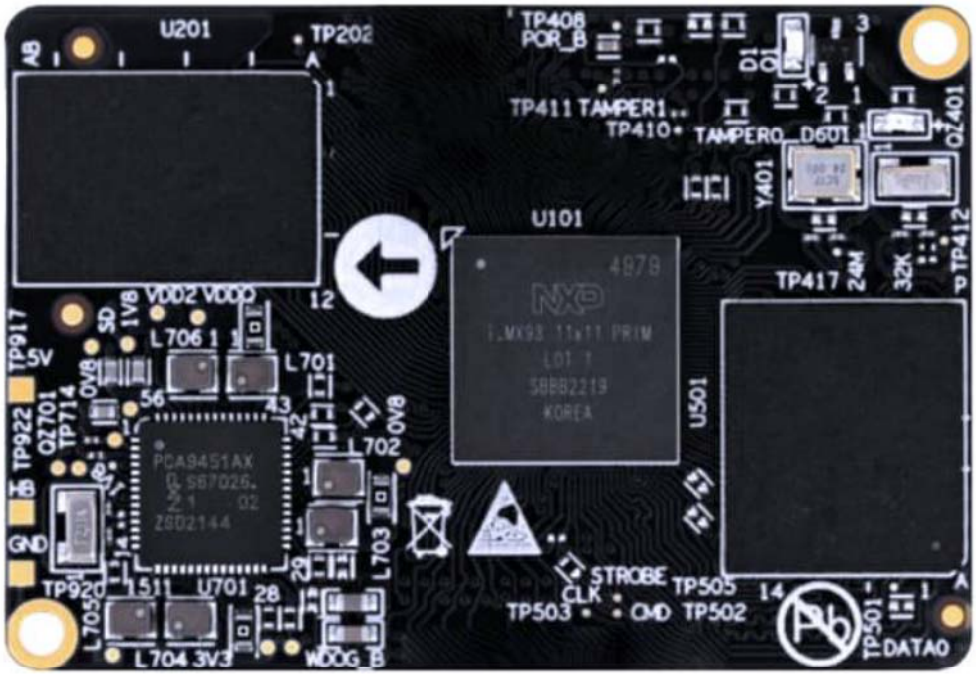


Рисунок 2.7 – Модель SoC DSOM-170N

Оснащений легким 0,5 Tops Arm Ethos™ U65 microNPU, кожен цикл з 256 MAC, DSOM-170N NXP i.MX 93 SOM може задовольнити потреби у високоефективному, швидкому та безпечному машинному навчанні на стороні краю, критичному для додатків. вимагають негайного реагування та зменшеної

затримки без потреби в хмарних службах ШІ. Таким чином, молодша платформа залишається хорошим вибором для проектів, які цінують стабільне, зріле середовище розробки та не вимагають новітніх функцій штучного інтелекту.

2.3 Платформа BeagleBone AI-64

Побудований на перевіреному підході Linux з відкритим вихідним кодом, надаючи розробникам величезну обчислювальну потужність у простому використання одноплатному комп'ютері. Використовуючи SOC Texas Instruments TDA4VM з двома 64-бітними процесорами Arm® Cortex®-A72, C7x DSP, а також прискорювачами глибокого навчання, машинного зору та мультимедіа, розробники отримують доступ до більш швидкої аналітики, більшої кількості варіантів зберігання даних, більшої кількості високошвидкісних, включаючи всі роз'єми. BeagleBone знадобиться для створення таких програм, як автономна робототехніка, відео- та відеоаналітика, висококласні дрони, медіа-сервери та розумні будівлі.

BeagleBone® AI-64 надає розробникам повну систему штучного інтелекту та машинного навчання із зручністю та розширюваністю платформи BeagleBone® та периферійними пристроями на борту, що дозволяють відразу ж розпочати навчання та швидке створення прототипів додатків.

На основі більш ніж десятирічного успіху одноплатних комп'ютерів Linux з відкритим апаратним забезпеченням, BeagleBone® AI-64 об'єднує величезну обчислювальну потужність у простій у використанні платформі.

Особливості чіпсету:

- Тип чіпсету: SoC Texas Instruments TDA4VM

- Подвійна 64-бітна підсистема мікропроцесора Arm Cortex-A72 із частотою до 2.0 ГГц

- Загальний кеш L2 об'ємом 1 МБ на двоядерний кластер Cortex-A72

32 КБ L1 DCache та 48 КБ L1 ICache на ядро Cortex-A72

- C7x з плаваючою комою, векторний DSP, до 1.0 ГГц, 80 GFLOPS, 256 GOPS

- Матричний багаторазовий прискорювач глибокого навчання (MMA) до 8 TOPS (8b) на частоті 1.0 ГГц

- Прискорювачі обробки зображень (VPAC) з процесором сигналів зображення (ISP) та декількома прискорювачами допомоги під час зору

- Прискорювачі обробки глибини та руху (DMPAC)

- Шість мікроконтролерів Arm Cortex-R5F із частотою до 1.0 ГГц

- Два DSP C66x з плаваючою комою, до 1.35 ГГц, 40 GFLOPS, 160 GOPS

- 3D-графічний процесор PowerVR Rogue 8XE GE8430, до 750 МГц, 96 гігафлопс, 6 Гпікс/с

- Підсистема пам'яті з об'ємом вбудованої оперативної пам'яті L3 об'ємом до 8 МБ із ECC та когерентністю.

- Дванадцять модулів багатоканального аудіо послідовного порту (MCASP)

Особливості плати:

- Сумісність з GPIO роз'ємом BeagleBone® Black для розширення за допомогою наявних додаткових шилдів.

- Роз'єм MikroBus забезпечує доступ до сотень існуючих датчиків та виконавчих механізмів у формфакторі Click.

Пам'ять:

- 4 ГБ LPDDR4

- Флеш-пам'ять eMMC ємністю 16 ГБ із високошвидкісним інтерфейсом

- Слот для картки MicroSD

Високошвидкісні інтерфейси

Роз'єм M.2 E-key PCIe для модулів Wi-Fi

Інтерфейс USB 3.0 Type-C для введення живлення та даних

2* інтерфейс USB 3.0 типу A

Гігабітний Ethernet

Роз'єм камери та дисплея:

Інтерфейс Mini Display Port для дисплеїв моніторів

2* 4-канальний роз'єм CSI для камери

Якщо модуль камери має 15-контактний роз'єм, потрібний кабель з 15-контактного на 22-контактний роз'єм.

4-канальний роз'єм DSI для плоских дисплеїв [7].

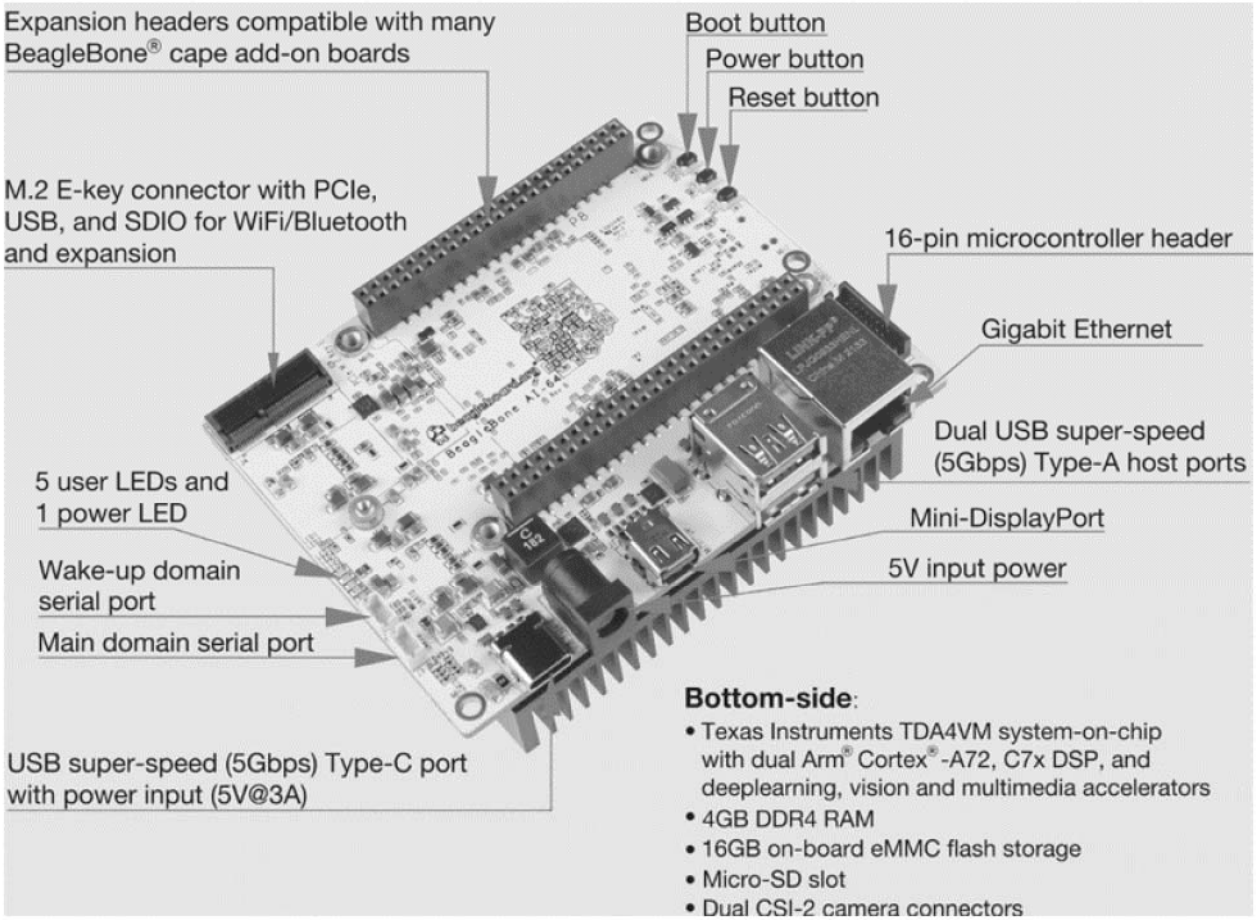


Рисунок 2.8 – Плата BeagleBone AI-64

2.4 Проблеми безпеки у світі IoT

Розвиток Інтернету речей (IoT) суттєво змінив уявлення про сучасні технології, забезпечуючи інтеграцію повсякденних пристроїв у єдину мережу для спрощення і автоматизації процесів. Однак разом із перевагами ця технологія породжує нові виклики, особливо у сфері безпеки. Серед основних

загроз — ризик несанкціонованого доступу до конфіденційних даних, можливість компрометації пристроїв або мережі, а також небезпека фізичного впливу через використання ненадійних або підроблених пристроїв.

Ці виклики обумовлюють необхідність глибокого аналізу вразливостей IoT-систем і розробки стратегій для їхньої мінімізації. У наступних розділах буде розглянуто ключові ризики, пов'язані з безпекою IoT, а також запропоновано ефективні заходи для захисту даних, пристроїв і мереж у цьому швидкозростаючому технологічному середовищі.

1. Конфіденційність даних та безпека:

IoT-пристрої постійно збирають і передають дані, які часто мають особистий і конфіденційний характер. Ця інформація може охоплювати широкий спектр — від медичних показників, отриманих із носимих гаджетів, до деталей повсякденного життя, які фіксують системи розумного дому. У разі порушення безпеки ці дані можуть стати мішенню для зловмисників, що відкриває можливості для крадіжки особистої інформації, фінансового шахрайства, маніпуляцій або навіть шантажу. Більше того, масштаб таких загроз зростає пропорційно до розширення мережі IoT-пристроїв, роблячи питання захисту даних критично важливим у сучасному світі.

2. Уразливості мережі:

Взаємопов'язаний характер систем IoT означає, що порушення безпеки в одному пристрої може мати ефект доміно, ставлячи під загрозу всю мережу. Це особливо критично для розумних будинків, промислових IoT-систем і міських інфраструктур, де один скомпрометований пристрій може відкрити доступ до інших компонентів мережі, включаючи більш критичні вузли. Такі уразливості можуть бути викликані слабкими паролями, застарілим програмним забезпеченням, відсутністю шифрування даних або недостатньо продуманими механізмами аутентифікації. Якщо зловмисник отримає доступ до мережі, це може призвести до витоку конфіденційної інформації, порушення роботи ключових сервісів або навіть фізичних пошкоджень обладнання. Усе це робить безпеку мереж IoT критичним аспектом, що

потребує регулярного аудиту, оновлення програмного забезпечення та впровадження багаторівневих заходів захисту.

3. Уразливості пристрою:

IoT-пристрої не завжди розроблені з урахуванням безпеки. Багато з них зроблені дешево і не мають основних функцій безпеки, таких як звичайні оновлення або безпечні налаштування за замовчуванням. Це робить їх вразливими до злому, як і у випадку з ботнетом Mirai, який використовував пристрої IoT для запуску потужних атак DDOS.

4. Автентифікація та авторизація:

Забезпечення того, щоб доступ до пристроїв і систем IoT отримували лише авторизовані користувачі, є важливим і водночас складним завданням. Багато IoT-пристроїв мають обмежені обчислювальні ресурси, що ускладнює впровадження складних механізмів автентифікації, таких як багатофакторна аутентифікація або криптографічні алгоритми. Крім того, слабкі паролі, стандартні облікові записи, які залишаються незмінними, або недостатньо захищені API можуть стати точками входу для зловмисників.

Проблеми також виникають через необхідність забезпечити баланс між зручністю для користувачів і високим рівнем безпеки. Недостатньо надійна авторизація може дозволити зловмисникам не тільки отримувати доступ до даних пристрою, але й контролювати його функціонал, що створює ризики для приватності, конфіденційності та фізичної безпеки.

Для подолання цих викликів важливо впроваджувати такі заходи, як унікальні облікові дані для кожного пристрою, регулярне оновлення паролів, впровадження сертифікатів та токенів для аутентифікації, а також застосування шифрування і контролю доступу на рівні мережі.

5. Ризики фізичної безпеки:

Крім порушень даних, пристрої IoT можуть створювати ризики фізичної безпеки. Наприклад, скомпрометована система IoT в інтелектуальному будинку може призвести до несанкціонованого контролю за замками,

термостатами або навіть камерами безпеки, що може наражати на ризик пасажирів.

6. Відповідність регулюючим органам:

Відповідність правилам, таким як GDPR, HIPAA або галузеві стандарти, може бути складною у ландшафті IoT. Компанії повинні орієнтуватися в юридичних та етичних вимогах обробки конфіденційних даних, які можуть бути складним завданням, особливо коли пристрої IoT працюють у глобальному масштабі.

7. Безпека ланцюжка поставок:

Виробники пристроїв IoT-пристрої вичерпні компоненти з усього світу, що робить їх ланцюжки постачання вразливими для підробки або атаки.

8. Відсутність стандартизації:

Відсутність єдиного набору стандартів безпеки та кращих практик у галузі IoT ускладнює проблеми безпеки. Оскільки різні виробники виготовляють пристрої, які можуть не дотримуватися тих самих рекомендацій щодо безпеки, стає важко підтримувати послідовність та безпеку в екосистемі.

Графічно концепція безпеки представлена на рис. 2.9.

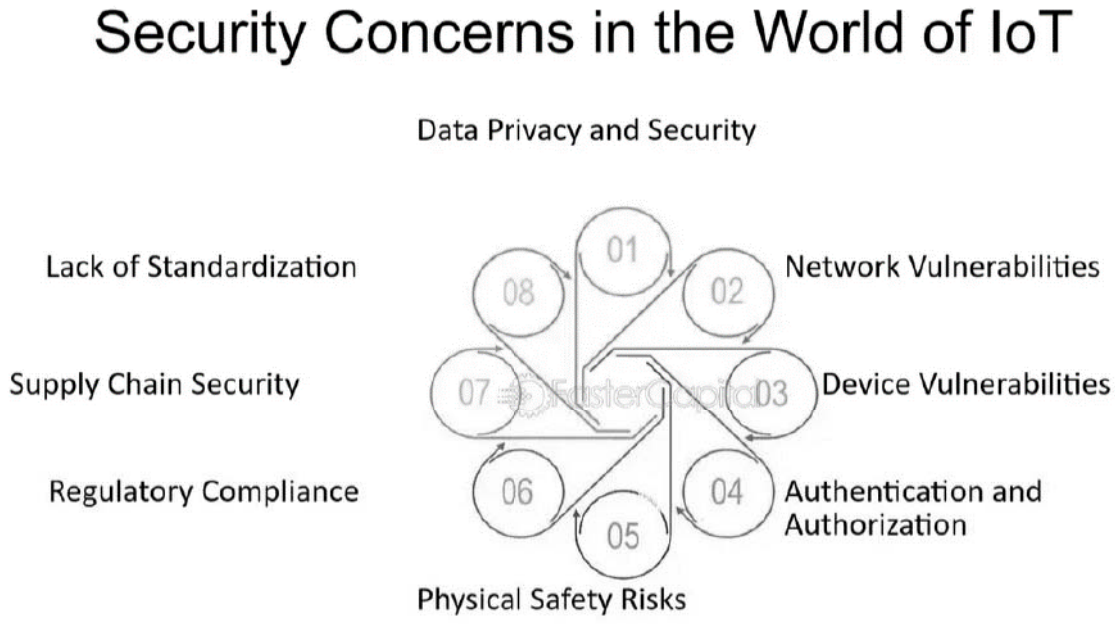


Рисунок 2.91 – Концепція безпеки IoT

Щоб проілюструвати серйозність цих проблем, ми можемо подивитися на приклад системи управління рухом розумного міста. Якщо хакери отримують доступ до цієї системи, вони можуть маніпулювати сигналами дорожнього руху, що призводить до хаотичного трафіку, нещасних випадків та потенційної загибелі життя. IoT продовжує зростати і розширюватися в різні сектори, дуже важливо, щоб ми вирішували ці проблеми безпеки колективно, впровадивши надійні протоколи безпеки та сприяючи культурі пильності та відповідальності в галузі IoT. Нездатність зробити це може призвести до широко поширеної вразливості, які підривають саму обіцянку пов'язаного, орієнтованого на IoT майбутнього.

2.5 Накопичування та аналіз даних

2.5.1 Сервіс ThingSpeak

Відкрита IoT-платформа із MATLAB-аналітикою. Сервіс компанії Math Works, створений для Інтернету речей, тісно пов'язаний із продуктами Math Works (MATLAB). ThingSpeak - це служба аналітичної платформи IoT, яка дозволяє збирати, візуалізувати та аналізувати потоки даних у реальному часі у хмарі. Ви можете надсилати дані до ThingSpeak зі своїх пристроїв, створювати миттєві візуалізації даних у реальному часі та надсилати оповіщення за допомогою веб-сервісів, таких як Twitter та Twilio. Завдяки аналітиці MATLAB усередині ThingSpeak ви можете писати та виконувати код MATLAB для виконання попередньої обробки, візуалізації та аналізу. ThingSpeak доступний як безкоштовний сервіс для некомерційних невеликих проектів (<3 мільйони повідомлень на рік або ~ 8200 повідомлень на день). Сервіс дозволяє накопичувати дані в своїх сховищах, після чого їх можна зручно переглядати у вигляді графіків [8].

З особливостей сервісу він має інтеграцію з MatLab Analytics з підтримкою скриптів MatLab. У безкоштовному обліковому записі сервіс

дозволяє створювати до чотирьох каналів, у кожному з каналів можна зберігати до 8 полів з різними даними. Ще в безкоштовному акаунті існує ще одне обмеження - не можна публікувати дані частіше одного разу на 15 секунд (рекомендується пауза в 20 секунд), це як би "захист" від перевищення ліміту 8200 повідомлень на день.

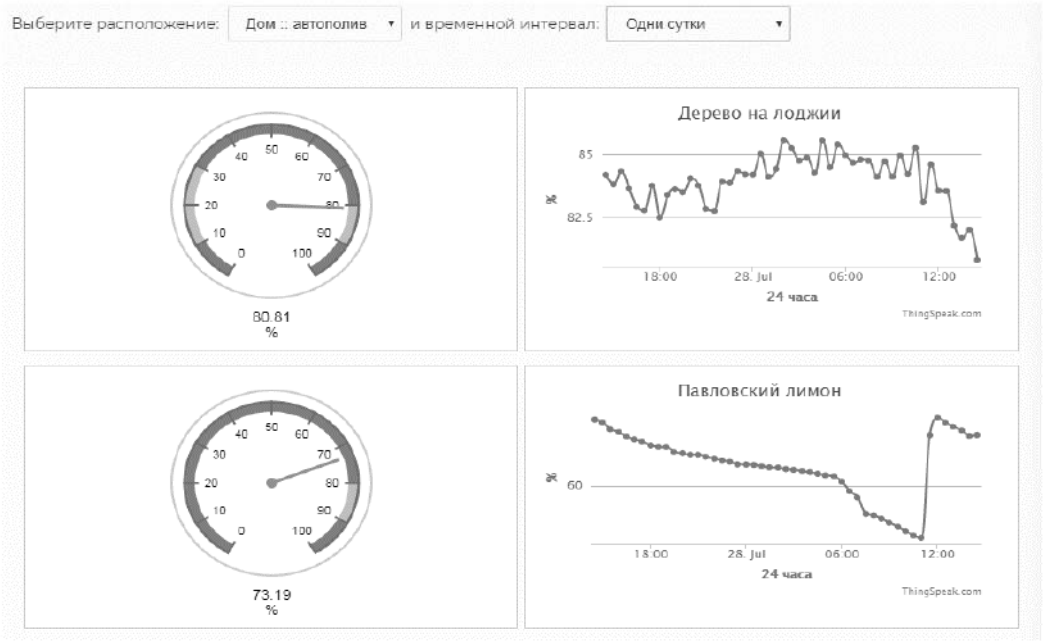


Рисунок 2.10 - Сервіс ThingSpeak

У принципі, пристроям легко вписатися в цей ліміт для даного завдання. Є кілька програм – клієнтів для Android, але набагато менше, ніж для MQTT.

Плюси: просте використання на ESP, зручний сайт.

Мінуси: багато обмежень на безкоштовному обліковому записі.

2.5.2 Сервіс open-monitoring.online

Цей сервіс у чомусь аналогічний ThingSpeak – на нього можна точно також надсилати дані та потім переглядати у вигляді таблиць, графіків та гістограм. Інтерфейс простіший, ніж у ThingSpeak, але й налаштовувати його набагато простіше. Крім того, графіки тут виглядають набагато "симпатичнішими", ніж на ThingSpeak, і керувати ними простіше - немає необхідності налаштовувати функції при зміні інтервалу вибірки, сервіс робить це автоматично. Дуже зручно. І найголовніше - сервіс з деяких пір вміє

відправляти повідомлення про вихід параметрів за допустимі межі або вимкнення пристрою.

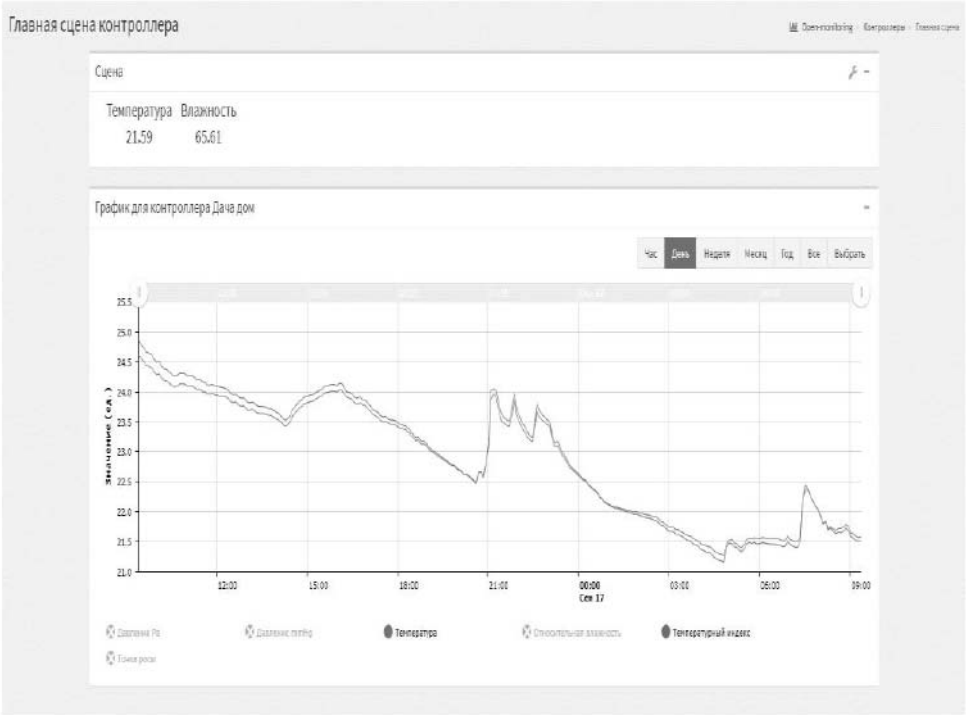


Рисунок 2.11 - Сервіс open-monitoring.online

Спочатку цей сервіс був створений, для моніторингу параметрів персональних сонячних електростанцій, але цілком підходить і для інших цілей. Сервіс доступний усім і безкоштовно, без суттєвих обмежень на даний момент. Єдине обмеження - відправка на сервер групи значень для одного контролера не може бути частіше одного разу на хвилину. На даний момент у кожному контролері можна зберігати до 30 значень (крім обчислюваних "на льоту"), на кількість контролерів обмежень як би немає. Надсилання даних на сервер здійснюється простим get-запитом, реалізація на ArduinoIDE займає не більше години. На відміну від ThingSpeak, збережені дані можна переглядати на одному графіку (з накладенням), а також налаштовувати якийсь dashboard для виведення останніх значень. Також можна переглядати збережені значення у вигляді простої таблиці. Бібліотека для надсилання даних для ESP32 + ESP-IDF знаходиться на GitHub.

Плюси: просте використання на ESP, зручний інтерфейс, майже немає обмежень.

Мінуси: немає можливості вивести графіки на сторонні сайти (на відміну від ThingSpeak).

2.5.3 Сервіс beebotte

На головній сторінці цього сервісу написано наступне: “підключення всього в режимі реального часу з використанням багатого API, що підтримує REST, WebSockets та MQTT”. У безкоштовному режимі кількість каналів та ресурсів не обмежена, але обмежена кількість повідомлень: 0.05 Million per day 1.5 Million per month. Для повідомлень, що зберігаються, ліміти ще менше: 5 000 per day 150 000 per month. Крім того, повідомлення зберігаються лише максимум три місяці, після чого видаляються. Про мобільний клієнт для смартфона мені поки що нічого не відомо [9].

Таким чином, робимо висновок о використанні сервісу ThingSpeak для обробки отриманих даних та подальшого отримання теплових карт розповсюдження сигналу.

3 ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРИСТРОЮ

У зв’язку зі складною ситуацією в енергетиці на підприємствах виникла гостра потреба у створенні сучасних пристроїв для моніторингу параметрів електромережі, зокрема напруги. Існуючі рішення не відповідають необхідним вимогам за своїми технічними характеристиками. Наприклад, у більшості джерел безперебійного живлення (ДБЖ) стандартний інтервал запису логів напруги та струму становить 60 секунд. У кращих сучасних моделях цей інтервал скорочений до 4 секунд. Проте навіть ці показники є занадто великими для ефективного моніторингу імпульсних викидів.

Для вирішення цієї проблеми виникла потреба у розробці пристрою, який забезпечить швидкість збору даних, вищу в тисячу разів. Головним завданням пристрою є виявлення та реєстрація аномальних значень напруги, що відрізняються від стандартного синусоїдального сигналу мережі живлення.

Розроблюваний пристрій повинен функціонувати здебільшого в режимі пошуку відхилень, а збереження даних до бази здійснювати лише при виявленні аномалій. Такий підхід забезпечить ефективне використання ресурсів та дозволить проводити глибокий аналіз критичних ситуацій фахівцями. Для вирішення цього завдання потрібно провести аналіз програмної та апаратної частини пристрою.

3.1 Аналіз програмної частини для завдань моніторингу напруги

Для моніторингу мережевої напруги та запису тільки аномальних точок (сплесків напруги) оптимально комбінувати методи реального часу та програмні фільтри. Підхід залежить від необхідної точності, частоти сплесків та складності проекту. Розглянемо два основні методи реалізації:

1. Розрахунок на льоту з пороговим контролем

Цей підхід дозволяє обробляти дані у реальному часі без значної затримки.

Як реалізувати:

• Паралельна обробка:

- ESP32 або інший мікроконтролер зчитує напругу через вбудований або зовнішній АЦП із заданою частотою (наприклад, 1–2 кГц для мережевого сигналу 50 Гц).

- Кожен лічений зразок порівнюється із заздалегідь встановленим пороговим значенням (або діапазоном, наприклад, ±10% від номінальної напруги).

• Виявлення сплесків:

Якщо напруга перевищує поріг, точка записується чи маркується. Можна додавати тимчасову позначку для аналізу.

• Фільтрування шуму:

Перед порівнянням даних застосовується цифрова фільтрація (ковзне середнє, ФНЧ або експонентне згладжування) для придушення дрібних перешкод.

Переваги:

• Простота реалізації.

• Висока швидкість роботи.

• Не потребує великих обчислювальних ресурсів.

Недоліки:

• Обмежена здатність виявляти складні патерни, такі як швидкі пульсації чи перехідні процеси.

2. Використання алгоритмів штучного інтелекту (ШІ)

Підхід із ШІ дозволяє аналізувати та класифікувати сплески напруги більш точно, включаючи нелінійні чи складні аномалії.

Як реалізувати:

• Збір даних:

Спочатку необхідно зібрати дані для навчання. Це може включати нормальні та аномальні сигнали напруги.

• Попередня обробка:

Використовується фільтрація та нормалізація даних.

• Навчання моделі:

Легковажна нейронна мережа або алгоритм машинного навчання, наприклад класифікатор на основі дерев рішень, навчається розпізнавати сплески. Навчання проводиться оффлайн (наприклад, у Python з використанням TensorFlow Lite або scikit-learn).

• Запуск пристрою:

Після навчання модель експортується та запускається на мікроконтролері (ESP32 підтримує TinyML та TensorFlow Lite).

Переваги:

• Можливість розпізнавання складних аномалій.

• Мінімізація помилкових спрацьовувань завдяки навчанню реальних даних.

• Гнучкість налаштування.

Недоліки:

• Складність розробки: потрібне навчання моделі та підготовка даних.

• Вимоги до пам'яті та обчислювальних ресурсів на пристрої.

• Можливо, буде потрібний більш потужний пристрій (наприклад, Raspberry Pi або STM32 з FPU).

Якщо завдання полягає в швидкому та ефективному моніторингу стандартних сплесків (наприклад, вище 240 або нижче 200 В), то розрахунок на льоту з пороговим контролем є оптимальним рішенням.

Якщо ж потрібний глибокий аналіз складних перехідних процесів (наприклад, короткочасних імпульсів або гармонійних спотворень), має сенс додати ІІ-модель для класифікації аномалій.

Пропонована архітектура системи

1. Апаратна частина:

- АЦП із частотою вибірки 1–2 кГц.

- Мікроконтролер ESP32 для обробки даних.

- Можливий зовнішній модуль для зберігання або передачі даних.

2. Програмна частина:

- Реальний час: Зчитування даних, фільтрація шуму (ФНЧ), порогове порівняння.

- Додатково (опціонально): Предиктивний алгоритм або TinyML для класифікації сплесків.

3. Логіка роботи:

- Якщо напруга перевищує заданий поріг або визначено як сплеск алгоритмом, точка записується на згадку або відправляється на сервер для подальшого аналізу.

Якщо потрібно, можу запропонувати приклад коду ESP32 або опис алгоритму обробки.

Приклад фрагменту програми яка реалізує такій функціонал наведено низче:

```
#include <Arduino.h>
const int adcPin = 34; // Пін для зчитування напруги (вхід АЦП)
const int sampleRate = 1000; // Частота вибірки у Гц
const int thresholdHigh = 3000; //Верхній поріг аномальної напруги (в одиницях АЦП)
const int thresholdLow = 1000; //Нижній поріг аномальної напруги (в одиницях АЦП)

// Параметри фільтрації (ковзне середнє)
const int filterWindowSize = 10; // Кількість точок для згладжування
float filterBuffer[filterWindowSize];
int filterIndex = 0;
// Для запису часу
unsigned long lastSampleTime = 0;
unsigned long sampleInterval = 1000/sampleRate;
// Функція для фільтрації (ковзне середнє)
float movingAverageFilter(float newSample) {
 filterBuffer[filterIndex] = newSample;
```

```
filterIndex = (filterIndex + 1) % filterWindowSize;
float sum = 0;
for (int i = 0; i < filterWindowSize; i++) {
sum += filterBuffer[i];
}
return sum/filterWindowSize;
}

void setup() {
Serial.begin(115200);
analogReadResolution(12); // Встановлюємо роздільну здатність АЦП на
12 біт (максимум для ESP32)
for (int i = 0; i < filterWindowSize; i++) {
filterBuffer[i] = 0; // Ініціалізація фільтра
}
}

void loop() {
// Перевіряємо, чи час знімати черговий відлік
if (millis() - lastSampleTime >= sampleInterval) {
lastSampleTime = millis();

// Зчитуємо значення з АЦП
int rawValue = analogRead(adcPin);
float filteredValue = movingAverageFilter(rawValue);

// Перевіряємо на аномалії
if (filteredValue > thresholdHigh || filteredValue < thresholdLow) {
// Запис аномального значення
Serial.print("Anomaly detected: ");
```

```
Serial.print("Voltage ADC value = ");
Serial.print(filteredValue);
Serial.print(", Timestamp = ");
Serial.println(lastSampleTime);
}
}
}
```

Пояснення коду, який наведено вище

1. Зчитування даних: Використовується вбудований АЦП ESP32 з роздільною здатністю 12 біт (значення від 0 до 4095).

2. Фільтрація: Реалізовано алгоритм ковзного середнього для придушення перешкод.

3. Порівняння з порогами: Значення напруги порівнюються із заданими порогами (thresholdHigh і thresholdLow).

4. Виведення аномальних точок: Якщо напруга виходить за межі порогів, дані (напруга та тимчасова мітка) виводяться через послідовний порт.

Для завдання моніторингу напруги та запису аномальних точок можна використовувати алгоритми штучного інтелекту (ШІ) різної складності. Вибір залежить від особливостей завдання (тип аномалій, обсяг даних, доступні обчислювальні ресурси). Основні варіанти наступні:

1. Прості методи машинного навчання

Ці методи підійдуть для мікроконтролерів з обмеженими ресурсами.

Методи:

1. Логістична регресія або метод опорних векторів (SVM):

Використовуються для бінарної класифікації (норма/аномалія). Навчаються на заздалегідь розмічених даних, включаючи нормальні та аномальні точки.

2. Дерева рішень або Random Forest:

Моделі добре підходять для інтерпретованого виявлення аномалій. Вони

розбивають дані на кілька простих умов і передбачають.

3. Кластеризація (наприклад, K-means):

Використовується для угруповання нормальних та аномальних точок без попередньої розмітки даних.

Переваги:

• Простота реалізації.

• Можливість роботи на малопотужних мікроконтролерах (ESP32, STM32).

Недоліки:

• Обмежена точність у складних типах аномалій.

2. Нейронні мережі (легковажні моделі)

Використання нейронних мереж можливе для складніших завдань розпізнавання патернів у сигналі.

Методи:

1. Рекурентні нейронні мережі (RNN) та LSTM:

Підходять для аналізу часових рядів та виявлення довгострокових аномалій чи нестабільностей у сигналі.

2. Згорткові нейронні мережі (CNN):

Використовуються для обробки сигналів, перетворених на спектрограми (наприклад, через перетворення Фур'є).

3. Автоенкодери:

Ці моделі навчаються реконструювати нормальні дані. Аномалії виявляються як дані із високою помилкою реконструкції.

4. Моделі TinyML (наприклад, TensorFlow Lite):

Легкові нейронні мережі, які можна запускати на мікроконтролерах, таких як ESP32 або STM32. Приклад: Multi-layer Perceptron (MLP).

Переваги:

• Висока гнучкість та точність для складних аномалій.

• Здатність враховувати складні нелінійні залежності.

Недоліки:

• Вимагають більше пам'яті та обчислювальних ресурсів.

• Навчання моделі має відбуватися на ПК, а потім переноситься на пристрій.

3. Аномалія-дискримінація (Anomaly Detection)

Ці методи спеціально розроблені пошуку аномалій без явної розмітки.

Методи:

1. Алгоритми на основі щільності даних (наприклад, DBSCAN, Isolation Forest):

Виявляють точки, які сильно відрізняються від щільності нормальних даних.

2. Statistical Thresholding:

Визначає статистично значущі відхилення на основі стандартного відхилення, медіани або квантилей.

3. One-Class SVM:

Алгоритм, який навчається тільки на нормальних даних, а точки, що не відповідають патерну, позначаються як аномалії.

Переваги:

• Не вимагає розмітки всіх даних.

• Добре працює з рідкісними аномаліями.

Недоліки:

• Може давати більше помилкових спрацьовувань у складних даних.

4. Гібридні підходи

Комбінують методи порогового аналізу та ІІ.

• Попередня фільтрація:

Прості алгоритми відсікають очевидні нормальні дані, і лише підозрілі точки передаються аналіз ІІ.

• Розпізнавання патернів:

ІІ використовується для складних ситуацій (наприклад, виявлення гармонійних спотворень, коротких перехідних сплесків).

Рекомендація для вирішення задачі

1. Якщо сплески напруги мають чіткі граничні значення (наприклад, вихід за діапазон 220–240 В):

Використовуйте пороговий метод із фільтрацією або дерева рішень.

2. Якщо сплески напруги включають складні перехідні процеси:

Застосуйте LSTM або автоенкодери для аналізу часових рядів.

3. Якщо даних багато і є невизначені аномалії:

Використовуйте One-Class SVM або Isolation Forest.

Далі наведемо приклад коду на Python для навчання простої моделі виявлення аномалій з використанням методу Isolation Forest, який добре підходить для виявлення відхилень даних напруги Цей код можна адаптувати під реальні дані.

1. Збір даних

Для початку необхідно зібрати дані про напругу: нормальні та з аномаліями. Дані можуть бути збережені у форматі CSV.

Приклад структури даних:

```
time,voltage
0,220
1,230
2,240
3,300 # Аномалія
4,210
...
```

2. Код для навчання моделі

Цей код обробляє дані, навчає модель Isolation Forest, зберігає її та визначає аномалії.

```
import pandas as pd
import numpy as np
від sklearn.ensemble import IsolationForest
import joblib # Для збереження моделі
```

```
# Крок 1. Завантаження даних
# Замініть 'voltage_data.csv' на файл з даними
data = pd.read_csv('voltage_data.csv')
# Перевіряємо структуру даних
print(data.head())
# Крок 2. Попередня обробка
# Використовуємо тільки стовпець з напругою
voltages = data['voltage'].values.reshape(-1, 1)
# Крок 3. Створення та навчання моделі Isolation Forest
model = IsolationForest(contamination=0.05, random_state=42)
# contamination задає частку очікуваних аномалій
model.fit(voltages)
# Крок 4. Передбачення
# -1 = аномалія, 1 = норма
predictions = model.predict(voltages)
# Додаємо результати в DataFrame
data['anomaly'] = predictions
data['is_anomaly'] = data['anomaly'].apply(lambda x: 'Yes' if x == -1 else 'No')
# Зберігаємо результати
data.to_csv('labeled_data.csv', index=False)
# Крок 5. Збереження моделі для використання на ESP32
joblib.dump(model, 'isolation_forest_model.pkl')
# Виводимо аномальні точки
print(data[data['is_anomaly'] == 'Yes'])
```

3. Приклад використання моделі

Збережену модель можна використовувати на пристрої реального часу. Приклад коду для перевірки нового виміру наведено низче:

```
# Завантаження збереженої моделі
model = joblib.load('isolation_forest_model.pkl')
```

```
# Приклад нового виміру напруги
new_voltage = np.array([[280]]) # Введення нового значення напруги
# Пророцтво
prediction = model.predict(new_voltage)
if prediction[0] == -1:
 print(f"Voltage {new_voltage[0][0]}: Anomaly detected!")
else:
 print(f"Voltage {new_voltage[0][0]}: Normal.")
```

4. Інтеграція на ESP32

Для інтеграції моделі на ESP32 можна використовувати TinyML або подібну бібліотеку:

1. Конвертуйте модель за допомогою sklearn-porter або ONNX у формат C-коду.

2. Завантажте на ESP32 і підключіть до аналізу нових даних.

Щоб інтегрувати модель машинного навчання, навчену на Python, в ESP32, можна використовувати підходи, які дозволяють запустити легку модель, таку як Isolation Forest, на мікроконтролері [10]. Ось поетапне керівництво:

1. Експорт моделі

Для використання на ESP32 необхідно перетворити модель на формат, сумісний з платформою. Ми будемо використовувати sklearn-porter, який конвертує модель у C-код.

Установка sklearn-porter:

```
pip install sklearn-porter
```

Конвертація моделі:

```
from sklearn_porter import Porter
import joblib
# Завантаження навченої моделі
```

```
model = joblib.load('isolation_forest_model.pkl')
# Конвертація моделі в C-код
porter = Porter(model, language='c')
output_c_code = porter.export(embed_data=True)
# Збереження згенерованого коду
with open('isolation_forest_model.c', 'w') as file:
 file.write(output_c_code)
print("Модель успішно експортована в C-код.")
```

На виході отримується файл isolation_forest_model.c, який містить функцію для передбачення аномалій.

2. Підключення C-коду до проекту ESP32

1. Інтеграція з Arduino IDE або PlatformIO:

- Помістіть isolation_forest_model.c у папку проекту.

- Підключіть файл в основному скетчі: #include "isolation_forest_model.c"

2. Приклад виклику функції передбачення: Згенерований код міститиме функцію, наприклад, predict. Приклад використання:

```
#include "isolation_forest_model.c"
 void setup() {
Serial.begin(115200);
 // Приклад значення напруги
float newVoltage = 280.0;
// Виклик функції передбачення
 int prediction = predict(&newVoltage);
if (prediction == -1) {
Serial.println("Anomaly detected!");
 } else {
Serial.println("Voltage is normal.");
 }
 }
void loop() {
```

// Основний цикл}

3. Альтернативний підхід: TensorFlow Lite

Якщо ви хочете використовувати більш складні моделі або підходи (наприклад, нейронні мережі), TensorFlow Lite Micro надає потужний та гнучкий інструмент для роботи з TinyML [11].

Кроки:

1. Навчіть модель у TensorFlow/Keras:
2. Конвертуйте модель у TFLite:
3. Підготуйте проект ESP32: Встановіть бібліотеку TensorFlow Lite Micro в Arduino IDE, PlatformIO або інтегруйте до ESP-IDF
4. Використовуйте модель на ESP32: Налаштуйте вхідні дані та виклик інтерпретатора TFLite
5. Компілюйте та завантажуйте проект: компілюйте та завантажте проект на ESP32

Для задач виявлення аномалій з обмеженими ресурсами краще використовувати sklearn-porter, оскільки:

• Він генерує компактний та швидкий код.

• Підходить для найпростіших алгоритмів, таких як Isolation Forest.



Рисунок 3.1 – Загальна структура алгоритмів обробки

3.2 Розробка схеми електричної принципової пристрою

Для побудови апаратної частини пристрою необхідно підібрати комплектуючі, які відповідатимуть функціональним вимогам, визначеним структурною схемою. Розроблена структурна схема пристрою представлена на рисунку 3.1. Вона відображає взаємозв'язок між ключовими компонентами системи, зокрема мікроконтролером ESP32, блоком живлення та модулем вимірювання напруги. Кожен компонент виконує свою роль у забезпеченні функціональності пристрою для моніторингу напруги в мережі.

Структурна схема пристрою включає такі основні компоненти:

- Мікроконтролерний блок ESP32, який виступає центральним елементом системи. Він забезпечує високопродуктивну обробку даних, отриманих із блоку вимірювання, завдяки вбудованому аналогово-цифровому перетворювачу та двоядерному процесору. ESP32 має розширений набір портів вводу-виводу (GPIO), які використовуються для взаємодії з периферійними пристроями, та вбудований модуль Wi-Fi і Bluetooth, що дозволяє організувати бездротову передачу даних. Наявність інтегрованого програматора значно спрощує налагодження та оновлення прошивки.



Рисунок 3.1 - Структурна схема пристрою

- Блок живлення, потрібен для стабільної роботи пристрою. Передбачено використання джерела постійного струму зі стабілізованою напругою 3.3 В. Від мережі змінного струму зниження напруги здійснюється за допомогою

трансформатора. Імпульне джерело не зважаючи на його сучасність в рамках цього завдання використовувати не бажано в звязку з можливістю виходу з ладу.

- Блок вимірювання напруги. Цей блок складається з ланцюгів які підготавлюють напругу до вимірювання аналогово-цифровимо перетворювачем, а саме резистивного подільника напруги та елементів які забезпечують вимірювання змінної напруги.

Завдяки чіткій організації елементів структурної схеми пристрій може бути легко масштабований або модифікований для вирішення додаткових завдань, таких як вимірювання струму, інтеграція з базою даних або підключення до хмарних сервісів.

Розробка блоку вимірювання повинна враховувати обробку блоком АЦП мікроконтролера сигналу який показано на рис. 3.1.

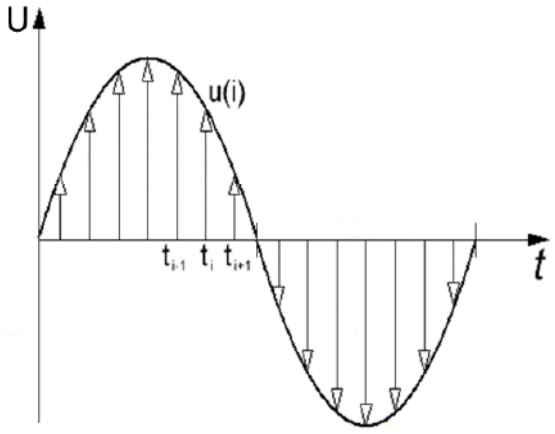


Рисунок 3.2 – Вхідна напруга з мережі живлення та точки вимірювання

Аналізуючи літературні джерела існуючих рішень стосовно вхідних ланцюгів можна навести приклади деяких з низ, як задовільняють завданню. Приклади наведені на рис. 3.3. Серед прикладів можна побачити схеми як для однофазної так і трехфазної мережі, як зі считуванням мгновенного значення так і середнькрадратичного. Мета у ціх методів різна, в нашому випадку треба звертати увагу на схеми з мгновенним значенням вимірювальної напруги.

Найбільш простою в реалізації та забезпечующа задовільну точність є однофазна схема з дільником та стабілітроном та гальванічною розвязкою. Яле

щоб адаптувати її до нашого випадка треба замінити стабілітрон с 5.1В на 3.6В в звязку з тим що модуль ESP32 живиться від 3.3В.

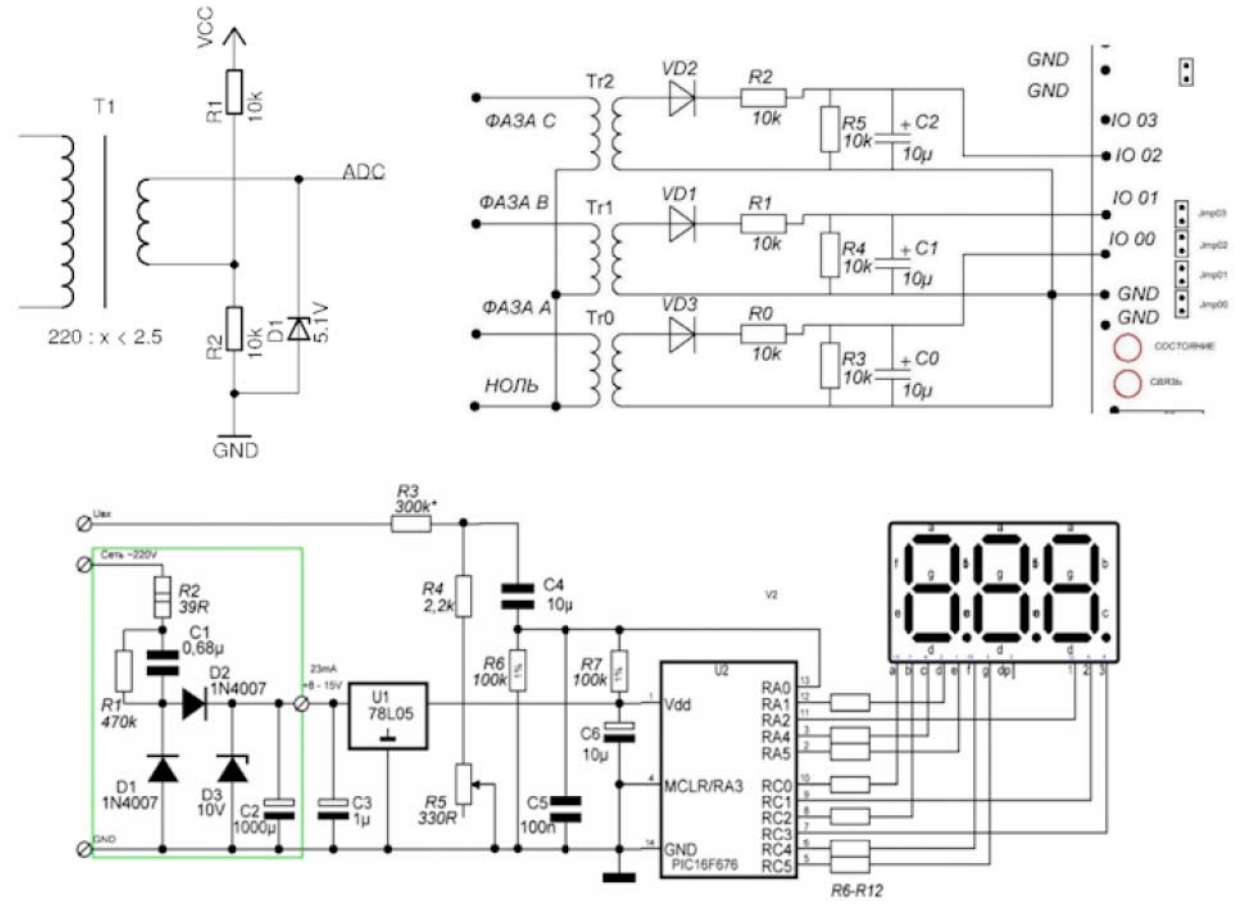


Рисунок 3.3 – Приклади вхідних ланцюгів

Блок живлення розробляємо на основі стандартної схеми включення лінейного стабілізатора LM7833. Схема електрична принципова наведена на рис. 3.4.

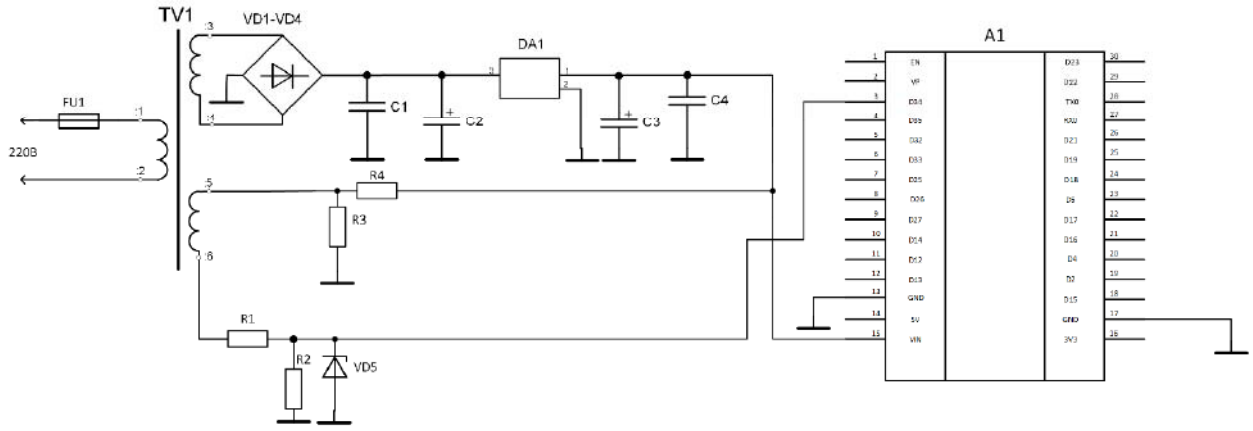


Рисунок 3.4 – Схема електрична принципова пристрою.

Блок А1 на схемі електричній принциповій представляє собою обраний модуль ESP32. Схема електрична також включає блок живлення на основі трансформатора та стабілізатора напруги з фільтруючими конденсаторами електролітичними та керамічними, останні забезпечують стабільність роботи лінейного стабілізатора.

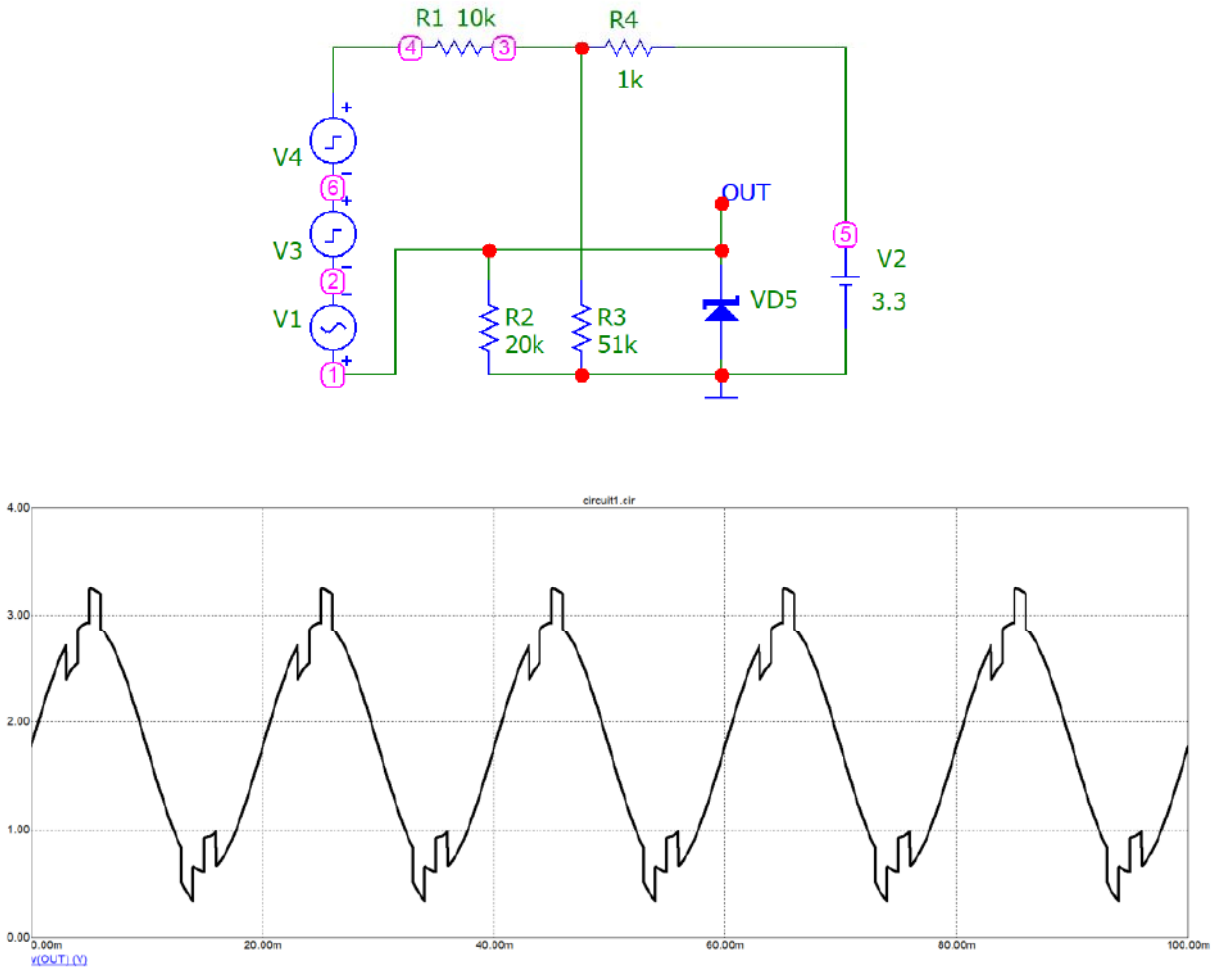


Рисунок 3.5 – Схема та результати моделювання вхідного блоку

Таким чином, провівши моделювання вхідного блоку ми впевнились в його работоздатності та тому, що розрахований вхідний сигнал знаходиться в допустимих межах роботи АЦП мікроконтролера.

4 КОНСТРУКТОРСЬКО-ТЕХНОЛОГІЧНА ЧАСТИНА

4.1 Конструкція пристрою моніторингу напруги

Розроблений пристрій моніторингу напруги на основі мікроконтролера ESP32 включає три основні функціональні блоки: модуль мікроконтролера ESP32 (у форматі блоку Arduino), блок живлення на основі трансформатора і випрямного моста зі стабілізатором, і блок вимірювання напруги. Конструкція передбачає їхнє оптимальне розміщення в корпусі для забезпечення надійної роботи, мінімізації перешкод та зручності обслуговування.

Корпус пристрою проектується у вигляді компактної прямокутної коробки із пластику, яка забезпечує захист компонентів від механічних пошкоджень та пилу. Блоки пристрою розташовані з урахуванням вимог щодо їх функціональності та безпеки:

- Блок мікроконтролера ESP32 розташований на окремій монтажній платі, що закріплена на основній платі. ESP32 у вигляді модуля Arduino має роз'єм для введення-виведення, які при розміщенні в корпусі повинні бути доступні для підключення інших блоків. Проводи підключення та доріжки основної плати повинні розташовуватися якнайдалі від високовольтних ланцюгів блоку живлення для мінімізації впливу перешкод. Безпосередньо сам блок живлення розміщується у нижній частині корпусу. Складається з понижуючого трансформатора, випрямного моста, конденсатора, що згладжує, і стабілізатора напруги. Високовольтні компоненти ізольовані від інших частин пристрою перегородкою для забезпечення безпеки.

- Блок вимірювання напруги містить дільник напруги, фільтри та вхідні ланцюги АЦП. Розміщується на основній платі якомога ближче до блоку мікроконтролера.

- Вхідні контакти для підключення напруги з'єднуються з клемами вхідної напруги живлення. Світлодіод стану виведено на передню панель.

4.2 Програмні продукти для проектування друкованих плат

Для розробки друкованої плати можна використовувати такі безкоштовні програмні продукти:

- KiCad. Повністю безкоштовний інструмент для розробки схем та друкованих плат із відкритим вихідним кодом. Забезпечує багатошаровий дизайн, трасування доріжок та симуляцію схем. Підходить для складних проектів та активно підтримується спільнотою [12].

- EasyEDA. Онлайн-інструмент для проектування схем та друкованих плат. Інтегрований із сервісами для замовлення друкованих плат, такими як JLCPCB. Пропонує інтуїтивно зрозумілий інтерфейс та бібліотеку компонентів [13].

- LibrePCB. Проста та легковажна програма для проектування друкованих плат. Підтримує всі основні функції трасування та експорту Gerber-файлів [14].

- DipTrace. Безкоштовна версія обмежена за кількістю пінів та розмірів плати, але дозволяє розробити невеликі проекти. Зручна для початківців завдяки інтуїтивному інтерфейсу [15].

Рекомендації для розведення плати:

- Високовольтні ланцюги блоку живлення необхідно розводити на окремій частині плати, забезпечуючи проміжок не менше 3 мм від низьковольтних ланцюгів.
- Аналогові ланцюги вимірювання напруги слід розміщувати ближче до АЦП ESP32, уникаючи довгих доріжок.
- Рекомендовано вмикати полігони для заземлення, щоб знизити рівень шумів.
- Для надійної фіксації в корпусі передбачено отвори кріплення на платі

4.3 Заходи з охорони праці

Дипломна робота, виконувана у лабораторії виробничого корпусу заводу з виробництва систем моніторингу енергії, потребує не лише фокусу на наукових аспектах дослідження, але й врахування питань безпеки та здоров'я розробника. Розглянемо заходи щодо мінімізації ризиків пов'язаних з вищезгаданими небезпечними та шкідливими факторами:

Підвищений рівень напруги:

Використання ізоляційних матів та взуття для зниження ризику ураження електричним струмом.

Застосування засобів захисту рук (ізоляційні рукавички).

Навчання правилам роботи з електроустановками та надання інструктажу з техніки безпеки.

Електромагнітне випромінювання:

Обмеження тривалості перебування в зоні високого випромінювання.

Використання захисних екранів та бар'єрів.

Шум:

Застосування індивідуальних засобів захисту слуху (наприклад, антишумові навушники).

Здійснення заходів щодо звукоізоляції приміщення.

Пил та озон:

Регулярне вологе прибирання лабораторії для зменшення кількості пилу.

Вентиляція та очищення повітря в приміщенні з використанням спеціалізованих фільтрів.

Напруження зору:

Регулювання освітленості робочого місця, використання антиблікових екранів.

Дотримання режиму роботи та відпочинку, виконання вправ для очей.

Емоційні перевантаження:

Планування робочого часу з урахуванням періодів відпочинку.

Впровадження технік стрес-менеджменту, наприклад, медитації або коротких перерв на релаксацію.

Навантаження на опорно-рухову систему:

Правильне ергономічне оформлення робочого місця.

Виконання фізичних вправ для зменшення м'язового напруження.

Забезпечення безпечних умов праці в лабораторії є важливою частиною підготовки до виконання дипломної роботи, що дозволяє не лише захистити здоров'я розробника, але й підвищити ефективність науково-дослідної роботи.

Вплив електромагнітного випромінювання на розробника. Вплив яскравих джерел світла, до яких належить дисплей, може викликати стомлення очей, запалення райдужної оболонки та спазм повік. Однак ці симптоми швидко минають і вплив видимого електромагнітного випромінювання не призводить до патологічних змін в органах зору у дослідника. Поверхнева щільність потоку енергії цього випромінювання перебуває у межах 0,1-1,5 Вт/м^2, що не перевищує норму в 10 Вт/м^2 [16].

Під час використання монітора на його екрані накопичується електростатичний заряд, що формує електростатичне поле. Цей наведений потенціал є ключовим фактором, який може викликати неприємні відчуття у дослідника. Негативний вплив електростатичного поля екрана проявляється в його здатності притягувати до робочого місця частки пилу, бруду та інших дрібних часток, які перебувають у повітрі навколо. Поверхневий електростатичний потенціал становить 3 кВ/м при гранично допустимій нормі в 20 кВ/м [16, 17].

Основними джерелами шуму на робочому місці в лабораторії є комп'ютерне обладнання, зокрема, системні блоки та принтери. Негативний вплив проявляється у зниженні розумової працездатності, швидкому втомленні, ослабленні уваги і виникненні головного болю. Реальний рівень шуму на робочому місці не перевищує 67 дБ при нормі в 60 дБ [16].

Проходження електричного струму через організм людини призводить до термічних, електролітичних і механічних впливів. Він може стимулювати

або пригнічувати функціональну активність клітин та тканин, залежно від параметрів струму. Така двойнята природа електричного струму робить його одночасно і лікувальним інструментом і потенційно небезпечним фактором для здоров'я людини. В медицині електричний струм використовується для стимуляції м'язів, нервових закінчень, лікування деяких видів паралічу та багатьох інших захворювань. Однак, неправильне або необережне використання електричного струму може призвести до опіків, порушення серцевого ритму, а в крайніх випадках – до летального результату.

Повертаючись до проблеми пилу та озону в лабораторних умовах, варто зауважити, що ці забруднювачі можуть мати не лише миттєві негативні ефекти на здоров'я людини, але й впливати на довгострокову перспективу. Доведено, що систематичне вдихання повітря з високим вмістом озону спричинює хронічні респіраторні захворювання, зменшує легеневу функцію, підвищує чутливість до респіраторних інфекцій і може посилити симптоми астми. Щодо пилу, то частки пилу можуть нести на собі алергени, токсичні речовини та мікроорганізми, що загрожує розвитком алергічних реакцій, токсичних та інфекційних захворювань.

З огляду на зазначені ризики, необхідно забезпечити адекватні заходи безпеки та охорони здоров'я в лабораторіях. До таких заходів можна віднести використання вентиляційних систем для зменшення концентрації шкідливих речовин у повітрі, регулярне технічне обслуговування лабораторного обладнання для запобігання його пошкодженню та уникнення витоку електричного струму, а також проведення інструктажів з безпеки для персоналу лабораторії. Крім того, важливо використовувати особисті засоби захисту, такі як респіратори та захисні окуляри, щоб мінімізувати вплив шкідливих речовин на організм.

Термічний вплив струму призводить до опіків окремих ділянок тіла, нагрівання до високої температури кровоносних судин, нервів, серця, мозку та інших органів, які перебувають на шляху струму, викликаючи серйозні функціональні порушення.

Електролітичний вплив струму виявляється в розкладанні органічних рідин, включаючи кров, і супроводжується значними порушеннями їх фізико-хімічного складу.

Механічний (динамічний) вплив струму проявляється у розриві, розшаруванні та інших пошкодженнях різних тканин організму, включаючи м'язову тканину, стінки кровоносних судин, судин легеневої тканини і т. д.

Біологічний вплив струму проявляється в подразненні і порушенні живих тканин організму, а також в порушенні внутрішніх біоелектричних процесів, які протікають при нормальному функціонуванні організму. Електричний струм подразнює живі тканини, викликаючи в них відповідну реакцію - збудження, яке є одним з основних фізіологічних процесів і характеризується тим, що живі утворення переходять зі стану відносного фізіологічного спокою в стан специфічної для них діяльності.

Праця в лабораторії під час проведення досліджень потребує тривалого, багатогодинного перебування у стійкому положенні перед персональним комп’ютером (ПК), що є невід'ємною частиною робочого процесу. Така діяльність характеризується значною статичною напругою м'язів спини, шиї та рук, а також обмеженою руховою активністю. Через це зростає ризик розвитку м’язово-скелетних розладів, особливо локальних динамічних навантажень, що припадають на кисті рук під час роботи з клавіатурою і мишкою.

Негативні наслідки такого робочого процесу можуть проявлятися у вигляді загальної втоми, болю, скутості або оніміння в шиї, спині, руках та ногах, що може знижувати продуктивність праці та викликати дискомфорт. Крім того, тривале перебування у сидячому положенні сприяє підвищенню ризику серцево-судинних захворювань та інших проблем зі здоров’ям, пов’язаних із недостатньою рухливістю.

З урахуванням шкідливих та небезпечних факторів, які виникають на робочому місці в лабораторії, було проведено детальний аналіз умов праці. На основі цього аналізу складена карта умов праці, що містить перелік факторів

ризику та заходів для їх мінімізації. Відповідна інформація наведена у таблиці 4.1.

Таблиця 4.1 – Карта умов праці на робочому місці розробника у лабораторії

№ п/п	Фактори виробничого середовища та трудового процесу	Нормативне значення	Фактичне значення	III клас: шкідливі та небезпечні умови, характер праці			Час дії фактора, %
				I ст.	II ст.	III ст.	
1	Шкідливі хімічні речовини, мг/м^3: I клас небезпеки Озон II клас небезпеки окисли азоту III-IV клас небезпеки	0,1 0,5	0,2 0,7	2 1,4			
2	Пил переважно фіброгенної дії, мг/м^3	-	-	-	-	-	-
3	Вібрація (загальна і локальна), дБ	107	110		3		
4	Шум, дБА	60	67	7			80%
5	Інфразвук, дБ	-	-	-	-	-	-
6	Ультразвук, дБ	-	-	-	-	-	-
7	Неіонізуючі випромінювання: - радіочастотний діапазон, В/м - діапазон промислової частоти, кВ/м - оптичний діапазон, Вт/м^2	25 -	40 -	15 -			80%
8	Мікроклімат в приміщенні: - температура повітря, ^{0}С - швидкість руху повітря, м/с - відносна вологість повітря, % - інфрачервоне випромінювання, Вт/м^2	23 – 25 не більше 0,2 не більше 75	27 0,1 60				100% 100% 100%
9	Атмосферний тиск	760	748				90%
10	Важкість і напруженість праці	категорія важкості праці - легка, I а категорія напруженості праці - помірно напружена					

Як видно з таблиці, у лабораторії фактичні умови виробничого процесу розробника більші за нормативних значень.

4.3.1 Заходи з поліпшення умов праці

Для підвищення якості трудового середовища в секторі збору платежів керівництву рекомендується вжити наступні дії:

Необхідно забезпечити, щоб кожен новоприбулий співробітник пройшов навчання з безпеки, яке включає правила роботи з електричними установками, користування комп’ютером та дотримання графіка роботи;

Застосування комбінованої системи вентиляції, що об'єднує механічне видалення забрудненого повітря з приміщення та природне провітрювання через відчинені вікна, допоможе покращити атмосферу в офісі;

Наявність якісного штучного освітлення в доповнення до природного світла є важливою, щоб забезпечити комфортні умови для зору співробітників при виконанні їхніх обов'язків.

Для мінімізації впливу електромагнітних випромінювань на працівників, рекомендується обмежити кількість електронних пристроїв, що одночасно використовуються на одному робочому місці.

Для зниження ризику негативного впливу електростатичних полів, слід застосовувати заземлення для металевих та електропровідних частин обладнання, здійснювати щоденне вологе прибирання приміщення та використовувати спеціалізовані серветки для очищення екранів.

Ефективним рішенням для нейтралізації впливу озону є встановлення витяжної вентиляції та розміщення принтерів на відстані від місць постійного перебування співробітників. Також слід вимикати невикористовуване електронне обладнання на робочих станціях.

Робоче місце з екраном розташоване на відстані не менше 1.5 метра від стіни з віконними отворами, а інші робочі місця розташовані на відстані 1 метра одне від одного, при цьому між ними забезпечено простір не менше 1.5 метра. Для розташування монітора на робочому місці відведено простір для

розробника розміром не менше 850 мм, враховуючи виступаючі частини обладнання. Монітори розташовані на робочому столі так, щоб поверхня екрана знаходилася на відстані не менше 400 міліметрів від очей розробника. Елементи робочого місця розміщені так, щоб відстань від очей користувача до екрану, клавіатури і тримача документів була однаковою.

Клавіатура розташована на поверхні столу на відстані 100-150 мм від краю для уникнення неправильного положення рук при друку. Конструкція клавіатури передбачає наявність опорного пристрою, що дозволяє змінювати кут нахилу поверхні клавіатури.

Робочий стілець є підйомно-поворотним з регульованою висотою та підлокітниками. Крісло забезпечує фізіологічно правильну робочу позу, не порушуючи циркуляцію крові та не викликаючи інших негативних впливів.

4.3.2 Виробнича санітарія

Умови праці розробників систем керування на базі мікропроцесорів класифікуються як роботи 1а категорії за ступенем складності. Ця діяльність належить до легкої праці, яка передбачає виконання завдань у сидячому положенні з мінімальним фізичним навантаженням. Рівень психоемоційної напруженості в процесі роботи оцінюється як помірний [16, 18]. Площа для одного робочого місця з комп'ютером повинна становити не менше 6 м^2, при об'ємі - не менше 20м^3. Для чотирьох людей, що постійно знаходяться в кімнаті площею 10*6=60 м^2, висотою=3,1м:

- Площа на одну людину складає 60/4=15 м^2;
- Об'єм на одну людину складає 60*3,1=186/4=46,5 м^3.
- Отже ці вимоги виконуються.

У лабораторії повинні бути забезпечені оптимальні умови для мікроклімату, зокрема температура, відносна вологість і швидкість руху повітря. Відповідні значення цих параметрів згідно з нормативами [18] наведені в таблиці 4.2.

Для освітлення лабораторних приміщень рекомендовано використовувати комбінований підхід, який включає як природне, так і штучне освітлення. Природне світло поступає через вікна та інші світлопроникні конструкції на бокових стінах.

Таблиця 4.2 – Загальні санітарно-гігієнічні вимоги до повітря робочої зони

Період року	Категорія робіт	Температура, °С					Відносна вологість, %		Швидкість вітру, м/с	
		Оптимальна	Допустима				Оптимальна	Допустима	Оптимальна	Допустима
			Верхня межа		Нижня межа					
			На робочих місцях							
			постійна	непостійна	постійна	непостійна				
Холодний	Легка Іа	22 - 24	25	26	21	18	40-60	75	0,1	0,1-0,2
Теплий		23 - 25	28	30	22	20	40-60	75	0,2	0,1-0,3

Згідно з нормами [16], для виконання робіт із середньою ступенем точності в зонах 4-го класу зорових завдань, загальна інтенсивність освітлення при використанні комбінації джерел світла має становити не менше 750 люмен.

4.3.3 Пожежна та техногенна безпека

Будинок, в якому знаходиться лабораторія, по вибуховій і пожежній небезпеці відноситься до приміщення категорії Д, оскільки в лабораторії є горючі (книги, документи, меблі, електропроводка) і речі, які при взаємодії з вогнем можуть горіти без вибуху [19].

За конструктивними характеристиками будівля відноситься до будівель з несучими та огороджувальними конструкціями з бетону і залізобетону, де для перекриттів використовується плиткові матеріалами захищених штукатуркою.

Отже, ступінь вогнестійкості будівлі відноситься до третьої (III) групи [19]. Можливі причини виникнення пожежі в лабораторії:

1) Використання пошкоджених (несправних) електроприладів;

2) Несправності електропроводки, розеток і вимикачів, які можуть призвести до короткого замикання або пробою ізоляції;

3) Необережне поводження з вогнем та недотримання заходів пожежної безпеки;

4) Паління в недозволених місцях;

5) Несправність захисного заземлення.

Отже вірогідні пожежі, які можуть бути в лабораторії відносяться до класу "Е" пов'язаний з горінням електрообладнання.

Для запобігання утворенню горючого середовища передбачено використання спеціальних меблів стійких до підвищених температур для робочого місця, покриття підлоги з негорючих матеріалів. Необхідними заходами для запобігання пожеж є своєчасний ремонт електроприладів, використання тільки справних електроприладів, паління в спеціально створених місцях, в кінці робочого дня відключати з електромережі електрообладнання, проходити протипожежний інструктаж, на якому працівники ознайомлюються з правилами протипожежної безпеки, призначення осіб відповідальних за пожежну безпеку.

Для ліквідації невеликих загорянь пропонується застосування первинних засобів пожежогасіння — вогнегасників. Для гасіння пожеж в лабораторії розробника площею 60 м^2 передбачається вуглекислотний вогнегасник ОУ-5 — 1 шт. (клас пожежі Е — горіння електроустановок під напругою) [19].

У приміщенні застосований пожежний оповісник ІП 104. який спрацьовує при перевищенні температури в приміщенні +60°С. А також димовий оповісник ІП 212, який спрацьовує при скупченні диму в приміщенні.

З метою попередження прямого удару і другорядних проявів блискавок, будівля обладнана системою блискавкозахисту. Категорія пристрою блискавкозахисту має бути 3 категорії для виробничих споруд з приміщеннями

по пожежній безпеці класу П-IIа [18].

Громовідвід складається з трьох основних частин: приймача блискавки, який безпосередньо приймає удар блискавки; струмовідводу (спуску), що сполучає приймача блискавки з заземлювачем, і заземлення, через яке струм блискавки переходить безпосередньо в землю.

Вертикальна конструкція — частина будівлі. яка призначена для закріплення приймача блискавки і струмовідводу — називається опорою. Опора встановлена на даху будівлі. У разі виникнення пожежі:

– негайно повідомити в пожежну охорону за телефоном 101,

– сповістити людей, що знаходяться в сусідніх приміщеннях про виникнення пожежі,

– приступити до гасіння пожежі за допомогою первинних засобів пожежогасіння,

– у разі загрози життю покинути небезпечну зону.

4.3.4 Електробезпека

Приміщення лабораторії, згідно з [18], віднесено до категорії без підвищеної небезпеки ураження струмом. Також лабораторія класифікується як пожежонебезпечна зона класу П-IIа. Температура навколишнього середовища знаходиться в межах +20 ± 5 °С, а відносна вологість повітря - 60±20%. В лабораторії встановлені непровідні підлоги, відсутній струмопровідний пил, відсутні високі температура і збільшена вологість, а також електрично-активне середовище. Опір захисних заземлювачів в електричних установках напругою 380/220 В не повинен перевищувати 4 Ом.

Основними заходами для запобігання ураженню електричним струмом у лабораторії є захист від дотику до частин електрообладнання, що знаходяться під напругою, використання захисного заземлення та автоматичного відключення. Для забезпечення безпеки працівників від ураження електричним струмом застосовується подвійна ізоляція проводів. Крім того, в лабораторії встановлено захисні автоматичні вимикачі, що окремо живлять

освітлення та розетки.

Організаційні заходи, спрямовані на запобігання ураженню електричним струмом, включають призначення відповідальних осіб за електробезпеку та проведення регулярних інструктажів для працівників.

4.3.5 Інженерні рішення з охорони праці

Захисне заземлення – це навмисне з'єднання з землею частин обладнання, які не знаходяться під напругою в нормальних умовах експлуатації, але які можуть знаходитись під напругою в результаті порушення ізоляції електроустановки.

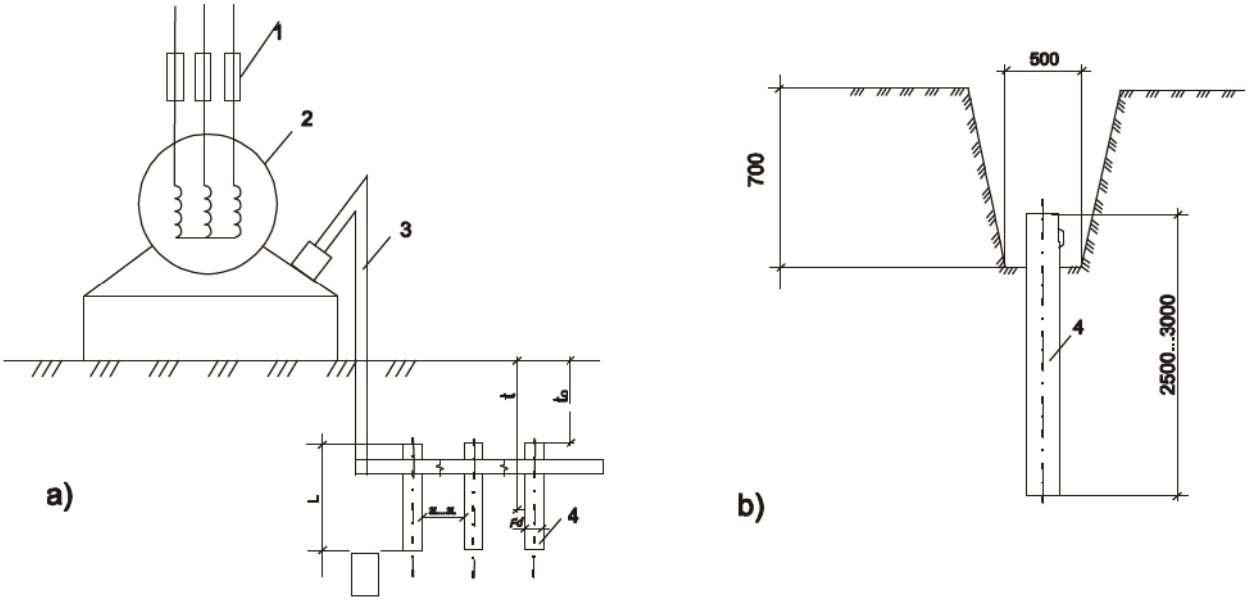


Рисунок 4.1 - Пристрій заземлення

а) – схема заземлюючого пристрою;

b) – розміщення одиночного заземлювача;

1-плавкі вставки; 2 – електрообладнання;

3- з'єднувальна штаба; 4- трубчатий заземлювач

В даному розділі дипломної роботи необхідно розрахувати заземлюючий пристрій для заземлення електрообладнання яке живеться від мережі електростанції при слідуючих вихідних даних:

- грунт – суглинок з питомим електричним опором ρ = 100 Ом*м;

- в якості заземлювачів прийнято сталеві труби діаметром d = 0.08 м і довжиною l = 2.5 м, розміщені вертикально і з'єднані зварюванням сталевою штабою 40*4 мм;
- потужність обладнання U=2 кВт;
- потужність трансформатора 100 кВ*А, допустимий по нормах опір заземлюючого пристрою [r3] <= 4 Ом.

Розрахунок захисного заземлення:

Визначаємо опір одиночного вертикального заземлювача Rв, по формулі:

$$R_B = \frac{\rho_{розр}}{2\pi \cdot l}\left(\ln\frac{2l}{d} + \frac{1}{2}\cdot\frac{4t+l}{4t-l}\right),$$

де t – відстань від середини заземлювача до поверхні ґрунту, м;

l, d – довжина і діаметр стержневого заземлювача, м.

Розрахунковий питомий опір ґрунту

$$\rho_{розр} = \rho \cdot \psi,$$

де ψ– коефіцієнт сезонності, який враховує можливість підвищення опору ґрунту на протязі року.

Приймаємо ψ = 1.7, для першої кліматичної зони, тоді

$$\rho_{розр} = \rho \cdot \psi = 100*1.7=170 \text{ Ом}$$

$$Rв = \frac{170}{2\pi 2.5}\left(\ln\frac{2\cdot 2.5}{0.08} + \frac{1}{2}\ln\frac{4\cdot 2.05+2.5}{4\cdot 2.05-2.5}\right) = 48 \text{ Ом}$$

Визначаємо опір сталевої штаби, яка з'єднує стержневі заземлювачі

$$Rn = \left(\frac{\rho_{розр}}{2\pi \cdot l}\right)\cdot\ln\left(\frac{l^2}{dt}\right),$$

де l – довжина полоси, м;

d=0.5b(b – ширина полоси, рівна 0.08 м).

Визначаємо розрахунковий питомий опір ґрунту $\rho_{розр}$ при використанні з'єднувальної штаби у вигляді горизонтального електрода довжиною 50 м. При довжині полоси 50 м, $\psi' = 5.9$, тоді

$\rho'_{розр} = \rho\psi = 100 * 5.9 = 590$ Ом*м

$$R_{П} = \frac{590}{2\pi 50} \ln \frac{50^2}{0.04 \cdot 0.8} = 21\ Ом$$

Визначаємо орієнтовне число n одиночних стержневих заземлювачів по формулі

$$n = \frac{R_B}{[r3] \cdot \eta_B} = \frac{48}{4 \cdot 1} = 12 шт,$$

де $[r3]$ - допустимий по нормах опір заземлюючого пристрою,

η_B – коефіцієнт використання вертикальних заземлювачів (приймемо його рівним 1).

Приймаємо розміщення вертикальних заземлювачів по контуру з відстанню між суміжними заземлювачами рівною 2l. По таблиці [20] знайдемо дійсні значення коефіцієнтів використання η_B та $\eta_Г$, виходячи з прийнятої схеми розміщення вертикальних заземлювачів, $\eta_B = 0.66$, $\eta_Г = 0.39$.

Визначаємо необхідне число вертикальних заземлювачів

$$n = \frac{R_B}{[r3]\eta_B} = \frac{48}{4 \cdot 0.66} = 18 шт$$

Визначаємо загальний розрахунковий опір заземлюючого пристрою R з врахуванням з'єднувальної штаби

$$R = \frac{R_B \cdot R_Г}{R_Г \eta_Г + R_Г \eta_Г n} = \frac{48 \cdot 21}{48 \cdot 0.39 + 21 \cdot 0.66 \cdot 18} = 3.76 Ом$$

Правильно розрахований заземлюючий пристрій повинен відповідати умові R<=[r3]. Розрахунок виконано вірно, так як $3.7 < 4$.

5 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

Одним з ключових показників, який використовується для оцінки економічної ефективності нової техніки, є розмір капітальних вкладень. До цих вкладень включаються витрати на науково-дослідні та дослідно-конструкторські роботи, а також на випробування та вдосконалення дослідних зразків.

Для визначення вартості конструкторської підготовки виробництва складається кошторис витрат, що охоплює період від отримання завдання до виготовлення та заводських випробувань дослідного зразка, включаючи коригування документації на основі отриманих результатів цих етапів [21].

5.1 Визначення стадій розробки

Стадії роботи, які необхідні для розробки системи моніторингу напруги, а також вміст робіт на кожній стадії зведені в таблицю 5.1.

Таблиця 5.1 – Стадії розробки системи моніторингу напруги

№ з/п	Стадії розробки	Вміст робіт	Тривалість етапу, днів	Примітка
А	Постановка завдання	Узгодження технічного завдання із замовником	1	1 інженер
Б	Вивчення об'єкту	Аналіз існуючих рішень	2	1 інженер
В	Розробка проекту	Проектування системи моніторингу	21	1 інженер
Г	Проведення дослідження та розробки	Розробка технічної документації	3	1 інженер

Д	Узгодження із замовником	Демонстрація проекту. Виправлення помилок.	1	1 інженер
Е	Передача замовнику	Передача результатів замовнику, підписання акту здачі робіт	2	1 інженер

Для визначення терміну виконання етапів розробки системи моніторингу напруги, а також витрат, будується лінійний графік, який відображує в наочному вигляді терміни виконання кожного етапу як окремо, так і в цілому. На рис. 5.1 зображений лінійний графік стадій вказаних в таблиці 5.1.

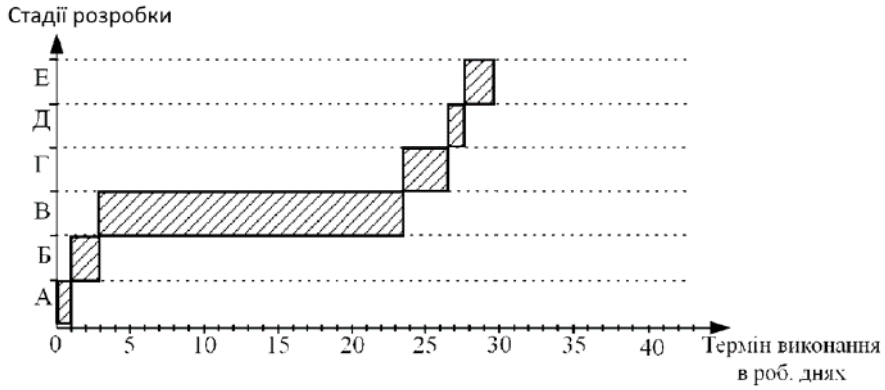


Рисунок 5.1 – Лінійний графік розробки системи моніторингу напруги

Відповідно до рис. 5.1 на види роботи А-Е, потрібно 30 восьмигодинних робочих днів.

Для виконання робіт по етапу А необхідно 1 людину – інженера технічного забезпечення проекту.

Для виконання робіт по етапу Б необхідно 1 людину – інженера технічного забезпечення проекту.

Для виконання робіт по етапу В необхідно 1 людину – 1 інженер електронної техніки.

Для виконання робіт по етапу Г необхідно 1людину – 1 інженер електронної техніки.

Для виконання робіт по етапу Д необхідно 1 людину –1 інженер технічного забезпечення.

Для виконання робіт по етапу Е необхідно 1 людину – 1 інженер технічного забезпечення.

У зв'язку з наведеним вище списком працівників для виду робіт, в таблицю 5.2 зводяться всі необхідні співробітники з кількістю робочих днів участі в проекті.

Таблиця 5.2– Співробітники проекту

Найменування	Кількість співробітників людей	Кількість робочих днів участі в розробці, роб. дні	К-ть часу, витраченого на участь в проекті, ч
Інженер технічного забезпечення проекту	1	6	48
Інженер електронної техніки	1	24	192

5.2 Розрахунок заробітної плати

Заробітна плата кожного співробітника нараховується виходячи з годинної тарифної ставки. Вони представлені в таблиці 5.3.

Таблиця 5.3 – Тарифні ставки співробітників

Найменування співробітника	Тариф Тсер, грн./год.
інженер технічного забезпечення проекту	65
інженер електронної техніки	75

Заробітна плата кожного співробітника визначається по формулі [21]

$$ЗП = N_{раб} \cdot T_{сер} \cdot B \quad (5.1)$$

де ЗП – заробітна плата, грн.;

Тсер – ставка кожного співробітника, грн./год;

Nроб – кількість працівників, людей;

В – кількість годин, витрачених на роботу над проектом, год.

Результати розрахунків представлені в таблиці 5.4.

Таблиця 5.4 – Заробітна плата

Найменування	Заробітна плата, грн.
інженер технічного забезпечення проекту	3120
інженер електронної техніки	14400
Разом	17520

5.3 Розрахунок кошторису витрат

Кошторис витрат складається виходячи з таких показників: основні засоби (комп'ютер з програмним забезпеченням), заробітна плата, відрахування до єдиного фонду – 37%; накладні витрати (60…150% від фонду заробітної плати), які включають різні господарські та адміністративні витрати.

Далі наводиться вартість устаткування і програмного забезпечення, представлені в таблиці 5.5.

Таблиця 5.5 – Вартість устаткування і програмного забезпечення

Найменування	Ед.вим.	К-ть	Ціна, грн.	Вартість, грн.
Комп'ютер	шт	1	18000,00	18000,00
Програмне забезпечення	шт	1	2500	2500
Разом				20500

Амортизація основних засобів (комп'ютер) [16]:

$$S_{ам} = \sum \frac{\alpha_{ам}}{100} \cdot вартість \cdot \frac{T_{вик}}{T_{можл.вик.}} \quad (5.2)$$

$$S_{аморт} = 0,15 \times 18000 \times (24 \times 8/2100) = 246,8 \text{ грн.}$$

Електроенергія, що витрачається при роботі інженера електронної техніки:

$$S_e = \text{тариф} \times \text{потужність} \times N \times T_{вик} \quad (5.3)$$

де N – кількість комп'ютерів, осцилографів, мультиметрів

$$S_e = 4,32 \times 0,25 \times 1 \times 192 = 207,4 \text{ грн.}$$

Кошторис витрат на розробку системи моніторингу напруги представлений в таблиці 5.6.

Таблиця 5.6 – Кошторис витрат

№ з/п	Найменування	Разом:
1	Вартість програмного забезпечення	2500
2	Основні засоби	18000
3	Амортизаційні відрахування	246,8
4	Витрати на електроенергію (машинний час)	207,4
5	Заробітна плата	17520
6	Відрахування 37%	6482,4
	Всього	44956,6

Економічні розрахунки підтвердили доцільність розробки системи моніторингу напруги для використання її в умовах серійного виробництва.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було здійснено комплексне дослідження, спрямоване на розробку ефективної системи моніторингу напруги на основі мікроконтролера. Основними результатами проведенного дослідження є наступні:

1. Проведено огляд технологій Інтернету речей, зокрема, їх застосування у сферах моніторингу та контролю, а також проаналізовано питання безпеки IoT-пристроїв. Особливу увагу приділено ризикам, які виникають при використанні IoT-систем, та заходам, які необхідно реалізувати для їхньої мінімізації.

2. Проведено детальний аналіз принципів роботи, типів схем моніторингу напруги та можливостей сучасних мікроконтролерів. Встановлено, що далеко не всі мікроконтролери підходять для даного завдання через відсутність критично важливих функціональних блоків, таких як бездротовий звязок та модулі швидких обчислень. На основі цього аналізу обрано оптимальну платформу для реалізації проєкту на основі ESP32.

3. Розроблено апаратну та програмну частини системи моніторингу напруги на основі обраного мікроконтролера. Проведено математичне моделювання вхідного блоку, що дозволило оптимізувати параметри схеми та забезпечити її відповідність поставленим вимогам. Система має високу точність вимірювання, здатність реєстрації аномальних подій та інтеграцію з базами даних для подальшого аналізу.

4. Виконано економічні розрахунки, які підтвердили доцільність впровадження розробленого пристрою у серійне виробництво. Розрахунки показали, що розробка є економічно вигідною, враховуючи її конкурентоспроможність, функціональні можливості та потенціал для застосування у різних галузях.

5. Розроблено комплекс заходів з охорони праці, спрямованих на створення безпечних умов роботи для розробників системи. Враховано всі

потенційно шкідливі фактори, характерні для роботи у лабораторних умовах, та запропоновано ефективні методи їхньої мінімізації.

Таким чином, виконана робота дозволила створити сучасний, функціональний та безпечний пристрій моніторингу напруги, що відповідає всім вимогам. Отримані результати демонструють перспективність застосування розробленої системи як у промислових, так і у побутових умовах, забезпечуючи надійність, точність та безпеку її роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Звіт: обсяг з'єднань підключених пристроїв IoT перевищує звичайні підключення до Інтернету [Електронний ресурс]. - Режим доступу: https://internetua.com/zvit-obsyag-z-yednan-pidkluacsenih-pristroyiv-iot-perevisxuye-zvicsaini-pidkluacsennya-do-internetu?utm_source=ukrnet_news

2. Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security by Perry Lea (Author)/ Packt Publishing - ebooks Account (January 22, 2018), 524 pages

3. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

4. Raspberry-PI 4 [Електронний ресурс]. - Режим доступу: https://evo.net.ua/mikrokomputer-raspberry-pi-4-model-b-8gb/

5. Як ESP32 IoT змінює гру для підключених пристроїв [Електронний ресурс]. - Режим доступу: https://www.dusuniot.com/uk/blog/how-esp32-iot-is-changing-the-game-for-connected-devices/

6. Dusun IoT - Born for Secure, Stable and Smart IoT Gateways [Електронний ресурс]. - Режим доступу: https://www.dusuniot.com

7. Плата BeagleBone AI-64 [Електронний ресурс]. - Режим доступу: https://vseplus.com/ua/product/beaglebone-ai-64-270801

8. Сервіс thingspeak [Електронний ресурс]. - Режим доступу: https://thingspeak.mathworks.com/

9. Сервіс beebotte [Електронний ресурс]. - Режим доступу: https://beebotte.com/

10. Використання моделі Isolation Forest для виявлення аномалій у даних вимірювань [Електронний ресурс]. - Режим доступу: https://itssi-journal.com/index.php/ittsi/article/view/473

11. LiteRT overview [Електронний ресурс]. - Режим доступу: https://ai.google.dev/edge/litert

12. KiCad EDA [Електронний ресурс]. - Режим доступу: https://www.kicad.org/

13. Easy-to-use & Free PCB Design Software [Електронний ресурс]. - Режим доступу: https://easyeda.com

14. САПР LibrePCB [Електронний ресурс]. - Режим доступу: https://librepcb.org/

15. САПР DipTrace [Електронний ресурс]. - Режим доступу: https://diptrace.com/ua/

16. Основи охорони праці: Л. Е. Винокурова, М. В. Васильчук, М. В. Гаман / Підручн. Для проф. - техн.. навч. Закладів. - 2-ге вид., допов., перероб. - К.: Вікторія, 2001. - 192 с.

17. Правила влаштування електроустановок. - Х.: Изд-во "Форт", 2009. 704 с.

18. НАПБ Б.03.002-2007 Норми визначення категорій приміщень, будівель та зовнішніх установок щодо вибухопожежної та пожежної небезпеки.

19. СНиП 2.01.02-85. Протипожежні норми.

20. Теорія з розрахунку захисного заземлення. [Електронний ресурс]. - Режим доступу: http://www.mastercity.ru /vforum/attachment.php?s= d0ae-aac68c0fd51 1e7430d2a5b 22a6dd& attachmentid=13256&d=1166795840

21. Економіка і організація виробництва: навчальний посібник для здобувачів ступеня бакалавра за технічними та інженерними спеціальностями / Петренко К. В., Скоробогатова Н. Є. - К.: КПІ ім. Ігоря Сікорського, 2019. – 177 с.

Формат	Зона	Поз.	Позначення	Найменування	Кіл.	Примітка
				Документація		
A1			ЕІСПЗ М.23329.00.00.00.00.Д1	Дослідження та розробка систем IoT		
				Постановка завдання	1	
A1			ЕІСПЗ М.23329.00.00.00.00.Д2	Дослідження та розробка систем IoT		
				Апаратні платформи	1	
A1			ЕІСПЗ М.23329.00.00.00.00.Д3	Дослідження та розробка систем IoT		
				Схемні рішення	1	
A1			ЕІСПЗ М.23329.00.00.00.00.Д4	Дослідження та розробка систем IoT		
				Моделювання	1	
A1			ЕІСПЗ М.23329.00.00.00.00.Е1	Дослідження та розробка систем IoT		
				Схема електрична структурна	1	
A1			ЕІСПЗ М.23329.00.00.00.00.Е3	Дослідження та розробка систем IoT		
				Схема електрична принципова	1	
A1			ЕІСПЗ М.23329.00.00.00.00.Д5	Дослідження та розробка систем IoT		
				Алгоритми роботи пристрою	1	
A1			ЕІСПЗ М.23329.00.00.00.00.Д6	Дослідження та розробка систем IoT		
				Охорона праці	1	

Перв. застосув.

Довід. №

Підп. і дата

Інв. № дубл.

Взам. інв. №

Підп. і дата

Інв. № подл.

Зм.	Арк.	№ докум.	Підп.	Дата
Розроб.		Грідін		2.12.24
Перевір.		Шмалій		2.12.24
Н.контр.		Туришев		2.12.24
Затверд.		Критська		2.12.24

ЕІСПЗ М.23329.00.00.00.00

Дослідження та розробка систем IoT

Літ.	Аркуш	Аркушів
		1

ІННІ ім. Ю.М. Потебні ЗНУ

8.1713

Копіював

Формат А4

Зона	Поз. позначення	Найменування	Кіл.	Примітка
	A1	Блок ESP32	1	Espressif Systems
		Конденсатори		
	C1	К73-5-0.1 мкФ 50В +/-5%Д1	1	
	C2	KF 1000 мкФ 25В	1	Capxon
	C3	KF 100 мкФ 25В	1	Capxon
	C4	К73-5-0.1 мкФ 50В +/-5%	1	
	DA1	Мікросхема LM7805	1	TI
	FU1	Запобіжник 220В 1А	1	
	R1	Резистор С5 - 0.25 - 10кОм +/-5%	1	
	R2	Резистор С5 - 0.25 - 20кОм +/-5%	1	
	R3	Резистор С5 - 0.25 - 51кОм +/-5%	1	
	R4	Резистор С5 - 0.25 - 1кОм +/-5%	1	
	VD1..VD4	Діодний міст DB107S	1	Fairchild Semiconductor
	VD5	Стабілітрон 1N4728	1	Fairchild Semiconductor
	TV1	Трансформатор ТТП 220/6	1	

Перв. застосув. | Довід. № | Підп. і дата | Інв. № дубл. | Взам. інв. № | Підп. і дата | Інв. № подл.

Зм.	Арк.	№ докум.	Підп.	Дата
Розроб.		Грідін		2.12.24
Перевір.		Шмалій		2.12.24
Н.контр.		Турищев		2.12.24
Затверд.		Критська		2.12.24

ЕІСПЗ М.23329.00.00.00 ПЕЗ

Дослідження та розробка систем IoT

Перелік елементів

Літ.	Аркуш	Аркушів
		1

ІННІ ім. Ю.М. Потебні ЗНУ

8.1713

Копіював

Формат А4