Центральноукраїнський національний технічний університет
Факультет будівництва, транспорту та енергетики
Кафедра «Автоматизації виробничих процесів»

«Допущено до захисту»
Зав. кафедри АВП
к.т.н., доцент
_____Олександр ДІДИК
“___“ _____2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти

на тему:
Дослідження та програмна реалізація системи управління розумним будинком з впровадженням системи захисту від кібератак

Виконав здобувач ІІ курсу групи АК-24М
ОПП «Автоматизація та комп’ютерно-інтегровані технології»
спеціальності 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка»
_____ Олександр ПАЛЬОННИЙ
«___»_____ 2025 р.

Керівник проекту
доцент, канд.техн.наук
_____ Ірина БЕРЕЗЮК
«___»_____ 2025 р.

Рецензент
_____ Іван САВЕЛЕНКО
«___»_____ 2025 р.

м. Кропивницький

Центральноукраїнський національний технічний університет

Факультет *будівництва, транспорту та енергетики*
Кафедра *автоматизації виробничих процесів*
Рівень вищої освіти *магістр*
Галузь знань *17 Електроніка, автоматизація та електронні комунікації*
Спеціальність *174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»*
Освітньо-професійна програма *«Автоматизація та комп'ютерно-інтегровані технології»*

ЗАТВЕРДЖУЮ

Завідувач кафедри Дідик О.К.

_____

"___" ___2025 року

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Пальонного Олександра Олександровича
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи управління розумним будинком з впровадженням системи захисту від кібератак*
2. Керівник роботи *Березюк Ірина Анатоліївна, канд. техн. наук, доцент,*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

3. Строк подання студентом роботи до захисту *02.12.2025 р.*

4. Мета та завдання випускної кваліфікаційної роботи *Метою розробки є програмне дослідження та програмна реалізація систем управління розумним будинком з впровадженням системи захисту 1. Призначення системи; 2. Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми магістерської роботи; 3. Опис функціонування системи; 4. Реалізація роботи. розрахунки і експериментальні дані, що підтверджують вірність проектних та програмних рішень. впровадження системи в промислову експлуатацію.*

5. Консультанти по роботі, із зазначенням розділів роботи

Розділ	Консультант	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	*Жесан Р.В.*		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Сучасний стан технології і засобів автоматизації*	*15.10.25*	
	для систем управління розумним будинку		
2.	*Аналіз об'єкту управління та розробка структурної*	*30.10.25*	
	схеми системи управління та захисту		
3.	*Перегляд аналогічних існуючих систем*	*05.11.25*	
3.	*Опис і обґрунтування проектних рішень*	*15.11.25*	
4.	*Практична реалізація системи управління розумним будинком з впровадженням системи захисту від кібератак*	*30.11.25*	

Дата видачі завдання 01.09.2025 р.

Керівник роботи _____ І.А. Березюк «____» _____2025 р.

Завдання прийнято до виконання

Здобувач _____ О.О. Пальонний «____» _____2025 р.

АНОТАЦІЯ

на випускну кваліфікаційну роботу студента групи АК-24М Пальонного Олександра Олександровича зі спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» на тему: «Дослідження та програмна реалізація системи управління розумним будинком з впровадженням системи захисту від кібератак».

Випускна кваліфікаційна робота присвячена дослідженню, розробці та програмній реалізації системи управління «розумним будинком» із впровадженням засобів захисту від кібератак. У роботі розглянуто сучасні тенденції розвитку технологій Інтернету речей (IoT), принципи побудови систем автоматизованого управління побутовими пристроями, а також питання кібербезпеки у сфері «розумного» житла.

Проведено аналіз архітектури системи «розумного будинку», визначено основні вимоги до апаратної та програмної частини. Розроблено структуру системи управління, яка включає мікроконтролерний модуль, сенсорну мережу та програмне забезпечення для моніторингу й керування пристроями.

Об'єктом дослідження є процес забезпечення управлінням «розумним будинком».

Предметом дослідження є методи забезпечення управління системами розумного будинку.

У результаті виконаної роботи створено діючу модель системи «розумного будинку», яка забезпечує автоматизоване керування освітленням, температурою, системами безпеки та доступу. Запропоновано заходи з підвищення кіберстійкості, що базуються на принципах шифрування даних, автентифікації користувачів і контролю доступу.

Робота має практичне значення, оскільки запропоновані рішення можуть бути використані при розробці побутових IoT-систем та навчанні

студентів спеціальності 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка».

Ключові слова: розумний будинок, Інтернет речей, автоматизація, система управління, кібербезпека, захист від кібератак, мікроконтролер.

ABSTRACT

on final qualification work of the student of the AK-24M group, Oleksandr Oleksandrovich Palyonny, majoring in 174 "Automation, Computer-Integrated Technologies and Robotics" on the topic: "Research and software implementation of a smart home control system with the implementation of a cyberattack protection system".

The final qualification work is devoted to the research, development and software implementation of a "smart home" control system with the implementation of cyberattack protection.

The work considers modern trends in the development of Internet of Things (IoT) technologies, the principles of building automated control systems for household appliances, as well as cybersecurity issues in the field of "smart" housing.

An analysis of the architecture of the "smart home" system was carried out, the main requirements for the hardware and software were determined.

The structure of the control system was developed, which includes a microcontroller module, a sensor network and software for monitoring and controlling devices.

The object of the study is the process of ensuring the management of a "smart house".

The subject of the study is methods for ensuring the management of smart house systems.

As a result of the work performed, a working model of a "smart house" system was created, which provides automated control of lighting, temperature, security and access systems. Measures to increase cyber resilience are proposed, based on the principles of data encryption, user authentication and access control.

The work is of practical importance, since the proposed solutions can be used in the development of household IoT systems and training students of specialty 174 "Automation, computer-integrated technologies and robotics".

Keywords: automation, microprocessor system, pumping station, control, modernization, energy efficiency, smart house.

ЗМІСТ

ВСТУП

Актуальність теми. З початку нового тисячоліття людство вступило в епоху стрімкого технологічного прогресу, однією з ключових ознак якого є розвиток побутової автоматизації. У сучасному світі час стає одним із найцінніших ресурсів людини, тому системи автоматизованого керування типу «розумний будинок» мають велике практичне значення, адже дозволяють суттєво заощаджувати цей ресурс. Такі системи здатні виконувати широкий спектр завдань - від увімкнення кондиціонера чи освітлення до активації нічної сигналізації, забезпечуючи комфорт і безпеку мешканців.

Однак одним із недоліків подібних пристроїв залишається їх висока вартість, що обмежує доступність для широкого кола користувачів. Саме тому створення відносно недорогої системи «розумного будинку» з аналогічним функціоналом є актуальним і перспективним напрямом досліджень.

Починаючи з 2010 року, технології «розумного дому» набули значного поширення в суспільстві, оскільки дозволяють зменшити витрати часу та коштів. Інноваційні розробки у цій сфері спрямовані не лише на підвищення комфорту, а й на покращення енергоефективності будівель. Прості приклади такої автоматизації можна спостерігати навіть у звичних побутових приладах - наприклад, у холодильнику, де освітлення вмикається при відкритті дверцят і автоматично вимикається після їх зачинення. Такий підхід сприяє зменшенню нераціонального використання електроенергії, що є особливо важливим з огляду на постійне зростання цін на енергоресурси.

Сучасні проєкти «розумних будинків» передбачають інтеграцію цілої мережі взаємопов’язаних модулів, розташованих у різних зонах житла. Кожен із таких пристроїв функціонує як мінікомп’ютер, об’єднаний у спільну систему керування. Завдяки цьому власник має можливість персоналізувати параметри навколишнього середовища, оперативно змінювати налаштування освітлення, температури чи навіть інтер’єру. У деяких рішеннях автоматизація

поширюється настільки, що людина майже не бере участі в управлінні побутовими процесами - система самостійно контролює споживання ресурсів, зберігання продуктів та інші повсякденні функції.

Метою даної роботи є дослідження та програмна реалізація системи керування “розумним будинком” із впровадженням підсистеми безпеки передачі даних.

Для досягнення поставленої мети було визначено такі основні **завдання дослідження:**

– провести аналіз існуючих систем керування “розумним будинком”, що включають підсистеми безпеки передачі даних;

– виконати дослідження принципів побудови систем керування “розумним будинком”;

– здійснити програмну реалізацію системи керування “розумним будинком” із підсистемою захисту та безпеки передачі даних.

Об’єктом дослідження є процес керування “розумним будинком”.

Предметом дослідження виступають методи розробки та реалізації систем керування “розумним будинком”.

Методологічна основа дослідження базується на методах теорії кодування, автоматизації, методах захисту інформації, математичної статистики, а також на сучасних підходах до розробки програмного забезпечення та систем автоматизації.

Наукова новизна отриманих результатів

У процесі виконання дослідження було досягнуто таких результатів:

– удосконалено систему керування “розумним будинком” шляхом інтеграції підсистеми безпеки передачі даних;

– проведено аналіз сучасних технологій зв’язку, що використовуються у системах типу “Smart Home”;

– розроблено вітчизняне програмне рішення системи керування “розумним будинком” із підсистемою безпеки, яке має ширші функціональні можливості порівняно з існуючими аналогами.

Практична цінність отриманих результатів

Практичне значення виконаної роботи полягає у тому, що розроблені алгоритми та програмні рішення дозволяють ефективно реалізувати системи керування технологіями “розумного будинку”, забезпечуючи підвищений рівень безпеки передачі даних і надійність роботи системи.

Достовірність результатів

Достовірність отриманих наукових результатів підтверджується теоретичними обґрунтуваннями, результатами комп’ютерного моделювання, експериментальними дослідженнями параметрів на діючій обчислювальній мережі, а також узгодженістю отриманих результатів із даними, наведеними в науковій літературі.

Таким чином, проведене дослідження та програмна реалізація системи керування “розумним будинком” із підсистемою безпеки передачі даних є актуальним та практично значущим завданням, розв’язання якого має важливе наукове та прикладне значення.

Основні результати досліджень викладені в одній науковій публікації.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1. Призначення системи

Системи типу «Розумний будинок»

Системи «Розумний будинок» (Smart Home, або домашня автоматизація) належать до одного з найбільш перспективних напрямів розвитку сучасних інформаційних та комунікаційних технологій. Такі системи забезпечують інтеграцію та взаємодію всіх електронних і побутових пристроїв будівлі, надаючи можливість централізованого керування ними як вручну - за допомогою пульта, сенсорної панелі чи мобільного застосунку, - так і автоматично, на основі попередньо визначених алгоритмів.

Мета роботи

Метою даної магістерської роботи є дослідження, проєктування та програмна реалізація системи керування «розумним будинком» із підсистемою безпеки передачі даних і захисту від кібератак.

Завдання дослідження

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз сучасних технологій і стандартів у сфері «розумних будинків» та засобів забезпечення безпеки передачі даних;

– розробити архітектуру системи, яка охоплюватиме модулі керування побутовими пристроями та підсистему кіберзахисту;

– створити програмне забезпечення для реалізації функцій керування та моніторингу із захистом даних від несанкціонованого доступу;

– здійснити тестування, налагодження та валідацію системи в умовах реального середовища;

– оцінити ефективність розробленої системи за критеріями продуктивності, зручності та безпеки.

Очікуваний результат

Результатом виконання роботи є ефективна, надійна та безпечна система управління розумним будинком, що відповідає сучасним вимогам технологічного розвитку, енергоефективності та кібербезпеки.

1.2 Огляд засобів автоматизації та область застосування

Характеристика розроблюваної системи

Розроблена система керування “розумним будинком” із підсистемою безпеки передачі даних передбачає реалізацію таких основних принципів та функціональних можливостей:

– впровадження базових концепцій у сфері інтелектуальної автоматизації житлових приміщень;

– наявність унікального функціоналу, який відрізняє її від наявних аналогів і забезпечує підвищену ефективність роботи;

– простота, доступність і надійність завдяки використанню мінімалістичного інтерфейсу та оптимізованої архітектури;

– зручність розгортання та налаштування, що дозволяє впроваджувати систему навіть користувачам без спеціальної технічної підготовки;

– підтримка автономного режиму роботи з можливістю інтеграції у хмарні сервіси для розширення функціональності та дистанційного керування.

Таким чином, дослідження та програмна реалізація системи керування “розумним будинком” із підсистемою безпеки передачі даних і захистом від кібератак є актуальним і практично значущим завданням, вирішення якого має важливе значення для подальшого розвитку технологій автоматизації побуту, енергоефективності та кіберзахисту.

Огляд існуючих систем

Системи типу «Розумний будинок»

Smart Home (розумний будинок або розумна будівля) - це сучасна концепція автоматизованого житлового або комерційного приміщення, у якому всі електронні пристрої взаємопов’язані між собою в єдину систему. Такі пристрої інтегруються у комп’ютерну мережу, що забезпечує їх централізоване керування, координацію дій та можливість дистанційного доступу через Інтернет. Завдяки цьому користувач отримує змогу контролювати роботу системи як локально, так і віддалено, використовуючи комп’ютер, планшет або смартфон.

Інтеграція інформаційних технологій у побут створює умови, за яких системи та пристрої здатні автоматично координувати виконання своїх функцій відповідно до заданих сценаріїв, алгоритмів і зовнішніх умов (температури, освітленості, часу доби тощо).

Особливості проектування системи

Розроблення системи «розумного будинку» вимагає професійного планування, проектування та програмування, які виконуються спеціалізованими компаніями. Алгоритми функціонування багатокімнатного «розумного будинку» формуються відповідно до індивідуальних потреб користувачів та специфіки середовища. Завдяки цьому користувач може створити бажану атмосферу одним натисканням кнопки, а система - самостійно аналізує навколишні умови та виконує необхідні дії згідно із закладеними сценаріями.

Побутові прилади, встановлені у такому будинку, можуть бути об’єднані в єдину домашню мережу на основі стандарту Universal Plug and Play (UPnP), що забезпечує автоматичне підключення пристроїв і доступ до них через мережу Інтернет.

Переваги та недоліки технології

Попри численні переваги - зручність, енергоефективність, безпеку та економію ресурсів - технологія «розумного будинку» має певні ризики та недоліки, серед яких:

– залежність від доступу до Інтернету, що може призвести до обмеження функціональності при відсутності зв’язку;

– недостатня зрілість технології, оскільки вона все ще перебуває на етапі активного розвитку й стандартизації.

Сучасні тенденції розвитку

На сьогодні існує значна кількість спеціалізованих платформ і протоколів для організації локальних мереж у системах «розумного будинку». Вони забезпечують взаємодію між різними типами пристроїв, часто використовуючи власні закриті стандарти. Проте останнім часом спостерігається тенденція до відкритості, і на ринку з’являються системи з відкритим вихідним кодом, що підтримують роботу з широким спектром обладнання та дають змогу розробникам і користувачам гнучко адаптувати систему під власні потреби.

Схематичне зображення типової інтеграції подібних систем наведено на рисунку 1.1.

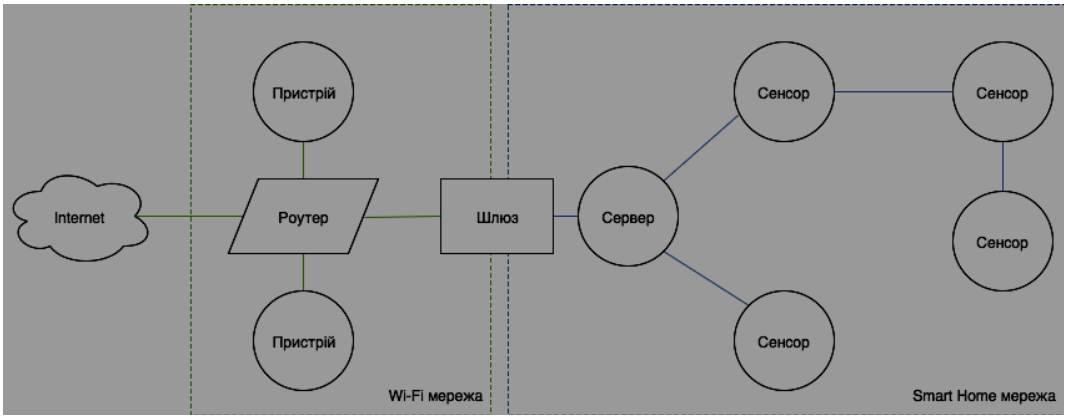


Рисунок 1.1 – Типова структура Smart Home системи

Використання стандартних комунікаційних технологій у системах «Розумний будинок»

Окрім спеціалізованих протоколів, у системах типу «Розумний будинок» часто застосовуються й стандартні бездротові технології зв’язку, такі як Wi-Fi та Bluetooth. Їх використання дозволяє розширити функціональні можливості системи, забезпечити сумісність із широким спектром пристроїв і спростити реалізацію комплексного управління.

Використання цих технологій сприяє підтримці єдиної архітектури системи, однак водночас ставить нові вимоги та виклики щодо забезпечення кібербезпеки, енергоефективності та надійності передавання даних.

Важливе значення має також топологія мережі, що визначає ефективність зв’язку між пристроями. У будівлях зі складним плануванням, великою кількістю бетонних або металевих конструкцій можуть виникати проблеми з радіопокриттям і стабільністю сигналу. Це потребує врахування особливостей розміщення пристроїв та оптимізації конфігурації мережі під час проєктування системи.

У подальших підрозділах буде наведено детальний аналіз найпоширеніших комунікаційних протоколів, що застосовуються в сучасних системах типу «Розумний дім», а саме: ZigBee, Wi-Fi та Bluetooth.

Протокол ZigBee. Створення та роль альянсу ZigBee

ZigBee Alliance - це міжнародна організація, яка об’єднує розробників, виробників та постачальників технологій для розвитку й стандартизації бездротового протоколу ZigBee. Головним завданням альянсу є створення технічних специфікацій, профілів застосувань та супровідної документації, необхідної для розробки сумісних пристроїв і забезпечення їх взаємодії у межах єдиної екосистеми.

Розробка стандарту відбувалася на основі узгоджених технічних рішень і практичних потреб галузі. Перша специфікація ZigBee 1.0 була ратифікована 14 грудня 2004 року, а оновлена версія ZigBee 2007 опублікована 30 жовтня 2007 року. Саме тоді з’явився перший офіційний

профіль застосування - «Home Automation», який визначив стандарти автоматизації побутових процесів.

Основні характеристики технології ZigBee

Протокол ZigBee базується на стандарті IEEE 802.15.4-2006, який призначений для організації бездротових персональних мереж (WPAN) з низьким енергоспоживанням і невеликою швидкістю передачі даних. Його ключовими перевагами є:

- самоорганізація мережі - пристрої автоматично виявляють один одного та формують стійку мережеву структуру без необхідності ручного налаштування;
- самовідновлення мережі - у разі збою або втрати зв'язку з окремими вузлами система здатна перебудувати маршрути передачі даних;
- низьке енергоспоживання - більшу частину часу пристрої перебувають у режимі сну, що значно подовжує строк роботи батареї;
- висока швидкість активації - перехід пристрою зі сплячого в активний режим триває менше 30 мс, що забезпечує мінімальні затримки обміну даними;
- економічність та простота реалізації - порівняно з іншими бездротовими протоколами, такими як Bluetooth, ZigBee є більш дешевим і менш енергозатратним рішенням для побутової автоматизації.

Архітектура та технічні параметри

Технологія ZigBee використовує неліцензовані частотні діапазони ISM:

- 868 МГц - для країн Європи;
- 915 МГц - для США та Австралії;
- 2,4 ГГц - для більшості країн світу.

Більшість мікросхем ZigBee поєднують у собі радіомодуль і мікроконтролер із флеш-пам'яттю обсягом від 60 до 128 КБ. Таке об'єднання дозволяє виробляти компактні й енергоефективні пристрої. При цьому виробники пропонують готове програмне забезпечення або відкриті бібліотеки для інтеграції в різні проєкти.

Сфера застосування

ZigBee знайшов широке застосування у таких напрямках:

- домашня автоматизація (Home Automation);
- раціональне використання енергії (Smart Energy 1.0/2.0);
- автоматизація комерційних будівель;
- телекомунікаційні системи;
- персональне спостереження та моніторинг;
- дистанційне керування пристроями.

Відносини між IEEE 802.15.4 та ZigBee можна порівняти з відносинами між IEEE 802.11 та Wi-Fi Alliance: перший визначає фізичний і канальний рівні зв'язку, тоді як другий - забезпечує стандартизацію прикладних профілів і сумісність пристроїв.

Типи пристроїв у мережі ZigBee

У типовій ZigBee-мережі використовуються три типи пристроїв, які взаємодіють між собою для забезпечення стабільної роботи:

1. Координатор (ZigBee Coordinator) - головний вузол, який ініціює створення мережі, керує її структурою та зберігає інформацію про маршрути.
2. Маршрутизатор (Router) - забезпечує передачу даних між вузлами мережі та підтримує розширення зони покриття.
3. Кінцевий пристрій (End Device) - енергозберігаючий вузол, який взаємодіє з мережею через маршрутизатор або координатор і виконує конкретні функції (наприклад, керування освітленням або сенсорну фіксацію).

Таким чином, ZigBee є однією з найважливіших технологій у сфері «розумних будинків». Її переваги - енергоефективність, самостійна організація, надійність і низька вартість реалізації - роблять її оптимальним вибором для систем автоматизації, моніторингу та дистанційного керування пристроями в побутових і промислових умовах.

Типи пристроїв у мережі ZigBee

Мережа ZigBee складається з трьох основних типів пристроїв, кожен із яких виконує специфічні функції в межах загальної структури мережі (рисунок 1.2).

Координатор ZigBee (ZC, ZigBee Coordinator) Координатор є центральним вузлом мережі, який ініціює її створення та визначає базову топологію - зокрема деревоподібну або сіткову структуру. У кожній мережі повинен бути щонайменше один координатор, який виконує такі функції:

– формує та підтримує таблицю маршрутизації;

– зберігає параметри мережі (ідентифікатор PAN, канали, ключі доступу тощо);

– виконує роль довіреного центру (Trust Center), що відповідає за автентифікацію вузлів та зберігання криптографічних ключів;

– забезпечує взаємодію з іншими мережами або шлюзами, зокрема дротовими системами (наприклад, Ethernet).

Маршрутизатор ZigBee (ZR, ZigBee Router) Маршрутизатор виконує функцію проміжного вузла, який передає дані між іншими пристроями, розширюючи покриття мережі. Основні функції маршрутизатора:

– передача пакетів даних від кінцевих пристроїв до координатора або до інших маршрутизаторів;

– підтримка динамічної маршрутизації для забезпечення самовідновлення мережі;

– можливість запуску додатків на рівні користувача (наприклад, керування окремими пристроями чи сенсорами).

Кінцевий пристрій ZigBee (ZED, ZigBee End Device) Кінцевий пристрій має мінімальний набір функцій, що забезпечує його економічність та низьке енергоспоживання. Він може обмінюватися даними лише з вузлом вищого рівня (координатором або маршрутизатором), але не бере участі у передачі даних інших пристроїв. Головні особливості ZED:

– робота в енергозберігаючому режимі з можливістю тривалого перебування у сплячому стані;

– низькі вимоги до обсягу пам’яті;

– мінімальна вартість виробництва порівняно з координаторами та маршрутизаторами.

Таким чином, завдяки поділу пристроїв за функціональним призначенням, технологія ZigBee забезпечує гнучкість побудови мережі, низьке енергоспоживання та високу надійність обміну даними.

Приклад типової ZigBee-мережі з інтеграцією дротової мережі Ethernet наведено на рисунку 1.2.

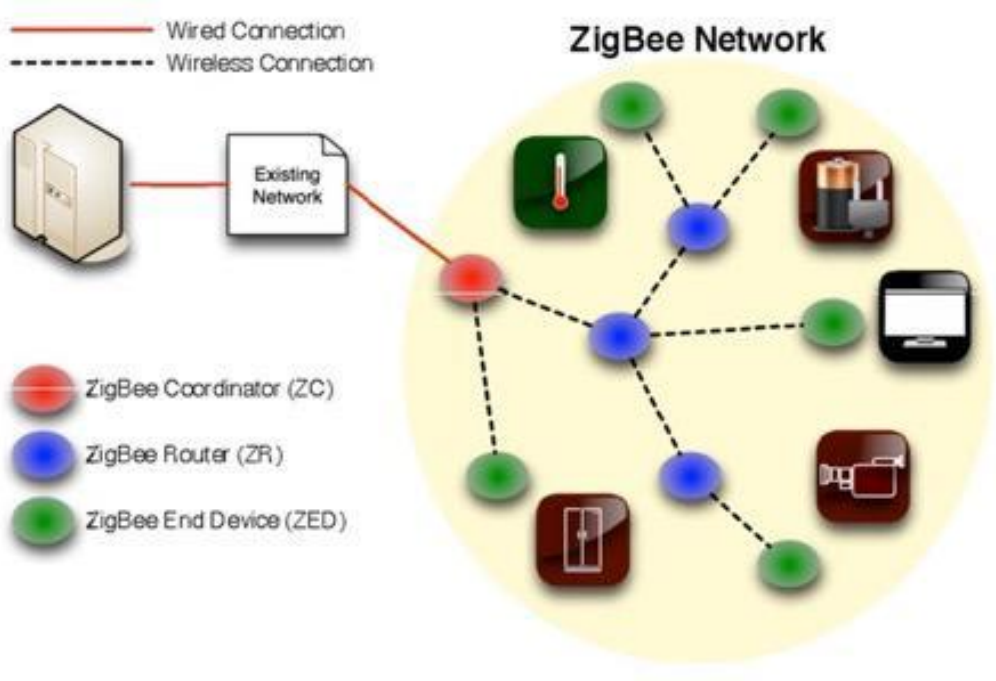


Рисунок 1.2 – Мережа ZigBee інтегрована з мережею Ethernet

Переваги та недоліки технології ZigBee

На завершення розгляду технології ZigBee доцільно узагальнити її ключові переваги та недоліки, що визначають доцільність використання даного протоколу в системах «Розумний будинок».

Основні переваги технології ZigBee:

– низьке енергоспоживання. Пристрої ZigBee здатні працювати тривалий час у режимі сну, активуючись лише під час передачі даних, що забезпечує ефективне використання енергії батарей.

– масштабованість мережі. Завдяки можливості створення розгалуженої сітчастої або деревоподібної топології забезпечується збільшення дальності передачі даних і кількості вузлів у мережі.

– швидкий вихід із режиму очікування. Пристрої ZigBee характеризуються коротким часом відновлення зв'язку при ініціалізації — близько 30 мс.

Підтримка різних топологій. Мережа може працювати у формі «зірки», «дерева» або «mesh»-структури з можливістю самовідновлення у випадку втрати зв'язку між вузлами.

Основні недоліки технології ZigBee:

– обмежена сумісність із іншими пристроями. Більшість персональних комп'ютерів і смартфонів не мають вбудованих адаптерів ZigBee, що ускладнює інтеграцію з популярними технологіями.

– необхідність додаткового обладнання. Для взаємодії з іншими мережами часто потрібен шлюз або адаптер Wi-Fi/ZigBee.

– низький рівень уніфікації стандартів. Існують відмінності у реалізації протоколів різними виробниками, що може призводити до проблем із сумісністю.

– обмежена пропускна здатність. Порівняно з Wi-Fi, швидкість передачі даних у ZigBee є невисокою (до 250 кбіт/с), що обмежує його використання у додатках із великими обсягами інформації.

Порівняння з технологією Wi-Fi

Для побудови комплексних систем «Розумний будинок» технологія ZigBee часто використовується у поєднанні з Wi-Fi, що дозволяє поєднати переваги обох підходів.

Wi-Fi - це технологія передачі цифрових даних через радіоканали, яка забезпечує високу пропускну здатність і широке покриття. У контексті систем Smart Home вона зазвичай використовується для зв’язку між шлюзом (контролером) і мережею Інтернет, тоді як ZigBee відповідає за взаємодію між локальними сенсорами та виконавчими пристроями.

Переваги Wi-Fi:

– висока швидкість передачі даних. Wi-Fi підтримує швидкості понад 100 Мбіт/с, що дозволяє передавати великі обсяги даних у реальному часі — наприклад, відеопотоки або мультимедіа.

– гнучкість у побудові мереж. Підтримується топологія «інфраструктури» з можливістю підключення кількох точок доступу, що забезпечує стабільне покриття у великих приміщеннях або офісах.

– широка сумісність. Майже всі сучасні мобільні пристрої, комп’ютери та мікроконтролери мають вбудовані Wi-Fi-модулі, що значно спрощує інтеграцію системи.

Обидві технології мають власні сфери застосування: ZigBee — у низькопотужних сенсорних мережах і системах автоматизації, тоді як Wi-Fi — для швидкої передачі великих обсягів даних і віддаленого доступу до мережі. Вибір технології залежить від поставлених цілей, масштабу системи та вимог до енергоефективності.

Структуру типової Wi-Fi-мережі з доступом до Інтернету наведено на рисунку 1.3.

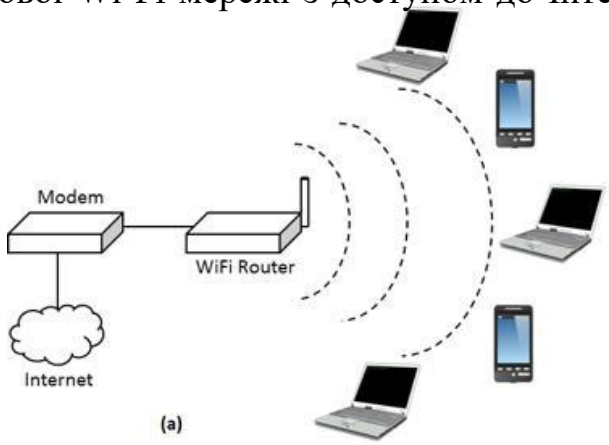


Рисунок 1.3 – Структурна схема звичайної Wi-Fi мережі

Технологія Wi-Fi Direct у системах «Розумний дім»

Wi-Fi Direct — це технологія бездротового зв’язку, що розширює можливості стандартного Wi-Fi, надаючи змогу встановлювати прямі з’єднання між пристроями без необхідності використання точки доступу або маршрутизатора. Завдяки цьому пристрої можуть взаємодіяти один з одним напряму, утворюючи локальні однорангові мережі (P2P, *peer-to-peer*), що значно спрощує обмін даними та розширює функціональність у межах «розумного будинку».

Основні особливості Wi-Fi Direct

– пряме з’єднання. Технологія дозволяє пристроям підключатися безпосередньо, минаючи центральні точки доступу, що знижує затримку передачі даних та підвищує ефективність обміну.

– масштабованість. Мережа Wi-Fi Direct може бути динамічно розширена за рахунок додавання нових пристроїв до існуючого з’єднання без складного налаштування.

– простота використання. Процес встановлення з’єднання подібний до підключення через Bluetooth, що робить технологію інтуїтивно зрозумілою навіть для користувачів без спеціальної технічної підготовки.

– широкий спектр застосувань. Використовується для обміну файлами, передачі аудіо- та відеопотоків, спільних ігор, друку документів тощо.

– сумісність із Wi-Fi. Пристрої, що підтримують Wi-Fi Direct, зберігають можливість підключення до звичайних Wi-Fi-мереж, що забезпечує гнучкість використання.

Переваги Wi-Fi Direct

– зручність та простота налаштування. Процес підключення не потребує додаткових мережевих пристроїв або складних конфігурацій.

– велика дальність передачі. Технологія забезпечує стабільне з’єднання на відстані до 100 метрів, що суттєво перевищує можливості Bluetooth.

– безпосередність зв’язку. Пристрої можуть швидко обмінюватися даними без підключення до Інтернету, що особливо корисно у випадках аварійного зв’язку або автономної роботи системи.

Використання у системах Smart Home

У контексті «розумного будинку» Wi-Fi Direct відкриває нові можливості для взаємодії між пристроями — наприклад, між смартфоном користувача, системами безпеки, мультимедійними центрами та побутовою технікою. Така технологія сприяє підвищенню автономності системи, зменшенню залежності від інтернет-з’єднання та створенню гнучких сценаріїв автоматизації.

Типи підключень Wi-Fi Direct у типових конфігураціях систем «Розумний дім» наведено на рисунку 1.4.

Рисунок 1.4 – Типи з’єднань Wi-Fi Direct

Принципи роботи Wi-Fi у бездротових мережах Smart Home

Технологія Wi-Fi (Wireless Fidelity) забезпечує бездротову передачу цифрових даних між пристроями в межах локальної або глобальної мережі. Її широке розповсюдження обумовлене високою швидкістю, надійністю та зручністю підключення. У системах «Розумний дім» Wi-Fi використовується для з’єднання контролерів, сенсорів, камер відеоспостереження та мобільних

пристроїв у єдину мережу, що забезпечує моніторинг і керування в реальному часі.

Ідентифікація мережі (SSID Broadcast)

Кожна точка доступу Wi-Fi періодично передає свій мережевий ідентифікатор SSID (Service Set Identifier) за допомогою керуючих кадрів (beacon frames). Ці сигнали дозволяють клієнтським пристроям розпізнавати наявні мережі та отримувати базову інформацію про них — назву мережі, тип шифрування, канал зв'язку, стандарт Wi-Fi тощо.

Передача ідентифікатора здійснюється на мінімальній швидкості 0,1 Мбіт/с, однак реальна швидкість залежить від стандарту Wi-Fi, який підтримує пристрій:

- IEEE 802.11b — до 11 Мбіт/с;
- IEEE 802.11g — до 54 Мбіт/с;
- IEEE 802.11n — до 600 Мбіт/с;
- IEEE 802.11ac — до 1 Гбіт/с і більше.

SSID не транслюється окремими пакетами, а вбудовується в керуючі та асоціаційні кадри, що використовуються під час встановлення та підтримки з'єднання між точкою доступу і клієнтським пристроєм. Знаючи SSID, клієнт може визначити, чи доступне підключення до конкретної мережі.

Перемикання між точками доступу (Roaming)

Під час переміщення користувача в зоні покриття кількох точок доступу з однаковим SSID, пристрій автоматично здійснює перемикання (roaming) для підтримання оптимального рівня сигналу. Це дозволяє забезпечити стабільність з'єднання, безперервну передачу даних та високу якість роботи мережі.

Процес роумінгу є важливим елементом у системах Smart Home, де безперервність з'єднання між контролерами, сенсорами та сервісами має критичне значення.

Можливості Wi-Fi у багатокористувацьких середовищах

Wi-Fi підтримує одночасне підключення кількох клієнтських пристроїв до однієї точки доступу, що дозволяє створювати локальні бездротові мережі для спільного доступу до ресурсів і даних. Це забезпечує взаємодію між численними пристроями розумного будинку — наприклад, смартфонами, мікроконтролерами, системами відеоспостереження, охоронними датчиками тощо.

Технологія Wi-Fi надає користувачеві повну свободу у виборі мережі або провайдера для підключення, що забезпечує гнучкість і сумісність при використанні пристроїв різних виробників.

Відстань передачі та вплив перешкод

Дальність передачі Wi-Fi сигналу залежить від потужності передавача, типу антени, стандарту зв'язку та особливостей середовища.

- у приміщеннях сигнал зазвичай поширюється на 30–50 метрів,
- на відкритих просторах — до 100 метрів і більше.

На якість сигналу впливають перешкоди у вигляді стін, перекриттів і металевих конструкцій, які спричиняють поглинання або відбиття хвиль, зменшуючи ефективну дальність передачі.

Wi-Fi є універсальною технологією бездротової комунікації, що поєднує високу швидкість передачі, надійність і простоту налаштування. Завдяки цим властивостям Wi-Fi широко використовується у системах «Розумний дім», забезпечуючи інтеграцію великої кількості пристроїв у єдину інтелектуальну мережу, керування якою може здійснюватися як локально, так і дистанційно.

Технологія Wi-Fi у системах «Розумний дім»

У системах Smart Home технологія Wi-Fi є одним із ключових засобів організації комунікації між пристроями. Вона забезпечує стабільну передачу даних, підтримує підключення багатьох користувацьких пристроїв і надає високий рівень інтеграції між компонентами системи.

Особливості використання Wi-Fi в «розумному будинку»

Можливість підключення декількох пристроїв. Зони Wi-Fi дають змогу користувачам одночасно підключати до мережі різні пристрої — комп'ютери, смартфони, контролери, побутову техніку тощо. Це створює комфортне середовище для взаємодії елементів системи та забезпечує централізоване керування.

Вплив на дальність передачі.

Радіус дії Wi-Fi залежить від потужності передавача, типу антени, наявності перешкод (стіни, бетон, металеві конструкції) та характеристик приймача. Ці чинники визначають реальні межі покриття точки доступу в межах будинку або офісу.

Регулювання програмної потужності.

Деякі моделі маршрутизаторів і Wi-Fi-модулів дозволяють програмно змінювати потужність передавання сигналу, що допомагає оптимізувати покриття, знизити споживання енергії та уникнути взаємних перешкод між кількома точками доступу.

Такі особливості є критично важливими для систем «Розумного дому», де якість зв'язку та стабільність сигналу безпосередньо впливають на ефективність роботи мережі автоматизації, безпеки й моніторингу.

Переваги технології Wi-Fi в системах Smart Home

Широка доступність і простота впровадження. Wi-Fi маршрутизатори є масово доступними, легко налаштовуються і сумісні з більшістю сучасних пристроїв, що спрощує інтеграцію системи «Розумний дім».

Підтримка різних режимів роботи.

Технологія Wi-Fi може функціонувати в режимах Ad-hoc та Wi-Fi Direct, забезпечуючи пряме з'єднання між пристроями без потреби у маршрутизаторі або модемі - це полегшує побудову автономних локальних мереж.

Високий рівень стандартизації.

Єдина архітектура Wi-Fi, визначена стандартами IEEE 802.11, забезпечує сумісність між пристроями різних виробників, що дозволяє гнучко розширювати систему та інтегрувати нові модулі.

Недоліки технології Wi-Fi в системах Smart Home

Високе енергоспоживання. Пристрої, що працюють через Wi-Fi, споживають більше енергії, ніж аналоги, що використовують Bluetooth або ZigBee, що зменшує тривалість автономної роботи сенсорів і контролерів на батарейному живленні.

Складність налаштування топології мережі.

Для забезпечення стабільного покриття іноді потрібно додаткове обладнання (репітери, точки доступу, контролери), а також ручна оптимізація каналів і потужності сигналу.

Надмірна швидкість передачі для деяких задач.

У більшості застосувань «розумного будинку» обсяг даних, що передається, є невеликим, тому висока швидкість Wi-Fi не завжди є перевагою - вона призводить лише до збільшення споживання енергії.

Залежність від потужності пристроїв.

Радіус дії та стабільність сигналу залежать від потужності передавачів і приймачів. Пристрої з низьким енергоспоживанням мають меншу дальність дії, що може знижувати надійність зв’язку.

Таким чином, Wi-Fi є універсальним рішенням для реалізації мережі «Розумного будинку», забезпечуючи зручність, високу швидкість і сумісність. Однак для енергообмежених систем, таких як бездротові датчики або автономні контролери, доцільно використовувати комбіновані підходи, поєднуючи Wi-Fi з енергоефективними технологіями - ZigBee, Bluetooth Low Energy або LoRaWAN.

Технологія Bluetooth у системах «Розумний дім»

Технологія Bluetooth є однією з найважливіших бездротових технологій, що широко використовується у системах «Розумний дім». Завдяки

своїй енергоефективності, простоті інтеграції та безпеці зв’язку, Bluetooth забезпечує надійну комунікацію між різними розумними пристроями — від сенсорів і контролерів до побутової техніки, систем доступу та мультимедійних пристроїв.

Ключові характеристики та переваги Bluetooth у Smart Home

– низьке енергоспоживання. Однією з головних переваг Bluetooth є його низька потужність роботи, особливо у режимі очікування. Це робить технологію оптимальною для пристроїв, що працюють на батарейках (наприклад, датчиків температури, замків чи фітнес-трекерів).

– зручна топологія мережі. Bluetooth підтримує просту процедуру підключення пристроїв (сполучення, *pairing*), що дозволяє легко створювати невеликі однорангові мережі без складного налаштування. Це спрощує використання технології у побутових умовах.

– висока швидкість передачі даних. Сучасні версії Bluetooth (наприклад, Bluetooth 5.0 і 5.3) забезпечують швидкість передачі даних до 2 Мбіт/с, що є достатнім для передачі аудіо-, відео- або сенсорної інформації в межах локальної мережі.

– безпека передачі даних. Для захисту комунікацій Bluetooth використовує шифрування та аутентифікацію пристроїв, що гарантує конфіденційність інформації та запобігає несанкціонованому доступу.

Частотне перестрибування (FHSS). Технологія Frequency-Hopping Spread Spectrum забезпечує надійну передачу даних навіть у зашумлених радіочастотних середовищах, автоматично змінюючи частоти сигналу для уникнення перешкод.

Bluetooth Mesh. Впровадження стандарту Bluetooth Mesh стало важливим кроком для інтеграції Bluetooth у системи Smart Home. Цей стандарт дозволяє створювати багатовузлові мережі (mesh), у яких кожен пристрій може передавати дані іншим, розширюючи зону покриття та підтримуючи велику кількість пристроїв в одній мережі.

Широке застосування. Bluetooth використовується у численних пристроях «розумного дому»:

- системах освітлення (керування лампами, димерами, RGB-підсвіткою);
- датчиках температури, вологості, руху;
- аудіосистемах і мультимедіа;
- розумних замках і системах доступу;
- персональних пристроях керування (пульти, панелі, смартфони).

Організація Bluetooth SIG. Розвитком стандартів і сертифікацією обладнання займається Bluetooth Special Interest Group (SIG) — міжнародна організація, яка підтримує інновації у сфері бездротових комунікацій і забезпечує сумісність пристроїв різних виробників.

Таким чином, Bluetooth є важливою складовою екосистеми «розумного дому», оскільки поєднує низьке енергоспоживання, високу швидкість передачі даних, безпеку та простоту підключення. Завдяки стандарту Bluetooth Mesh технологія успішно масштабується для великих мереж автоматизації, що дозволяє ефективно взаємодіяти десяткам і навіть сотням пристроїв у межах одного будинку.

Загальна електрична схема системи Bluetooth у Smart Home наведена на рисунку 1.5.

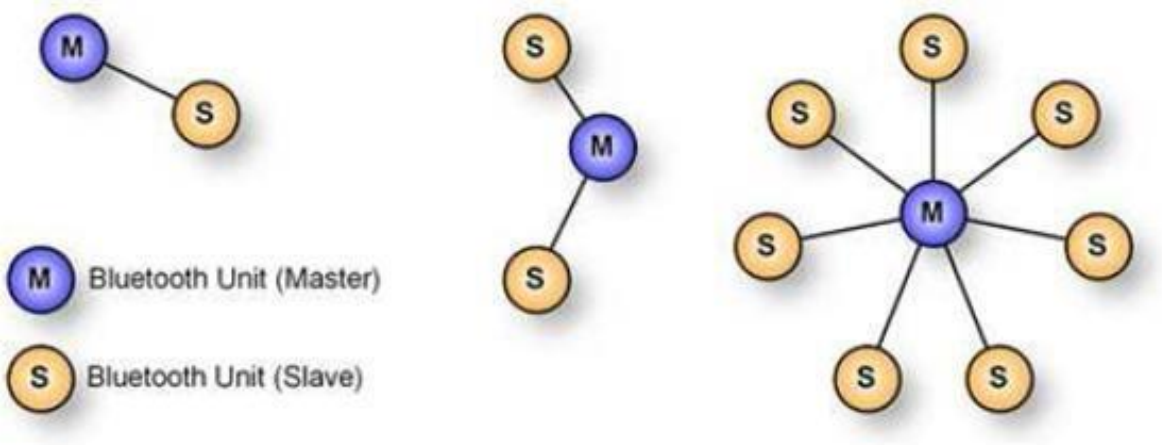


Рисунок 1.5 – Мережа Bluetooth Piconet

Організація мережі Bluetooth

У мережах Bluetooth комунікація між пристроями організовується за принципом ієрархічної структури, де один пристрій виступає у ролі активного (master), а інші - як пасивні (slave). Активний пристрій визначає схему обміну даними, координує роботу підлеглих пристроїв та синхронізує їхню діяльність у межах мережі.

Bluetooth дозволяє створювати не лише прості пікомережі (piconet), а й більш складні об’єднання - «скатернети» (scatternet), у яких взаємодіють кілька незалежних або частково синхронізованих пікомереж. У таких мережах кожен пристрій може одночасно брати участь у декількох пікомережах, виконуючи різні ролі - бути master в одній і slave в іншій. Це забезпечує гнучкість у побудові великих і динамічних топологій для систем Smart Home.

Згідно зі стандартом Bluetooth, в одній пікомережі може бути до 10 активних з’єднань, що дозволяє об’єднувати різноманітні сенсори, контролери, мультимедійні та керувальні пристрої. Для розширення зони покриття використовуються шлюзові пристрої (gateway nodes), які виконують роль посередників між пікомережами, забезпечуючи передачу даних на більші відстані та інтеграцію з Інтернетом.

Загальна гранична схема мережі розсіювання (scatternet) наведена на рисунку 1.6.

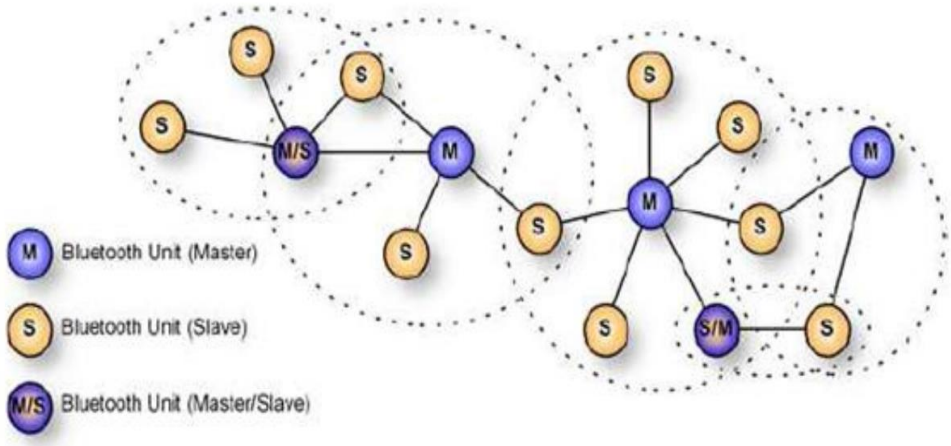


Рисунок 1.6 – Мережа Bluetooth Scatternet

Технологія Bluetooth Low Energy (BLE) у системах «Розумний дім»

Bluetooth Low Energy (BLE), також відомий як Bluetooth Smart, є сучасною технологією бездротового зв'язку, розробленою для забезпечення стабільного обміну даними між пристроями при мінімальному енергоспоживанні. Технологія входить до складу стандарту Bluetooth версії 4.0 і вище та орієнтована на потреби пристроїв Інтернету речей (IoT), у тому числі систем «Розумний дім».

Основною метою BLE є забезпечення енергоефективної комунікації з низьким рівнем споживання енергії при збереженні достатньої швидкості обміну для передачі даних сенсорів, команд управління та службової інформації.

Основні характеристики BLE

– енергоефективність. Однією з ключових переваг BLE є його наднизьке споживання енергії. Пристрої можуть працювати від батареї протягом кількох місяців або навіть років, що робить технологію оптимальною для автономних сенсорів і контролерів.

– безперервне підключення. BLE підтримує постійний канал зв'язку між пристроями при мінімальному навантаженні на джерело живлення. Завдяки цьому забезпечується регулярний обмін даними без потреби постійного перепідключення, що особливо важливо для систем моніторингу чи автоматизації.

– підтримка коротких передач даних. Стандарт BLE орієнтований на передачу невеликих пакетів інформації - наприклад, даних від датчиків температури, вологості, руху або стану пристрою. Такий підхід мінімізує енергозатрати та підвищує ефективність роботи мережі.

– використання у Smart Home та IoT. Завдяки поєднанню енергоефективності, компактності протоколу та стабільності зв'язку, BLE став одним із ключових стандартів у сфері інтелектуальних будинків і інтернету речей. Технологія використовується для взаємодії між різними типами пристроїв:

- сенсорами (температури, руху, освітленості);
- системами освітлення та клімат-контролю;
- «розумними» замками та камерами;
- термостатами та приладами керування побутовою технікою.

Використання BLE у системах Smart Home

У контексті розумного будинку Bluetooth Low Energy забезпечує гнучку та енергоощадну комунікацію між пристроями. BLE може слугувати як локальний канал зв’язку між мобільним пристроєм користувача та мережею домашніх приладів, так і внутрішнім протоколом для взаємодії між компонентами системи.

Багато сучасних розумних замків, сенсорів, ламп і термостатів використовують BLE для прямого зв’язку зі смартфонами або шлюзами, що інтегрують систему у Wi-Fi або ZigBee-мережу.

Технологія Bluetooth Low Energy поєднує у собі енергоефективність, стабільність та безпеку зв’язку, що робить її надзвичайно придатною для систем розумного дому та Інтернету речей. BLE забезпечує можливість реалізації автономних і масштабованих систем, у яких пристрої здатні обмінюватися даними в реальному часі, не потребуючи частого обслуговування чи заміни елементів живлення.

Процес з’єднання в Bluetooth Low Energy зображено на рисунку 1.7.

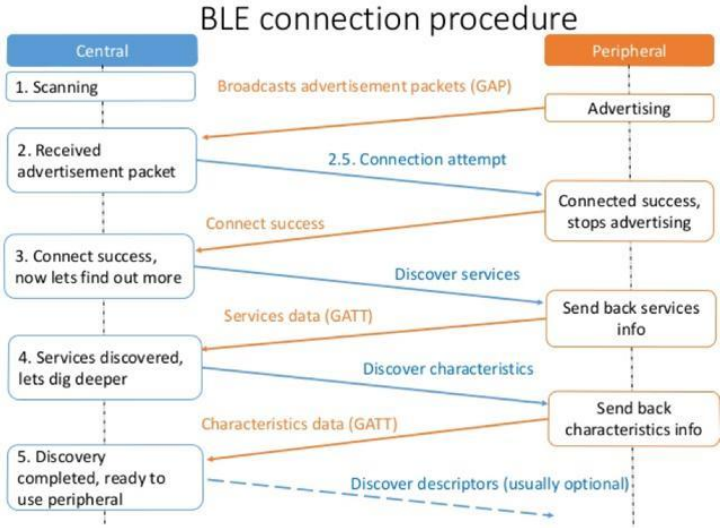


Рисунок 1.7 – Процес встановлення з’єднання Bluetooth

Схема стандартів Bluetooth представлена на рисунку 1.8

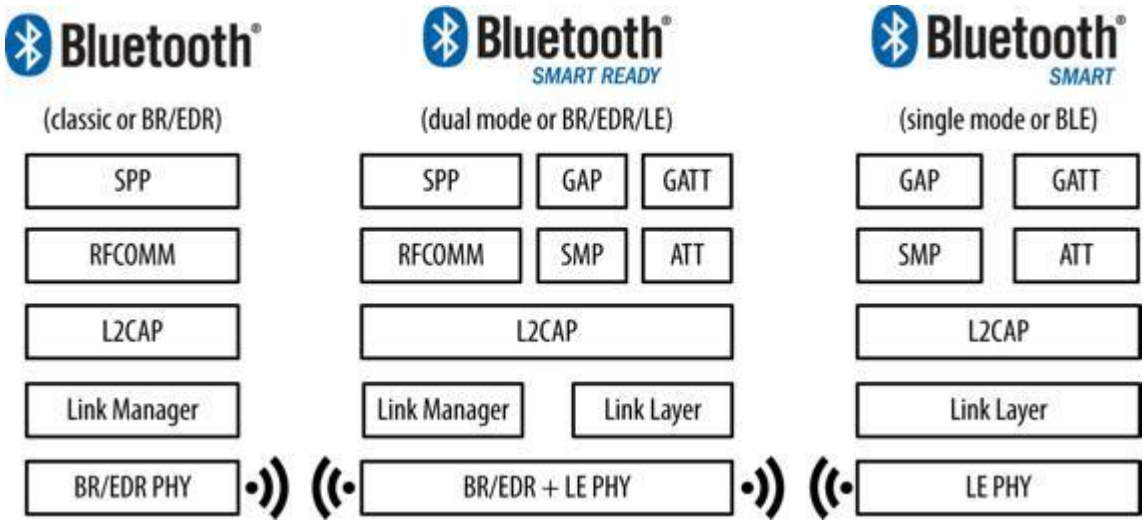


Рисунок 1.8 - Схема стандартів Bluetooth

Основні блоки Bluetooth-пристроїв та їх архітектура

Bluetooth-пристрій являє собою багаторівневу систему, що забезпечує повноцінну реалізацію бездротового обміну даними — від фізичного рівня до прикладної логіки користувача. Архітектура таких пристроїв включає три основні функціональні блоки: додаток, хост (host) та контролер (controller).

а) Додаток (Application)

Цей рівень реалізує прикладну логіку роботи пристрою, орієнтовану на кінцевого користувача. У контексті Bluetooth додаток відповідає за:

– взаємодію з користувачем (керування, налаштування, обмін даними);

– виконання визначених функцій або сервісів (наприклад, моніторинг сенсорів, управління освітленням, передавання аудіосигналів тощо).

Додаток використовує сервіси стеку Bluetooth, що реалізовані на рівнях хоста та контролера.

b) Головний пристрій (Host)

Хост відповідає за реалізацію верхніх рівнів стеку протоколів Bluetooth, включаючи мережеву логіку, управління безпекою та обмін даними між пристроями. До складу хоста входять такі основні протоколи та модулі:

– GAP (Generic Access Profile) – профіль загального доступу, який визначає режими виявлення, з'єднання та взаємодії між пристроями (наприклад, «видимість», «сполучення»).

– GATT (Generic Attribute Profile) – профіль загальних атрибутів, що описує структуру та правила обміну даними у вигляді атрибутів (характеристик) між пристроями.

– L2CAP (Logical Link Control and Adaptation Protocol) – протокол логічного з'єднання та адаптації, який забезпечує мультиплексування каналів і передавання даних між різними рівнями стеку.

– ATT (Attribute Protocol) – протокол обміну атрибутами, що забезпечує доступ до характеристик пристроїв через GATT-профілі.

– SM (Security Manager) – менеджер безпеки, який реалізує процедури автентифікації, шифрування та управління ключами.

– HCI (Host Controller Interface) – інтерфейс між хостом і контролером, що дозволяє здійснювати обмін командами, подіями та даними.

c) Контролер (Controller)

Контролер реалізує нижні рівні стеку протоколів Bluetooth, що відповідають за фізичний обмін даними. До його складу входять:

– HCI (Host Controller Interface) – інтерфейс на стороні контролера, який забезпечує зв'язок з хостом через стандартні шини (UART, USB, SPI тощо).

– LL (Link Layer) – рівень з'єднання, який відповідає за встановлення, підтримку та завершення зв'язку між Bluetooth-пристроями.

– PHY (Physical Layer) – фізичний рівень, що визначає параметри радіочастотного сигналу, модуляцію, потужність передавання та частотний діапазон (зазвичай 2,4 ГГц ISM-діапазон).

d) Апаратні реалізації Bluetooth-систем

Комерційні Bluetooth-рішення можуть реалізовуватися за різними апаратними сценаріями:

1. SoC (System-on-Chip) Універсальна система-на-чипі, яка об’єднує додаток, хост і контролер на одному кристалі. Використовується в компактних і енергоефективних пристроях (наприклад, сенсори, фітнес-браслети, замки, термостати).

2. Рішення на двох мікроконтролерах. У такій конфігурації прикладна програма (application) і хост-частина взаємодіють із контролером через інтерфейси UART, USB або SDIO. Така архітектура характерна для мобільних або багатофункціональних пристроїв.

3. Двоетапна (гібридна) конфігурація. Передбачає підключення прикладного рівня до комунікаційного пристрою (host-controller pair) за четирирівневим протоколом, що дозволяє підвищити стабільність і гнучкість системи при складних мережевих взаємодіях.

Таким чином, архітектура Bluetooth-пристроїв забезпечує модульність, масштабованість і сумісність, що робить можливим використання цієї технології у широкому спектрі пристроїв - від простих сенсорів до комплексних систем розумного будинку.

Технологія Bluetooth 5.0 та її можливості у Smart Home

Bluetooth 5.0 - це оновлена версія стандарту бездротового зв’язку, розроблена для підвищення швидкості, дальності та стабільності передачі даних, а також для розширення функціональності у сфері Інтернету речей (IoT) та розумних будинків. Завдяки низці інженерних удосконалень Bluetooth 5.0 став більш універсальним, енергоефективним і надійним засобом бездротової комунікації.

Основні вдосконалення Bluetooth 5.0

– збільшення дальності та швидкості передачі даних. У порівнянні з попередньою версією, Bluetooth 5.0 забезпечує у чотири рази більшу дальність дії та удвічі вищу швидкість передачі даних (до 2 Мбіт/с). Це дозволяє

ефективно передавати великі обсяги інформації між пристроями без втрати якості сигналу, навіть на значних відстанях.

- підвищена стабільність і безпека. Новий стандарт реалізує покращені алгоритми шифрування, захисту від перешкод і автентифікації, що підвищує надійність комунікації та захист персональних даних користувачів. Bluetooth 5.0 є оптимальним вибором для критичних систем — наприклад, охоронних датчиків і замків у «розумному домі».
- підтримка mesh-топології. Вбудована підтримка Bluetooth Mesh дозволяє створювати масштабовані мережі, у яких кожен пристрій може взаємодіяти з іншими без необхідності в центральному вузлі. Це особливо важливо для побудови розподілених мереж автоматизації в системах Smart Home або промислових застосуваннях.
- обробка даних для Bluetooth-маяків (Beacons). Bluetooth 5.0 підтримує покращену роботу з маяками (beacons) — пристроями, що передають сигнали для ідентифікації місця розташування або сповіщення користувачів про події. Це розширює можливості Bluetooth для реалізації розумних сценаріїв навігації, трекінгу та контекстної автоматизації у приміщеннях (наприклад, у магазинах, офісах чи музеях).
- сумісність і доступність. Bluetooth 5.0 зберігає зворотну сумісність із попередніми версіями, що дозволяє легко інтегрувати нові пристрої у вже наявні системи. Продукти з підтримкою Bluetooth 5.0 активно впроваджуються у комерційних рішеннях — прикладами є смартфони Samsung Galaxy S8, iPhone 8 та сучасні розумні датчики й контролери.

Отже, технологія Bluetooth 5.0 є суттєвим кроком уперед у розвитку бездротового зв’язку для систем Smart Home та IoT. Вона забезпечує:

- вищу продуктивність і стабільність передачі даних;
- покращений рівень безпеки;
- розширену зону покриття та енергоефективність;
- масштабованість завдяки підтримці mesh-мереж.

Ці вдосконалення роблять Bluetooth 5.0 універсальною технологією для побудови інтелектуальних мереж, які поєднують десятки та сотні пристроїв у єдину енергоефективну екосистему «розумного дому».

Технологія Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) - це енергоефективна технологія бездротового зв'язку, яка поєднує високу сумісність, низьке енергоспоживання та простоту інтеграції. Вона стала ключовим елементом сучасних систем «Розумний дім» і Інтернету речей (IoT), де важлива автономність роботи пристроїв та стабільність передачі даних.

Переваги технології Bluetooth LE

- високий рівень стандартизації та сумісність.BLE має єдиний міжнародний стандарт, розроблений організацією Bluetooth SIG, що гарантує сумісність між пристроями різних виробників і підтримку на основних операційних платформах (Android, iOS, Windows, Linux).
- низька вартість реалізації. Вартість впровадження Bluetooth LE є невисокою, що робить його привабливим рішенням для виробників розумних пристроїв і сенсорів, особливо у масовому виробництві.
- ультранизьке енергоспоживання.Однією з ключових переваг BLE є мінімальне споживання енергії. Пристрої можуть працювати від однієї батареї кілька місяців або навіть років, що є критично важливим для датчиків, носимих пристроїв і автономних модулів системи Smart Home.
- достатня швидкість передачі даних. Bluetooth LE забезпечує швидкість передачі даних понад 1 Мбіт/с, що є цілком достатнім для обміну короткими повідомленнями, даними сенсорів або керування пристроями в реальному часі.
- гнучкість у налаштуванні продуктивності. BLE дозволяє адаптувати параметри модуля залежно від потреб: збільшити швидкість обміну або зменшити радіус дії для економії енергії. Це робить технологію універсальною для різних сценаріїв використання.

– простота підключення. Процес встановлення з’єднання у BLE максимально спрощений, що полегшує інтеграцію пристроїв та робить технологію зручною для користувача.

– безпека передавання даних. BLE підтримує шифрування та автентифікацію, що забезпечує надійний захист від несанкціонованого доступу. Це особливо важливо для систем моніторингу, замків, охоронних та медичних пристроїв.

– уніфіковані API для розробників. BLE має єдині прикладні інтерфейси (API), що спрощують створення універсальних додатків і полегшують інтеграцію пристроїв у різні платформи.

Недоліки технології Bluetooth LE

– обмежена підтримка mesh-топології. Повноцінна підтримка mesh-мереж з’явилася лише у версії Bluetooth 5.0, тому значна кількість старих пристроїв не має цієї функціональності.

– відносно низька швидкість для великих обсягів даних. Незважаючи на вдосконалення, швидкість BLE залишається нижчою, ніж у Wi-Fi або класичного Bluetooth, тому технологія не підходить для передачі мультимедійних потоків або великих файлів.

Загалом, Bluetooth Low Energy є оптимальним стандартом для побудови бездротових систем, які вимагають енергоефективності, безпеки та сумісності. Технологія успішно застосовується у таких сферах, як:

– розумні будинки (сенсори, замки, освітлення, термостати);

– медицина та фітнес (монітори стану здоров’я, фітнес-браслети);

– індустрія IoT (датчики контролю, маяки, системи автоматизації).

BLE поєднує простоту реалізації, низьке енергоспоживання та достатню продуктивність, що робить її невід’ємним компонентом екосистеми Smart Home.

Концепції розумного будинку та принципи його роботи

У сучасних житлових будинках використовується велика кількість технологічного обладнання, яке забезпечує комфорт, безпеку,

енергоефективність і комунікацію. Поєднання цих систем у єдину інтегровану мережу створює так званий «розумний будинок» - комплексну інтелектуальну систему, здатну автоматично реагувати на зміни зовнішніх умов і потреб користувача.

Розумний будинок може:

- автоматично підтримувати оптимальний мікроклімат у приміщеннях;
- керувати освітленням, вентиляцією, мультимедійними системами;
- забезпечувати безпеку мешканців, контролюючи витоки газу, диму, пожежу або спроби несанкціонованого доступу;
- зменшувати енергоспоживання завдяки автоматичному вимкненню непотрібних приладів у відсутності користувачів;
- інформувати власника про поточний стан систем через мережу Інтернет.

Таким чином, розумний будинок - це не лише комфорт, а й підвищення рівня безпеки та оптимізація витрат енергії.

Система інтелектуальної автоматизації

Система «Розумний дім» є інтелектуальною системою автоматизації, яка керує інженерними мережами та побутовими пристроями будівлі для забезпечення комфорту, енергоефективності та безпеки. Основні цілі впровадження такої системи:

- створення зручного та безпечного середовища для мешканців;
- оптимізація споживання енергоресурсів;
- інтеграція усіх підсистем в єдину мережу управління.

До складу системи входять такі компоненти:

- керування освітленням та електроприводами (димери, жалюзі, освітлювальні прилади);
- контроль часу та сценарії автоматизації (наприклад, «нічний режим» або «режим відсутності»);
- системи вентиляції, кондиціонування та опалення;

– пожежна сигналізація, відеоспостереження та охоронна система;

– системи контролю доступу та протипожежного захисту;

– домашній кінотеатр, мультимедіа та аудіосистеми.

Сучасні інтелектуальні системи дозволяють централізовано керувати всіма цими функціями через один інтерфейс - мобільний додаток, сенсорну панель, веб-інтерфейс або голосові команди.

Користувач може налаштовувати індивідуальні параметри свого середовища (освітлення, температуру, рівень вологості), забезпечуючи максимально комфортні умови проживання.

Функціонування системи «Розумний дім» базується на взаємодії кількох основних компонентів, об’єднаних у єдину мережу управління (рисунок 1.9):

– центральний блок управління (контролер). Це головний модуль системи, який координує роботу всіх підключених пристроїв, збирає інформацію з датчиків, обробляє команди користувача та передає їх до виконавчих елементів.

– датчики. Система оснащена різними сенсорами — температури, вологості, освітлення, руху, диму, витоку газу тощо. Вони забезпечують збір інформації про навколишнє середовище та передають її до центрального блоку.

– виконавчі пристрої. До них належать нагрівальні прилади, димери, лампи, кондиціонери, жалюзі, системи опалення та інші елементи, що виконують команди контролера.

– шнтерфейси управління. Це засоби взаємодії користувача із системою: кнопкові перемикачі, сенсорні панелі, інфрачервоні пульти, мобільні додатки, а також web-інтерфейси для віддаленого доступу.

– мережа управління. Внутрішня мережа об’єднує всі пристрої та забезпечує обмін даними між ними. У сучасних рішеннях використовуються як дротові (Ethernet, KNX), так і бездротові технології (Wi-Fi, ZigBee, Bluetooth, BLE).

– допоміжні мережі. Система може бути інтегрована з телефонними, аудіо- та відеосистемами, а також із зовнішніми каналами зв’язку для віддаленого моніторингу та керування.

Система «Розумний дім» - це комплексна архітектура, що поєднує в собі елементи автоматизації, інформаційних технологій та енергоменеджменту. Її головна мета - створення безпечного, комфортного та енергоефективного житлового простору, яким можна керувати як локально, так і дистанційно.

Реалізація концепції «Розумного будинку» дозволяє підвищити рівень життя мешканців, оптимізувати використання ресурсів і зробити будівлі більш адаптивними до потреб людини.

Програмне забезпечення системи «Розумний дім»

Програмне забезпечення є ключовим елементом функціонування системи «Розумний дім», оскільки саме воно забезпечує взаємодію між апаратною частиною, сенсорними пристроями, виконавчими модулями та користувачем. Від ефективності роботи програмної складової залежить стабільність, надійність і функціональність усієї системи.

Центральний процесор виконує основну роль у системі - координує роботу всіх підключених пристроїв і підсистем. Для цього він взаємодіє з обладнанням через різні інтерфейси зв’язку, серед яких:

– Ethernet - забезпечує мережеве з’єднання та віддалене керування;

– RS-232 - використовується для зв’язку з окремими пристроями або контролерами;

– RS-485 - підтримує багатоточкове підключення пристроїв у промислових або побутових умовах;

– ІЧ-порт (інфрачервоний) - застосовується для бездротового управління побутовими приладами;

– аналогові та цифрові входи/виходи (I/O) - забезпечують зчитування сигналів із датчиків і керування виконавчими механізмами.

Центральний процесор функціонує під керуванням багатозадачної операційної системи, яка дозволяє одночасно виконувати кілька процесів: обробку даних від сенсорів, генерацію керуючих сигналів, моніторинг стану системи, а також комунікацію з користувачем через інтерфейс управління. У деяких конфігураціях процесор також містить вбудований веб-сервер, що дозволяє здійснювати дистанційне керування системою через браузер або мобільний додаток.

Структура сенсорної мережі

Датчики системи «Розумний дім» розташовуються у ключових зонах приміщення та підключаються до центрального контролера через єдину мережу - безпосередньо або через проміжні вузли (хаби або екрани збору даних).

Вони відстежують такі параметри, як температура, вологість, освітленість, рух, дим, витік води тощо. Отримані від датчиків сигнали передаються до центрального процесора, де відбувається їх аналіз і обробка програмними засобами.

Інтерфейси управління

Для взаємодії користувача із системою використовуються різноманітні інтерфейси управління — від фізичних кнопок і сенсорних панелей до web-інтерфейсів і мобільних застосунків. Вони забезпечують:

– моніторинг поточного стану системи (температура, освітлення, стан дверей тощо);

– керування окремими пристроями або групами приладів;

– налаштування режимів роботи (ручний, автоматичний, віддалений).

– Алгоритм роботи програмного забезпечення

Загальний принцип роботи системи «Розумний дім» полягає у послідовній взаємодії між компонентами:

1. Збір даних. Датчики або інтерфейси управління передають інформацію до центрального блоку управління.

2. Обробка інформації. Програмне забезпечення центрального процесора аналізує отримані дані, порівнює їх із заданими параметрами та визначає необхідні дії.

3. Формування команд. На основі аналізу створюються керуючі команди, які передаються на виконавчі пристрої або допоміжні контролери.

4. Виконання дій. Система в реальному часі регулює роботу підключених пристроїв (наприклад, вмикає освітлення, змінює температуру, активує охоронний режим тощо).

Методи формування команд, структура даних та порядок обміну інформацією визначаються на етапі розробки програмного забезпечення з урахуванням вимог проєкту та особливостей використовуваного обладнання.

Таким чином, програмне забезпечення системи «Розумний дім» є ядром її функціонування. Воно забезпечує збір, аналіз і обробку даних, виконання алгоритмів автоматизації та інтерактивну взаємодію з користувачем. Від якості програмної реалізації залежать ефективність, безпека та стабільність роботи всієї системи.

1.3 Обґрунтування вибору методів розробки ситеми управління

Засоби та інструменти програмної реалізації системи управління розумним будинком

Для дослідження, розробики автоматизованої системи та програмної реалізації системи управління розумним будинком із підсистемою безпечної передачі даних було обрано відповідний комплекс апаратних, програмних і комунікаційних засобів. Основна мета цих заходів полягає у забезпеченні надійної, безпечної та ефективної роботи системи, а також у створенні зручного інтерфейсу для взаємодії користувача з усіма компонентами «розумного дому».

Складові системи «Розумний дім»

1. Електроприлади. Це основні виконавчі елементи системи, до яких належать усі електронні пристрої, керування якими має бути автоматизованим (освітлення, опалення, кондиціонування, системи поливу тощо). Їхня робота координується центральним контролером відповідно до заданих сценаріїв.

2. Сенсори (датчики). Сенсорна підсистема виконує моніторинг стану навколишнього середовища та параметрів житлового простору - температури, вологості, освітленості, наявності руху, витоку газу чи води. Саме сенсори забезпечують збір інформації, створюючи єдине інформаційне поле системи.

3. Мікроконтролери. Мікроконтролери виконують роль автономних вузлів обробки та передавання даних. Вони об’єднують групи датчиків і забезпечують обмін інформацією з центральним блоком управління. Центральний контролер виконує функції координації, обробки даних і формування керуючих команд, передаючи їх на виконавчі пристрої.

4. Інтернет-інтерфейс (комп’ютер або шлюз). Комп’ютерна система або шлюз забезпечує інтерфейс між користувачем і мережею розумного будинку, а також доступ до системи через Інтернет. Вона відповідає за надійність, функціональність та безпеку підключення.

5. Канали передачі даних. Для обміну інформацією між усіма компонентами системи використовуються логічні та фізичні канали зв’язку - дротові (Ethernet, RS-485) і бездротові (Wi-Fi, Bluetooth, ZigBee). При розробці системи враховуються вимоги до каналів зв’язку: захист переданих даних, пропускна здатність, стабільність і затримки сигналу.

6. Зовнішня служба (база даних). Цей компонент відповідає за збір, зберігання та обробку статистичних і службових даних системи. База даних використовується для аналітики, журналювання подій, моніторингу стану обладнання та формування звітів про роботу системи.

7. Мобільні пристрої. Смартфони або планшети виступають як засоби взаємодії користувача з системою. Через мобільний застосунок користувач може віддалено контролювати параметри будинку, змінювати режими роботи пристроїв, отримувати сповіщення про події чи аварійні ситуації.

8. Мова програмування. Для програмної реалізації використано мову програмування C, що є однією з найефективніших для розробки програм під мікроконтролери сімейства AVR. Архітектура AVR і система команд розроблені з урахуванням особливостей компілятора мови C, що дозволяє створювати компактний, оптимізований та швидкодіючий код. Компіляція вихідних даних відбувається швидко, а результат — високопродуктивні програми, які забезпечують стабільну роботу мікроконтролерів у системі управління.

9. Підсистема безпечної передачі даних. Для захисту переданої інформації між компонентами системи використовується модуль шифрування, побудований на алгоритмах Base64, AES (Advanced Encryption Standard) та RSA (Rivest–Shamir–Adleman). Це забезпечує конфіденційність, цілісність і автентичність даних, що є особливо важливим при віддаленому доступі через Інтернет.

Таким чином, система «Розумний дім» складається з комплексу апаратних та програмних засобів, які взаємодіють через стандартизовані

канали передачі даних. Застосування мови програмування С та алгоритмів шифрування AES/RSA дозволяє створити гнучку, надійну й безпечну систему управління, здатну адаптуватися до різних умов експлуатації та вимог користувача.

Розгорнута постановка завдання

Відповідно до технічного завдання на магістерську роботу, реалізації підлягає програмне забезпечення, призначене для системи управління розумним будинком із підсистемою безпечної передачі даних та захистом від кібератак. Розробка спрямована на створення надійної, масштабованої та безпечної системи, яка забезпечуватиме моніторинг, контроль і автоматизацію інженерних підсистем будівлі в умовах підвищених вимог до інформаційної безпеки.

Основні завдання магістерської роботи

У процесі виконання магістерської роботи необхідно реалізувати такий обсяг робіт:

а) провести аналіз існуючих систем-аналогів для визначення їхніх позитивних і негативних характеристик. Результати аналітичного огляду мають бути враховані під час розробки власного програмного продукту;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання в автоматизованому режимі. На основі вибраної методики розробити функціональну та структурну схеми системи управління розумним будинком;

в) створити програмне забезпечення системи, яке реалізує завдання, поставлені технічним завданням. Передбачити розробку блок-схем алгоритмів основної програми та підпрограм, що забезпечують взаємодію з сенсорами, контролерами, базою даних та користувачем;

г) розробити користувацький інтерфейс, який забезпечить зручну взаємодію оператора з системою, а також формування повідомлень на екран ЕОМ про некоректні дії користувача або нестандартні ситуації у роботі технологічного обладнання;

д) підготувати рекомендації щодо організаційних та методичних заходів, які забезпечать ефективне впровадження системи у промислову експлуатацію, її адаптацію до реальних умов функціонування та подальше вдосконалення;

е) провести розрахунки економічної ефективності впровадження розробленої системи, визначивши очікувані економічні та енергетичні вигоди від її застосування;

ж) розробити заходи з охорони праці при впровадженні та експлуатації системи, а також сформулювати заходи цивільного захисту, спрямовані на мінімізацію ризиків під час експлуатації електронних та енергетичних компонентів системи;

з) сформувати висновки щодо виконаного обсягу робіт, узагальнити отримані результати та надати оцінку ефективності створеного програмного забезпечення.

Таким чином, у межах магістерської роботи передбачається повний цикл дослідження, проектування, розробки та оцінювання системи управління розумним будинком із підсистемою безпечної передачі даних. Отримані результати мають забезпечити практичну реалізацію сучасних технологій автоматизації, що поєднують функціональність, надійність і кіберзахист у єдиній інтегрованій системі управління.

2.ОГЛЯД ОБ'ЄКТА УПРАВЛІННЯ. СТВОРЕННЯ СТРУКТУРНОЇ ТА ФУНКЦІОНАЛЬНОЇ СХЕМИ. ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

2.1 Опис функціонування системи

З огляду на тему роботи, необхідно створити програмне забезпечення для системи управління у проєкті «Розумний дім», реалізувавши максимально автоматизовану структуру керування шляхом встановлення відповідних датчиків і впровадження системи кіберзахисту.

Розумний дім - це інтелектуальна система автоматизації, призначена для керування інженерними мережами сучасної будівлі. Основною метою такої системи є забезпечення комфорту, енергоефективності та безпеки мешканців у житлових, робочих чи громадських приміщеннях. Інтелектуальна автоматика здійснює контроль усіх інженерних систем, дозволяючи централізовано регулювати параметри мікроклімату - температуру, вологість, рівень освітлення - та гарантує безпечне функціонування обладнання.

Система «Розумний будинок» покликана забезпечити механізм централізованого моніторингу й інтелектуального управління у приміщеннях різного призначення. Її впровадження дозволяє користувачеві:

- керувати ключовими системами (освітленням, опаленням, кондиціонуванням тощо);
- отримувати інформацію про стан усіх життєво важливих систем будинку як локально, так і дистанційно.

Загальна структура системи управління охоплює такі компоненти:

- центральний або головний блок керування;
- сенсори (температури, освітленості, диму, пилу тощо);
- виконавчі пристрої (нагрівальні елементи, діммери, лампи, ІЧ-випромінювачі);

– інтерфейси керування (механічні перемикачі, ІЧ- та радіопульти, панелі керування, web/vap-інтерфейси);

– локальну мережу керування, що об’єднує всі елементи системи;

– побутову техніку (лампи, кондиціонери, елементи мультимедійних систем тощо);

– допоміжні мережі (Ethernet, телефонні, аудіо- та відеолінії);

– програмне забезпечення, яке забезпечує взаємодію між усіма підсистемами.

Основні функції системи керування

Центральний процесор виконує ключову функцію управління всіма пристроями системи через різноманітні інтерфейси - Ethernet, RS-232, RS-485, ІЧ-порт, а також аналогові та цифрові входи/виходи. Він обладнаний багатозадачною операційною системою, засобами програмування та, за потреби, вбудованим веб-сервером для віддаленого доступу та моніторингу.

Датчики, розміщені в різних частинах приміщення, об’єднані в єдину мережу, що забезпечує передачу даних безпосередньо або через проміжні вузли. Інтерфейси управління формують централізовану структуру керування системою «Розумний дім».

Концепція системи. Система управління являє собою комплекс програмно-апаратних засобів, спрямованих на раціональне використання ресурсів та зниження енергоспоживання, зокрема електроенергії та теплової енергії, що накопичується в акумуляторах. Поряд із цим, система може виконувати додаткові функції - наприклад, контроль присутності осіб у приміщенні.

З урахуванням зазначених особливостей, система розроблена з орієнтацією на енергоефективність, зручність користувача та мінімальний екологічний вплив.

Безпека та енергозбереження. Одним із ключових напрямів проєкту є створення енергозберігаючої системи керування освітленням у багатоповерхових будинках - у під’їздах, на стоянках, відкритих терасах, у

підвалах і на горищах. Її застосування дозволяє знизити споживання електроенергії у 10–15 разів.

У системі передбачено використання розподілених енергетичних компонентів, здатних дублювати існуючі лінії електропередач. Важливим аспектом енергозбереження є оптимізація технічного обслуговування освітлювального обладнання.

Ефективна стратегія енергозбереження включає:

– централізоване керування освітленням;

– застосування автоматичних графіків увімкнення та вимкнення світла;

– використання енергозберігаючих ламп та оптимальне архітектурне планування приміщень;

– впровадження інфрачервоних та електронних датчиків, які автоматично регулюють освітлення відповідно до рівня освітленості та присутності людей.

Електронні сенсори вимірюють інтенсивність світла та генерують команди на ввімкнення або вимкнення освітлення. Датчики присутності визначають наявність людини в кімнаті, що забезпечує точне та економне керування енергоспоживанням.

Крім того, система включає різні типи електронних вимикачів, здатних працювати як автономно, так і у складі комплексної системи «Розумний дім». У деяких випадках датчики пилу інтегровані в вимикачі, що дозволяє автоматично регулювати освітлення залежно від умов середовища.

Технічна реалізація. Система передбачає новітній захист електропостачання, побудований на електромагнітному обладнанні провідних європейських виробників. Монтаж та підключення здійснюються із використанням телефонного кабелю, що значно спрощує інтеграцію, налаштування та подальшу експлуатацію.

Отже, запропонована енергозберігаюча система керування освітленням для багатоповерхових будинків реалізує інноваційні підходи до оптимізації

енергоспоживання, забезпечуючи високу ефективність, надійність і зручність у користуванні.

Система управління освітленням. Централізована система управління освітленням забезпечує ефективне керування всіма світловими приладами будівлі. Її робота базується на використанні попередньо розроблених графіків увімкнення та вимкнення освітлення, сформованих з урахуванням добових режимів користувачів і рівня природного освітлення. Це дозволяє досягти раціонального споживання електроенергії та підвищити комфорт мешканців.

Енергозберігаючі технології. У системі застосовуються енергозберігаючі джерела світла, зокрема світлодіодні (LED) лампи, які споживають значно менше електроенергії порівняно з традиційними лампами розжарювання. Крім того, вони відзначаються високою ефективністю, довговічністю та низькими витратами на обслуговування, що робить їх оптимальним рішенням для автоматизованих систем освітлення.

Автоматизовані вимикачі. Для підвищення рівня автоматизації в системі використовуються автоматичні вимикачі, оснащені інфрачервоними та електронними датчиками. Ці сенсори визначають поточний рівень освітленості в приміщенні та автоматично подають команду на ввімкнення або вимкнення світла залежно від умов навколишнього середовища.

Датчики присутності. Додатково система використовує датчики присутності, які реагують на рух або інфрачервоне випромінювання тіла людини. Завдяки цьому система здатна автоматично регулювати освітлення: вмикати світло при вході користувача в приміщення та вимикати після його виходу. Це значно знижує непродуктивне споживання електроенергії.

Електромагнітне обладнання. Для забезпечення стабільності та надійності роботи системи використовується електромагнітне обладнання провідних європейських виробників. Воно гарантує ефективний захист електромережі від перевантажень, коротких замикань і коливань напруги, що підвищує загальний рівень безпеки.

Дистанційне керування. Система передбачає можливість дистанційного керування освітленням через телефонний або мережевий кабель. Такий підхід дає змогу здійснювати моніторинг і регулювання освітлення з віддалених пристроїв, забезпечуючи зручність експлуатації та контроль за роботою всієї системи в реальному часі.

Комплексне застосування зазначених технологій забезпечує ефективне, енергозберігаюче та безпечне освітлення в будівлі. Це сприяє значній економії електроенергії, підвищенню комфорту користувачів та зменшенню негативного впливу на навколишнє середовище.

Освітлення

В інтелектуальній системі «Розумний дім» керування освітленням здійснюється максимально просто - за допомогою однієї кнопки, настінної панелі або пульта дистанційного управління. Користувач може зручно налаштовувати роботу світильників, підсвічування та декоративних ламп відповідно до власних потреб або настрою.

Система дозволяє автоматично змінювати інтенсивність і сценарії освітлення - наприклад, для створення певної атмосфери під час прийому гостей чи відпочинку. Так, обравши сценарій «Вечір», користувач може активувати одну групу світильників із м’яким світлом, вимкнути інші, закрити жалюзі та перевести клімат-контроль у комфортний режим.

Датчики пилу та руху забезпечують автоматичне вмикання освітлення при наближенні людини. Це особливо зручно у темний час доби — наприклад, у коридорах чи передпокоях, де світло активується лише за необхідності.

Інтелектуальна система значно скорочує кількість механічних вимикачів, замінюючи їх компактними багатофункціональними панелями керування. Один такий вимикач може контролювати до дванадцяти груп освітлення, дозволяючи регулювати яскравість або повністю вмикати та вимикати світло.

Система передбачає також створення індивідуальних сценаріїв освітлення, які можна активувати вручну або автоматично. Наприклад:

– у нічний час світло в під’їздах чи коридорах працює на частковій потужності;

– під час повернення додому активується фасадне, ландшафтне та доріжкове освітлення;

– уранці система визначає оптимальний рівень освітлення, враховуючи природне світло та погодні умови.

Крім локального керування, передбачена можливість дистанційного управління освітленням з ноутбука, смартфона або пульта - що забезпечує повний контроль навіть поза межами будинку.

Завдяки інтелектуальному програмуванню зменшується споживання електроенергії та підвищується комфорт користувача. Освітлення вимикається автоматично після виходу людини з кімнати або зачинення дверей, а вночі система вмикає м’яке, неяскраве світло, щоб уникнути різкого контрасту для очей.

Таким чином, автоматизована система керування освітленням у «Розумному домі» забезпечує:

– енергоефективність і безпеку;

– гнучке налаштування режимів освітлення;

– високий рівень комфорту та ергономіки користування.

Система клімат-контроль

Система клімат-контролю в інтелектуальному будинку функціонує на основі вбудованих алгоритмів, що дозволяють підтримувати оптимальні параметри мікроклімату у різних приміщеннях з мінімальними енергетичними витратами. Вона забезпечує автоматичне регулювання температури, вологості та вентиляції, формуючи комфортні кліматичні зони відповідно до заданих користувачем параметрів.

Система підтримує режим відкладених операцій, що дає змогу автоматично вмикати або вимикати опалення, кондиціонування чи вентиляцію у певний час. Наприклад, у нічний період може відключатися кондиціонер і

опалення, окрім системи “тепла підлога”, що сприяє зниженню енергоспоживання та створює комфортні умови для сну.

Крім того, система забезпечує енергоощадну роботу під час відсутності людей у будинку, використовуючи спеціальні сценарії, такі як «щоденна відсутність» або «відпустка». Наприклад, користувач може налаштувати автоматичне зниження температури у вихідні дні або в нічний час. Це особливо актуально для приватних котеджів та будинків з автономним опаленням.

Інтелектуальна система дозволяє індивідуально регулювати параметри мікроклімату — температуру, рівень вологості та кількість свіжого повітря — у кожному приміщенні, забезпечуючи персоналізований комфорт для кожного мешканця.

Додатково реалізовано дистанційне керування системою через Інтернет або мобільний телефон: користувач може віддалено вмикати котел опалення, змінювати налаштування або переводити систему в економічний режим.

Завдяки використанню датчиків, перемикачів і панелей управління, система постійно контролює основні параметри повітряного середовища, підтримуючи їх на заданому рівні. Такий підхід забезпечує стійкий комфортний мікроклімат, зниження енергоспоживання та підвищення рівня безпеки й автономності житла.

Контроль проникнення

Постановка та зняття будинку з охорони здійснюється за допомогою кодового пульта керування, розміщеного у тамбурі біля вхідних дверей. Після відкриття дверей користувач має 30 секунд для введення правильного коду. Якщо протягом цього часу код не буде введено, інтелектуальна система «Розумний дім» автоматично активує звукову сирену та надсилає SMS-сповіщення на заздалегідь визначені телефонні номери власника або служби охорони.

У приміщеннях будинку - кухні, спальні та вітальні - встановлено датчики руху, які дозволяють виявляти спроби несанкціонованого проникнення через двері або вікна. У разі спрацювання будь-якого з датчиків система одразу

фіксує подію, активує відповідні сигнали тривоги та передає повідомлення користувачеві.

Схема розташування та взаємодії охоронних датчиків наведена на рисунку 2.1.

Рисунок 2.1 - Схема застосування датчиків

Під час виходу з квартири користувачеві достатньо ввести особистий код на охоронній панелі, після чого система автоматично активує охоронний режим. Одночасно з цим інтелектуальна система «Розумний дім» виконує низку додаткових дій:

- вимикає освітлення в усіх приміщеннях;
- переводить систему опалення в енергозберігаючий режим;
- за необхідності - блокує неавторизований доступ до електроприладів.

Таким чином, система забезпечує комплексний перехід у режим охорони та оптимізує енергоспоживання під час відсутності мешканців.

Контроль протікання води

Система виявлення протікання води

Витік води у системі водопостачання є однією з найбільш поширених аварійних ситуацій, яка може призвести не лише до пошкодження власного майна, але й до завдання збитків сусідам. У межах системи «Розумний дім» реалізовано механізм автоматичного виявлення та запобігання протіканню води, що значно знижує ризик подібних інцидентів.

Контроль охоплює санвузли, кухню та інші приміщення, де прокладені труби холодного й гарячого водопостачання. У цих зонах встановлюються датчики протікання, які реагують на появу вологи або перелив води за межі сантехнічних приладів.

У разі виявлення протікання система автоматично перекриває подачу води до квартири, активує сигнал тривоги та надсилає повідомлення користувачеві (SMS або push-сповіщення) на заздалегідь задані телефонні номери.

Таким чином, інтелектуальна система забезпечує швидке реагування на аварійні ситуації, мінімізує матеріальні збитки та підвищує рівень безпеки житла.

Схема використання датчиків протікання води наведена на рисунку 2.2.

Рисунок 2.2 – Схема використання датчиків протікання води

Отже, у процесі розроблення даного підрозділу було обґрунтовано вибір системи управління «Розумним домом», яка являє собою комплекс взаємопов’язаних підсистем, що забезпечують керування окремими параметрами середовища та групами датчиків і контролерів.

2.2 Розробка структурної схеми

Структурна схема системи - це узагальнена модель, яка відображає складові елементи системи та взаємозв’язки між ними. Її основним призначенням є наочне подання компонентів розробленої системи, зокрема її основних блоків, функціональних вузлів і каналів зв’язку, що забезпечують взаємодію між ними.

Структурна схема розробленої системи подана на рисунку 2.3

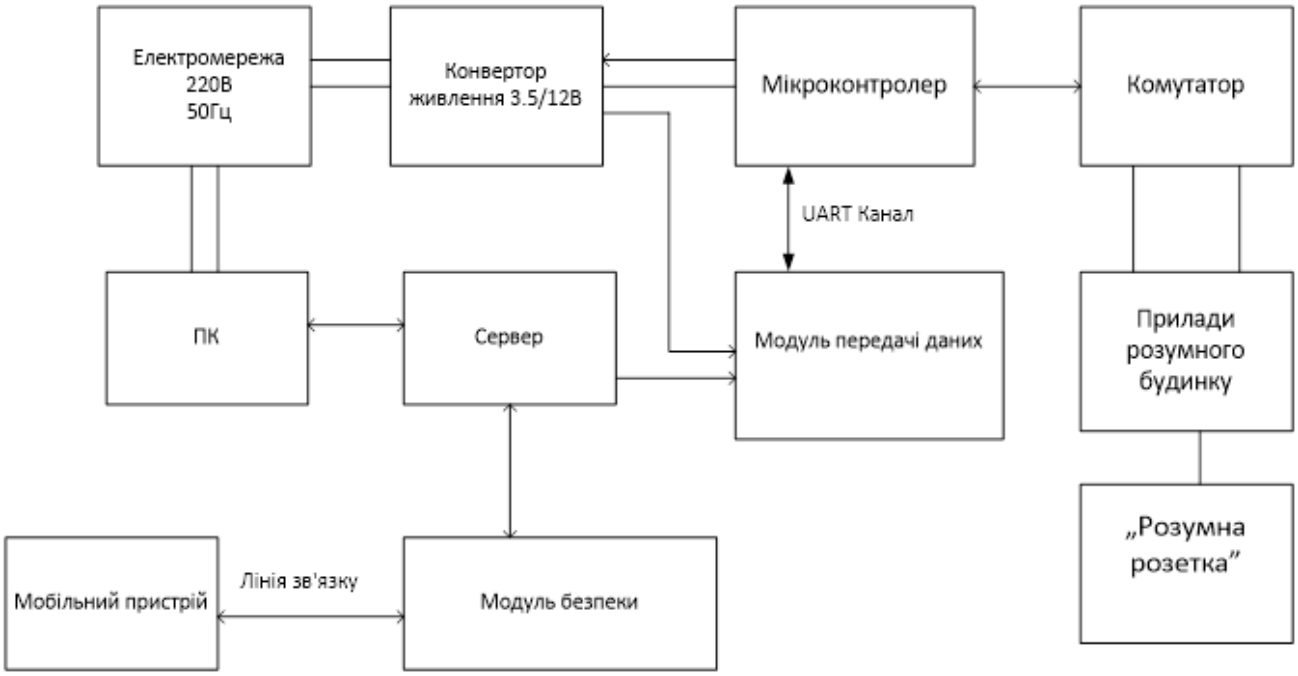


Рисунок 2.3 – Структурна схема системи «Розумний дім»

Пристрій, розроблений відповідно до наведеної конструктивної схеми, живиться від електричної мережі змінного струму 220 В, 50 Гц. Вхідна змінна напруга за допомогою підсилювача-перетворювача перетворюється на стабілізовану постійну напругу 3,5 В, необхідну для живлення основних елементів системи.

Живлення отримують мікроконтролер DSPIC33FJ16 та модуль бездротового зв’язку Bluetooth Low Energy RN4020 виробництва Microchip. Модуль RN4020 забезпечує двосторонній обмін даними між пристроєм і комп’ютером, реалізуючи бездротовий канал зв’язку.

Мікроконтролер DSPIC33FJ16 здійснює послідовний обмін даними з модулем RN4020 через інтерфейс UART, а також генерує допоміжні сигнали керування. Крім того, він виконує вимірювання аналогових параметрів електричного пристрою - струму, напруги та температури - з подальшим перетворенням їх у цифровий формат для оброблення.

Для керування виконавчим елементом мікроконтролер формує сигнали на оптотріак MOC3023, який здійснює комутацію навантаження електричного пристрою. У конструкцію пристрою інтегровані датчики напруги та струму,

які формують аналогові сигнали рівнем 0–3,5 В, що подаються на входи АЦП мікроконтролера для подальшої обробки.

2.3 Розробка функціональної схеми

На рисунку 2.4 представлено функціональну схему складної системи управління розумним домом. Із рисунка видно, що система складається з таких основних блоків:

- сервер розумного будинку;
- веб-сервер;
- контролер із супутнім обладнанням;
- модуль Bluetooth RN4020;
- модуль безпеки та шифрування;
- веб-інтерфейс;
- мобільний додаток;
- виконавчі механізми;
- розумна розетка.

Усі перелічені компоненти взаємодіють між собою, утворюючи єдину інтегровану систему керування «Розумним домом», що забезпечує обмін даними, аналіз інформації та виконання команд користувача

Веб-сервер

Веб-сервер зберігає дані, отримані від сервера Bluetooth LE. На їх основі, використовуючи алгоритм оптимізації, він приймає рішення про підключення/відключення побутової техніки до мережі для обмеження навантаження на електромережу або уникнення аварійних ситуацій. Крім того, веб-сервер надає API для ручного керування системою через графічний інтерфейс користувача.

Модулі Bluetooth Low Energy (BLE) серії RN4020, розроблені компанією Microchip Technology Inc., містять вбудований стек BLEnergy, набір ASCII-команд та підтримку користувацьких скриптів. Завдяки цьому

забезпечується можливість швидкої розробки готових BLE-пристроїв без необхідності виконання низькорівневого програмування або використання спеціалізованих середовищ розробки, бібліотек та компіляторів.

Розробник може здійснювати конфігурування модуля за допомогою звичних інструментів програмування, а всі налаштування зберігаються у незалежній пам’яті пристрою. Модуль підтримує як стандартні BLE-профілі SIG (Bluetooth Special Interest Group), так і приватний профіль MLDP (Microchip Low-power Data Profile), який призначений для передавання потокових даних між пристроями з низьким енергоспоживанням.

Розумна розетка (Smart Socket) - це електронний пристрій, який дозволяє вмикати або вимикати електроживлення підключеного обладнання як автоматично, так і за допомогою команд зі смартфона, комп’ютера або центрального контролера системи «Розумний дім».

Вона забезпечує можливість дистанційного керування побутовими приладами, моніторингу споживання електроенергії та інтеграції у загальну систему енергоменеджменту. Завдяки цьому користувач може автоматизувати роботу освітлення, обігрівачів, зарядних пристроїв та іншої техніки, що підключається через стандартну розетку.

Функціональна схема системи «Розумний дім» наведена на рисунку 2.4, де відображено взаємозв’язок між основними модулями - контролером, сервером, BLE-комунікаційним модулем, виконавчими пристроями та інтерфейсами користувача.

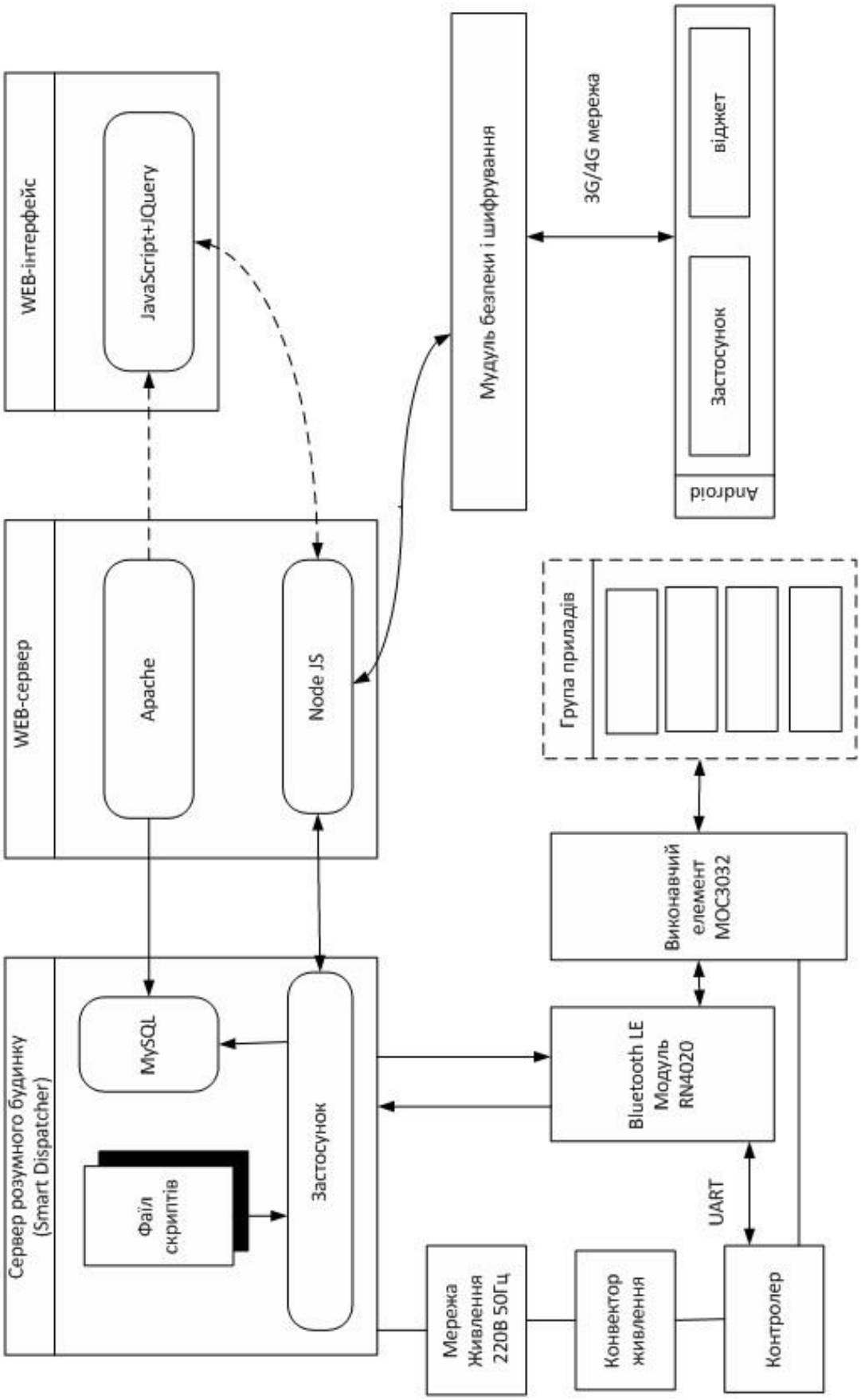


Рисунок 2.4 – Фукціональна схема системи «Розумний дім».

Розробка діаграми процесів

Діаграма процесів розробленої системи, подана на рисунку 2.5, відображає взаємодію основних компонентів системи «Розумний дім». Для її побудови використано модель проектування на основі потоків даних (Data Flow Diagram, DFD), яка демонструє, як інформаційні потоки циркулюють між різними підсистемами, модулями та зовнішніми елементами.

Діаграма дає змогу візуалізувати процеси обробки даних, структуру проєкту та взаємозв’язки між ключовими елементами системи - контролером, сервером, користувацькими інтерфейсами та модулями зв’язку.

У процесі проєктування спочатку формується контекстна діаграма, яка показує загальну взаємодію системи із зовнішнім середовищем. Подальша деталізація включає розбиття процесів на підпроцеси та уточнення потоків даних для представлення логіки функціонування системи на нижчих рівнях.

Застосовуючи сучасні методи системного аналізу та моделювання, було розроблено систему управління розумним будинком із підсистемою безпечної передачі керуючих сигналів від смартфона до мікроконтролера. Це дозволяє забезпечити захищений канал зв’язку під час дистанційного керування системою за допомогою Інтернет-технологій.

Після розгляду структурної та функціональної схем, а також діаграми взаємодії процесів, подано огляд блок-схеми хмарної програми та відповідних підпрограм, які реалізують роботу всієї системи.

Діаграма процесів системи «Розумний дім» наведена на рисунку 2.5.

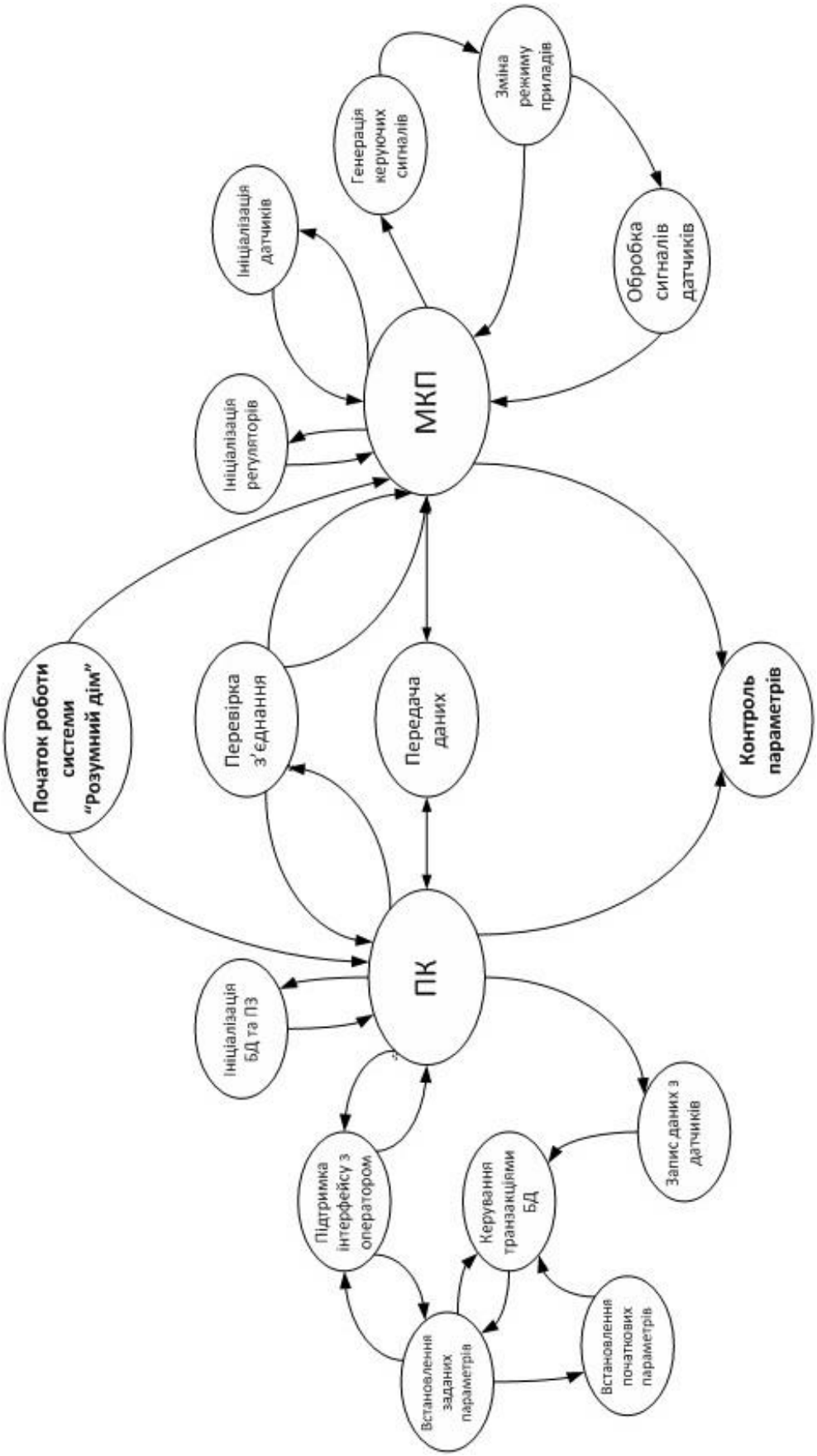


Рисунок 2.5 – Діаграма процесів системи «Розумний дім»

3 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ ТА ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ І ПРОГРАМНИХ РІШЕНЬ

3.1 Реалізація системи управління розумним будинком

Розроблена програма призначена для моніторингу та контролю потоку електроенергії, що споживається або генерується електричними пристроями у межах системи «Розумний дім». Вона забезпечує збирання, обробку та передавання даних про стан електромережі та роботу підключених приладів.

Під час проєктування системи були сформульовані такі основні вимоги:

– живлення пристрою здійснюється від стандартної мережі змінного струму 220 В, 50 Гц;

– пристрій повинен мати високопродуктивний модуль Bluetooth Low Energy (RN4020) для бездротового підключення до мережі системи;

– у складі пристрою має бути мікроконтролер, який забезпечує роботу модуля Bluetooth LE, вимірювання аналогових параметрів (струм, напруга, температура) з подальшим перетворенням їх у цифровий код, а також формування керуючих сигналів для вмикання або вимикання електроприладів;

– пристрій повинен мати оптичний інтерфейс для керування подачею живлення на електроприлади.

Пристрій, побудований за наведеною конструктивною схемою, живиться від електричної мережі 220 В, 50 Гц. Вхідна змінна напруга за допомогою перетворювального блока живлення знижується і стабілізується до постійної напруги 3,5 В, необхідної для живлення мікроконтролера DSPIC33FJ16 і модуля Bluetooth Low Energy RN4020 від компанії Microchip Technology Inc.

Модуль RN4020 забезпечує бездротовий обмін даними між пристроєм і центральним сервером або комп’ютером, здійснюючи передачу інформації в обох напрямках у межах Bluetooth-мережі.

Мікроконтролер DSPIC33FJ16 організовує зв’язок із модулем RN4020 через послідовний інтерфейс UART, генерує допоміжні сигнали керування, а також виконує вимірювання аналогових параметрів електричного кола - струму, напруги та температури - з подальшим перетворенням їх у цифровий формат для оброблення.

Крім того, мікроконтролер формує сигнали керування для виконавчого елемента - оптронного модуля MOC3023, який виконує комутацію навантаження електричного пристрою.

До складу системи також входять датчики струму та напруги, вихідні сигнали яких (у межах 0–3,5 В) подаються на входи аналогово-цифрового перетворювача (АЦП) мікроконтролера. Це дозволяє точно вимірювати параметри електричної мережі й контролювати споживання енергії в реальному часі.

Bluetooth LE модуль Microchip RN4020

Компанія Microchip Technology Inc. є одним із світових лідерів у галузі виробництва мікроконтролерів та мікрокомп’ютерних систем. Вона пропонує широкий спектр рішень на основі технології Bluetooth Low Energy (BLE) - від окремих інтегральних мікросхем до повнофункціональних модулів.

Однією з головних переваг використання BLE-модулів Microchip є те, що вони попередньо сертифіковані виробником та мають відповідні міжнародні сертифікати - FCC (США) та CE/ETSI (ЄС). Крім того, модулі проходять тестування та сертифікацію Bluetooth SIG, що гарантує їхню сумісність і стабільність роботи у стандартних BLE-мережах.

Ще однією важливою перевагою модулів Microchip є гарантовано працездатна радіочастотна частина, яка вже інтегрована в корпус пристрою. Завдяки цьому відпадає потреба в додатковому проектуванні або налаштуванні радіотракта.

Конфігурація модуля виконується за допомогою декількох ASCII-команд, що значно спрощує процес інтеграції та скорочує час розробки кінцевого пристрою. Модулі серії RN дозволяють швидко реалізувати бездротове підключення, не вдаючись до складного низькорівневого програмування або створення спеціального програмного забезпечення.

Одним із найпоширеніших представників цієї серії є модуль RN4020, принципова схема якого наведена на рисунку 3.1.

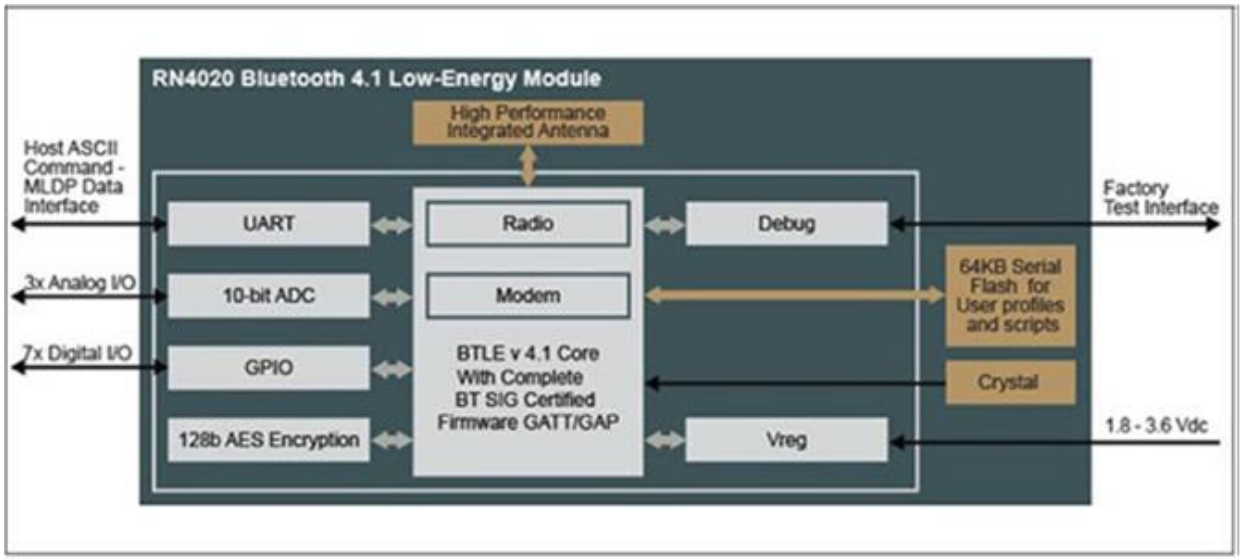


Рисунок 3.1 - Структурна схема модуля RN4020

Рисунок 3.2 – Модуль Bluetooth LE RN4020

Мікроконтролер Microchip dsPIC33FJ16

У якості основного контролера в системі використовується спеціалізований мікроконтролер компанії Microchip Technology Inc. - DSPIC33FJ16MC102, який дозволяє реалізувати весь описаний функціонал в межах однопроцесорної архітектури. Застосування цього мікроконтролера забезпечує високу швидкодію, точність оброблення сигналів та оптимальне використання ресурсів системи.

Мікроконтролери серії dsPIC33 поєднують переваги цифрових сигнальних процесорів (DSP) та мікроконтролерів загального призначення (MCU), що робить їх ефективним рішенням для реалізації енергоефективних, вимірювальних та керуючих систем.

До основних особливостей DSPIC33FJ16MC102 належать:

– 16-розрядне ядро із розширеною системою команд;

– апаратна підтримка математичних операцій з фіксованою точністю;

– наявність інтерфейсів UART, SPI, I^2C для обміну даними;

– вбудовані модулі ШІМ, АЦП та таймери;

– підтримка енергозберігаючих режимів роботи;

– висока надійність і стабільність функціонування у промислових умовах.

Використання цього мікроконтролера дозволяє інтегрувати всі функціональні блоки системи «Розумний дім» — обробку сенсорних сигналів, передачу даних, управління виконавчими пристроями — у єдину процесорну платформу.

Структурна схема мікроконтролера DSPIC33FJ16MC102 наведена на рисунку 3.3.

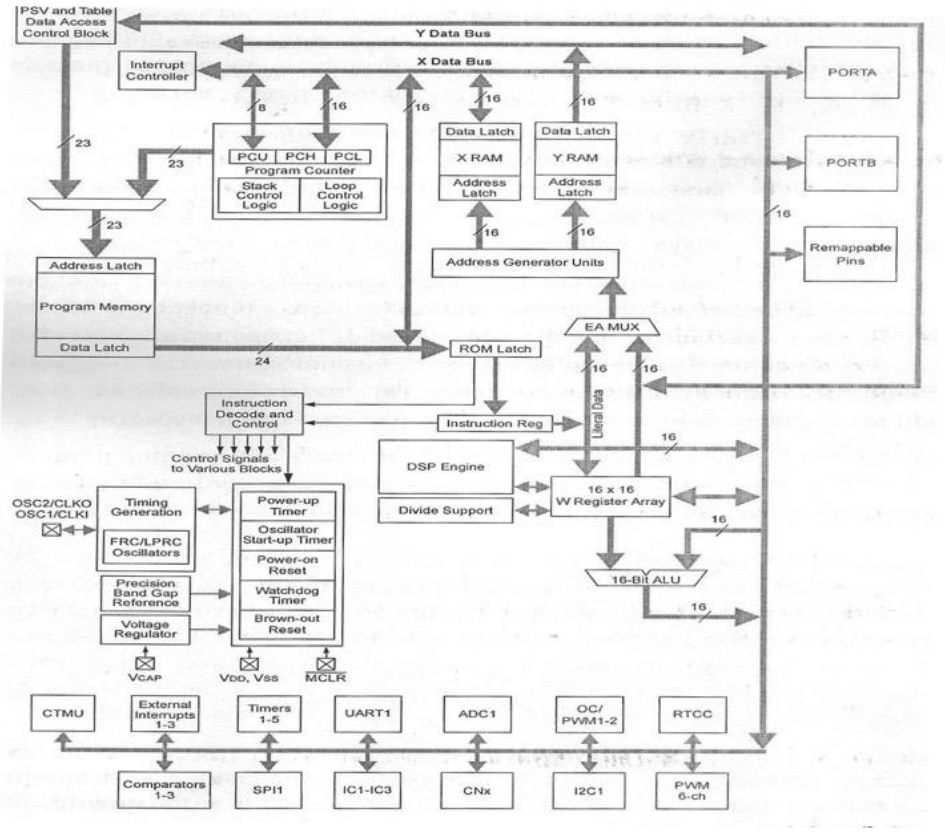


Рисунок 3.3 – Структурна схема мікроконтролера DSPIC33FJ16MC102

Схему входів/виходів мікроконтролера з позначеннями входів/виходів показано на рисунку 3.4

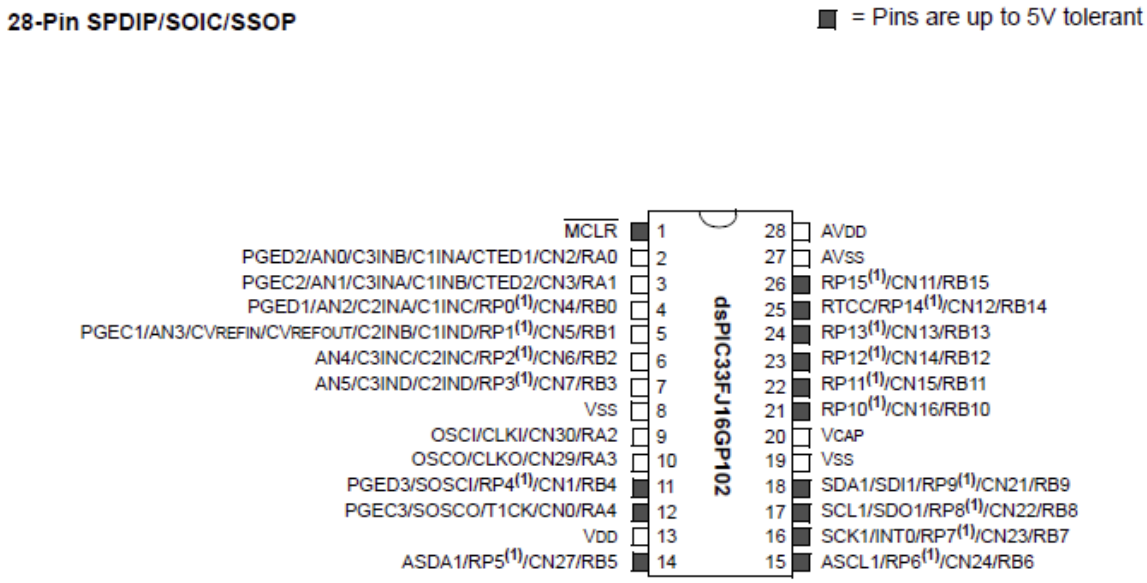


Рисунок 3.4 – Загальна структура мікроконтролера DSPIC33FJ16MC102

3.2 Проектування електричної схеми

На рисунку 3.5 наведено електричну схему з’єднання модуля RN4020 із мікроконтролером DSPIC33FJ16MC102, а також підключення до нього зовнішнього конектора, що забезпечує взаємодію з іншими елементами системи.

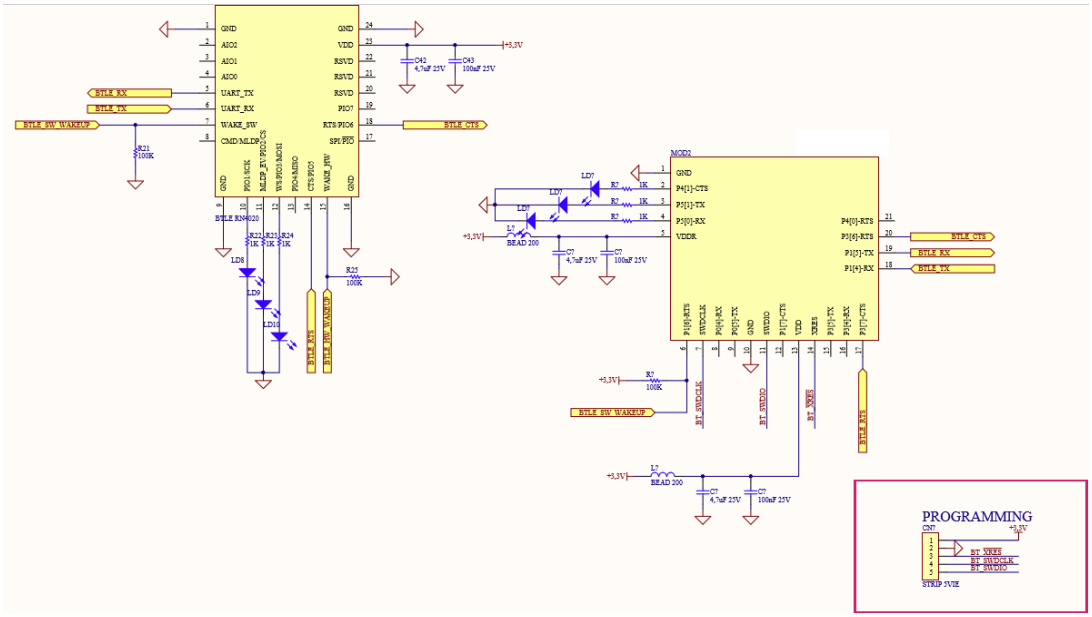


Рисунок 3.5 – Схема з’єднання RN4020 та мікроконтролера.

Програмування мікроконтролера

Програмне забезпечення для мікроконтролера розроблено у середовищі MPLAB X IDE, яке надає зручні інструменти для створення, налагодження та тестування програмного коду для мікроконтролерів сімейства Microchip.

Під час розробки використовувалися апаратні засоби відладки та програмування PICkit 3, що дозволяють здійснювати завантаження прошивки безпосередньо до мікроконтролера, а також покрокове налагодження програми в режимі реального часу.

Апаратний засіб програмування та відладки PICkit 3 наведено на рисунку 3.6.

Рисунок 3.6 – відладчик-програматор PICkit

PICkit 3 - це простий у використанні налагоджувач і програматор, що працює у зв'язці з персональним комп'ютером, на якому встановлено середовище MPLAB X IDE. Пристрій є невід'ємною частиною комплексу апаратних та програмних інженерних засобів компанії Microchip Technology Inc., призначених для роботи з мікроконтролерами сімейства PIC (MCU) та цифровими сигнальними контролерами dsPIC (DSP).

Програматор PICkit 3 реалізує інтерфейс ICSP (In-Circuit Serial Programming), що забезпечує двонаправлений послідовний обмін даними між мікроконтролером і комп'ютером під час програмування або налагодження. Це дозволяє виконувати покрокове тестування, перегляд змінних у реальному часі та оновлення прошивки безпосередньо в схемі.

MPLAB X IDE - це інтегроване середовище розроблення (IDE), що функціонує під сучасними операційними системами (Windows, macOS, Linux). Воно створене на основі відкритої платформи NetBeans і забезпечує повний цикл розробки програмного забезпечення для мікроконтролерів і цифрових сигнальних процесорів Microchip - від написання та компіляції коду до відлагодження і тестування.

Увесь програмний проєкт у середовищі MPLAB X IDE структуровано у декілька папок і файлів, згрупованих відповідно до їхнього функціонального призначення, що продемонстровано на рисунку 3.7.

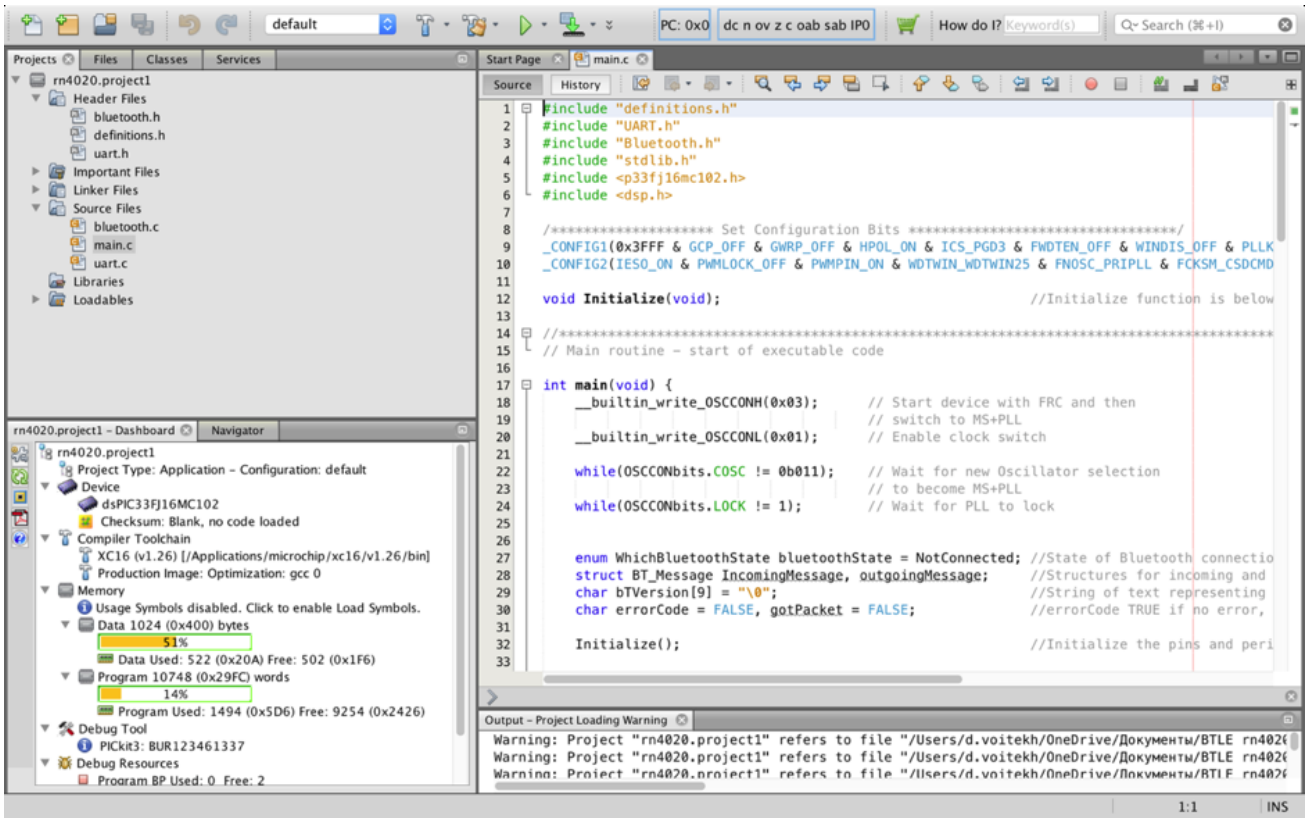


Рисунок 3.7 – Проект у програмному середовищі MPLAB X IDE

Нижче наведено основні фрагменти коду розробленого проєкту.

Файл “definitions.h” містить оголошення глобальних змінних і визначення констант, що використовуються у програмі. У цьому файлі здійснюється присвоєння програмним змінним номерів портів мікроконтролера, визначається розмір буферів для обміну даними та задається формат передаваних повідомлень.

Таким чином, цей файл виконує роль централізованого модуля параметрів конфігурації, який забезпечує узгодженість усіх програмних компонентів системи. Одна з частин коду даного файлу:

```
#define BLE_CONNECTED PORTBbits.RB1 //Bluetooth module is
connected to central
#define SIZE_RxBuffer 256 //UART_RX buffer size in bytes
#define SIZE_TxBuffer 256 //UART_TX buffer size in bytes
enum WhichBluetoothState {NotConnected, Connected};
```

```
struct BT_Message //form of message
{
char Command;
char Data;
};
```

Файл “bluetooth.c” містить реалізацію функцій, відповідальних за передавання та приймання даних між мікроконтролером і модулем Bluetooth RN4020. У цьому модулі зосереджено логіку взаємодії з бездротовим інтерфейсом, включно з ініціалізацією з’єднання, обробкою запитів і передаванням інформації у двосторонньому режимі.

Нижче наведено приклад функції, яка ініціалізує роботу Bluetooth-модуля за допомогою набору команд, що активують необхідні сервіси та характеристики пристрою. Ця функція виконує первинне налаштування RN4020, зокрема:

– встановлення параметрів обміну даними через UART;

– запуск BLE-сервісу;

– активацію характеристик пристрою;

– підготовку модуля до приймання та передавання даних у реальному часі.

```
char BT_SetupModule()
{
BT_SendCommand("sf,1\r"); //reset module settings
BT_SendCommand("ss,30000000\r");
BT_SendCommand("sr,32000000\r");
BT_SendCommand("sn, Ener1 \r"); //set name
BT_SendCommand("r,1\r"); //reload module to enable changes
return TRUE
}
```

Далі наведено функцію, яка реалізує передавання повідомлень через інтерфейс UART до модуля Bluetooth RN4020. Ця функція забезпечує послідовну передачу даних у форматі, сумісному з протоколом RN4020, та використовується для обміну інформацією між мікроконтролером і бездротовим модулем у процесі роботи системи.

```
char BT_SendPacket(struct BT_Message *MessageOut)
{
WriteTxBuffer(BT_SOF_1);
WriteTxBuffer(BT_SOF_2);
WriteTxBuffer((int)MessageOut->Command);
WriteTxBuffer((int)MessageOut->Data);
WriteTxBuffer('\r'); //Load carriage return
WriteTxBuffer('\n'); //Load line feed
UART_TxStart(); //Start the transmission
return TRUE;
}
```

Далі наведено функцію, яка здійснює приймання повідомлень від модуля Bluetooth RN4020 через інтерфейс UART. Вона відповідає за зчитування вхідних даних, їх буферизацію та подальшу обробку мікроконтролером, що забезпечує коректний обмін інформацією між бездротовим модулем і системою керування.

```
char BT_ReceivePacket(struct BT_Message *Message)
{
char messageChar;
if (IsNewRxData())
{
messageChar = ReadRxBuffer();
if(messageChar == '\n')
return TRUE;
```

```
}
return FALSE;
}
```

Файл “main.c”

Нижче наведено фрагмент основного нескінченного циклу програми, у якому реалізовано підключення до пристрою Bluetooth RN4020, передавання даних та перевірку наявності вхідних повідомлень. Отримані повідомлення аналізуються мікроконтролером, після чого відбувається керування комутацією навантаження відповідно до отриманих команд користувача або стану системи.

```
if(bluetoothState == Connected)
{
sendADCvalues();
gotPacket = BT_ReceivePacket(&IncomingMessage);
if(gotPacket == TRUE)
{
if(IncomingMessage.Command == SWITCH)
{
TRIAC_1 = (TRIAC_1 + 1) % 2;
}
}
}
```

Таким чином, розроблена програма забезпечує двосторонню взаємодію між мікроконтролером і смартфоном. Після встановлення з’єднання через інтерфейс Bluetooth, система розпочинає передавання даних вимірюваних параметрів - таких як струм, напруга та температура - у режимі реального часу.

У зворотному напрямку смартфон або інший керуючий пристрій може надсилати на мікроконтролер керуючі команди типу SWITCH, які обробляються програмою. У відповідь мікроконтролер активує оптронний комутатор, здійснюючи вмикання або вимикання електричного обладнання системи «Розумний дім».

Для реалізації системи, яка інтегрує всі описані нижче компоненти в єдину архітектуру, було розроблено сучасну програмну структуру керування системою «Розумний дім». Вона передбачає взаємодію між апаратними пристроями, серверними компонентами та користувацькими інтерфейсами.

Архітектура включає такі основні етапи та компоненти:

– чіп Bluetooth Low Energy (BLE) забезпечує підключення та отримання даних від пристроїв типу SmartSwitch за протоколом Bluetooth Low Energy. У штатному режимі він передає отримані дані на веб-сервер, який виконує обробку за допомогою алгоритму оптимізації. На підставі отриманих результатів BLE-сервер формує керуючий сигнал, який передається на відповідний пристрій SmartSwitch для виконання команд (вмикання або вимикання навантаження).

– веб-плагін виконує функції зберігання даних, отриманих від BLE-пристроїв, а також реалізує обробку та оптимізацію інформації. На основі аналізу даних формуються інструкції для вмикання чи вимикання побутових приладів, що дозволяє обмежувати навантаження на електричне коло або запобігати аварійним ситуаціям.

Крім того, веб-плагін надає API-інтерфейс, який забезпечує зручне керування файловою системою через графічний інтерфейс браузера.

На рисунку 4.8 наведено контекстну діаграму DFD (Data Flow Diagram) системи, яка відображає основні потоки даних між її компонентами.

Рисунок 3.8 – Початкова контекстна DFD діаграма

На рисунку 3.9 представлено деталізацію блока A0 відповідно до архітектури програмної системи. Цей блок реалізує взаємодію між двома сокетами, що обмінюються даними за допомогою протоколу WebSocket, а також містить інтерфейс копіювання (mirror-interface), який використовується для моніторингу та керування роботою системи у режимі реального часу.

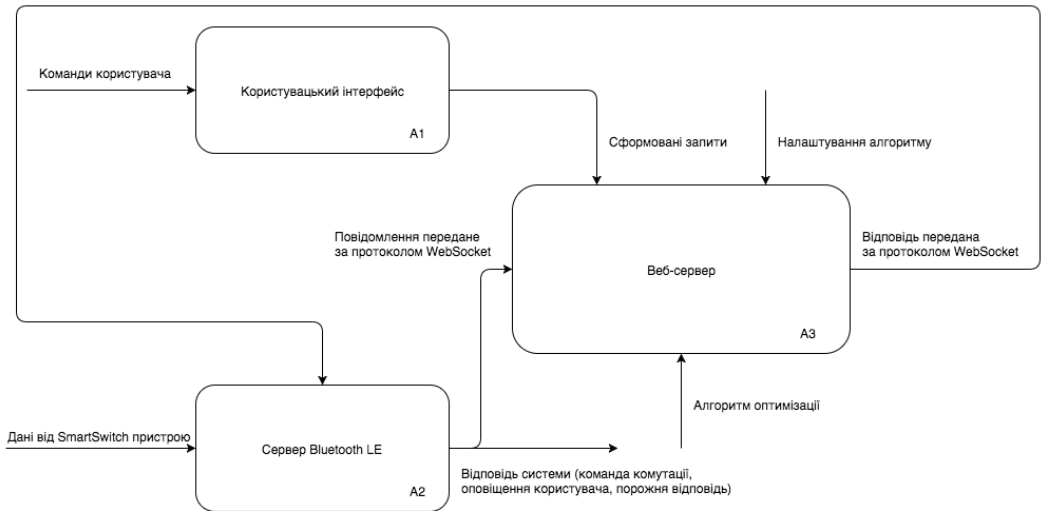


Рисунок 3.9 – Деталізована контекстна DFD діаграма

Для реалізації програмної частини системи було обрано мову програмування JavaScript та платформу Node.js, яка забезпечує асинхронну обробку подій і є ефективним інструментом для створення високопродуктивних мережевих застосунків у реальному часі.

У якості системи керування базами даних (СКБД) використано PostgreSQL, що забезпечує надійне зберігання структурованих даних. Для кешування проміжних результатів та системних налаштувань застосовано Redis — нереляційну базу даних типу “ключ–значення”, яка відзначається високою швидкодією доступу до даних.

Для обміну даними в реальному часі між веб-інтерфейсом і пристроями Bluetooth Low Energy (BLE) обрано протокол WebSocket, який забезпечує двонапрямлений постійний зв’язок між клієнтською та серверною частинами системи.

Програмний код системи подано у вкладенні, де використано такі бібліотеки та фреймворки:

– Noble – багатоплатформна бібліотека на JavaScript, призначена для роботи з пристроями Bluetooth Low Energy у середовищах MacOS, Linux та Windows;

– Express.js – програмний фреймворк для створення веб-застосунків і REST API у середовищі Node.js; відзначається мінімалістичною архітектурою та широкими можливостями розширення за рахунок плагінів;

– Socket.IO – бібліотека, що реалізує протокол WebSocket для обміну даними в реальному часі між клієнтами та сервером; підтримує також альтернативні методи зв’язку (JSONP, AJAX) залежно від мережевих умов;

– pg-promise – JavaScript API для зручної роботи з базою даних PostgreSQL, що забезпечує підключення, виконання SQL-запитів та обробку результатів;

– redis – JavaScript API для взаємодії з базою Redis, який дозволяє ефективно оперувати кешованими даними без необхідності використання SQL-запитів;

– Vue.js – фронтенд-фреймворк для створення динамічного користувацького інтерфейсу (UI), що підтримує реактивне оновлення даних і спрощує інтеграцію з серверною частиною.

Сервер Bluetooth LE. Бібліотека Noble

Бібліотека Noble використовується у вигляді вихідного коду на мові JavaScript і надає зручний прикладний програмний інтерфейс (API) для реалізації всіх необхідних типів взаємодії за протоколом Bluetooth Low Energy (BLE). Її робота побудована на подієвій (event-driven) парадигмі програмування, що є характерною для середовища JavaScript та дозволяє ефективно обробляти асинхронні процеси обміну даними між пристроями.

1) Сканування активних пристроїв мережі:

```
noble.on('stateChange', function(state) {
if (state === 'poweredOn') {
noble.startScanning();
} else {
noble.stopScanning();
}
});
```

2) К Callback-функція (зворотний виклик) використовується для обробки події виявлення нового пристрою під час сканування Bluetooth Low Energy (BLE)-мережі. У середині тіла цієї функції реалізується основна логіка взаємодії з виявленим пристроєм, зокрема:

– встановлення з’єднання;
– ініціалізація сеансу обміну даними;
– передавання та приймання інформації;
– виконання необхідних команд або налаштувань.

```
noble.on('discover', function(peripheral) {
console.log('peripheral: ', peripheral.advertisement.localName);
});
```

3) Підключення до виявленого пристрою. Ідентифікація пристроїв у процесі сканування та встановлення з’єднання здійснюється за унікальними ідентифікаторами:

– UUID (Universally Unique Identifier) - унікальний ідентифікатор пристрою або сервісу, який використовується для його розпізнавання в мережі Bluetooth;

– MAC-адреса Bluetooth-адаптера - апаратний ідентифікатор, що дозволяє однозначно визначити конкретний пристрій серед інших.

Після розпізнавання цих параметрів система ініціює процес підключення до обраного пристрою, встановлює сеанс зв’язку та готує канал для передачі і приймання даних через протокол Bluetooth Low Energy.

```
peripheral.connect(function(error) {
console.log('connected to peripheral: ', peripheral.uuid);
});
```

4) Відключення:

```
peripheral.disconnect(function(error) {
console.log('disconnected from peripheral: ', peripheral.uuid);
});
```

5) Отримання всіх сервісів пристрою. У системі Bluetooth Low Energy (BLE) сервіси виступають своєрідними функціональними модулями пристрою, кожен з яких виконує певне призначення - наприклад, вимірювання температури, контроль рівня заряду, передавання даних або керування станом пристрою.

Кожен сервіс має власний унікальний ідентифікатор (UUID), який дозволяє ідентифікувати його серед інших. Кількість сервісів у межах одного пристрою не обмежується - залежно від призначення, пристрій може підтримувати один або декілька сервісів одночасно.

Після встановлення з’єднання програмна частина системи виконує отримання списку всіх доступних сервісів BLE-пристрою, що дає змогу

визначити можливості взаємодії та виконати подальшу ініціалізацію характеристик для обміну даними.

```
peripheral.discoverServices(null, function(error, services) {
console.log('discovered the following services:', services);
});
```

6) Отримання всіх характеристик певного сервісу.

Після визначення доступних сервісів пристрою виконується отримання всіх характеристик (characteristics) обраного сервісу. Характеристики виступають інтерфейсами взаємодії, через які інші пристрої можуть зчитувати, записувати або отримувати сповіщення про зміну даних у межах конкретного сервісу.

Кожна характеристика має власний унікальний ідентифікатор (UUID) та визначає тип операції, яку дозволено виконувати. Залежно від призначення, характеристики поділяються на три основні типи:

– read - характеристики, призначені для зчитування даних із пристрою (наприклад, температури, напруги, струму тощо);

– write - характеристики, що дозволяють передавати дані або команди на пристрій для зміни його стану чи параметрів;

– indicate - характеристики, які використовуються для сповіщення про зміни даних або подій, ініційованих самим пристроєм.

Отримання повного набору характеристик певного сервісу забезпечує повноцінну взаємодію системи з BLE-пристроєм і дозволяє реалізувати двонапрямлений обмін даними в реальному часі.

```
service.discoverCharacteristics(null, function(error, characteristics) {
console.log('discovered characteristics:', characteristics);
});
```

7) Зчитування даних характеристики пристрою (для характеристик типу read). Для отримання поточних значень параметрів пристрою використовується операція зчитування характеристики (read characteristic). Вона дозволяє отримати значення змінної, збереженої в межах певного

сервісу, наприклад - температуру, напругу, струм або інший технологічний параметр.

У процесі виконання операції програма надсилає запит на зчитування до відповідної характеристики пристрою, після чого отримує відповідь у вигляді байтового масиву. Далі дані інтерпретуються та перетворюються у зручний формат (наприклад, у числові значення фізичних величин), що дає змогу відображати їх у веб-інтерфейсі або передавати для подальшої обробки.

Таким чином, операція read забезпечує пасивний режим збору даних із пристрою та використовується для моніторингу стану елементів системи в режимі реального часу.

```
characteristic.read(function(error, data) {
console.log(data.toString('utf8'));
});
```

8) Підписка на нові дані від характеристики (для характеристик типу indicate). Для забезпечення автоматичного отримання оновлених даних від пристрою використовується механізм підписки на характеристику типу indicate. У цьому режимі пристрій самостійно ініціює передачу повідомлення щоразу, коли значення характеристики змінюється, без необхідності періодичного опитування з боку програми.

Після активації підписки клієнт (наприклад, сервер або веб-додаток) реєструє спеціальну callback-функцію, яка автоматично викликається при отриманні нових даних. Це забезпечує роботу системи в реальному часі, зокрема в процесах моніторингу стану обладнання, енергоспоживання або температурних змін.

Такий підхід значно підвищує ефективність обміну даними, оскільки зменшує кількість запитів до пристрою та мінімізує затримку отримання актуальної інформації.

```
characteristic.on('data', function(data, isNotification) {
console.log(data.toString('utf8'));
});
```

9) Надсилання даних до характеристики пристрою (для характеристик типу write). Операція запису даних (write) використовується для передавання керуючих команд або параметрів від програми до пристрою Bluetooth Low Energy. Такий тип характеристик дозволяє змінювати стан або режим роботи пристрою, наприклад - вмикати чи вимикати навантаження, оновлювати налаштування або задавати нові порогові значення вимірюваних параметрів.

У процесі виконання цієї операції програма формує пакет даних у відповідному форматі та надсилає його через інтерфейс BLE до характеристики пристрою. Після отримання повідомлення пристрій обробляє команду й виконує відповідну дію, що дозволяє реалізувати активне керування компонентами системи «Розумний дім».

Таким чином, характеристики типу write забезпечують зворотний зв’язок у системі, створюючи можливість інтерактивного управління обладнанням у реальному часі write):

```
characteristic.write(new Buffer([0x01]), true, function(error)
{
console.log('sent’);
});
```

Слід зазначити, що бібліотека Noble має певні обмеження щодо кількості одночасних підключень до мережі Bluetooth Low Energy. Це обмеження залежить від продуктивності та типу Bluetooth-адаптера (вбудованого або зовнішнього) і зазвичай становить близько 10 активних з’єднань одночасно.

Втім, бібліотека передбачає ефективний механізм динамічного підключення пристроїв, який дозволяє встановлювати з’єднання лише на час передавання або отримання даних. Завдяки такому підходу забезпечується раціональне використання ресурсів адаптера та практично усувається обмеження щодо кількості одночасних підключень у мережі BLE.

Express.js

Фреймворк Express.js, написаний мовою JavaScript, використовується як основний веб-сервер системи та є де-факто стандартом для більшості інтерактивних застосунків, розроблених на платформі Node.js.

Express.js створено за аналогією з фреймворком Ruby Sinatra, і його головною метою є забезпечення високої швидкодії та точності оброблення HTTP-запитів. Завдяки мінімалістичній архітектурі Express.js дозволяє гнучко керувати маршрутизацією, middleware-компонентами та API-запитами, що робить його оптимальним рішенням для побудови веб-інтерфейсів і REST-сервісів у системі «Розумний дім».

Як приклад, нижче наведено текстовий код програми:

```
var express = require('express')
var app = express
()
app.get('/', function (req, res)
 {
res.send('Hello World')
})
app.listen(3000)
```

Наведений фрагмент коду створює екземпляр веб-застосунку Express.js та запускає його на порту 3000. Після успішного запуску сервер очікує вхідні запити, а при зверненні до веб-сторінки за адресою http://localhost:3000 у браузері відображається повідомлення «Hello, World!», що підтверджує коректну роботу веб-сервера.

Спеціалізація

У цьому блоці описано архітектуру комплексного веб-сервера системи «Розумний дім», а також алгоритм оптимізації енергоспоживання побутової техніки.

Функціональність веб-сервера умовно поділяється на дві основні групи:

– обробка запитів від користувацького веб-інтерфейсу (інтерфейсу копіювання) - забезпечує відображення поточного стану пристроїв, взаємодію користувача із системою та відправлення керуючих команд;

– обробка даних, отриманих за протоколом WebSocket від BLE-сервера, який відповідає за збір інформації з пристроїв Bluetooth Low Energy і передачу її до центрального веб-сервера для подальшого аналізу.

– системна база даних веб-сервера складається з двох основних таблиць:

– Devices - містить інформацію про зареєстровані пристрої системи, їхній поточний стан, параметри роботи та ідентифікаційні дані;

– Logs - зберігає журнал подій, зокрема історію отриманих даних від пристроїв Bluetooth LE, керуючих команд та результатів їх виконання.

Нові записи в базі даних створюються автоматично під час надходження даних від BLE-пристроїв. На основі цих записів формується зведена інформаційна сторінка, що відображає актуальний стан кожного побутового приладу та всієї системи загалом.

Зв’язки сутностей бази даних системи зображено на рисунку 3.10, який демонструє логічну структуру та взаємодію між таблицями Devices і Logs.

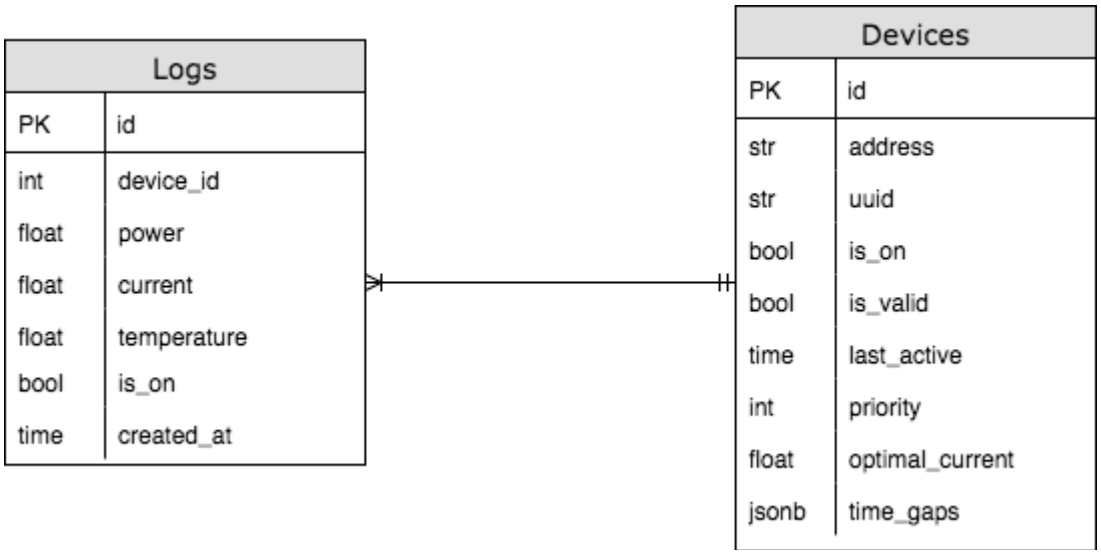


Рисунок 3.10 – ER діаграма бази даних

3.3 Розробка алгоритму оптимізації системи

Деталі реалізації алгоритму оптимізації енергоспоживання системи наведено нижче. Основні системні параметри (Settings) зберігаються у вигляді пар “ключ–значення”, кожна з яких визначає певний показник, що впливає на роботу системи. Для підвищення швидкодії доступу до параметрів використовується сховище Redis, що забезпечує високу конкурентність при операціях читання та запису.

Перелік основних системних налаштувань:

– AUTO_MODE = <bool> - встановлює режим роботи системи.Якщо значення false, система працює лише в режимі навчання через інтерфейс введення, тобто автоматичні дії не виконуються. Якщо значення true, система переходить у автоматичний режим, у якому алгоритм самостійно приймає рішення про необхідність комутації навантажень.

– POWER = <float> - параметр алгоритму, що визначає максимально допустиме сумарне навантаження системи (у ватах). При перевищенні цього значення пристрій автоматично відключається від електромережі, після чого з певною періодичністю здійснюються спроби повторного підключення.

– TEMPERATURE = <float> — параметр, що задає граничне значення температури для окремого пристрою. У разі перевищення цього порогу система відключає відповідний пристрій, а його стан позначається як is_valid = false, що забороняє його повторне підключення до моменту стабілізації параметрів.

На рисунку 3.11 подано інтерфейс редагування системних параметрів, який дає змогу додавати, змінювати або видаляти налаштування безпосередньо з панелі керування системи.

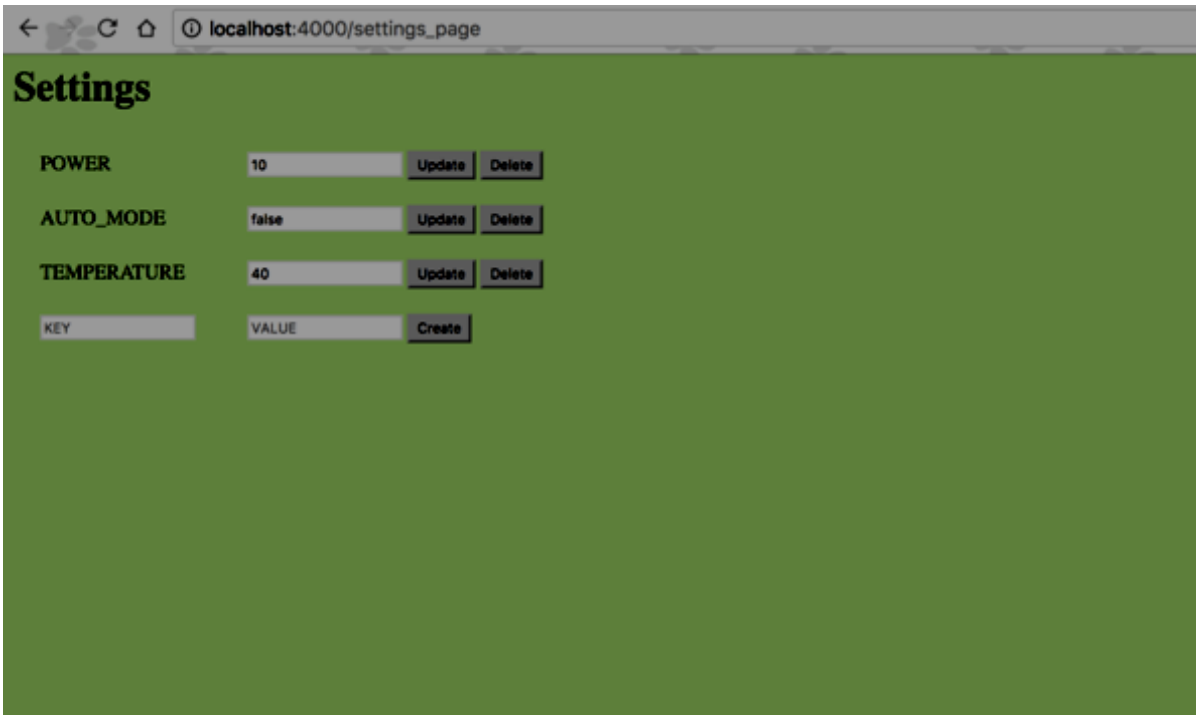


Рисунок 3.11 – Користувацький інтерфейс для управління налаштуваннями

Веб-інтерфейс системи

Для реалізації веб-інтерфейсу веб-сервера було обрано фреймворк Vue.js, який забезпечує зручне шаблонування HTML-компонентів за допомогою анотацій, подібних до Angular, а також підтримує двостороннє зв’язування даних (two-way data binding) та автоматичне оновлення стану інтерфейсу.

Обмін даними між клієнтською частиною (Vue.js) і веб-сервером здійснюється за допомогою AJAX-запитів у форматі JSON. Для цього використано AJAX API бібліотеки jQuery, яке пройшло попереднє тестування на сумісність із серверною частиною. Такий підхід дозволяє оновлювати дані у браузері без перезавантаження сторінки, забезпечуючи інтерактивність і динамічність користувацького інтерфейсу.

Інтервал автоматичного оновлення даних становить 1 секунду, що дає змогу контролювати стан системи «Розумний дім» у реальному часі, відображаючи актуальні показники з пристроїв.

На рисунку 3.12 наведено зовнішній вигляд головної сторінки веб-сервера, яка відображає інформацію про поточний стан системи, параметри пристроїв і результати роботи алгоритмів оптимізації.

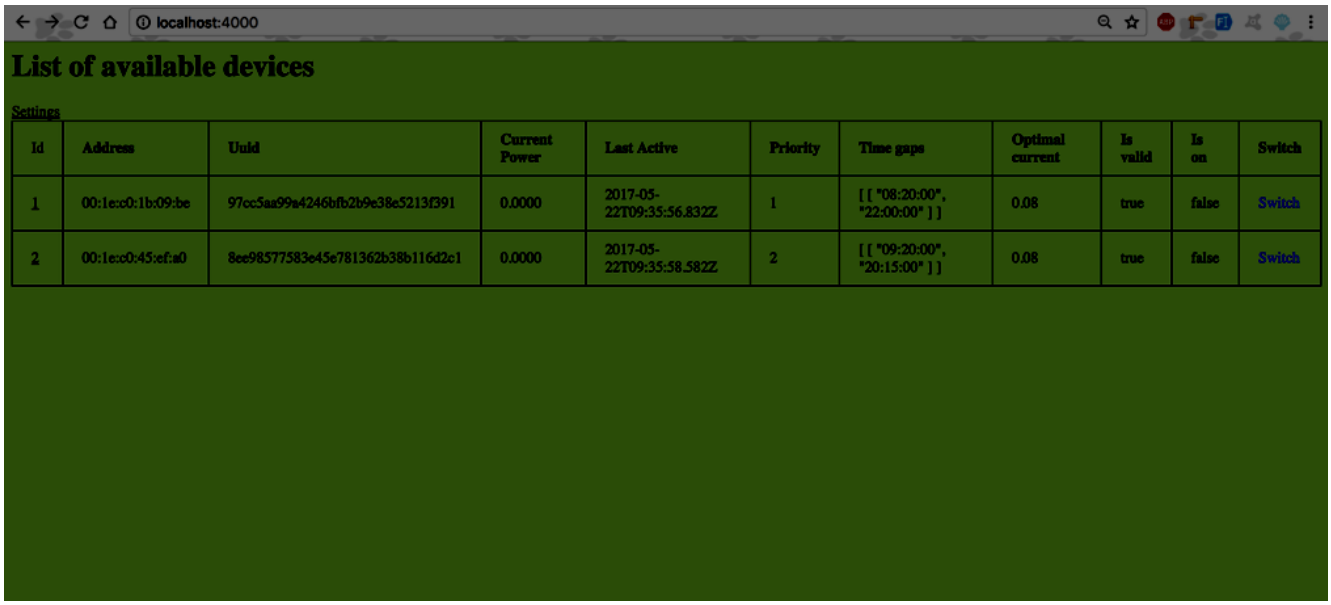


Рисунок 3.12 – Домашня сторінка додатка

Підсистема безпеки

Загрозою інформаційній безпеці вважається подія або дія, яка може призвести до зміни у функціонуванні системи, що спричинює порушення конфіденційності, цілісності або доступності інформації, яка в ній обробляється.

Вразливість інформації - це можливість виникнення такого стану, за якого створюються умови для реалізації потенційних загроз інформаційній безпеці.

Атака на інформаційну систему (ІС) - це сукупність цілеспрямованих дій зловмисника, спрямованих на виявлення та використання вразливостей системи. Іншими словами, атака на комп’ютерну систему є реалізацією конкретної загрози інформаційній безпеці.

Проблеми, що виникають у процесі передачі інформації в комп’ютерних мережах, можна поділити на три основні типи [17]:

– перехоплення інформації - зберігається цілісність даних, однак порушується конфіденційність;

– модифікація інформації - вихідне повідомлення змінюється або підмінюється іншим, яке згодом надсилається адресатові;

– зміна авторства інформації - порушується автентичність джерела повідомлення, наприклад, шляхом спуфінгу (spoofing), коли зловмисник видає себе за іншу особу або веб-ресурс.

Такі дії можуть мати серйозні наслідки, наприклад - викрадення даних банківських карток через фальшиві веб-сайти або підміну електронної пошти.

Особливість комп'ютерних мереж, з точки зору інформаційної безпеки, полягає в тому, що вони забезпечують інтенсивну інформаційну взаємодію між віддаленими та різнорідними елементами, що значно підвищує рівень уразливості. Уразливими є майже всі складові інформаційних систем:

– робочі станції;

– сервери (хост-машини);

– мережеві шлюзи та комутатори;

– канали передавання даних.

Існує велика кількість загроз інформаційній безпеці різного походження. У науковій літературі наведено численні класифікації загроз, у яких як критерії використовуються тип небезпеки, джерело походження, ступінь злого умислу та наслідки реалізації.

Одну з найпоширеніших класифікацій загроз інформаційній безпеці подано на рисунку 3.13.

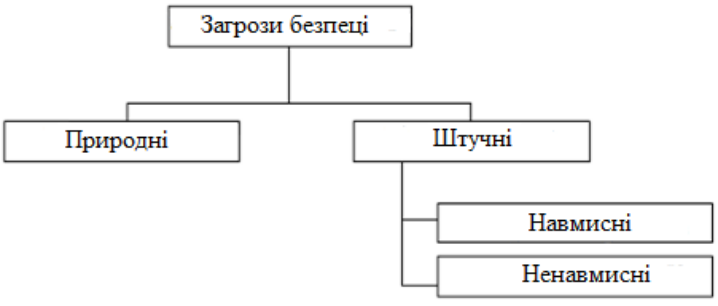


Рисунок .13 - Загальна класифікація загроз безпеки.

Природні загрози - це загрози, що виникають унаслідок впливу на інформаційну систему або її елементи об’єктивних фізичних процесів чи стихійних природних явищ, незалежних від людської діяльності. До таких загроз належать, зокрема, грози, пожежі, повені, землетруси, перепади напруги в електромережі, вплив магнітних полів тощо.

Штучні загрози - це загрози, спричинені діяльністю людини, які можуть бути як ненавмисними, так і навмисними.

– ненавмисні (випадкові) загрози виникають унаслідок помилок проєктування або експлуатації інформаційної системи, недоліків програмного забезпечення, збоїв обладнання чи неправильних дій персоналу.

– навмисні загрози пов’язані з цілеспрямованими діями зловмисників, які мають корисливі або руйнівні мотиви, наприклад спроби несанкціонованого доступу, знищення або викрадення даних.

На рисунку 3.14 подано класифікацію основних видів загроз безпеці інформації в комп’ютерних мережах, що охоплює природні, техногенні та антропогенні фактори впливу.

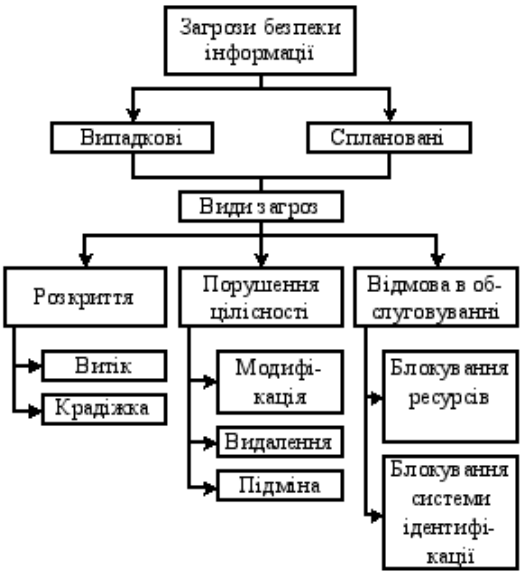


Рисунок 3.14 – види загроз безпеки інформації в КМ

Ненавмисні загрози інформаційній безпеці

Найпоширенішими та водночас найнебезпечнішими загрозами для інформаційної безпеки є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують комп'ютерну мережу.

Такі помилки можуть проявлятися у вигляді неправильно введених даних, помилок у програмному забезпеченні, що призводять до збоїв системи, або у формі адміністративних помилок, які створюють додаткові вразливості, якими можуть скористатися зловмисники. За статистичними даними, до 65 % усіх втрат у сфері інформаційної безпеки є наслідком саме ненавмисних дій персоналу.

Отже, необережність і недостатня компетентність користувачів завдають значно більше шкоди, ніж стихійні лиха- пожежі чи повені. Найбільш ефективними заходами протидії цим загрозам є максимальна автоматизація процесів і жорсткий контроль за діями персоналу.

Інші загрози доступності можна класифікувати за компонентами інформаційної системи, на які вони спрямовані:

– відмова користувача - свідоме або вимушене припинення роботи з системою;

– збій внутрішньої мережі - втрата зв'язку між вузлами системи або недоступність серверних ресурсів;

– вихід з ладу підтримуючої інфраструктури - відмова енергопостачання, охолодження, комунікаційного обладнання тощо.

– людський фактор як джерело загроз.

Для користувачів інформаційних систем типовими є такі проблеми:

– небажання працювати з системою, що часто виникає при необхідності опанування нових функцій або у випадках, коли можливості системи не відповідають очікуванням користувача;

– невміння працювати з програмним забезпеченням через відсутність відповідної підготовки, низький рівень комп'ютерної грамотності,

нерозуміння діагностичних повідомлень або нездатність користуватися технічною документацією;

– неможливість роботи із системою через нестачу технічної чи довідкової підтримки, неповну документацію або відсутність інструкцій.

Таким чином, людський фактор залишається одним із найкритичніших елементів інформаційної безпеки, і його вплив необхідно мінімізувати шляхом навчання, автоматизації та регламентування дій персоналу.

Програмні атаки

Надмірне навантаження на ресурси інформаційної системи (пропускну здатність мережі, обчислювальні можливості процесора або обсяг оперативної пам’яті) може бути використане як інструмент для виведення системи з нормального режиму роботи.

За місцем виникнення джерела загрози надмірне споживання ресурсів поділяється на:

– локальне, коли через прорахунки у конфігурації системи окрема програма може практично монополізувати процесор чи пам’ять, знижуючи швидкодію інших процесів до мінімуму;

– віддалене, коли навантаження створюється через мережеві атаки.

Одним із найпростіших прикладів віддаленого перевантаження є атака типу “SYN-flood”, під час якої зловмисник переповнює таблицю “напіввідкритих” TCP-з’єднань на сервері, ініціюючи їх створення без завершення процесу встановлення. У результаті сервер стає недоступним для легальних користувачів, оскільки не може опрацьовувати нові запити.

Останніми роками набули поширення розподілені атаки на відмову в обслуговуванні (DDoS-атаки), коли велика кількість легітимних запитів одночасно надсилається на сервер із багатьох різних адрес. Такі атаки здатні перевантажити мережеві канали або процесорні ресурси сервера, що призводить до припинення його нормального функціонування. Перші масштабні випадки таких атак були зафіксовані у лютому 2000 року, коли жертвами стали провідні системи електронної комерції. Якщо в архітектурі

системи існує дисбаланс між пропускною здатністю мережі та продуктивністю сервера, захист від подібних атак є надзвичайно складним завданням.

Для забезпечення комплексного захисту інформації в комп'ютерних мережах необхідно реалізувати такі завдання:

– захист інформації в каналах зв'язку та базах даних за допомогою криптографічних методів;

– аутентифікація користувачів і об'єктів даних, тобто підтвердження достовірності сторін, що здійснюють обмін;

– виявлення порушень цілісності інформаційних об'єктів;

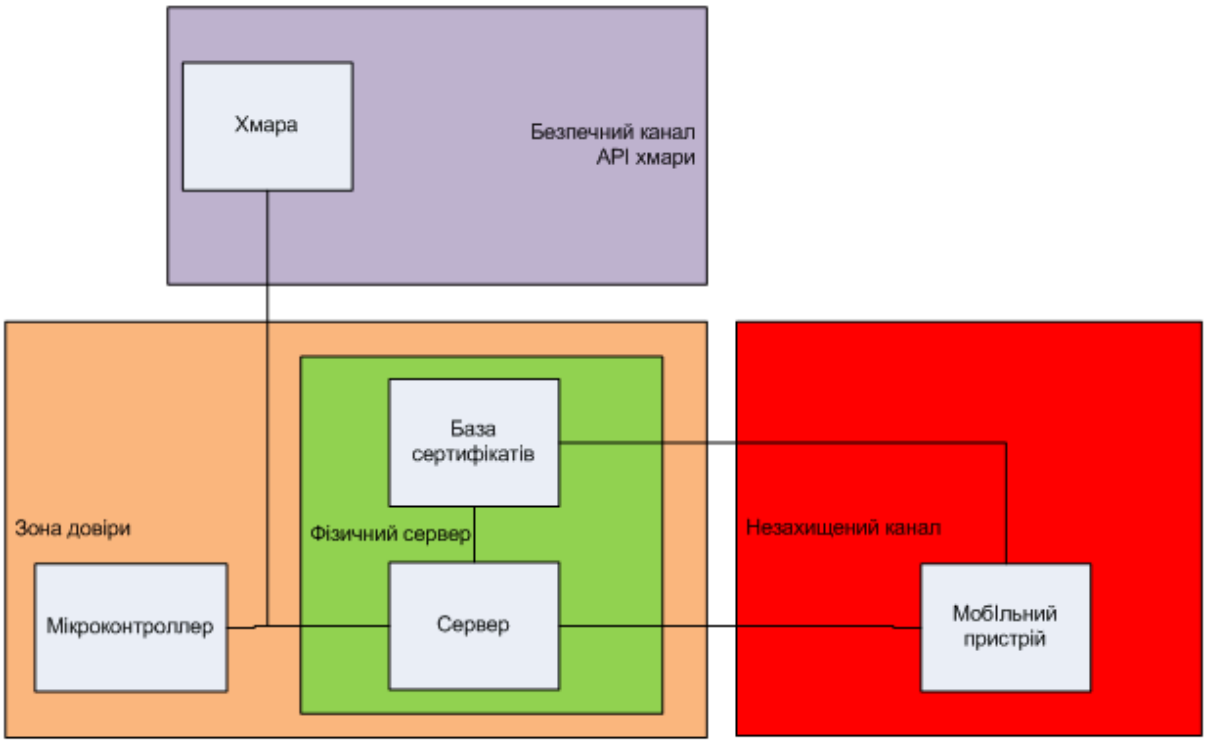
– захист технічних засобів і приміщень, у яких обробляється конфіденційна інформація, від витоку через побічні канали або встановлених шкідливих пристроїв перехоплення;

– захист програмного забезпечення та комп'ютерної техніки від вірусів, шкідливих закладок і несанкціонованих модифікацій;

– захист каналів зв'язку від несанкціонованого втручання, коли сторонні особи намагаються скомпрометувати секретну інформацію або порушити роботу абонентських пунктів;

– організаційно-технічні заходи, спрямовані на підтримання безпеки конфіденційних даних, включно з політиками доступу, резервним копіюванням та контролем активності користувачів.

Схема передачі даних розумного дому та виявлення потенційної небезпеки.



Рисунко 3.15 – Схема передачі даних в системі «Розумний дім»

3.4 Захист інформації в системі

База сертифікатів є частиною фізичного сервера, де зберігаються всі цифрові підписи та ключі шифрування. Логічний сервер має повний доступ до цих даних, тоді як користувач отримує обмежений (частковий) доступ через свій мобільний пристрій.

Мікроконтролер виступає як основний апаратний елемент, що безпосередньо керує пристроями «розумного будинку». Обмін даними між мікроконтролером, сервером і користувачем здійснюється через локальну мережу, де інформація вважається умовно захищеною.

Основна небезпека виникає в зоні користувацького каналу зв’язку, який часто є незахищеним. Одним із типових сценаріїв атаки є «людина посередині» (Man-in-the-Middle, MITM), коли зловмисник перехоплює комунікацію між сервером і клієнтом, видаючи себе за одну зі сторін, що дозволяє читати або змінювати передані дані.

Для запобігання таким загрозам необхідно використовувати системи криптографічного захисту даних, зокрема схеми симетричного та асиметричного шифрування.

Вибір системи шифрування. Серед сучасних рішень найбільш ефективною є система, що базується на інфраструктурі відкритих ключів (PKI - Public Key Infrastructure). Вона забезпечує надійний та захищений канал обміну сеансовими ключами між сервером і клієнтом.

У такій системі використовується сертифікат користувача, який містить пару ключів — відкритий і секретний.

– секретний ключ зберігається виключно у користувача.

– відкритий ключ - у базі сертифікатів на сервері.

Ця база виконує роль центру довіри, що перевіряє справжність сертифікатів і керує обміном ключами.

Механізм авторизації

Процес обміну даними поділяється на дві фази:

1. Фаза 1. Авторизація (Authentication phase)

Мета цієї фази - встановити довіру між клієнтом і сервером та підтвердити справжність обох сторін. У ході авторизації відбувається перевірка сертифікатів і обмін ключами для подальшого захищеного з’єднання.

Послідовність дій:

1. Клієнт ініціює з’єднання, надсилаючи запит авторизації, підписаний своїм секретним ключем (наприклад, код SH0).

2. Сервер приймає запит і звертається до бази сертифікатів, щоб перевірити дійсність підпису клієнта.

3. Якщо підпис підтверджено, сервер отримує відкритий ключ клієнта з бази сертифікатів.

4. Сервер створює сеансовий (одноразовий) ключ, шифрує його відкритим ключем клієнта за алгоритмом AES або RSA, і надсилає клієнту відповідь із кодом SH1.

5. Клієнт розшифровує повідомлення за допомогою свого секретного ключа, після чого обидві сторони мають спільний сеансовий ключ, який використовується надалі для шифрування даних.

Таким чином, на цьому етапі формується захищений канал зв’язку, який гарантує, що жодна стороння особа не може отримати доступ до даних чи підмінити повідомлення.

2. Фаза 2. Прямий захищений обмін даними (Secure Data Exchange phase)

Після успішної авторизації відбувається безпосередній обмін інформацією між клієнтом і сервером за допомогою сеансового ключа, отриманого у першій фазі.

Послідовність дій:

1. Клієнт і сервер переходять у режим зашифрованого обміну, у якому всі передані дані шифруються симетричним алгоритмом AES із використанням сеансового ключа.

2. Перед кожним повідомленням додається ідентифікатор сесії та контрольна сума (хеш), щоб забезпечити цілісність і запобігти повторному відтворенню повідомлень (replay attack).

3. У разі необхідності система може періодично оновлювати сеансовий ключ, щоб підвищити безпеку тривалих з’єднань.

4. При завершенні сеансу з’єднання сеансовий ключ знищується, що виключає можливість його повторного використання.

У результаті обидві сторони отримують повністю захищений двосторонній канал, який гарантує:

– конфіденційність - сторонні не можуть прочитати передані дані;

– цілісність - дані не можуть бути змінені під час передавання;

– автентичність - обидві сторони підтверджують, що взаємодіють із довіреним партнером.

Сесія «спілкування»

Після узгодження сеансового ключа клієнт і сервер можуть обмінюватися даними, використовуючи парольну фразу «SH2». По завершенні роботи клієнт посилає повідомлення «SH3» із закодованою фразою «вихід», що ініціює закриття сеансу та знищення сеансового ключа. Щонайменше раз на рік система сертифікації повинна оновлювати ключі, щоб мінімізувати ризики злому. Також слід пам’ятати про мікроконтролери, які безпосередньо відповідають за зчитування і керування пристроями. Хоча локальна мережа сервера визначена як «зона довіри», не виключено, що зловмисник опиниться поруч із сервером хоча б на короткий час — настільки, що його не вдасться виявити. Через це неможливо полагатися лише на пошук складних ключів для простих схем кодування типу Base64. Саме Base64 підходить для таких застосунків тим, що не навантажує малопотужні мікроконтролери, даючи базовий рівень захисту без зайвих затримок.

Тест підсистеми безпеки

Для перевірки коректності роботи описаного модуля запропоновано такі тести:

1. Перевірка розпізнавання/диференціації команд

– надіслати повідомлення SH2. Очікуваний результат - відключення (SH4).

– надіслати запит на авторизацію SH0 з дійсним сертифікатом. Очікуваний результат - відповідь SH1.

– надіслати запит на авторизацію SH0 з неіснуючим сертифікатом. Очікуваний результат - SH4.

– завершити сеанс, після чого повторно надіслати SH2. Очікуваний результат - SH4.

2. Тести шифрування невеликих обсягів даних

– локальне шифрування повідомлення «Hello, world!».

– зашифрувати це повідомлення і передати його через Інтернет.

– зашифрувати та переслати зображення мережею.

3. Тести шифрування великих обсягів даних

– зашифрувати файли, заповнені однотипними символами; перевірити створений файл на «простоту» (примітивність вмісту).

– зашифрувати й передати повідомлення розміром до 1 МБ.

Перевірити роботу системи сертифікації:

– використати сертифікат, прив’язаний до цього мобільного пристрою — очікується позитивна реакція.

– використати сертифікат іншого пристрою - очікувано відключення.

– використати неіснуючий сертифікат - очікується виняткова ситуація.

Імітація атаки «людина посередині»:

– створити на сервері міні-програму, яка виконує роль посередника між логічним сервером і клієнтом.

– внести зміни в коди передачі/даних - очікуваний результат для всіх варіантів: завершення роботи з кодом SH4.

Під час виконання цього блоку також було досліджено роботу застосованих схем шифрування.

Симетричні системи

Симетричні системи; системи відкритих ключів; інфраструктура відкритих ключів.

Алгоритми шифрування:

– симетричні: Base64*, AES, DES;

– асиметричні: RSA, криптографія на еліптичних кривих.

Розроблено змішану (гібридну) схему, що поєднує Base64*, AES і RSA, а також визначено набір тестів для її валідації та створено програмну реалізацію, яка цим вимогам відповідає.

Base64 коректніше називати кодуванням, але в межах опису включено до переліку симетричних засобів обробки даних.

3.5 Розробка блок-схем та опис алгоритмів функціонування системи

На рисунку 4.16 показана блок-схема алгоритму роботи основної програми управління.

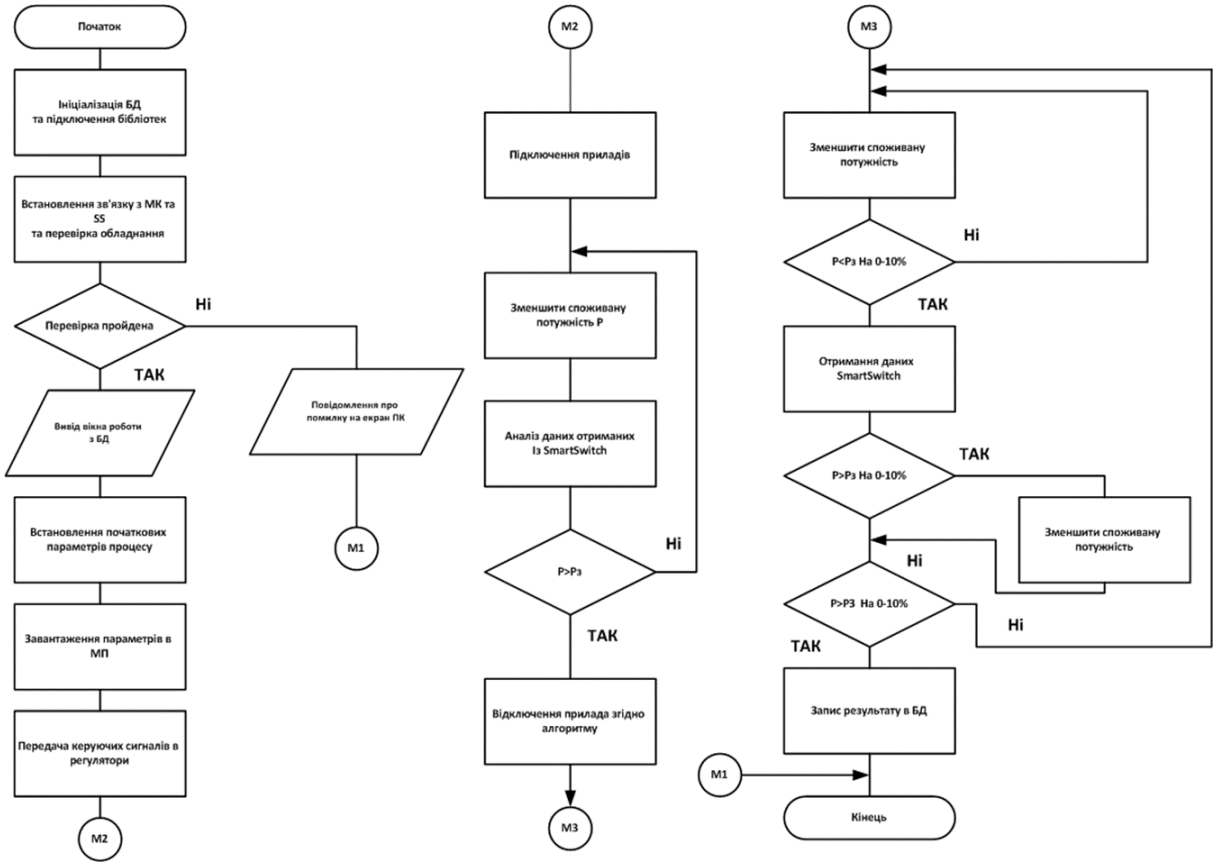


Рисунок 4.16 - блок-схема роботи основної програми управління

Розглянемо принцип роботи програмного забезпечення онлайн-керування. Структурна схема алгоритму подана на рисунку 4.17. Із наведеної схеми видно, що після запуску програми на екрані з’являється головне вікно інтерфейсу користувача. Далі виконується ініціалізація бази даних і підключення необхідних бібліотек.

На наступному етапі програма автоматично встановлює зв’язок між мікроконтролером і «розумними розетками» системи. Якщо зв’язок успішно підтверджено, система розпочинає сканування підключених пристроїв із відображенням результатів на моніторі.

Після цього задаються параметри системи за замовчуванням і формуються керуючі сигнали, що надсилаються на мікропроцесор. Отримані дані аналізуються, і в разі перевищення встановленого рівня енергоспоживання система автоматично відключає резервні пристрої відповідно до алгоритму, збереженого в базі даних.

Таким чином реалізується один із етапів управління системою «Розумний дім». Інші підсистеми функціонують за подібним принципом.

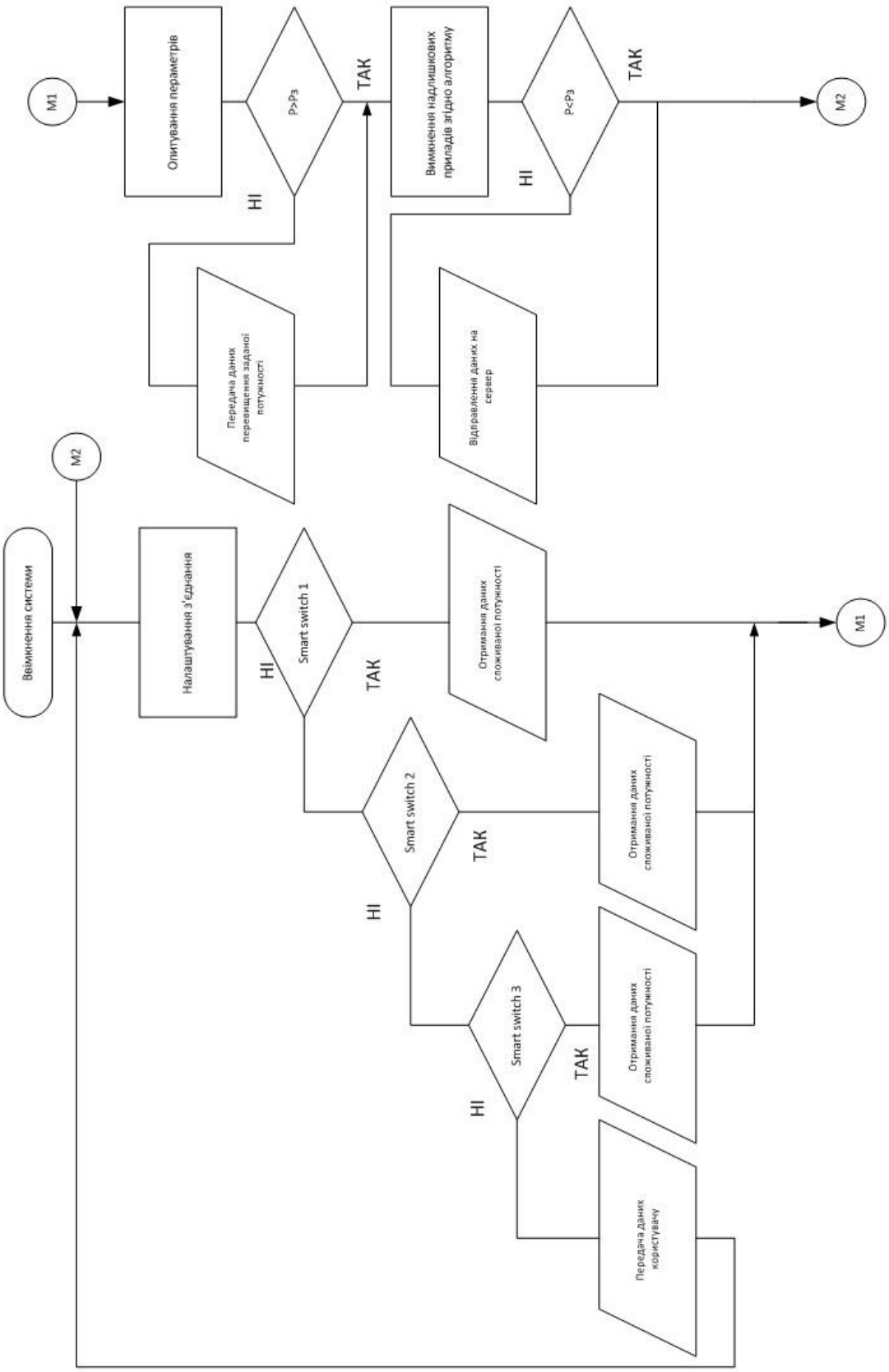


Рисунок 4.17 - блок-схема алгоритму з системи

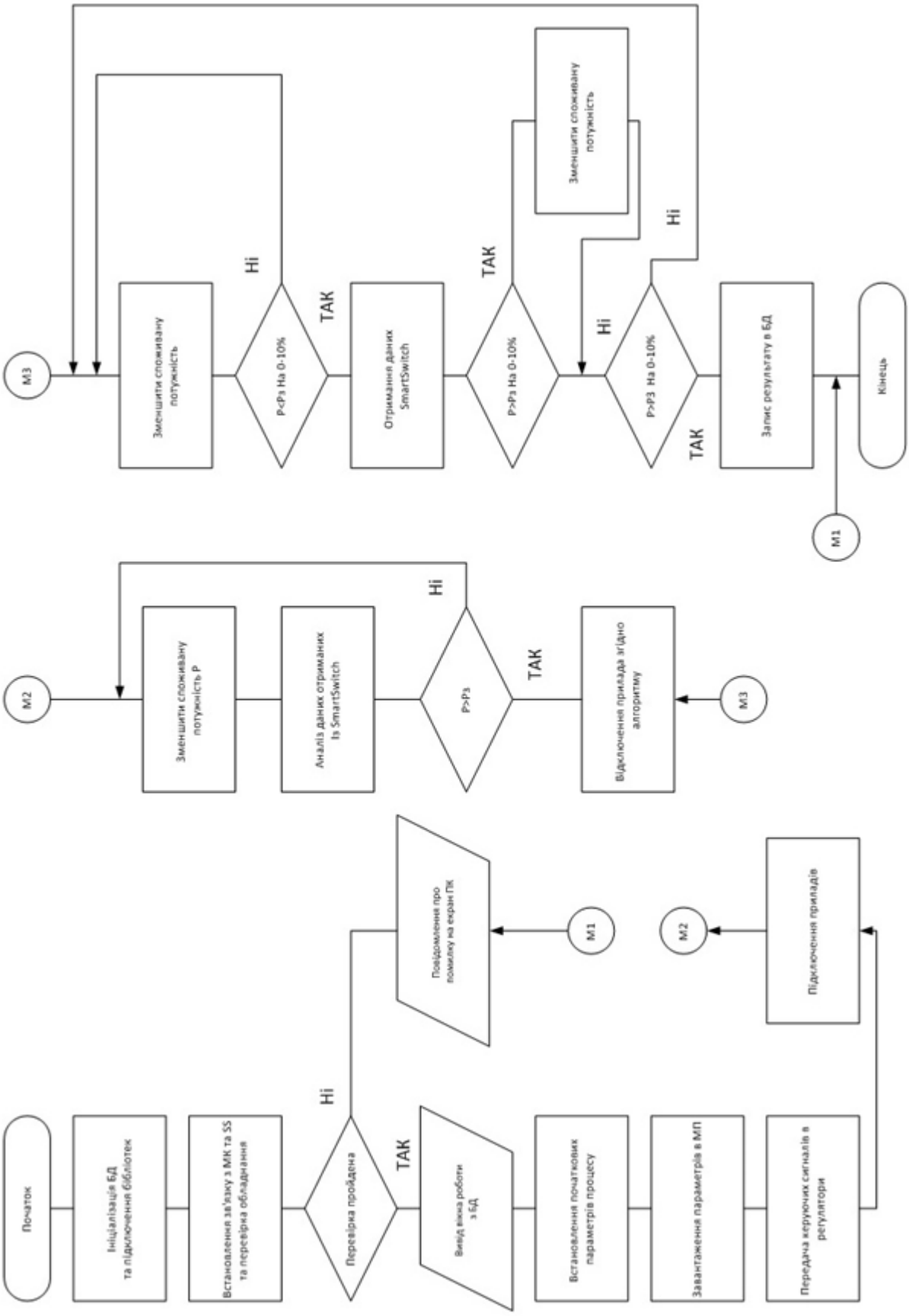


Рисунок 3.18 - Блок-схема основного алгоритму роботи системи

4 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Для наочного пояснення принципів роботи системи розглянемо реальні сценарії, що демонструють окремі особливості запропонованого алгоритму оптимізації, а також механізми загального контролю та керування налаштуваннями:

– Під’єднайте блок живлення до пристрою Smart Switch.

– Запустіть обидва сервери за допомогою команди npm start.

Журнали роботи пристрою, який підключається до мережі Bluetooth LE і здійснює обмін повідомленнями з веб-середовищем, наведено на рисунку 4.1.

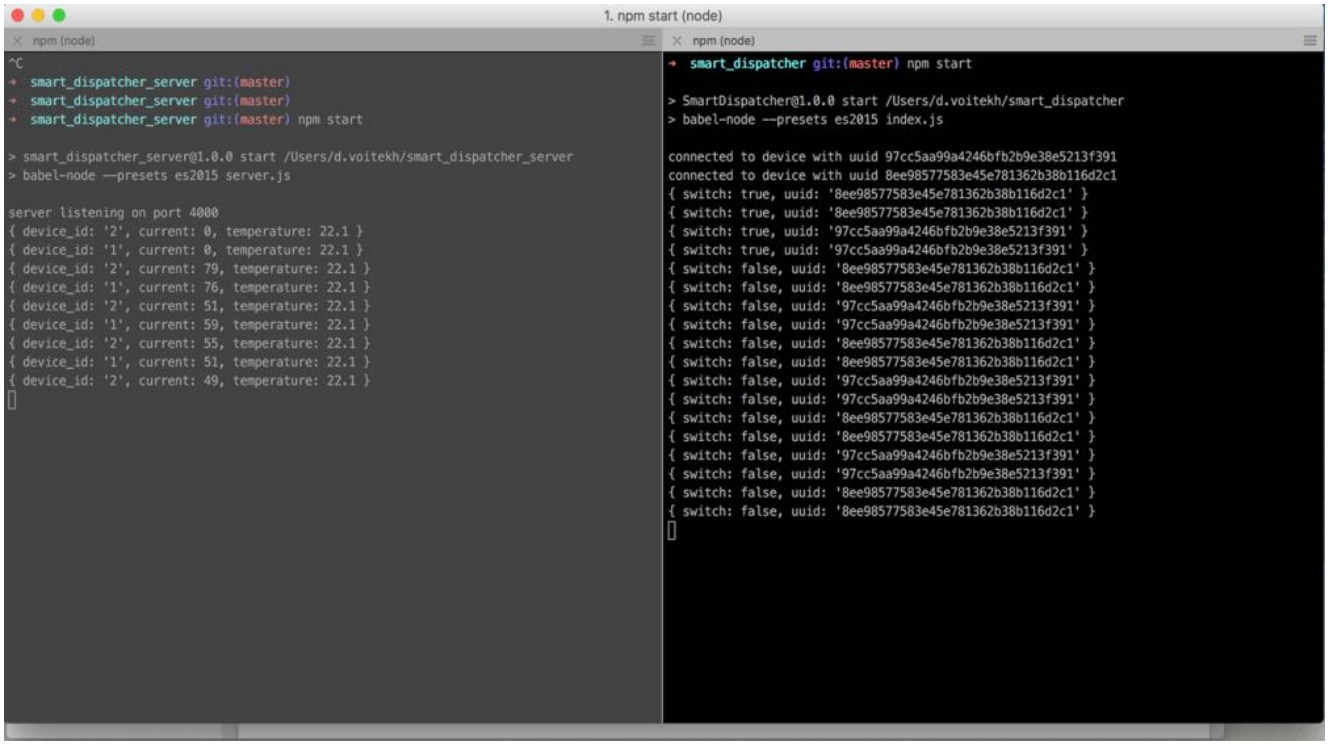


Рисунок 4.1 – Процес запуску системи

3) Далі в браузері необхідно перейти за посиланням http://localhost:3000/device/1, щоб переглянути поточний стан підключеного пристрою. На рисунку 3.8 представлено інтерфейс цього розділу. У вікні

відображаються такі параметри, як поточний стан пристрою та рівень енергоспоживання. На даний момент двигун споживає 2,1120 Вт електроенергії, і його робочий стан визначається як задовільний. Крім того, агреговані дані з таблиці журналів візуалізуються у вигляді графіка добового споживання енергії пристроєм, що дозволяє відстежувати зміни показників у динаміці.

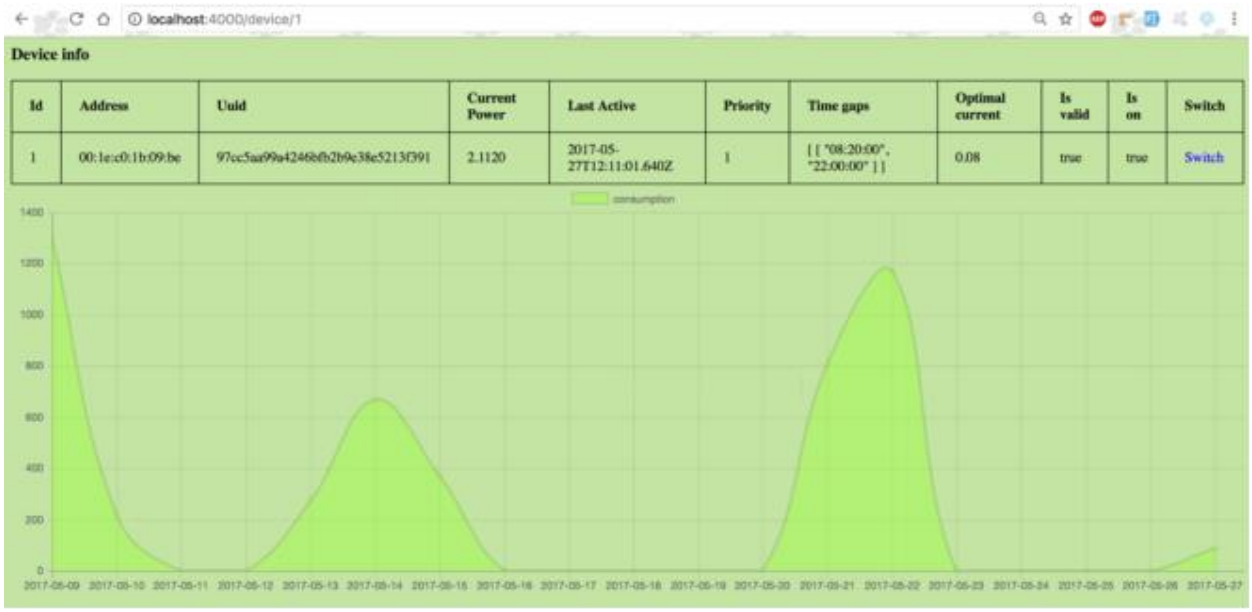


Рисунок 4.2 – Дані про споживання приладу

Перемикання навантаження пристрою. Натискаємо кнопку «Переключити», у результаті чого двигун зупиняється. Інформація на екрані оновлюється: параметр is_on = false, а значення current_power змінюється на 0.

Перехід до автоматичного режиму роботи. На сторінці налаштувань http://localhost:3000/settings_page активується параметр AUTO_MODE = true, що переводить систему в автоматичний режим.

Робота алгоритму в автоматичному режимі. Після активації автоматичного режиму двигун, який був вимкнений раніше, автоматично запускається, оскільки алгоритм виявив відповідність поточного часу встановленому інтервалу ['08:20:00', '22:00:00']. Якщо ж змінити цей часовий

діапазон так, щоб поточний час не входив до нього, двигун буде автоматично вимкнено.

Алгоритм контролю стану пристрою та пошуку дефектів. У наведеному прикладі параметр optimal_current задано як 0,08 А. Для зниження енергоспоживання двигун зупиняється. Коли сила струму перевищує 0,16 А, система сприймає це як відхилення, і двигун автоматично вимикається. При цьому параметр is_valid набуває значення false. Для подальшої коректної роботи пристрою (наприклад, принтера) необхідно скоригувати порогове значення струму.

Алгоритм балансування навантаження. На сторінці налаштувань задається максимальна потужність системи — POWER = 5 Вт. При одночасному включенні двох двигунів сумарне споживання становить 4,3 Вт. Далі зупиняється двигун першого принтера кнопкою Stop, унаслідок чого споживаний струм збільшується до 0,12 А, а загальна потужність — до 5 Вт. Це призводить до автоматичного вимкнення двигуна. Під час наступного циклу опитування пристроїв система повторно ввімкне двигун, відновивши баланс споживання.

Таким чином, розроблена система забезпечує виконання всіх зазначених вимог до автоматизованого управління енергоспоживанням у межах «розумного» середовища.

ВИСНОВКИ

У результаті виконання магістерської роботи створено систему управління розумним будинком із реалізованою підсистемою безпеки передавання даних та захисту від кібератак.

В межах України подібні вітчизняні розробки у цій сфері представлені недостатньо, що підкреслює актуальність теми дослідження.

У магістерській роботі наведено теоретичне узагальнення та вирішено наукове завдання, пов’язане з дослідженням методів управління розумним будинком із впровадженням системи кіберзахисту.

Рішення поставленого наукового завдання полягало у виконанні таких основних етапів:

– проведено аналіз і порівняльний огляд існуючих систем управління розумним будинком із підсистемами безпеки передавання даних;

– досліджено принципи побудови та функціонування системи управління розумним будинком із впровадженням підсистеми захисту інформації від кібератак;

– на основі отриманих результатів розроблено програмну реалізацію системи управління розумним будинком, що забезпечує безпечну передачу даних та підвищений рівень кіберзахисту.

Розроблені в ході виконання магістерської роботи алгоритми забезпечують ефективне вирішення завдань управління системою «Розумний дім» та підтверджують працездатність запропонованих технічних і програмних рішень.

Проведено аналіз предметної області, у ході якого визначено основні об’єкти, взаємодія між якими має ключове значення для функціонування системи, а також встановлено їхні основні характеристики та взаємозв’язки. На основі результатів аналізу було побудовано алгоритм роботи системи та обрано оптимальне середовище розробки програмного забезпечення.

Розроблене програмне забезпечення характеризується простим, інтуїтивно зрозумілим і зручним інтерфейсом користувача, що забезпечує легкість у освоєнні, комфорт у використанні та не вимагає спеціальної технічної підготовки.

Під час створення програмного продукту застосовано об’єктно-орієнтований підхід, який відповідає сучасним тенденціям у галузі розроблення комерційних інформаційних систем і дозволяє підвищити гнучкість, масштабованість та надійність програмного рішення.

Розроблена програма реалізована мовами високого рівня C++ та JavaScript, що забезпечують ефективну обробку даних і стабільну роботу системи. Використання цих мов дозволило оптимізувати процес розроблення програмного забезпечення, скоротивши терміни створення та, відповідно, зменшивши витрати на його реалізацію.

Запропоноване програмне забезпечення структурно поділяється на дві частини:

– загальне програмне забезпечення, яке постачається разом із засобами обчислювальної техніки;

– спеціальне програмне забезпечення, створене безпосередньо для конкретної системи й таке, що реалізує основні функції управління та взаємодії компонентів «розумного будинку».

Програма призначена для виконання під керуванням багатозадачних операційних систем сімейства Windows: XP, Vista, 7, 8, 10 та 11, що забезпечує її сумісність із більшістю сучасних комп’ютерних платформ.

Надано необхідні рекомендації щодо встановлення та налаштування розробленого програмного забезпечення.

Для підвищення рівня інформаційної безпеки в системі запропоновано використовувати змішану схему шифрування, що поєднує алгоритми Base64, AES та RSA. Такий підхід забезпечує оптимальне співвідношення між швидкодією, надійністю та стійкістю до кібератак.

У цілому створене програмне забезпечення підтверджує правильність прийнятих проєктних рішень і повністю відповідає вимогам технічного завдання.

Розроблений програмний продукт має потенціал для подальшого вдосконалення та може бути адаптований для використання в інших галузях, де необхідні системи автоматизованого управління з підвищеним рівнем захисту даних.

СПИСОК ЛІТЕРАТУРИ

1. Саліхов М.М. Самокеровані автомобілі та системи їх навігації// Навч. посібник / В. Є. Бахрушин. – Запоріжжя: КПУ, 2011. – 268 с

2. Кузнецов Ю.М., Луців І.В., Дубиняк С.Г. Теорія технічних систем. -К.: Тернопіль, 1998.-310с.

3. Стеклов В.К. Проектування систем автоматичного керування. - К.:Вища школа,1995.-231 с.

4. Мигаль В. Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Х.: Майдан, 2018. 262 с.

5. Романенко В.Д. Методи автоматизації прогресивних технологій.- К.:Вища школа,1995.-519 с.

6. Рудик А. В. Наукові основи та принципи побудови приладової системи.

7. Koval V., Adamiv O., Proc. of the Third IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2005). – Sofia (Bulgaria). – 2005. – P. 120- 124.

8. Зайцев Г.Ф., Стеклов В.К., Бріцький О.І. Теорія автоматичного управління. – К.: Техніка, 2002. – 688 с.

9. Довідник по автоматизації с/г виробництва //За ред. І.І. Мартиненка.-К.:Урожай,1985.-212 с.

10. Мигаль В. Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Х.: Майдан, 2018. 262 с.

11. Попович М.Г., Ковальчук О.В. Теорія автоматичного керування: Підручник. – 2-ге вид., – К.: Либідь, 2007. - 656 с.

12. Автоматизація технологічних процесів і виробництв харчової промисловості: Підручник/ Ладанюк А.П.,Трегуб В.Г., Ельперін І.В., Цюцюра В.Д. – К.: Аграрна освіта, 2001 – 224 с.

13. Навігаційні системи [Електронний ресурс] : навч. посіб. для студ. Спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» / С.Л. Лакоза; КПІ ім. Ігоря Сікорського, 2021. — 80 с

14. Simulink Documentation [Електронний ресурс]. - Режим доступу: http://www.mathworks.com/ access/ helpdesk/ help/ toolbox/ simulink.

15. Жидецький В. Ц. Основи охорони праці : підруч. Львів : Афіша, 2005. 350 с.

16. Гогіташвілі Г. Г., Лапін В. М. Основи охорони праці : навч. посіб. 3-є вид., стереотипн. Львів : «Новий Світ – 2000». 2006. 232 с.

17. Босов Є. П., Жесан Р. В., Каліч В. М., Голик О. П., Зубенко В. О. Охорона праці при проектуванні систем автоматизації виробництва : навч. посіб. 2-е вид., перероб. і доп. Кропивницький : ЦНТУ, 2022. 208 с.

18. Конституція України. Київ : Андронум, 2020. 60 с.

19. Про охорону праці : Закон України. URL: https://zakon.rada.gov.ua/laws/main/2694-12#Text (дата звернення: 21.10.2024).

20. Основи законодавства України про охорону здоров’я : Закон України. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text (дата звернення 03.11.2024).

21. Про систему громадського здоров’я : Закон України. URL: https://zakon.rada.gov.ua/laws/show/2573-20#n840 (дата звернення 03.11.2024).

22. Про використання ядерної енергії та радіаційну безпеку : Закон України. URL: https://zakon.rada.gov.ua/laws/show/39/95-%D0%B2%D1%80 (дата звернення 29.10.2024).

23. Про загальнообов’язкове державне соціальне страхування : Закон України. URL: https://zakon.rada.gov.ua/laws/show/1105-14 (дата звернення 24.10.2024).

24. Кодекс цивільного захисту України. URL: https://zakon.rada.gov.ua/laws/main/5403-17#Text (дата звернення: 17.11.2024).

25. Кодекс законів про працю України. URL: https://zakon.rada.gov.ua/laws/main/322-08#Text (дата звернення: 07.10.2024).

26. Правила улаштування електроустановок : вид. офіц. Київ : Міненерговугілля України, 2017. 617 с.

27. ВікіпедіЯ. Вільна енциклопедія : веб-сайт. URL: https://uk.wikipedia.org/wiki/ (дата звернення: 31.09.2024).

28. Жидецький В. Ц., Джигирей В. С., Сторожук В. М., Туряб Л. В., Лико Х. І. Практикум з охорони праці. Львів : Афіша, 2000. 352 с.

29. Іванов В. Г., Дзюндзюк Б. В., Олександров Ю. М. Охорона праці в електроустановках : навч. посіб. / за ред. В. Г. Іванова. Київ : Око, 1994. 226 с.