Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та охоронних систем
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

IoT ІНФРАСТРУКТУРА СУПЕРМАРКЕТУ

IoT INFRASTRUCTURE FOR A SUPERMARKET

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Мельничук Богдан Олександрович

(підпис)

Керівник:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» _____ 2026 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
«23» 12 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Мельничуку Богдану Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *IoT інфраструктура супермаркету*

Керівник роботи *к.т.н., доцент Лавренчук Світлана Василівна*

затверджені наказом закладу вищої освіти від «20» грудня 2025 року № 536/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026 р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Загальні відомості про IoT
Загальна структура проекту та засоби розробки
Реалізація та тестування проекту
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Цифровий план супермаркету
Структурна схема IoT-інфраструктури супермаркету
Схема комп'ютерної мережі супермаркету
Результати моделювання та тестування системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Загальні відомості про IoT	*Лавренчук С. В., доцент*		
Загальна структура проекту та засоби розробки	*Лавренчук С. В., доцент*		
Реалізація та тестування проекту	*Лавренчук С. В., доцент*		
Нормоконтроль	*Багнюк Н. В., доцент*		
Гарант ОП	*Лавренчук С. В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О. І., ст. викладач*		

7. Дата видачі завдання 23.12.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2026 р.	
2.	*Аналіз існуючих IoT-рішень та постановка завдань дослідження*	до 02.03.2026 р.	
3.	*Проєктування структури IoT-інфраструктури та вибір засобів розробки*	до 02.04.2026 р.	
4.	*Реалізація цифрової моделі супермаркету та моделювання мережі та формування додатків*	до 10.04.2026 р.	
5.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 01.05.2026 р.	
6.	*Нормоконтроль*	до 23.05.2026 р.	
7.	*Інструментальна перевірка на академічний плагіат*	до 26.05.2026 р.	
8.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 28.05.2026 р.	

Здобувач вищої освіти _____ Богдан МЕЛЬНИЧУК
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Світлана ЛАВРЕНЧУК
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Мельничук Б. О. IoT інфраструктура супермаркету. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота присвячена розробці та моделюванню IoT інфраструктури сучасного супермаркету, що забезпечує автоматизацію процесів моніторингу, керування та підвищення енергоефективності об'єкта. У роботі розглянуто концепцію Інтернету речей, її архітектуру, основні компоненти та сфери застосування, зокрема в комерційних будівлях та роздрібній торгівлі.

У першому розділі виконано аналіз предметної області, розглянуто принципи функціонування IoT-систем, типи датчиків та виконавчих пристроїв, а також сучасні підходи до побудови інтелектуальних мереж.

Другий розділ присвячено вибору інструментальних засобів розробки, зокрема AutoCAD для створення цифрового плану об'єкта та Cisco Packet Tracer для моделювання мережевої інфраструктури та IoT-пристроїв. Обґрунтовано вибір архітектури системи та описано її структурну організацію.

У третьому розділі реалізовано цифрову модель супермаркету, налаштовано фізичний та мережевий рівні системи, а також змодельовано роботу датчиків руху, освітлення, температури та систем безпеки.

Результатом роботи є розроблена модель IoT-інфраструктури супермаркету, яка демонструє можливості автоматизації, моніторингу та підвищення ефективності управління торговим об'єктом.

Ключові слова: IoT, Cisco Packet Tracer, AutoCAD, датчики, автоматизація, розумний супермаркет.

ANNOTATION

Melnichuk B. IoT Infrastructure for a Supermarket. Manuscript.

Bachelor's qualification thesis of the Educational Program «Computer Engineering», specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

The qualification thesis is devoted to the development and modeling of an IoT infrastructure for a modern supermarket, which ensures automation of monitoring and control processes as well as improves the energy efficiency of the facility. The work examines the concept of the Internet of Things, its architecture, main components, and application areas, particularly in commercial buildings and retail environments.

The first chapter provides an analysis of the subject area, examines the principles of IoT system operation, types of sensors and actuators, as well as modern approaches to building intelligent networks.

The second chapter is dedicated to the selection of development tools, in particular AutoCAD for creating a digital layout of the facility and Cisco Packet Tracer for modeling the network infrastructure and IoT devices. The system architecture is justified and its structural organization is described.

The third chapter implements a digital model of the supermarket, configures the physical and network layers of the system, and simulates the operation of motion, lighting, temperature sensors, and security systems.

The result of the work is a developed model of a supermarket IoT infrastructure that demonstrates the capabilities of automation, monitoring, and improved management efficiency of a retail facility.

Keywords: IoT, Cisco Packet Tracer, AutoCAD, sensors, automation, smart supermarket.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації економіки особливого значення набуває концепція Інтернету речей (IoT), яка забезпечує інтеграцію фізичних об’єктів із цифровими системами. Використання IoT-рішень дозволяє автоматизувати процеси, підвищити ефективність управління ресурсами, зменшити витрати та покращити рівень безпеки. Особливо актуальним є впровадження таких технологій у сфері роздрібної торгівлі, зокрема в супермаркетах, де існує необхідність постійного контролю за умовами зберігання продукції, енергоспоживанням, безпекою та комфортом для відвідувачів. Створення IoT інфраструктури супермаркету дає змогу об’єднати всі підсистеми в єдину мережу та забезпечити їх ефективну взаємодію в режимі реального часу.

Метою роботи є проєктування та моделювання IoT-інфраструктури супермаркету з використанням сучасних програмних засобів, що забезпечує автоматизацію основних процесів, підвищення енергоефективності та рівня безпеки об’єкта.

Об’єкт дослідження – комп’ютерні мережі та IoT-системи в комерційних об’єктах.

Предмет дослідження – архітектура та функціонування інфраструктури Інтернет речей супермаркету з використанням датчиків, мережевих технологій і систем автоматизації.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– проаналізувати предметну область Інтернету речей та існуючі рішення у сфері автоматизації комерційних об’єктів;

– здійснити огляд сучасних технології IoT-систем;

– розробити структуру IoT-інфраструктури супермаркету;

– спроєктувати цифрову модель об’єкта з урахуванням функціонального зонування;

– реалізувати мережеву модель системи в середовищі моделювання;

– провести тестування системи.

Практичне значення отриманих результатів полягає у можливості використання розробленої моделі для впровадження IoT-рішень у реальних торгових об’єктах, що дозволить підвищити ефективність управління, зменшити експлуатаційні витрати та покращити якість обслуговування клієнтів.

РОЗДІЛ 1
ЗАГАЛЬНІ ВІДОМОСТІ ПРО IoT

1.1 Теоретичні основи IoT

IoT (англ. Internet of Things, IoT) – це сучасна концепція мережі взаємопов'язаних фізичних об'єктів («речей»), оснащених датчиками, програмним забезпеченням та іншими технологіями, що забезпечують підключення до Інтернету та обмін даними між собою і з комп'ютерними системами. Такі пристрої можуть не лише збирати інформацію про навколишнє середовище, але й виконувати певні дії без безпосереднього втручання людини завдяки інтелектуальним інтерфейсам [3, 8, 15].

Ключовими елементами Інтернету речей є датчики, що здійснюють контроль фізичних та навколишніх параметрів, зокрема температури, вологості, тиску, рівня освітлення та руху. Отримана інформація у режимі реального часу надсилається до хмарних сервісів, де виконується її обробка, аналіз і подальше використання для формування відповідних рішень. Завдяки цьому забезпечується автоматизація різних процесів, підвищується ефективність функціонування систем, зменшується ймовірність виникнення помилок та покращується рівень безпеки [8, 15].

Базовими компонентами Інтернету речей є сенсори, призначені для моніторингу фізичних і навколишніх показників, таких як температура, вологість, тиск, освітленість та рух. Зібрані дані передаються через мережу до хмарних платформ, у яких здійснюється їхня обробка та аналіз для подальшого прийняття необхідних рішень. Використання таких технологій сприяє автоматизації роботи систем, підвищенню продуктивності їх функціонування, мінімізації помилок і забезпеченню вищого рівня безпеки [8, 12].

Інтернет речей знаходить застосування у багатьох сферах діяльності. У медичній галузі IoT використовується для моніторингу стану пацієнтів та підвищення точності проведення діагностики. У транспортній сфері технології забезпечують контроль технічного стану транспортних засобів і сприяють

оптимізації перевезень. У сільському господарстві IoT застосовується для автоматизації процесів вирощування та контролю умов навколишнього середовища. У побуті ці технології реалізуються у вигляді «розумних будинків», які підвищують рівень комфорту та безпеки користувачів. Крім того, IoT активно впроваджується у промисловості для здійснення прогнозного обслуговування обладнання та підвищення ефективності виробничих процесів [8, 14].

Незважаючи на численні переваги, створення IoT-систем супроводжується певними труднощами. Розробка таких рішень потребує використання апаратних компонентів, підтримки різних протоколів зв'язку, зокрема Bluetooth, а також інтеграції програмного забезпечення з фізичними пристроями. Усе це ускладнює процес розробки та вимагає забезпечення надійної й безперервної взаємодії між усіма елементами системи [8, 14].

1.2 Історія Інтернету Речей

Термін «інтернет речей» зобов'язаний своєю появою Кевін Ештон, який у 1997 р., працюючи в Procter & Gamble, застосував технологію радіочастотної ідентифікації (RFID) для керування системою поставок. Завдяки цій роботі у 1999 році його запросили до Массачусетського технологічного інституту, де він разом із групою однодумців організував дослідницький консорціум Auto-ID Center. Саме цей центр став одним із перших осередків розвитку концепції Інтернету речей та технологій автоматичної ідентифікації об'єктів. З того часу Інтернет речей здійснив перехід від простих радіочастотних міток до масштабної екосистеми та окремої індустрії, що охоплює мільярди взаємопов'язаних пристроїв у всьому світі [8].

Аж до 2012 р. ідея підключення речей до Інтернету переважно стосувалася смартфонів, планшетів, персональних комп'ютерів і ноутбуків. По суті, це пристрої, які у всіх відношеннях виступали як повноцінні комп'ютери та мали достатню обчислювальну потужність для роботи в мережі. До цього

часу, починаючи з моменту появи перших зачатків Інтернету, таких як створена у 1969 р. мережа ARPANET, більшість технологій, на яких сьогодні базується Інтернет речей, ще не існували або перебували на ранніх етапах розвитку. Не було сучасних бездротових мереж, компактних датчиків, енергоефективних мікроконтролерів та хмарних платформ для обробки великих обсягів даних [8].

До 2000 року більшість пристроїв, які можна було підключити до Інтернету, являли собою комп'ютери різних типів і розмірів. Проте з розвитком мікроелектроніки, бездротових технологій зв'язку та мобільного Інтернету ситуація почала стрімко змінюватися. З'явилися компактні сенсори, вбудовані системи та смарт-пристрої, здатні автоматично збирати, передавати й аналізувати інформацію без безпосереднього втручання людини. Це дало поштовх до активного розвитку концепції «розумних» будинків, промислової автоматизації, інтелектуальних транспортних систем, медичних пристроїв та цифрових торговельних мереж (рис. 1.1) [8].

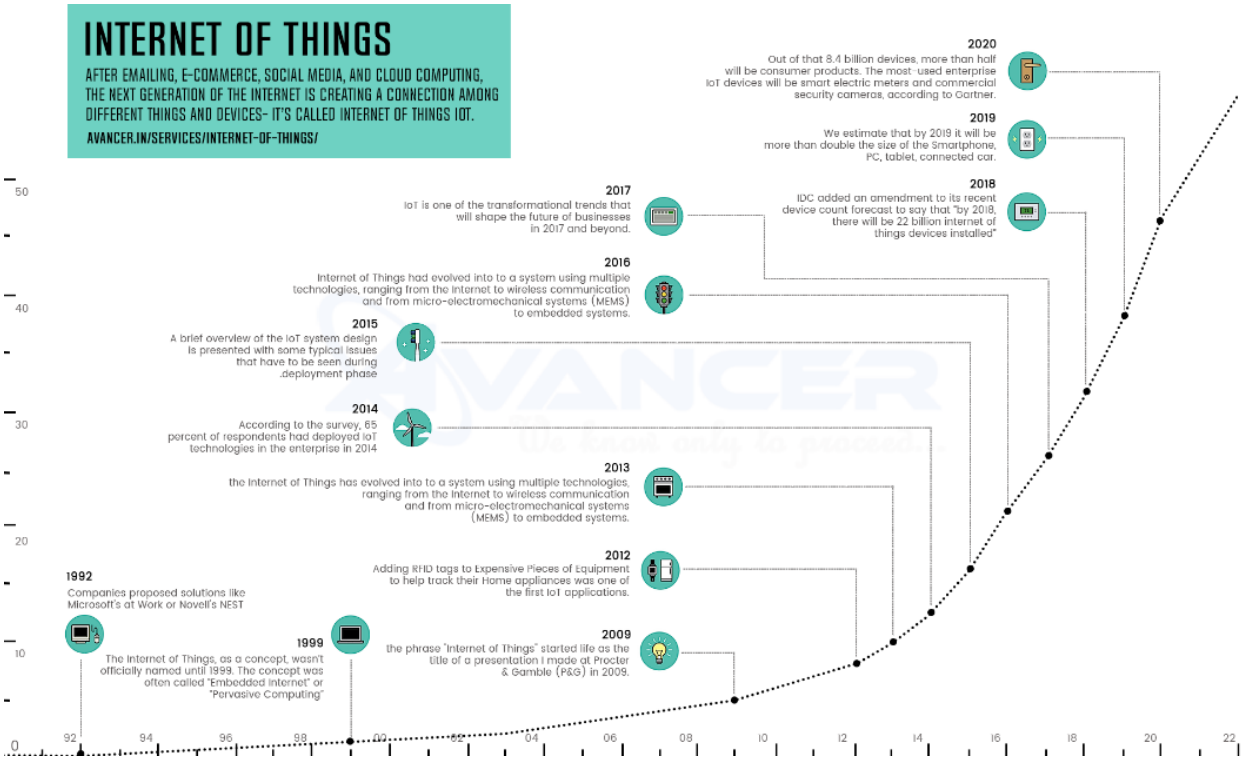

Рисунок 1.1 – Історія Інтернет Речей [8]

1.3 Інтернет речей в промисловості

Промисловий Інтернет речей (Industrial IoT, IIoT) є одним із наймасштабніших напрямів розвитку Інтернету речей як за кількістю підключених пристроїв, так і за практичною цінністю для автоматизації виробничих процесів і діяльності підприємств. Цей сегмент традиційно виступає основою операційно-технологічних систем, до складу яких входять програмні та апаратні засоби для моніторингу й контролю фізичних пристроїв. На відміну від класичних інформаційних технологій, що орієнтовані на обробку, зберігання та надання даних, операційні технології зосереджуються на забезпеченні безперервної роботи обладнання, контролі продуктивності, швидкому реагуванні в реальному часі та підтримці безпеки систем. Із поширенням технологій Інтернету речей у промисловій сфері відбувається поступове об’єднання IT та OT, особливо у сфері технічного обслуговування виробничого обладнання. Це дозволяє формувати великі обсяги даних, які можуть оброблятися як приватними, так і публічними хмарними платформами [5, 8, 10].

Однією з головних характеристик промислового сегмента Інтернету речей є необхідність забезпечення роботи систем у режимі реального або майже реального часу. У виробничому середовищі ключовим показником стає мінімальний час відгуку системи, оскільки від цього залежить стабільність технологічних процесів. Також важливими чинниками є надійність роботи обладнання, мінімізація простоїв і високий рівень безпеки. Для цього необхідно забезпечувати резерв потужностей, а також використовувати приватні хмарні мережі та сховища даних. Промисловий Інтернет речей належить до найбільш динамічних сегментів ринку IoT. Водночас характерною особливістю IIoT є активне використання застарілих технологій та обладнання. На багатьох підприємствах досі експлуатуються виробничі верстати та системи, створені десятки років тому, які працюють через послідовні інтерфейси типу RS485 замість сучасних бездротових мережевих архітектур [6, 8].

1.3.1 Школи та кампуси

Датчики Інтернету речей відіграють важливу роль у забезпеченні безпеки студентів і викладачів, оскільки питання захисту та комфортних умов навчання є пріоритетними для шкіл і університетських кампусів. Камери, оснащені датчиками руху, дозволяють здійснювати постійний візуальний контроль території та підвищують рівень безпеки. Датчики якості повітря допомагають підтримувати здоровий мікроклімат у навчальних приміщеннях, контролюючи рівень забруднення, вологість і температуру. Водночас датчики електричного струму забезпечують стабільну та ефективну роботу обладнання, зокрема систем опалення, вентиляції та кондиціонування повітря. Крім цього, інтелектуальні IoT-датчики можуть застосовуватися для виявлення випадків вейпінгу, куріння та інших порушень правил поведінки на території навчального закладу, що сприяє створенню більш безпечного та контрольованого освітнього середовища [10].

1.3.2 Охорона здоров’я та догляд за людьми похилого віку

Технології датчиків Інтернету речей забезпечують широкі можливості для підвищення якості медичного обслуговування та догляду за людьми похилого віку. Використання біосенсорів дозволяє контролювати фізіологічні показники пацієнтів у режимі реального часу. Наприклад, сучасні системи безперервного моніторингу глюкози (CGM) у вигляді портативних пластирів здатні постійно вимірювати рівень цукру в крові. Крім того, інтелектуальні кардіостимулятори можуть передавати інформацію про серцевий ритм та автоматично формувати сповіщення у разі виявлення відхилень від норми. У сфері догляду за людьми похилого віку активно застосовуються розумні ліжка, оснащені датчиками руху, які здатні фіксувати падіння або інші небезпечні ситуації [10].

1.3.3 Комерційні будівлі та офіси

Датчики Інтернету речей мають широке застосування у комерційних та офісних будівлях від забезпечення безпеки до автоматизованого управління нерухомістю. Використання датчиків руху та освітленості сприяє створенню безпечнішого й комфортнішого середовища для працівників. IoT-сенсори

можуть інтегруватися із системами тривожних кнопок, що дозволяє оперативно реагувати на надзвичайні ситуації та підвищує рівень безпеки на робочому місці [10].

1.3.4 Розумні будинки та будівлі, гостинність і готелі

Розумні будинки та будівлі набули значного поширення протягом останніх років завдяки активному розвитку технологій Інтернету речей. Їх функціонування базується на використанні різноманітних сенсорів, інтегрованих у побутові та інженерні системи будівлі. Датчики температури, вологості, освітленості, руху та звуку забезпечують автоматизований контроль параметрів середовища, що дозволяє підвищити комфорт проживання, оптимізувати енергоспоживання та покращити рівень безпеки. Зібрані дані аналізуються системою управління, яка може автоматично регулювати освітлення, вентиляцію, опалення чи роботу охоронних систем [10].

У сфері гостинності технології Інтернету речей використовуються для покращення комфорту гостей, підвищення рівня безпеки та оптимізації використання ресурсів. Датчики температури, вологості, руху та освітленості забезпечують автоматичне керування кліматичними системами й освітленням у номерах та загальних приміщеннях. Завдяки постійному збору та аналізу даних готелі можуть ефективніше контролювати енергоспоживання, швидше реагувати на потреби клієнтів і підтримувати високий рівень сервісу [10].

1.3.5 Промислові заводи

Розумні будинки та будівлі набули значного поширення протягом останніх років завдяки активному розвитку технологій Інтернету речей. Їх функціонування базується на використанні різноманітних сенсорів, інтегрованих у побутові та інженерні системи будівлі. Датчики температури, вологості, освітленості, руху та звуку забезпечують автоматизований контроль параметрів середовища, що дозволяє підвищити комфорт проживання, оптимізувати енергоспоживання та покращити рівень безпеки. Зібрані дані аналізуються системою управління, яка може автоматично регулювати освітлення, вентиляцію, опалення чи роботу охоронних систем [10].

1.3.6 Роздрібна торгівля та логістика

У сфері роздрібної торгівлі та логістики датчики Інтернету речей застосовуються для автоматизації управління запасами, підвищення безпеки та оптимізації ланцюгів постачання. Сенсори руху та системи відеоспостереження допомагають запобігати крадіжкам і контролювати роботу торгових приміщень. У магазинах зі швидкопсувними товарами використовуються температурні датчики, які забезпечують контроль умов зберігання продукції. IoT-технології дозволяють відстежувати переміщення товарів у режимі реального часу, що підвищує ефективність логістичних процесів та зменшує ризик втрат [10].

1.4 Технології Інтернет речей

1.4.1 Засоби ідентифікації та вимірювання

Кожен фізичний об’єкт, що є складовою Інтернету речей, навіть за відсутності прямого підключення до мережі, повинен мати власний унікальний ідентифікатор. Для автоматизованої ідентифікації таких об’єктів застосовуються різні технології, зокрема радіочастотна ідентифікація, за якої до предмета прикріплюється RFID-мітка, а також оптичні та інфрачервоні системи маркування. [17-18].

Завдання засобів вимірювання забезпечити перетворення інформації про зовнішнє середовище в дані, придатні для передачі їх засобам обробки. Це можуть бути як окремі датчики температури, освітленості тощо, так і складні вимірювальні комплекси. Для досягнення автономності засобів вимірювання бажано забезпечити електроживлення датчиків за рахунок засобів альтернативної енергетики (сонячні батареї тощо), щоб не витрачати час і кошти на підзарядку акумуляторів або заміну батарей [17-18].

1.4.2 Засоби передачі даних

Для передачі даних може бути використана будь-яка з існуючих технологій. У разі використання бездротових мереж особливу увагу приділяють

підвищенню надійності передачі даних. При використанні дротових мереж активно використовують технологію передачі даних по лініях електропередач, оскільки багато «речей» (такі як торгові автомати, банкомати тощо) підключені до електромереж [17-18].

1.4.3 Засоби обробки даних

Тридцять і більше мільярдів пристроїв, які підключені в 2020 році до Інтернету, згенерували більше 44 мільярдів терабайт даних. Це приблизно в сім разів перевищує кількість оцифрованої інформації в усьому світі станом на 2010-ті роки. Тому в компанії Microsoft вважають, що головна частина Інтернету речей – це не датчики і засоби передачі даних, а хмарні системи, що забезпечують високу пропускну здатність і здатні швидко реагувати на певні ситуації (наприклад, вміти за показаннями датчиків з'ясувати, що в будинку вже п'ять хвилин нікого немає, а вхідні двері залишилася відкритими). Допоможуть впоратися з величезними потоками інформації також туманні обчислення, які будуть не конкурувати з хмарними, а ефективно їх доповнювати [17-18].

1.4.4 Виконуючі пристрої

Це пристрої, здатні перетворювати цифрові електричні сигнали, що надходять від інформаційних мереж, в дії. Наприклад, для того, щоб через смартфон можна було включити систему опалення в будинку, вона повинна мати відповідний пристрій. Виконавчі пристрої часто конструктивно поєднуються з датчиками [17-18].

1.5 Впровадження технології датчиків Інтернету речей

«Як зазначено у списку датчиків Інтернету речей, ця технологія надає численні переваги для різних галузей промисловості та повсякденного життя, покращуючи, захищаючи та автоматизуючи. Однак впровадження цих пристроїв для підвищення рівня успішності виконання завдань пов'язане зі значними труднощами» [10].

1.5.1 Безпека та конфіденційність даних датчиків Інтернету речей

Безпека є пріоритетом як для бізнесу, так і для суспільства в цілому. Однак, проблеми з впровадженням пристроїв з даними датчиків Інтернету речей є більш пріоритетними, ніж прості несправності; дані, які вони передають, постійно перебувають під кіберзагрозами [2, 9-11].

Шифрування, автентифікація та дотримання місцевих правил щодо даних є важливими міркуваннями при впровадженні датчиків для Інтернету речей. Необхідно вжити надійних заходів для захисту безпеки, запобігання несанкціонованому доступу та зменшення ризику витоків даних [9-11].

1.5.2 Інтеграція датчиків Інтернету речей з існуючими системами

«Не кожна організація, об’єкт чи пристрій має однакове програмне чи апаратне забезпечення для інтеграції з різними типами датчиків у мережах Інтернету речей. Підприємства можуть зіткнутися з проблемами інтеграції датчиків Інтернету речей, коли застаріла інфраструктура підтримує операції» [10].

1.5.3 Надійність та зв’язок мережі

«Забезпечення найефективнішої передачі даних означає наявність надійної мережі. Безперебійне з’єднання між датчиком Інтернету речей та мережею є надзвичайно важливим для ефективної роботи, особливо там, де задіяні дані в режимі реального часу та механізми швидкого реагування» [10].

«Пристрої повинні враховувати фактори, які можуть перешкоджати роботі мережі та її надійності. Правильні комунікаційні засоби, такі як Wi-Fi та 5G, мають вирішальне значення для мінімізації перебоїв у роботі мережі та перешкод» [10].

1.5.4 Масштабованість і перспективність

«Впровадження датчиків Інтернету речей може бути частиною ширшої бізнес-картини. Ключовим фактором має бути забезпечення ефективного масштабування інфраструктури разом із зростанням. Інтеграція хмарних рішень, аналітики на основі штучного інтелекту та модульних сенсорних мереж

може допомогти подолати проблеми масштабованості та забезпечити майбутнє експлуатації» [10].

1.5.5 Аналіз вартості та рентабельності інвестицій

«Пристрої з датчиками Інтернету речей обмежують бюджет, враховуючи витрати на встановлення, апаратне та програмне забезпечення, а також на обслуговування. Підприємства та приватні особи повинні враховувати, чи окупиться впровадження цього активу порівняно з пов'язаними з ним витратами. Особи, що приймають рішення, можуть пріоритезувати справи з високим рівнем впливу, автоматизацію технічного обслуговування та енергоефективні датчики, щоб виправдати бюджетні витрати та отримати максимальну рентабельність інвестицій» [10].

«Оскільки використання датчиків та пристроїв Інтернету речей розширюється, зосередження уваги на цих п'яти критичних областях може допомогти зменшити ризики, підвищити ефективність та сприяти довгостроковому успіху під час впровадження датчиків Інтернету речей» [10].

1.6 Екосистема Інтернету речей

До екосистеми Інтернету речей належать усі технології, сервіси та технічні засоби, що забезпечують функціонування IoT-систем. Основними складовими такої екосистеми:

– sensors (розумні датчики та виконавчі пристрої) – вбудовані системи, операційні системи реального часу, джерела безперебійного живлення, а також мікроелектромеханічні системи (МЕМС), які забезпечують збір даних і керування обладнанням;

– системи зв'язку з датчиками – мережі для передавання інформації між пристроями на невеликих відстанях, зазвичай від кількох сантиметрів до 100 метрів. Для цього використовуються енергоефективні низькошвидкісні канали зв'язку, які не завжди базуються на IP-протоколах;

– локальні обчислювальні мережі (LAN) – мережі обміну даними, побудовані переважно на основі IP-протоколів. Найчастіше Wi-Fi-мережі застосовуються стандарту 802.11, які забезпечують швидкий бездротовий зв’язок у межах локальної інфраструктури. Такі мережі можуть мати зіркоподібну або пірингову структуру;

– агрегатори, маршрутизатори, шлюзи та пограничні пристрої (Edge Device) – компоненти, що відповідають за обробку та передавання даних між локальними пристроями і глобальними мережами. До цієї категорії належать виробники вбудованих систем, процесорів, оперативної пам’яті, систем зберігання даних, радіомодулів, тонких клієнтів, бездротових систем зв’язку, міжплатформового програмного забезпечення, а також інструментів для туманних обчислень, граничної аналітики та захисту пристроїв;

– глобальні обчислювальні мережі – оператори стільникового, супутникового зв’язку та малопотужних глобальних мереж LPWAN. Для передавання даних у таких системах використовуються IoT-протоколи, зокрема MQTT, CoAP та HTTP;

– хмарні технології – сервіси інфраструктури та платформ як послуги, системи управління базами даних, засоби потокової й пакетної обробки інформації, аналітичні платформи, програмне забезпечення як сервіс (SaaS), озера даних, програмно-визначені мережі та сервіси машинного навчання;

– сервіси аналізу даних – системи, призначені для обробки великих масивів інформації, що надходять від IoT-пристроїв. Для ефективного використання таких даних застосовуються засоби аналітики, комплексної обробки подій і методи машинного навчання;

– безпека (security) – один із ключових компонентів екосистеми Інтернету речей. Захист повинен охоплювати всі рівні архітектури: датчики, процесори, апаратне забезпечення, канали зв’язку та протоколи передавання даних. На кожному етапі необхідно забезпечити конфіденційність, цілісність і достовірність інформації, оскільки IoT-системи є потенційною ціллю для кібератак [8].

1.7 Архітектура Інтернету Речей

«Архітектура Інтернету речей відрізняється в залежності від реалізації. Тим не менше вона дещо схожа на архітектуру класичних систем АСУТП» [8]. Один із прикладів архітектури показаний на рисунку 1.2.

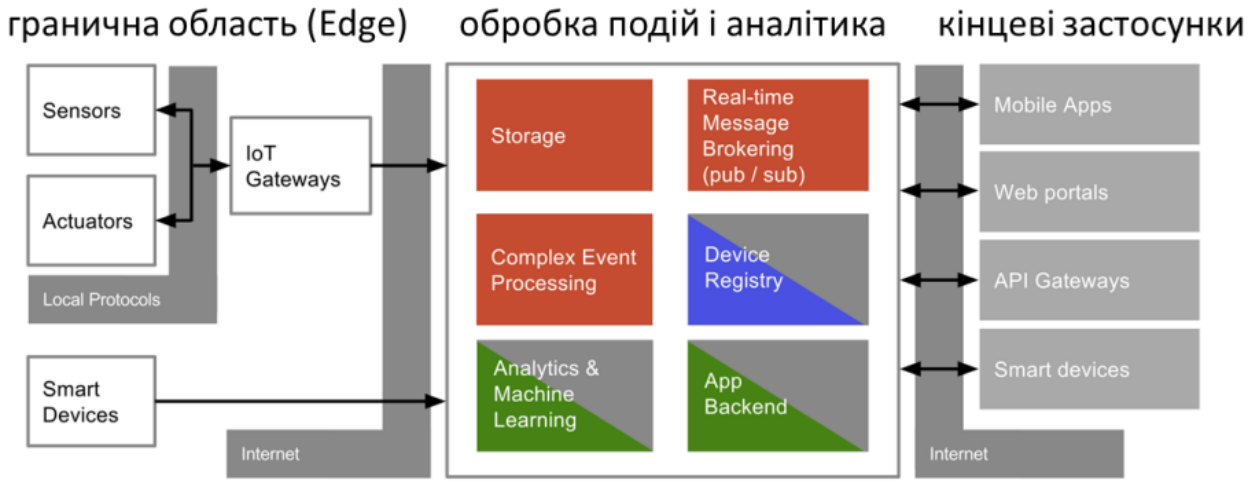

Рисунок 1.2 – Архітектура IoT [8]

«Взаємодія з «речами» відбувається через датчики (sensors) та виконавчі механізми (Actuators), аналогічно як це робиться в АСУТП для будь якого об’єкту керування. Ці датчики разом з усією інфраструктурою для інтеграції з рівнем обробки подій через мережу Internet формують так звану граничну область (Edge)» [8].

Події, що надходять із граничного рівня, зберігаються та обробляються відповідно до поставлених завдань системи. На цьому етапі здійснюється накопичення даних, їх аналіз, обробка та передача необхідним прикладним сервісам. Для обробки подій використовуються аналітичні сервіси, а також методи машинного навчання, що дає можливість формувати висновки та прогнозувати стан об’єктів. Якщо порівнювати з автоматизованими системами керування технологічними процесами (АСУТП), то цей рівень відповідає рівню контролерів і SCADA-систем. Отримання результатів роботи системи, моніторинг, дистанційне керування та адміністрування виконуються через

кінцеві прикладні програми з використанням мережі Internet. У структурі АСУТП даний рівень можна умовно порівняти з HMI-системами [3, 8].

На рисунку 1.3. показана подібна наведеній вище архітектура, однак у вигляді сервісів. «На ньому область Edge представлений у вигляді датчиків, Device Hub/Gateway та Device Management. Останні частково виконуються як хмарні обчислення так і на граничних пристроях. Усі функції збереження та первинної обробки подій (даних) зведені до Data Management. Усі інші функції обробки, в тому числі аналітичні показані як додатки PaaS, що взаємодіють з сервісами керування даних через API (Application Program Interface)» [8].

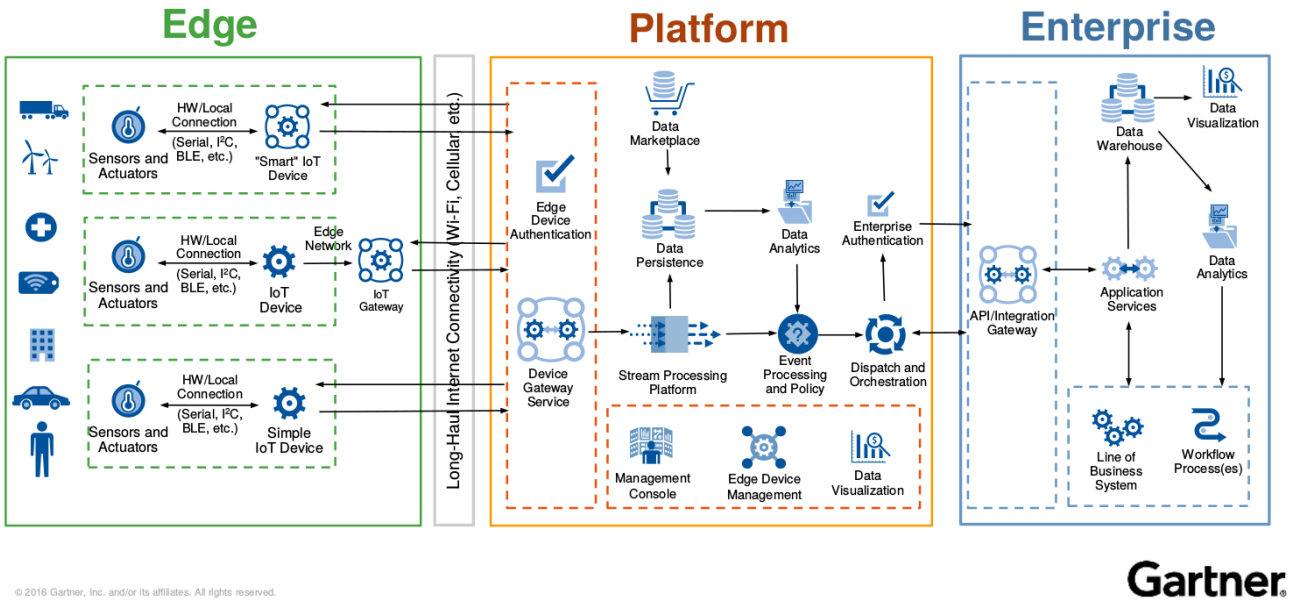

Рисунок 1.3 – Архітектура у вигляді сервісів [8]

Ще один приклад архітектури Інтернету Речей показаний на рисунку 1.4. Як видно, усі наведені архітектури мають спільні риси: наявність трьох рівнів, подібні функції, наявність хмарних обчислень, використання Інтернету як інтеграційного рівня [8].

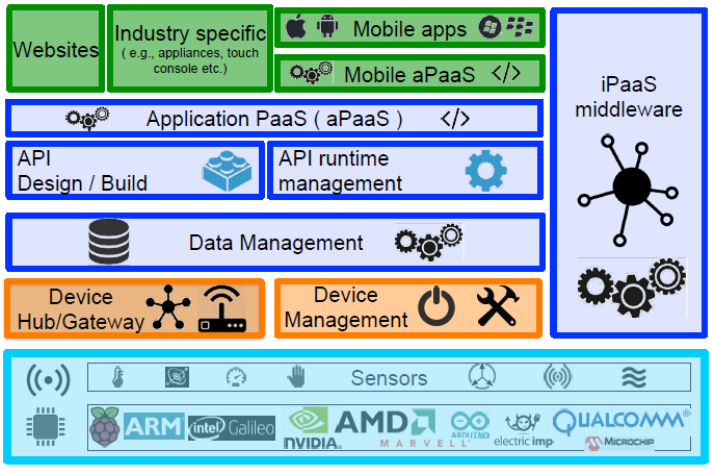

Рисунок 1.4 – Архітектура Інтернет Речей [8]

Далі коротко розглянемо основні компоненти архітектури.

1.7.1 Датчики та живлення

«Інтернет починається або закінчується однією подією: простий рух, зміна температури або, може бути, важіль замикає замок. На відміну від багатьох існуючих IT-пристроїв, Інтернет речей здебільшого пов'язаний з фізичною дією або подією. Він формує реакцію на якийсь фактор реального світу. Іноді при цьому один-єдиний датчик може згенерувати величезний обсяг даних, наприклад, акустичний датчик для профілактичного огляду обладнання. В інших випадках всього одного біта даних достатньо, щоб передати життєво важливі відомості про стан здоров'я пацієнта. Якою б не була ситуація, системи датчиків еволюціонували і, відповідно до закону Мура, зменшилися до субнанометрових розмірів і стали істотно дешевше. Саме до цього апелюють ті, хто прогнозує, що до Інтернету речей будуть підключені мільярди пристроїв, і саме тому ці прогнози виправдаються» [8].

«Тому, розглядаючи Інтернет Речей, необхідно розглядати мікроелектромеханічні системи, датчики і інші типи недорогих граничних пристроїв і їх електрофізичних властивостей. Також це стосується силових і енергетичних систем, необхідних для живлення цих граничних пристроїв. Не можна вважати, що граничні пристрої забезпечуються енергією за замовчуванням. Мільярди маленьких датчиків все одно потребують великої

кількості енергії. З питанням живлення також пов’язані питання організації хмарних сервісів IoT» [8].

1.7.2 Передача даних

«Велика увага при розробці IoT приділяється встановленню з’єднання і роботі мереж. Інтернету речей не існувало б без надійних технологій передачі даних з найвіддаленіших і несприятливих областей в найбільші центри збору даних компаній Google, Amazon, Microsoft і IBM. Словосполучення «Інтернет речей» містить слово «Інтернет», тому необхідно вивчати питання, що стосуються мережних технологій, обміну даними та навіть теорії сигналів. Базова опора Інтернету речей – це не датчики і не програми, а можливість встановити з’єднання» [8].

«Передача даних і встановлення мережевого з’єднання базуються на базі систем зв’язку ближньої дії персональних мереж (PAN), зазвичай побудованих без дотримання правил IP-протоколу. Це може бути як дротові так і бездротові мережі. До бездротових IoT-мереж/протколів як правило відносяться протоколи Bluetooth, mesh-мережі, Zigbee, Z-Wave. Для IIoT це також Wireless Hart та ISA100. Це яскравий приклад різноманіття бездротових систем зв’язку IoT. Перелік дротових мереж ще більший, так як сюди входять усі можливі промислові мережі та протоколи» (рис. 1.5) [8].

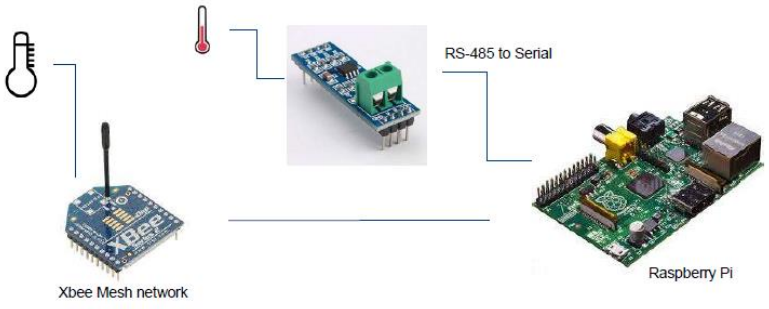

Рисунок 1.5 – Personal Area Network [8]

«Крім PAN використовуються бездротові локальні мережі та системи зв’язку на основі IP-протоколу, включаючи широкий діапазон Wi-Fi-мереж на основі стандартів IEEE 802.11, 6LoWPAN і технології Thread. Нерідко

використовуються телекомунікації на основі стільникових стандартів (3G, 4G LTE) і нові стандарти, що забезпечують роботу Інтернету речей і міжмашинної взаємодії, такими як Cat-1 і Cat-NB, а також пропрієтарні протоколи LoRaWAN і Sigfox, що використовуються саме для IoT» (рис. 1.6) [8].

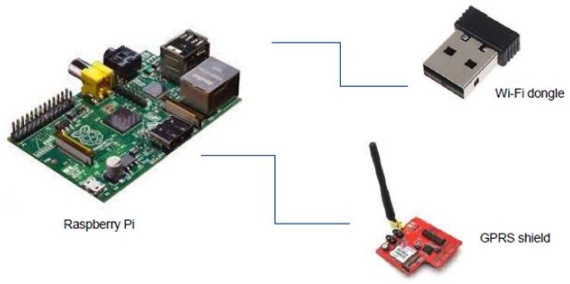

Рисунок 1.6 – Системи зв’язку на основі IP-протоколу [8]

1.7.3 Маршрутизація

Для передачі даних від датчиків в Інтернет-простір необхідні дві технології: маршрутизатор-шлюз і опорні інтернет-протоколи, що забезпечують ефективність обміну даними. Маршрутизатор особливо важливий в таких аспектах, як безпека, управління і напрям даних. Граничні маршрутизатори (Edge routers) керують і стежать за станом відповідних mesh-мереж, а також вирівнюють і підтримують якість даних. Також велике значення належить конфіденційності та безпеки даних. Маршрутизатор відіграє важливу роль в створенні віртуальних приватних мереж, віртуальних локальних мереж і програмно-визначених глобальних мереж. Вони в буквальному сенсі можуть містити тисячі вузлів, що обслуговуються єдиним граничним маршрутизатором, і в якійсь мірі маршрутизатор служить розширенням для хмари (edge device) [1, 8, 16].

На цьому рівні використовується ряд протоколів, необхідних для обміну між вузлами, маршрутизаторами і хмарними сервісами в межах IoT-системи. Інтернет речей відкрив дорогу новим IoT-протоколам, які виходять на один рівень з традиційними протоколами HTTP і SNMP, які застосовуються вже кілька десятків років. Для передачі IoT-даних потрібні ефективні,

енергозберігаючі протоколи з малою затримкою, здатні легко і безпечно відправляти дані в хмару і з нього. Зокрема тут використовуються такі протоколи, як всюдисущий MQTT, AMPQ і CoAP [1, 8, 16].

1.7.4 Туманні і граничні обчислення, аналітика і машинне навчання

«На цьому етапі необхідно вирішити, що робити з потоком даних, що надходять в хмарний сервіс з граничного вузла (Edge Device). Щоб навчитися правильно оцінювати, як система буде розвиватися і рости, необхідно розібратися у всіх тонкощах і складнощах архітектури хмарних систем, який вплив на IoT-систему робить запізнювання. Крім того, не все треба відправляти в хмару. Пересилання всіх IoT-даних обходиться значно дорожче, ніж їх обробка на кордоні мережі (граничні обчислення, Edge Computing) або включення граничного маршрутизатора в зону, яку обслуговує хмарний сервіс (туманні обчислення, Fog computing). Туманні обчислення також стандартизуються, зокрема є стандарт туманних обчислень, наприклад архітектура OpenFog» [8].

«Дані, які були отримані шляхом перетворення аналогового фізичного впливу в цифровий сигнал, можуть мати велику вагу. Саме тут в гру вступають засоби аналітики і процесори правил IoT-системи. Ступінь складності введення в дію IoT-системи залежить від того, яке рішення проєктується. У деяких ситуаціях все досить просто: наприклад, коли на граничний маршрутизатор, який контролює кілька датчиків, потрібно встановити простий процесор правил, що відслідковує аномальні скачки температури. Інша ситуація – величезна кількість структурованих і неструктурованих даних в режимі реального часу передається в хмарне озеро даних, що вимагає високої швидкості обробки (для прогнозної аналітики) і довгострокового прогнозування на базі високотехнологічних моделей машинного навчання, таких як рекурентна нейронна мережа в пакеті аналізу сигналів з кореляцією по часу. Тут є певні проблеми і складнощі аналітики, які вирішуються різними підходами та методами, наприклад складними обробниками подій, байесовськими мережами і формування нейронних мереж» [8].

1.7.5 Загроза і безпека в Інтернеті речей

Багато IoT-систем не будуть обмежені безпечним простором будинку або офісу. Вони будуть розташовуватися в громадських місцях, в дуже віддалених областях, в рухомих транспортних засобах або навіть всередині людини. Інтернет речей – це величезна єдина мішень для хакерських атак. Вже було виявлено нескінченна кількість направлених на IoT-пристрої навчальних атак, добре організованих зломів і навіть уразливостей в системі безпеки національного масштабу. Розробник IoT рішень повинен знати особливості таких вразливостей і способи їх усунення, стандартні заходи, спрямовані на захист Інтернету речей або будь-якого компонента мережі [1, 4, 11].

РОЗДІЛ 2
ЗАГАЛЬНА СТРУКТУРА ПРОЄКТУ ТА ЗАСОБИ РОЗРОБКИ

2.1 Вибір та огляд засобів розробки

У межах розробки IoT-інфраструктури супермаркету здійснено обґрунтований вибір інструментальних засобів, що забезпечують як моделювання фізичної топології об’єкта, так і емуляцію поведінки інтелектуальних пристроїв у мережевому середовищі. Такий підхід дозволяє не лише візуалізувати майбутню систему, але й провести попередній аналіз її ефективності, виявити потенційні вузькі місця та оцінити рівень масштабованості ще до етапу фізичної реалізації.

Для створення цифрового плану об’єкта використано програмне середовище AutoCAD, яке є одним із найпоширеніших інструментів автоматизованого проєктування. Застосування цього програмного продукту дозволило детально відтворити просторову структуру супермаркету з урахуванням архітектурних особливостей приміщення, зонування торгових площ, складських приміщень, технічних зон та службових приміщень. Окрему увагу приділено логістиці переміщення покупців і персоналу, що є важливим фактором при розміщенні сенсорних систем та виконавчих пристроїв. Крім того, цифрова модель дає змогу врахувати такі аспекти, як потенційні джерела перешкод для бездротового сигналу, щільність розташування обладнання та оптимальні точки встановлення мережевих вузлів. Усе це створює надійну основу для подальшого коректного та ефективного розміщення IoT-пристроїв у реальному середовищі [7].

Реалізація мережевої частини проєкту виконана в середовищі Cisco Packet Tracer, яке надає широкі можливості для моделювання сучасних комп’ютерних мереж, включаючи підтримку концепції Інтернету речей. Використання цього інструменту дозволило змоделювати взаємодію між різними типами пристроїв, такими як сенсори температури, освітлення, диму, руху, а також виконавчі механізми системи кондиціонування, освітлення та сигналізації. Окрім цього,

Packet Tracer забезпечує можливість налаштування мережевих протоколів, адресації, маршрутизації та сервісів, що дає змогу створити повноцінну модель функціонування інфраструктури [7].

Важливою перевагою використання Cisco Packet Tracer є можливість імітації реальних сценаріїв роботи системи, зокрема обробки подій, передачі даних між пристроями та реакції системи на зміну параметрів середовища. Це дозволяє перевірити логіку роботи IoT-рішень, оцінити швидкість реагування системи та визначити надійність функціонування в умовах, наближених до реальних. Додатково, середовище підтримує інтеграцію з мікроконтролерами та програмування поведінки пристроїв, що відкриває можливості для реалізації інтелектуальних алгоритмів керування [7].

2.1.1 AutoCAD

Програма AutoCAD (рис. 2.1) існує з 1982 року. В основі її спроба перейти від систем автоматизованого проєктування на базі надзвичайно дорогих мейнфреймів і міні-комп’ютерів, що коштували десятки тисяч доларів, до програм, що працюють на відносно недорогих мікрокомп’ютерах (так тоді називали настільні персональні комп’ютери), які коштували декілька тисяч доларів [13].

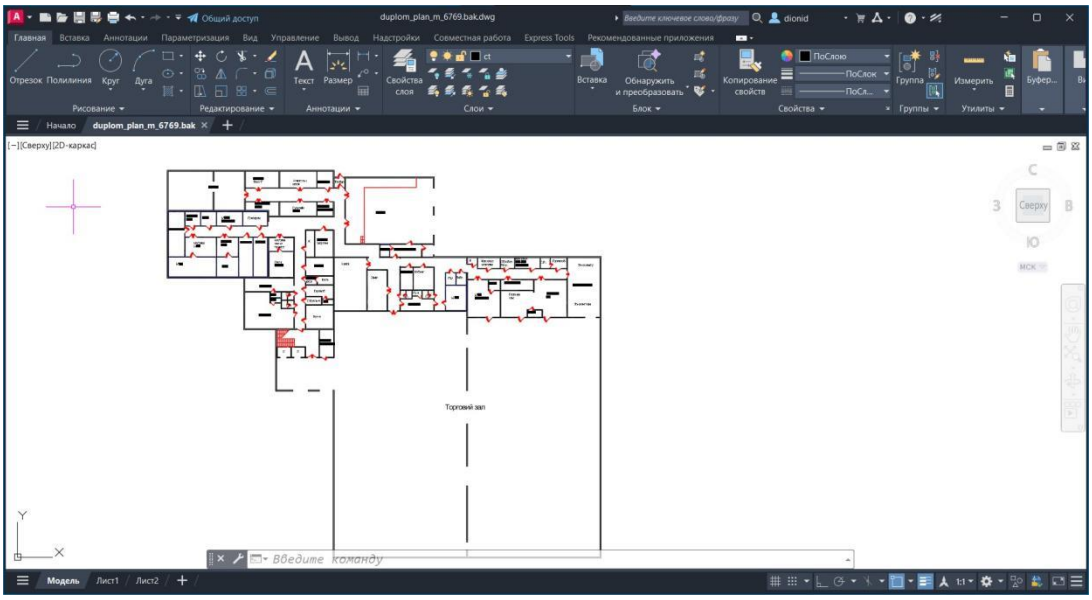

Рисунок 2.1 – Інтерфейс AutoCAD

Призначена програма AutoCAD першочергово для створення креслеників. Кресленики, створені з її допомогою, повинні відповідати державним стандартам, встановленим до різних видів креслярської продукції, які традиційно виконували вручну і часто створюють так і тепер. Безумовно, капіталовкладення в технологію AutoCAD вище, ніж витрати на олівці і папір; цикл навчання тривалішій: слід освоїти і комп'ютер, і саму систему AutoCAD [13].

Використання AutoCAD у процесі проєктування цифрових планів та схем має низку важливих переваг, які роблять це програмне забезпечення одним із найпоширеніших інструментів для створення технічної документації. Насамперед AutoCAD забезпечує високу точність побудови креслень і схем, що є особливо важливим під час розроблення планів приміщень, розташування мережевого обладнання та IoT-пристроїв. Використання координатної системи, інструментів вимірювання та прив'язки дозволяє уникнути помилок і забезпечити правильне позиціонування всіх елементів інфраструктури [14].

Суттєвою перевагою також є зручність редагування та внесення змін до вже створених проєктів. У процесі проєктування часто виникає необхідність коригування розташування обладнання, зміни параметрів приміщень або оновлення структури мережі. AutoCAD дозволяє виконувати такі зміни швидко та без необхідності повного перероблення креслення, що значно економить час і спрощує роботу над проєктом [13].

Програмне забезпечення характеризується високою продуктивністю під час створення складних технічних планів і великих схем. Завдяки автоматизації багатьох процесів та наявності великої кількості професійних інструментів можна ефективно працювати навіть із масштабними проєктами, що містять значну кількість об'єктів і деталей. Це особливо важливо під час розроблення інфраструктури супермаркетів, систем Smart Home або інших комплексних об'єктів [13].

Додатковою перевагою є можливість багаторазового використання вже створених елементів і шаблонів. Блоки, умовні позначення, мережеві

компоненти та інші об’єкти можуть зберігатися в бібліотеках і повторно використовуватися в інших проєктах. Такий підхід дозволяє стандартизувати оформлення документації, прискорити процес розроблення та зменшити кількість однотипної роботи [13].

Важливе значення має також підтримка масштабування та точного позиціонування обладнання на плані приміщення. Це дає змогу правильно розраховувати відстані між пристроями, визначати оптимальні місця встановлення датчиків, точок доступу чи серверного обладнання, а також забезпечувати відповідність цифрової моделі реальному об’єкту. Завдяки цьому створені схеми можуть використовуватися не лише для візуалізації, а й для практичної реалізації проєкту [13].

2.1.2 Cisco Packet Tracer

Cisco Packet Tracer (рис. 2.2) – це програмне середовище моделювання комп’ютерних мереж, розроблене компанією Cisco Systems, яке широко використовується у навчанні, проєктуванні та тестуванні мережевих рішень, зокрема у сфері IoT. Його функціональні можливості дозволяють створювати віртуальні топології різної складності без потреби у фізичному обладнанні.

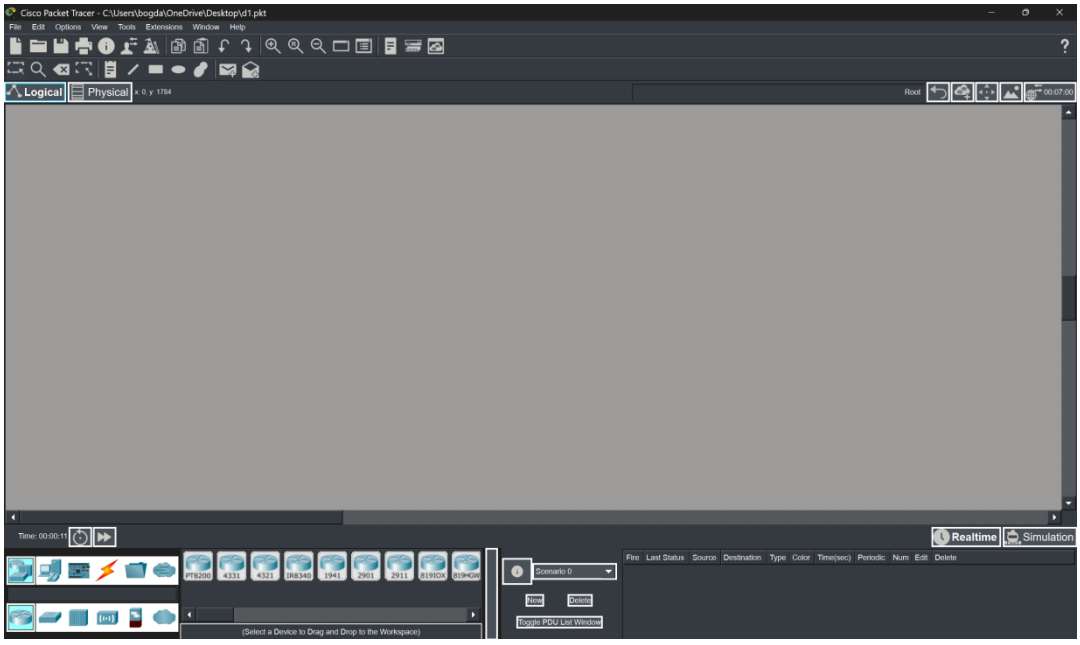

Рисунок 2.2 – Інтерфейс Cisco Packet Tracer

Однією з переваг є висока доступність і простота використання. Інтерфейс системи забезпечує інтуїтивну взаємодію з мережевими пристроями, такими як маршрутизатори, комутатори, сервери та IoT-компоненти. Це важливо у навчальних цілях, оскільки дозволяє швидко освоїти принципи побудови мереж навіть без глибоких попередніх знань.

Суттєвим плюсом є можливість моделювання різноманітних мережевих сценаріїв. У середовищі можна налаштовувати протоколи маршрутизації, VLAN, бездротові мережі, а також взаємодію пристроїв Інтернету речей. Наприклад, у проєктах типу «розумний супермаркет» можлива інтеграція датчиків руху, температури, освітлення та сигналізації в єдину систему з централізованим керуванням. Це дозволяє не лише перевірити працездатність системи, але й оцінити ефективність її архітектури.

Ще однією важливою перевагою є режим симуляції. Він дозволяє покроково аналізувати передачу пакетів у мережі, що є критично важливим для розуміння принципів роботи протоколів і виявлення помилок у конфігурації. Такий підхід значно спрощує процес навчання та діагностики мереж.

Також варто відзначити підтримку IoT. У сучасних версіях Cisco Packet Tracer реалізовано модулі для роботи з «розумними» пристроями датчиками, виконавчими механізмами та мікроконтролерами. Це робить програму актуальною для проєктів, пов’язаних із Smart Home або автоматизацією підприємств, що безпосередньо відповідає сучасним тенденціям розвитку технологій.

З економічної точки зору, плюсом є відсутність потреби у дорогому фізичному обладнанні. Створення реальної лабораторії з мережевими пристроями потребує значних фінансових витрат, тоді як Packet Tracer дозволяє реалізувати аналогічні сценарії у віртуальному середовищі.

Слід підкреслити можливість інтеграції в IoT-пристрої логіки програмування. У Packet Tracer доступне налаштування поведінки пристроїв за допомогою скриптів або вбудованих правил, що дозволяє моделювати складні сценарії автоматизації.

2.1.3 Протоколи взаємодії IoT-пристроїв

Невід'ємною складовою будь-якої IoT-системи є набір комунікаційних протоколів, які забезпечують обмін даними між пристроями, сервером та адміністративними засобами. Вибір протоколів здійснювався з урахуванням вимог до надійності, ефективності передачі та особливостей середовища моделювання Cisco Packet Tracer.

MQTT (Message Queuing Telemetry Transport) є основним прикладним протоколом у проєкті для взаємодії між IoT-пристроями та центральним сервером. Він функціонує за принципом «видавець-підписник» (publish/subscribe): пристрій публікує дані у визначений топік, а сервер або інші клієнти, підписані на цей топік, отримують їх. Ключовою перевагою MQTT є мінімальне споживання ресурсів: протокол розроблений спеціально для пристроїв з обмеженою обчислювальною потужністю та нестабільним каналом зв'язку. Він підтримує три рівні якості обслуговування (QoS 0, 1, 2), що дозволяє регулювати гарантії доставки повідомлень залежно від критичності даних. В рамках проєкту MQTT використовується для передачі показань датчиків температури, руху, диму та стану дверних сенсорів [9].

HTTP/HTTPS (Hypertext Transfer Protocol / Secure) застосовується для взаємодії адміністративних клієнтів з IoT-сервером через веб-інтерфейс управління. Протокол забезпечує доступ до панелі моніторингу, журналів подій та налаштувань системи. HTTPS додатково шифрує трафік за допомогою TLS, що є обов'язковою вимогою для захисту адміністративного доступу. На відміну від MQTT, HTTP є синхронним протоколом типу «запит-відповідь», що робить його менш придатним для потокової передачі даних від численних датчиків, однак оптимальним для адміністративних запитів [9].

DNS (Domain Name System) використовується у проєкті для спрощення адресації пристроїв та сервісів. Замість звернення до сервера за IP-адресою адміністратор використовує символьне ім'я. DNS-сервер налаштований на централізованому IoT-сервері та обслуговує запити пристроїв обох підмереж.

Це забезпечує гнучкість адміністрування: у разі зміни IP-адреси сервера достатньо оновити DNS-запис, не змінюючи конфігурацію кожного пристрою.

DHCP (Dynamic Host Configuration Protocol) забезпечує автоматичне призначення IP-адрес підключеним пристроям. У проєкті DHCP-сервер налаштований на IoT-сервері і видає адреси з окремих пулів для IoT-пристроїв та офісних пристроїв. Це усуває необхідність ручного налаштування адрес при підключенні нових датчиків або виконавчих пристроїв, що суттєво знижує трудовитрати при масштабуванні системи. Критично важливі вузли мають статичні IP-адреси, що гарантує їхню незмінну доступність у мережі.

2.2 Структура проєкту

Проєкт IoT-інфраструктури супермаркету сформовано як багаторівневу кіберфізичну систему, у межах якої цифрове відображення реального об’єкта виступає не лише як допоміжний інструмент проєктування, а як повноцінна основа для моделювання, тестування та подальшої оптимізації функціонування всієї інфраструктури.

Початковий план приміщення, розроблений у середовищі AutoCAD, детально адаптовано до середовища Cisco Packet Tracer, що дозволило створити цифровий двійник супермаркету з урахуванням топології мережі, розташування обладнання та сценаріїв взаємодії між пристроями. Такий підхід забезпечує високий рівень деталізації моделі та дозволяє ще на етапі проєктування виявляти потенційні вузькі місця, перевіряти сценарії відмов і оцінювати ефективність рішень без необхідності фізичного розгортання системи.

Архітектура системи організована за ієрархічним принципом із чітким поділом на фізичний, мережевий і прикладний рівні, що забезпечує логічну структурованість, масштабованість і зручність адміністрування. Такий підхід дозволяє ізолювати функціональні компоненти, спрощуючи модернізацію системи, інтеграцію нових пристроїв або зміну конфігурації без суттєвого впливу на інші підсистеми. Крім того, ієрархічна модель сприяє підвищенню

надійності, оскільки локальні збої не призводять до повної втрати працездатності всієї інфраструктури.

Фізичний рівень представлений широким спектром IoT-пристроїв, розміщених відповідно до функціонального зонування супермаркету. У торгових залах, де спостерігається висока динаміка переміщення відвідувачів, інтеграція датчиків руху та освітленості дозволяє реалізувати інтелектуальні сценарії керування освітленням.

Освітлювальні системи автоматично адаптуються до умов навколишнього середовища, що не лише знижує енергоспоживання, але й підвищує комфорт перебування клієнтів, створюючи сприятливу атмосферу для здійснення покупок. Додатково це зменшує навантаження на електромережу та продовжує термін служби освітлювального обладнання.

У складських і технічних приміщеннях впровадження сенсорів сприяє підвищенню ефективності логістичних процесів. Система здатна фіксувати активність персоналу, контролювати освітлення та формувати аналітичні дані щодо використання приміщень, що в перспективі може бути використано для оптимізації внутрішніх процесів і скорочення витрат.

Особливу увагу приділено підсистемі безпеки. Інтеграція датчиків диму, тривожних сенсорів і систем сигналізації формує багаторівневу систему реагування на надзвичайні ситуації. У разі виявлення небезпеки система здатна не лише генерувати сповіщення, але й ініціювати автоматизовані сценарії, такі як активація сигналізації, передача повідомлень до центру моніторингу або навіть запуск додаткових механізмів безпеки. Це суттєво скорочує час реагування та мінімізує ризики для персоналу і майна.

Кліматичний контроль реалізовано через інтеграцію термостатів і систем кондиціонування у зонах із підвищеними вимогами до температурного режиму, зокрема у морозильних камерах. Постійний моніторинг температури дозволяє підтримувати стабільні умови зберігання продукції, що є критично важливим для забезпечення її якості. Додатково система може фіксувати відхилення від

норми та автоматично коригувати параметри, запобігаючи псуванню товарів і фінансовим втратам.

Контроль доступу реалізовано за допомогою дверних датчиків, що інтегровані у критично важливі зони. Це дозволяє не лише відстежувати факти відкриття та закриття дверей, але й формувати журнал подій, який може використовуватися для аудиту безпеки. Такий підхід підвищує рівень захисту інформаційних і матеріальних ресурсів, а також сприяє дисципліні персоналу.

Мережевий рівень виступає основою для взаємодії всіх компонентів системи. Побудова єдиної IP-мережі із використанням комутаторів і маршрутизаторів забезпечує стабільну та швидку передачу даних між пристроями. Централізація обробки інформації через IoT-сервер дозволяє ефективно агрегувати дані, виконувати їх аналіз і забезпечувати доступ до них у реальному часі. Використання DNS-служби спрощує адресацію пристроїв, роблячи систему більш гнучкою та зрозумілою для адміністрування.

Впровадження DHCP-сервісу є важливим елементом автоматизації мережевої інфраструктури. Завдяки цьому процес налаштування нових пристроїв значно спрощується, зменшується ймовірність помилок конфігурації та підвищується загальна керованість системи. Це особливо актуально в умовах масштабування, коли кількість підключених пристроїв може швидко зростати.

Інтеграція мережі для персоналу розширює функціональні можливості системи, забезпечуючи централізований доступ працівників до внутрішніх ресурсів і сервісів супермаркету. Такий підхід відповідає сучасним тенденціям цифровізації, де співробітники можуть швидко отримувати доступ до необхідної інформації та взаємодіяти з системою в межах єдиної мережевої інфраструктури.

Працівники отримують можливість оперативно обмінюватися даними, контролювати стан обладнання, працювати з інформаційними сервісами та виконувати службові завдання безпосередньо через локальну мережу підприємства.

Взаємодія всіх компонентів системи формує єдиний інформаційний простір, у якому дані безперервно циркулюють між рівнями, забезпечуючи актуальність і достовірність інформації. Це створює основу для впровадження аналітичних інструментів, прогнозування та подальшої автоматизації процесів. У результаті досягається значне підвищення енергоефективності, зниження експлуатаційних витрат, покращення рівня безпеки та оптимізація управління супермаркетом.

Таким чином, розроблена IoT-інфраструктура демонструє не лише технічну реалізацію взаємопов’язаних компонентів, але й комплексний підхід до цифрової трансформації торгового об’єкта. Її переваги проявляються у гнучкості, масштабованості, надійності та здатності адаптуватися до змінних умов експлуатації, що робить дане рішення перспективним для впровадження у сучасних комерційних середовищах.

2.2.1 Перелік IoT-пристроїв та обґрунтування їхнього вибору

Склад IoT-пристроїв системи визначався виходячи з функціонального зонування супермаркету та переліку автоматизованих процесів, що підлягають реалізації. Обрані пристрої охоплюють задачі безпеки, енергозбереження, кліматичного контролю та управління доступом (табл. 2.1).

Таблиця 2.1 – Перелік IoT-пристроїв проєкту

Пристрій	Функція	Зона розміщення	Обґрунтування вибору
Датчик руху	Виявлення присутності людини	Склад	Зниження енергоспоживання
Датчик температури	Контроль температурного режиму	Морозильні камери	Контроль умов зберігання
Датчик диму	Виявлення задимлення	Торговий зал, склад	Пожежна безпека
Дверний датчик	Контроль відкриття дверей	Сервісні входи	Підвищення безпеки
Smart Light	Автоматичне освітлення	Службові зони	Енергоефективність

Подовження таблиці 2.1

Пристрій	Функція	Зона розміщення	Обґрунтування вибору
Комутатор	Комутація трафіку	Технічні зони	Сегментація мережі
Маршрутизатор	Міжмережева маршрутизація	Серверна	Ізоляція підмереж
Термостат	Керування температурою	Морозильні камери	Контроль умов зберігання
IoT-сервер	Централізована обробка даних	Серверна	Центральний вузол

2.2.2 Сценарії роботи системи

Функціонування IoT-інфраструктури супермаркету визначається набором сценаріїв роботи, що описують взаємодію пристроїв у відповідь на конкретні події. Кожен сценарій складається з тригера (вхідної події), набору дій системи та кінцевого результату, який отримується після виконання відповідних операцій. Використання сценарного підходу дозволяє детально описати логіку функціонування системи, визначити взаємозв’язки між окремими компонентами та оцінити ефективність автоматизації процесів.

Реалізація сценаріїв роботи забезпечує адаптивність системи до змін умов навколишнього середовища та дозволяє автоматично реагувати на події без безпосереднього втручання людини. Це сприяє підвищенню рівня енергоефективності, безпеки та надійності функціонування супермаркету. Крім того, сценарії є важливим елементом проєктування IoT-систем, оскільки дають змогу моделювати поведінку інфраструктури ще на етапі розробки та тестування.

У межах проєкту реалізовано низку базових сценаріїв, пов’язаних із керуванням освітленням, контролем температури, пожежною безпекою, моніторингом доступу та адмініструванням мережевої інфраструктури. Усі сценарії функціонують у реальному часі та базуються на взаємодії сенсорів,

виконавчих пристроїв і центрального IoT-сервера. Завдяки централізованій обробці даних система здатна швидко аналізувати отриману інформацію та виконувати відповідні дії згідно із заданими правилами.

Особливістю реалізованої системи є можливість подальшого розширення переліку сценаріїв без суттєвої зміни архітектури мережі. Це дозволяє інтегрувати нові пристрої, сервіси та механізми автоматизації відповідно до потреб торгового об’єкта. Такий підхід забезпечує масштабованість рішення та створює основу для подальшої цифрової трансформації супермаркету.

У таблиці 2.2 наведено основні сценарії роботи системи, які реалізовані або передбачені в рамках проєкту.

Таблиця 2.2 – Основні сценарії роботи системи

Тригер	Дія системи	Результат
Виявлення руху	Увімкнення освітлення	Економія електроенергії
Підвищення температури	Активація кондиціонування	Підтримка температурного режиму
Виявлення диму	Запуск сигналізації	Підвищення пожежної безпеки
Відкриття дверей	Формування запису в журналі	Контроль доступу
Втрата зв’язку з пристроєм	Надсилання сповіщення адміністратору	Оперативне реагування
Підключення нового пристрою	Автоматичне отримання IP-адреси	Спрощення масштабування системи

Наведені сценарії демонструють комплексний підхід до організації роботи IoT-інфраструктури супермаркету. Їх реалізація забезпечує автоматизацію ключових процесів, підвищує ефективність управління ресурсами та сприяє створенню безпечного й комфортного середовища для персоналу та відвідувачів. Крім того, автоматичне реагування на події дозволяє мінімізувати вплив людського фактора, зменшити ймовірність помилок і підвищити стабільність роботи всієї системи.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОЄКТУ

3.1 Побудова цифрової моделі супермаркету

На початковому етапі використано план супермаркету, створений у середовищі AutoCAD продемонстрований на рисунку 3.1. Цей план слугує базою для формування топології в Cisco Packet Tracer. У процесі адаптації враховано геометричні параметри приміщень, їх функціональне призначення та логіку переміщення відвідувачів і персоналу.

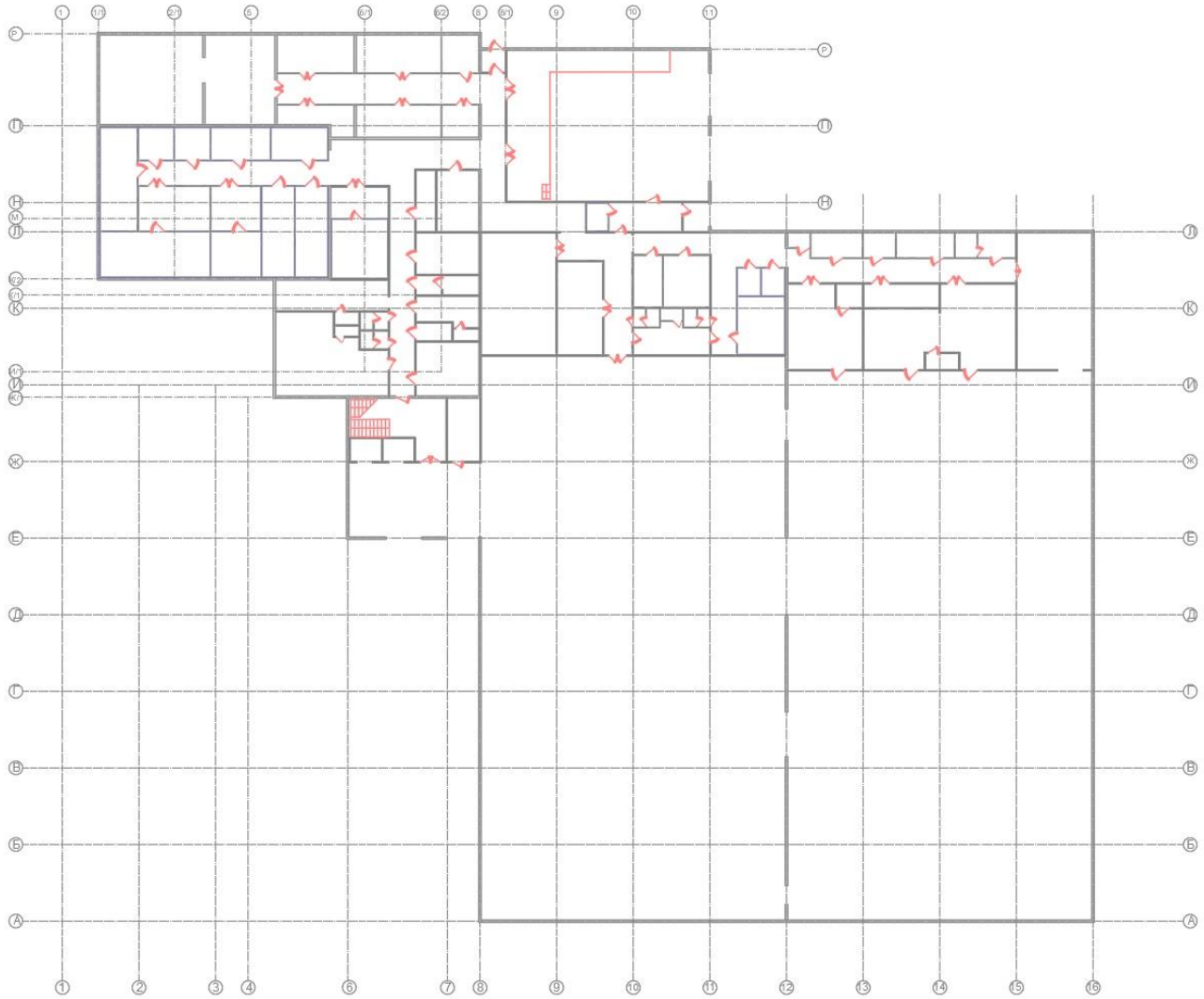

Рисунок 3.1 – План супермаркету

Цифрова модель включає торгові зали, складські приміщення, технічні зони, морозильні камери, серверну кімнату та адміністративні приміщення. Така деталізація дозволяє коректно розмістити IoT-пристрої відповідно до їх функціонального призначення. Додатково виконано зонування, що забезпечує логічне групування пристроїв і спрощує подальше налаштування системи.

3.2 Налаштування фізичного рівня системи

Фізичний рівень IoT-інфраструктури супермаркету реалізовано з урахуванням просторового зонування об’єкта та принципів раціонального розміщення обладнання. План приміщення умовно поділено на три функціональні зони які продемонстровані на рисунках 3.2-3.4, що дозволяє оптимізувати підключення пристроїв та зменшити навантаження на мережеву інфраструктуру. Перша зона підключена до окремої точки доступу, тоді як друга та третя зони обслуговуються іншою точкою доступу. Незважаючи на таке фізичне розділення, усі пристрої функціонують у межах єдиної логічної мережі, що забезпечує їхню повну взаємодію та централізоване управління.

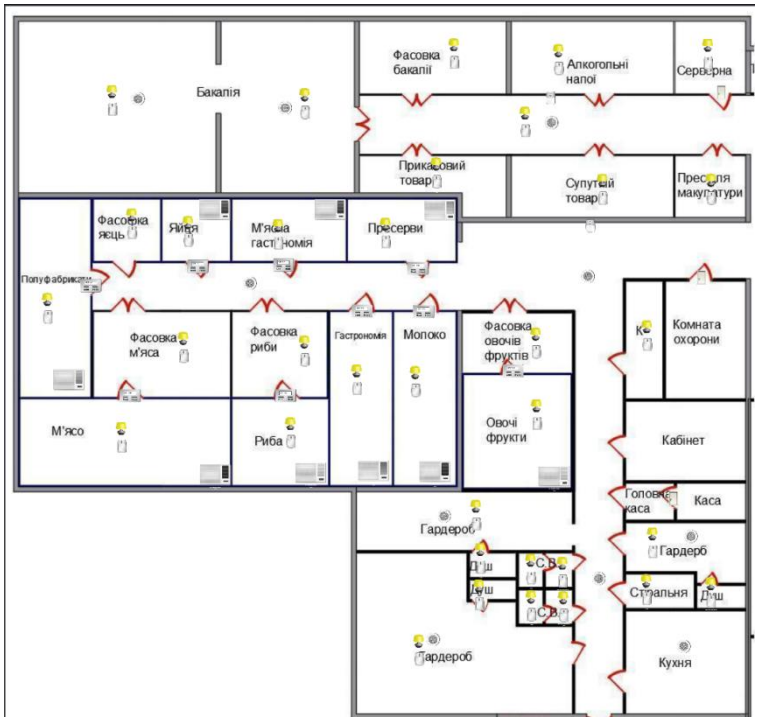

Рисунок 3.2. – План супермаркету, зона 1

Такий підхід дозволяє досягти балансу між продуктивністю та масштабованістю системи. Розподіл навантаження між точками доступу зменшує ризик перевантаження мережі, підвищує стабільність передачі даних і забезпечує більш рівномірне покриття сигналом. Водночас єдина мережева адресація спрощує адміністрування та інтеграцію пристроїв.

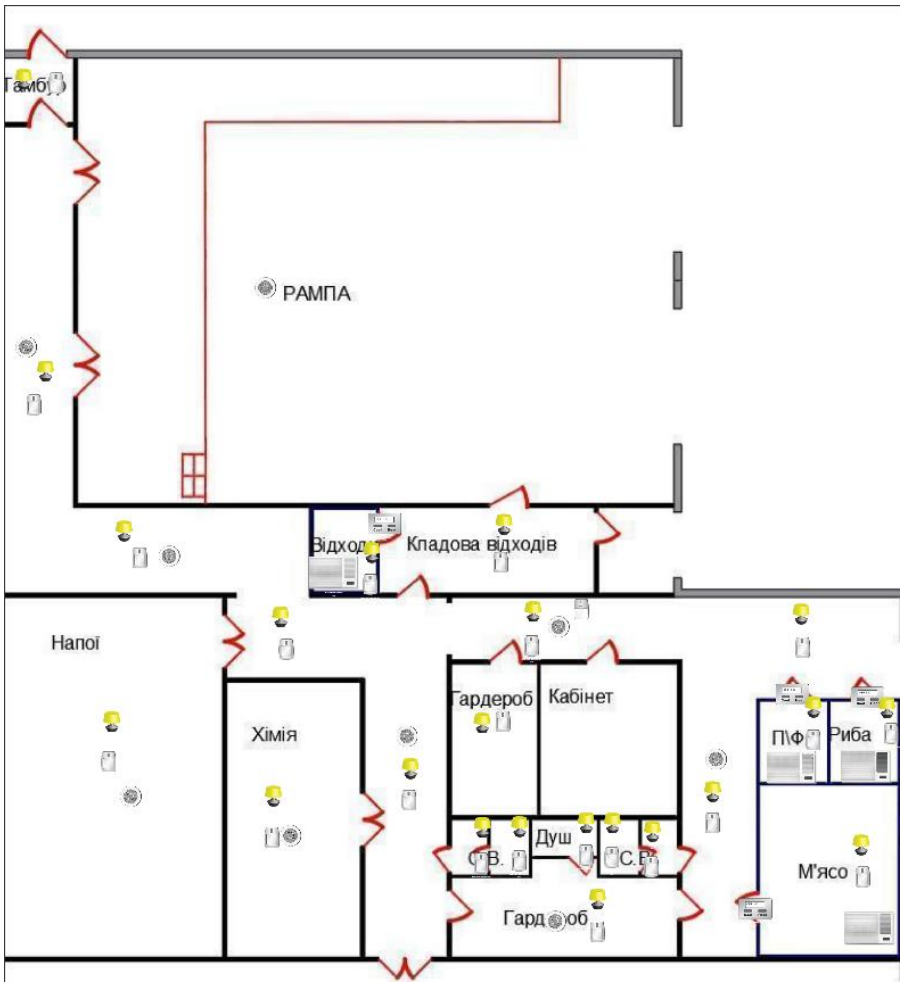

Рисунок 3.3 – План супермаркету, зона 2

Розміщення IoT-датчиків виконано за принципом функціональної доцільності, тобто сенсори встановлено лише у тих зонах, де їх використання є обґрунтованим і приносить практичну користь. Це дозволяє уникнути надлишковості обладнання, зменшити витрати ресурсів та спростити обслуговування системи. Такий підхід забезпечує оптимальний баланс між ефективністю функціонування системи та економічною доцільністю її впровадження.

При проєктуванні мережі враховувалися особливості кожного приміщення, інтенсивність використання окремих зон, а також потенційні ризики та потреби автоматизації. Наприклад, датчики руху та освітлення встановлювалися у приміщеннях із змінною присутністю персоналу або відвідувачів, що дозволяє автоматично керувати освітленням та знижувати енергоспоживання. Датчики температури й вологості розміщені у складських та холодильних приміщеннях для забезпечення належних умов зберігання продукції. У місцях із підвищеними вимогами до безпеки передбачено використання датчиків диму та систем сигналізації.

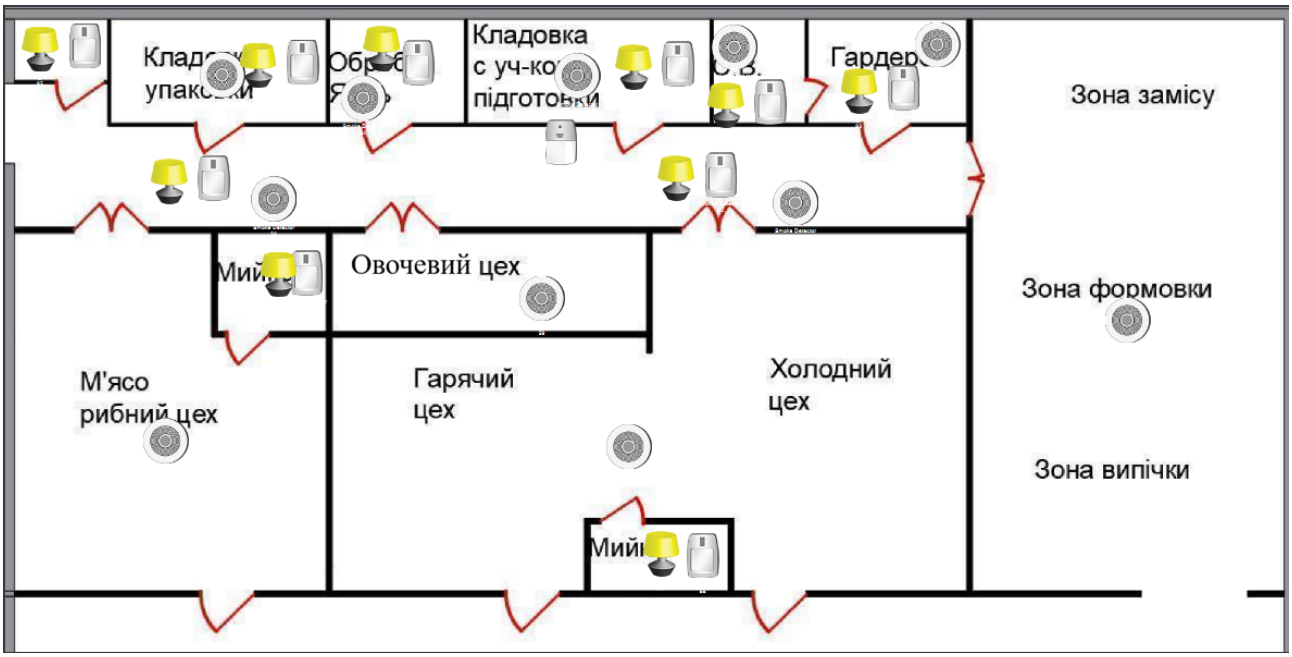

Рисунок 3.4 – План супермаркету, зона 3

Система освітлення автоматизована у ключових зонах, де це має найбільший ефект. Зокрема, датчики руху та освітленості встановлено у складських приміщеннях, коридорах, морозильних камерах і гардеробі. У цих зонах освітлення активується лише за наявності руху або недостатнього рівня освітленості, що забезпечує значну економію електроенергії та підвищує енергоефективність об’єкта. Вибір саме цих приміщень обумовлений нерегулярним перебуванням людей, що робить автоматизацію найбільш доцільною.

Контроль температурного режиму реалізовано виключно у морозильних камерах, де стабільність температури є критично важливою для зберігання продукції. Використання термостатів дозволяє підтримувати задані параметри мікроклімату, а також оперативно реагувати на їх відхилення. Така локалізація системи клімат-контролю є економічно обґрунтованою та відповідає реальним потребам супермаркету.

Підсистема пожежної безпеки організована більш комплексно. Датчики диму встановлено по всій площі супермаркету без винятку, що забезпечує повне покриття та мінімізує ризик невиявлення загоряння. Аналогічно по всьому об’єкту розміщено сирени, які виконують функцію оповіщення у разі виникнення небезпечної ситуації. Такий підхід формує єдину інтегровану систему реагування, здатну швидко інформувати персонал і відвідувачів про загрозу.

Загалом, реалізація фізичного рівня з урахуванням зонування, доцільного розміщення датчиків та оптимального використання точок доступу дозволяє підвищити ефективність роботи IoT-системи. Це забезпечує не лише стабільність функціонування, але й економічність, гнучкість та можливість подальшого розширення інфраструктури без суттєвих змін у її архітектурі.

3.3 Логічна структура мережі

У даному проєкті розроблено логічну структуру мережі супермаркету з використанням технологій Інтернету речей (IoT). Архітектура мережі передбачає поділ на окремі функціональні сегменти: серверний, клієнтський, бездротовий та міжмережевий (WAN). Такий підхід дозволяє забезпечити масштабованість, підвищити рівень безпеки та оптимізувати маршрутизацію трафіку.

3.3.1 Адресація серверної мережі

Серверна мережа призначена для розміщення центрального вузла керування IoT-пристроями та DNS-сервера. Вона є критичною частиною

інфраструктури, оскільки забезпечує обробку даних та взаємодію між пристроями (табл. 3.1).

Таблиця 3.1 – Адресація серверної мережі

№	Адреса підмережі	Діапазон IP	Перша IP	Остання IP	Broadcast	Шлюз
1	192.168.1.0/24	192.168.1.0-192.168.1.255	192.168.1.1	192.168.1.254	192.168.1.255	192.168.1.1

У таблиці 3.1 наведено параметри адресації серверної підмережі, яка виконує ключову роль у функціонуванні всієї системи. Для цієї мережі використано приватний діапазон IPv4 з маскою /24, що дозволяє підключити до 254 пристроїв і забезпечує достатній запас адрес для подальшого розширення інфраструктури.

Шлюзом за замовчуванням є маршрутизатор з IP-адресою 192.168.1.1, який виконує функції зв’язку між підмережами та забезпечує доступ до інших сегментів мережі. Сервер має статичну IP-адресу 192.168.1.2, що гарантує стабільний доступ до мережевих сервісів, зокрема DNS та IoT-платформи.

Діапазон IP-адрес з 192.168.1.20 до 192.168.1.254 зарезервовано для використання IoT-пристроїв, що дозволяє впорядкувати адресний простір, спростити адміністрування та забезпечити логічну структуризацію мережі.

3.3.2 Адресація клієнтської мережі

Клієнтська мережа призначена для підключення персональних комп’ютерів, ноутбуків та мобільних пристроїв користувачів (табл. 3.2).

Таблиця 3.2 – Адресація клієнтської мережі

№	Адреса підмережі	Діапазон IP	Перша IP	Остання IP	Broadcast	Шлюз
1	192.168.2.0/24	192.168.2.0-192.168.2.255	192.168.2.1	192.168.2.254	192.168.2.255	192.168.2.1

Таблиця 3.2 відображає параметри мережі, яка є основною середою для роботи користувачів. Для цієї мережі використано маску /24, що дозволяє забезпечити підключення до 254 пристроїв, чого цілком достатньо для середовища супермаркету. IP-адреси в мережі призначаються автоматично за допомогою DHCP-сервера, що значно зменшує навантаження на системного адміністратора, прискорює процес підключення нових пристроїв і мінімізує ризик виникнення помилок при ручному налаштуванні. Шлюзом за замовчуванням виступає маршрутизатор з адресою 192.168.2.1, який забезпечує вихід у зовнішню мережу та маршрутизацію трафіку між підмережами.

3.3.3 Адресація між маршрутизаторами (WAN)

Для організації взаємодії між маршрутизаторами використовується окрема WAN-підмережа. З'єднання між маршрутизаторами забезпечує передачу даних між локальними сегментами мережі та підтримує маршрутизацію між різними зонами IoT-інфраструктури супермаркету. Для WAN-з'єднання використовується підмережа 10.0.0.0/30, яка дозволяє підключити два маршрутизатори з мінімальною кількістю доступних адрес (табл. 3.3).

Таблиця 3.3 – WAN адресація

Назва з'єднання	Адреса підмережі	Діапазон адрес	IP Router 1	IP Router 2	Broadcast
Router0 - Router1	10.0.0.0/30	10.0.0.0 - 10.0.0.3	10.0.0.1	10.0.0.2	10.0.0.3

У таблиці 3.3 наведено адресацію WAN-з'єднань, яка використовується для організації взаємодії між мережевими вузлами на рівні міжмережевої інфраструктури. Використання маски /30 є стандартною практикою для з'єднань типу «точка-точка», оскільки така підмережа містить лише дві доступні IP-адреси по одній для кожного з кінців з'єднання. Це дозволяє максимально ефективно використовувати адресний простір, уникати його перевитрати та наближує модель до умов реального інтернет-провайдера, де

подібна схема широко застосовується. Крім того, така адресація спрощує маршрутизацію та підвищує зрозумілість структури мережі.

3.3.4 Адресація мережевих пристроїв

Таблиця 3.4 містить інформацію про адресацію пристроїв у серверному сегменті, який є одним із найбільш важливих елементів мережевої інфраструктури. У сегменті розміщуються ключові сервіси, що забезпечують функціонування всієї системи. Маршрутизатор у даній підмережі виконує роль шлюзу за замовчуванням, забезпечуючи вихід пристроїв у зовнішню мережу та взаємодію з іншими сегментами. Сервер має статичну IP-адресу, що є необхідною умовою для стабільної роботи DNS-служби та інших мережевих сервісів.

Таблиця 3.4 – Серверна частина

Пристрій	Інтерфейс	IP	Маска	Шлюз
Router (Main)	Fa0/0	192.168.1.1	255.255.255.0	-
Router (Main)	Fa0/1	10.0.0.1	255.255.255.252	-
Server (IoT + DNS)	NIC	192.168.1.2	255.255.255.0	192.168.1.1

Таблиця 3.5 відображає конфігурацію пристроїв мережі, включаючи їхні мережеві параметри та роль у загальній інфраструктурі. Використання DHCP у даному випадку дозволяє централізовано керувати адресним простором мережі та уникати конфліктів IP-адрес. Автоматичне призначення адрес значно спрощує процес адміністрування, особливо в умовах зростання кількості пристроїв.

Таблиця 3.5 – Частина для персоналу

Пристрій	Інтерфейс	IP	Маска	Шлюз
Router	Fa0/0	192.168.2.1	255.255.255.0	-
Router	Fa0/1	10.0.0.2	255.255.255.252	-
ПК / Laptop	DHCP	192.168.2.10- 192.168.2.254	255.255.255.0	192.168.2.1

3.3.5 Налаштування DHCP

У таблиці 3.6 наведено параметри DHCP-сервера, який відіграє ключову роль у процесі автоматизації налаштування мережі. DHCP-сервер забезпечує динамічне призначення IP-адрес клієнтським пристроям, що дозволяє уникнути необхідності ручного налаштування кожного вузла. Окрім IP-адреси, сервер також передає клієнтам такі важливі параметри, як адреса шлюзу за замовчуванням, DNS-сервера та інші мережеві налаштування. Це забезпечує коректну та стабільну роботу мережевих служб, а також сприяє швидкому підключенню нових пристроїв до мережі без додаткових налаштувань.

Таблиця 3.6 – Параметри DHCP

Параметр	Значення
Пул адрес	192.168.2.10 - 192.168.2.254
Шлюз	192.168.2.1
DNS	192.168.1.2

3.3.6 DNS система

Таблиця 3.7 демонструє відповідність доменного імені IP-адресі, що є важливим елементом функціонування мережі. Завдяки використанню служби DNS користувачі можуть звертатися до серверів не за складними числовими адресами, а за зрозумілими символьними іменами. Це значно підвищує зручність роботи, зменшує ймовірність помилок при введенні адреси та спрощує взаємодію з мережевими ресурсами. Крім того, централізоване керування доменними іменами дозволяє швидко змінювати IP-адреси серверів без необхідності внесення змін на кожному клієнтському пристрої.

Таблиця 3.7 – Параметри DNS

Домен	IP
m1124.iot	192.168.1.2

3.3.7 IoT пристрої

У таблиці 3.8 наведено перелік IoT-пристроїв, що використовуються в системі, із зазначенням їх основних характеристик та мережевих параметрів. До складу таких пристроїв можуть входити датчики температури, освітленості, руху, диму, а також виконавчі елементи, що забезпечують автоматизацію відповідних процесів. Кожен із пристроїв інтегрований у загальну мережеву інфраструктуру та взаємодіє з центральним сервером або контролером.

Таблиця 3.8 – IoT датчики

№	Пристрій	Тип	IP	Призначення
1	TempSensor	Датчик температури	192.168.1.20-254	Контроль температури
2	SmokeSensor	Датчик диму	192.168.1.20-254	Пожежна безпека
3	LightSensor	Датчик освітлення	192.168.1.20-254	Автоматизація світла
4	DoorSensor	Датчик дверей	192.168.1.20-254	Контроль доступу
5	Thermostat	Термостат	192.168.1.20-254	Керування кліматом

Всі пристрої мають статичні IP-адреси, що є доцільним рішенням для подібних систем. Це забезпечує стабільний і передбачуваний зв’язок із сервером, спрощує налаштування мережевих сервісів, а також полегшує адміністрування та моніторинг. Завдяки фіксованим адресам можна швидко ідентифікувати кожен пристрій у мережі, що особливо важливо при діагностиці або усуненні несправностей.

Зазначені IoT-пристрої виконують функції моніторингу та автоматизації процесів у супермаркеті. Вони забезпечують збір даних про стан навколишнього середовища та обладнання в режимі реального часу, що дозволяє оперативно реагувати на зміни умов. Автоматизація, у свою чергу, сприяє підвищенню ефективності роботи об’єкта, зменшенню витрат енергії та покращенню рівня безпеки. Таким чином, впровадження IoT-рішень є

важливим кроком у створенні сучасної інтелектуальної інфраструктури супермаркету.

3.3.8 Бездротова мережа

Таблиця 3.9 містить параметри бездротової мережі, які визначають основні характеристики її функціонування та рівень безпеки. У ній наведено такі показники, як ім’я мережі (SSID), тип шифрування, метод автентифікації користувачів, а також додаткові параметри, що впливають на стабільність та продуктивність з’єднання. Коректне налаштування цих параметрів є важливим для забезпечення надійної та безперебійної роботи всієї мережевої інфраструктури.

Таблиця 3.9 – Wi-Fi параметри

SSID	Тип захисту	Пароль
w1	WPA2-PSK	w1w1w1w1
w2 11242026	WPA2-PSK WPA2-PSK	w2w2w2w2 11242026

Використання протоколу WPA2-PSK забезпечує базовий рівень захисту бездротової мережі шляхом застосування попередньо узгодженого ключа доступу. Це дозволяє обмежити підключення сторонніх користувачів та захистити передані дані від несанкціонованого перехоплення. Незважаючи на те, що WPA2-PSK не є найсучаснішим стандартом безпеки, він залишається достатньо надійним рішенням для більшості практичних завдань, особливо в умовах локальної мережі з контрольованим доступом.

3.4 Моделювання комп’ютерної мережі

Моделювання комп’ютерної мережі виконано з використанням середовища Cisco Packet Tracer, що дозволяє створювати віртуальні топології мереж, налаштовувати мережеві пристрої та перевіряти їх роботу в режимі реального часу без використання фізичного обладнання. Дане середовище є

зручним інструментом для проєктування, тестування та аналізу мережевих рішень, що дає можливість виявити потенційні проблеми ще на етапі розробки.

У процесі моделювання реалізовано мережу супермаркету, яка включає серверний сегмент із IoT-пристроями, клієнтську мережу, бездротову інфраструктуру, а також канал зв’язку через провайдера.

3.4.1 Загальна топологія мережі

На початковому етапі створено загальну топологію мережі (рис. 3.5), яка включає маршрутизатори, комутатори, сервер, клієнтські пристрої та точки бездротового доступу. Побудова топології є одним із ключових етапів проєктування мережевої інфраструктури, оскільки саме на цьому етапі визначається структура взаємодії між усіма компонентами системи, способи передачі даних та організація мережевих сегментів.

Під час створення топології враховано необхідність забезпечення стабільного з’єднання між усіма пристроями, можливість централізованого керування мережею, а також подальше масштабування системи у разі підключення нових IoT-пристроїв. Маршрутизатори забезпечують передачу даних між окремими підмережами та доступ до зовнішньої мережі, тоді як комутатори виконують об’єднання пристроїв у локальні сегменти мережі. Сервер використовується для зберігання даних, обробки інформації від сенсорів та забезпечення роботи мережевих сервісів.

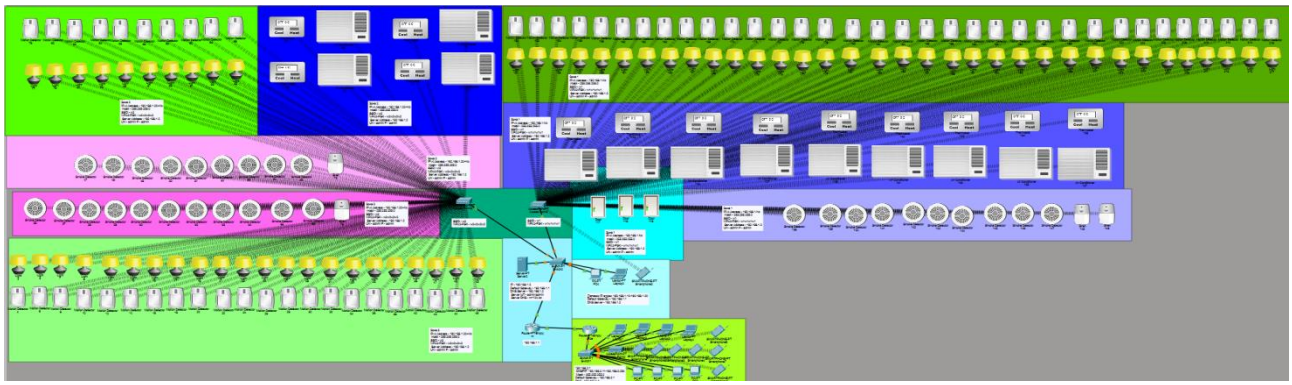

Рисунок 3.5 – Загальна топологія мережі

Як видно з рисунку 3.5, мережа складається з двох основних частин: серверної та персоналу. Кожен із сегментів виконує окремі функції, а їх взаємодія забезпечується через маршрутизатори, які здійснюють маршрутизацію трафіку між підмережами та організовують обмін даними.

3.4.2 Налаштування серверного сегменту

На наступному етапі налаштовано сервер, який виконує функції DNS та IoT-контролера, забезпечуючи централізоване управління пристроями та обробку запитів (рис. 3.6).

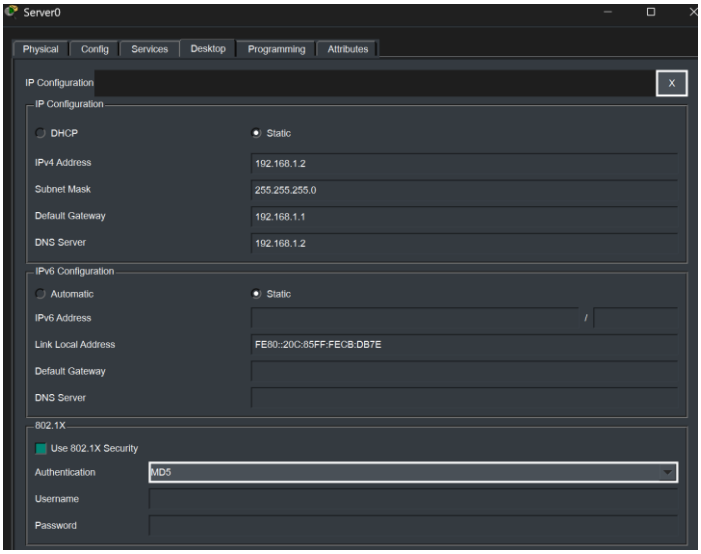

Рисунок 3.6 – Налаштування серверу

Як показано на рисунку 3.6, сервер має статичну IP-адресу 192.168.1.2, шлюз за замовчуванням 192.168.1.1 та DNS-адресу 192.168.1.2, що дозволяє йому одночасно виконувати роль DNS-сервера в межах локальної мережі супермаркету. Використання статичної IP-адреси є важливим для забезпечення стабільної роботи серверного обладнання, оскільки всі IoT-пристрої та мережеві вузли повинні мати постійний доступ до центрального сервера за незмінною адресою.

Шлюз за замовчуванням 192.168.1.1 забезпечує взаємодію сервера з іншими мережевими пристроями та дозволяє передавати дані між різними сегментами мережі. Налаштування DNS-адреси на значення 192.168.1.2 дає

змогу серверу виконувати функції локального DNS-сервера, забезпечуючи обробку доменних імен та спрощуючи процес звернення пристроїв до мережевих ресурсів. На рисунку 3.7 показано налаштування DNS-служби, де доменне ім’я m1124.iot спів ставлено з IP-адресою сервера. Це дозволяє клієнтам звертатися до сервера за зручним іменем замість числової адреси.

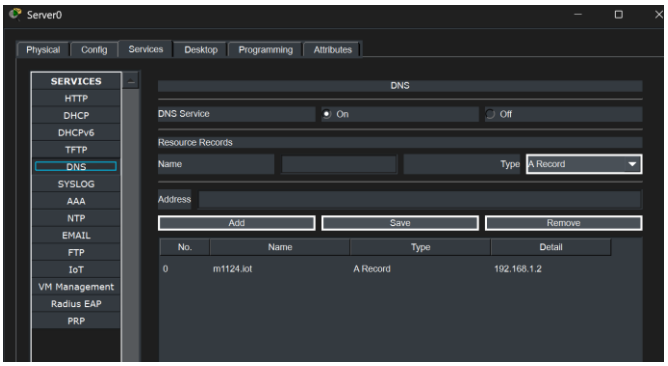

Рисунок 3.7 – Налаштування DNS-служби

У результаті проведеного тестування підтверджено правильну роботу DNS-служби та успішне перетворення доменного імені в IP-адресу. Це свідчить про коректне налаштування мережевих параметрів сервера та функціонування служби DNS у межах локальної IoT-інфраструктури супермаркету (рис. 3.8).

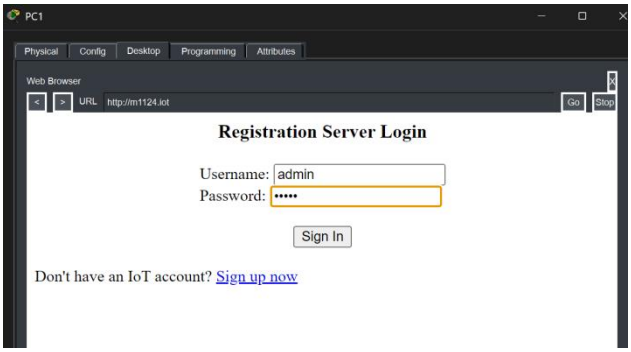

Рисунок 3.8 – Робота DNS-служби

3.4.3 Налаштування сегменту пристроїв для персоналу

Для забезпечення стабільної та безпечної роботи внутрішньої інфраструктури супермаркету реалізовано окремий сегмент мережі для

персоналу. До даного сегменту підключаються службові комп’ютери, ноутбуки працівників, касові термінали, мережеві принтери, сканери штрихкодів та інші пристрої, які використовуються співробітниками супермаркету під час виконання повсякденних робочих завдань. Виділення окремого мережевого сегменту дозволяє забезпечити більш ефективну організацію роботи всієї системи та підвищити рівень її надійності (рис. 3.9).

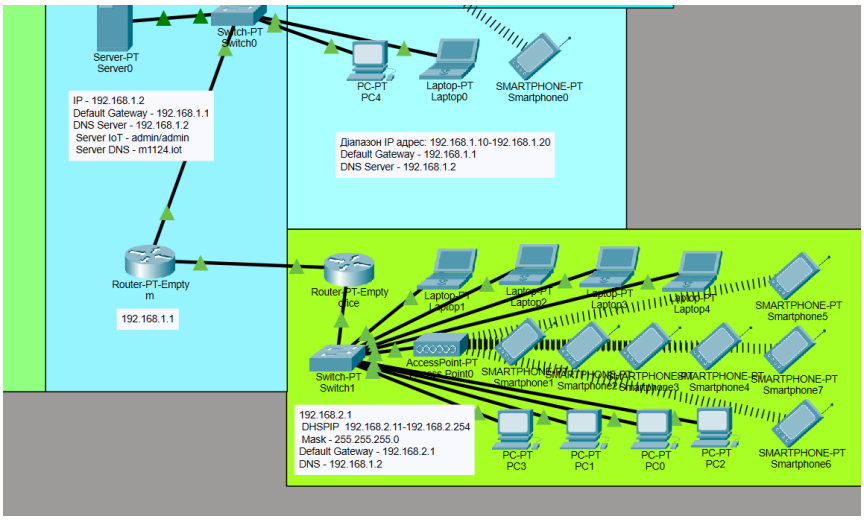

Рисунок 3.9 – Сегмент мережі для персоналу

Сегментація мережі є важливим етапом побудови сучасної комп’ютерної інфраструктури, оскільки вона дозволяє розподілити мережеві ресурси між різними категоріями пристроїв. Завдяки цьому зменшується навантаження на основну мережу IoT-пристроїв, покращується швидкодія системи та підвищується рівень інформаційної безпеки. Крім того, ізоляція службових пристроїв від інших сегментів мережі дозволяє запобігти несанкціонованому доступу до внутрішніх ресурсів супермаркету та конфіденційної інформації.

Для організації роботи сегменту персоналу використано окрему підмережу з власним діапазоном IP-адрес. Це забезпечує зручність адміністрування та дозволяє легко контролювати всі підключені пристрої. Також у мережі налаштовано DHCP-сервер, який автоматично виконує розподіл мережевих параметрів між клієнтськими пристроями. Використання

динамічної адресації значно спрощує процес підключення нового обладнання до мережі та мінімізує ризик виникнення конфліктів IP-адрес.

У середовищі Cisco Packet Tracer до мережі персоналу підключено комутатори доступу, через які здійснюється з'єднання робочих станцій із центральним маршрутизатором. Комутатори забезпечують передачу даних між пристроями локальної мережі та дозволяють організувати стабільну комунікацію між усіма елементами системи. На маршрутизаторі налаштовано відповідний інтерфейс шлюзу за замовчуванням, який забезпечує взаємодію між сегментами мережі, а також доступ до серверного обладнання та мережевих сервісів.

Для автоматичного призначення мережевих параметрів використано DHCP-сервіс. Після підключення до мережі кожен пристрій персоналу автоматично отримує IP-адресу, маску підмережі, адресу шлюзу за замовчуванням та DNS-сервера. Такий підхід значно полегшує адміністрування мережі, скорочує час налаштування обладнання та дозволяє уникнути помилок, пов'язаних із ручним введенням параметрів мережі. Крім цього, централізоване керування адресним простором забезпечує більш ефективний контроль за використанням мережевих ресурсів (рис. 3.10).

```
Router#show running-config | include dhcp
ip dhcp excluded-address 192.168.2.1 192.168.2.10
ip dhcp pool LAN
Router#show ip dhcp pool

Pool LAN :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 1
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.2.1          192.168.2.1      - 192.168.2.254     2    / 1     / 254
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.2.11     0060.3E1B.2D2C           --                     Automatic
192.168.2.12     0001.969E.3120           --                     Automatic
```

Рисунок 3.10 – Налаштування DHCP

Додатково реалізовано бездротовий доступ для мобільних пристроїв персоналу за допомогою Wi-Fi точок доступу. Це дозволяє працівникам використовувати планшети, смартфони або ноутбуки для виконання службових

завдань без необхідності підключення через кабельну мережу. Для захисту бездротового сегменту використано механізм автентифікації WPA2-PSK із встановленим паролем доступу. Такий метод захисту забезпечує базовий рівень безпеки бездротової мережі, обмежує підключення сторонніх користувачів та сприяє захисту службової інформації від несанкціонованого доступу (рис. 3.11).

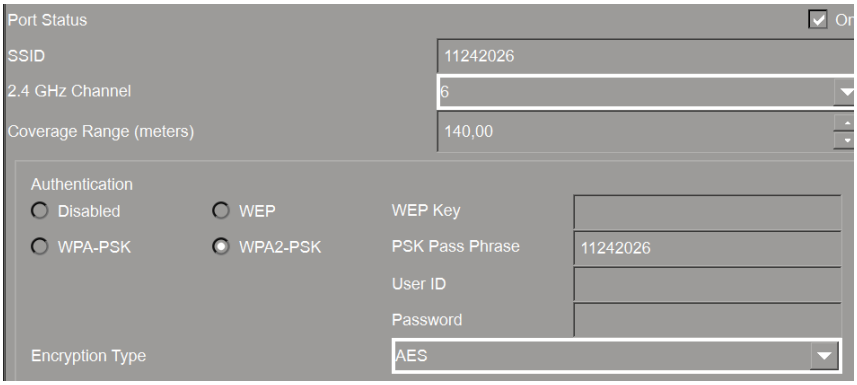

Рисунок 3.11 – Бездротовий доступ для робочих мобільних пристроїв

У процесі моделювання мережевої інфраструктури проведено перевірку працездатності всіх компонентів сегменту персоналу. Зокрема, перевірено коректність автоматичного отримання IP-адрес, доступність мережевих сервісів, роботу DHCP-сервера, а також можливість обміну даними між пристроями персоналу та сервером системи. Для тестування мережевого з'єднання використовувались стандартні мережеві утиліти, зокрема команди ping та перевірка доступу до мережевих ресурсів (рис. 3.12).

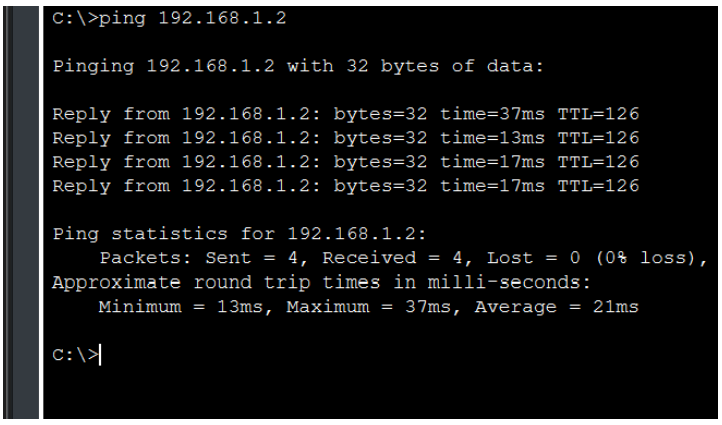

Рисунок 3.12 – Тестування мережевого з'єднання

Отримані результати підтвердили правильність виконаних налаштувань та стабільну роботу створеного сегменту мережі. Усі пристрої успішно отримували мережеві параметри, мали доступ до необхідних ресурсів і могли взаємодіяти між собою без помилок та затримок. Реалізований сегмент мережі персоналу забезпечує ефективну організацію роботи співробітників супермаркету та створює надійну основу для подальшого розширення мережевої інфраструктури.

3.4.4 Налаштування бездротової мережі

У мережі реалізовано бездротовий доступ за допомогою точок доступу, що забезпечують підключення IoT-пристроїв (рис. 3.13-3.14).

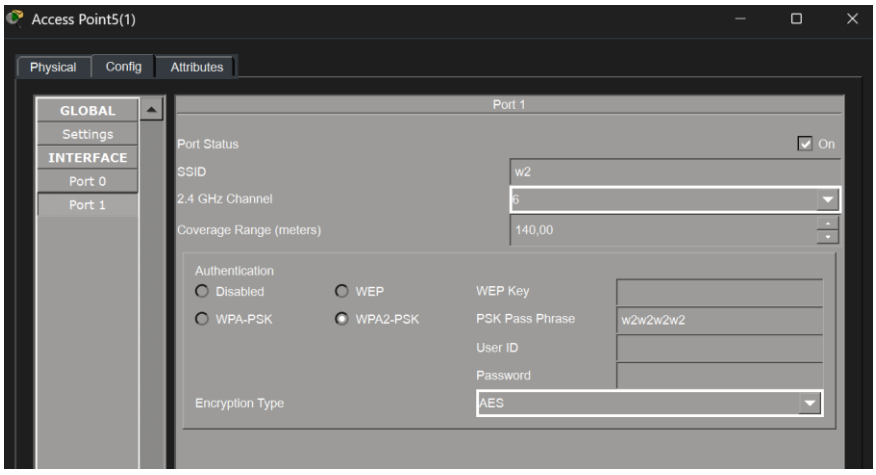

Рисунок 3.13 – Налаштування бездротової мережі

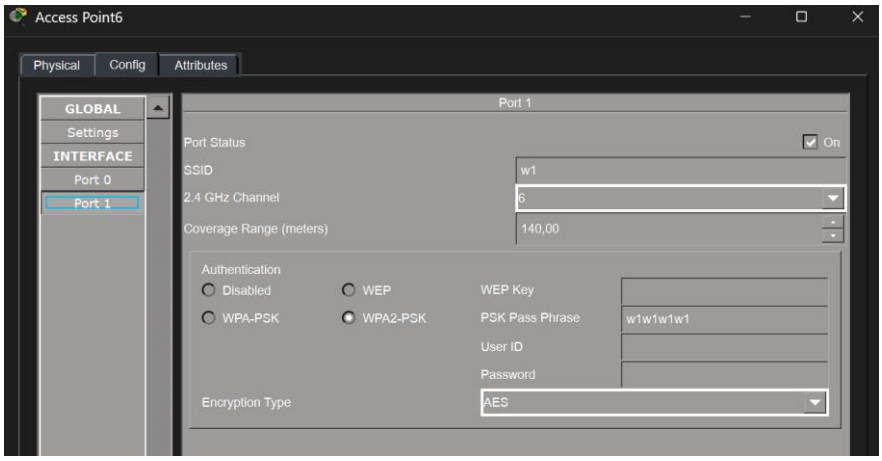

Рисунок 3.14 – Налаштування бездротової мережі

Як показано на рисунку 3.13 та 3.14, створено дві бездротові мережі (SSID) із використанням захисту WPA2-PSK, що дозволяє розмежувати доступ між різними групами IoT-пристроїв та забезпечити підвищений рівень безпеки мережевої інфраструктури. Використання окремих бездротових мереж дає змогу ефективніше організувати підключення пристроїв відповідно до зон їх розташування та зменшити навантаження на окремі точки доступу.

Технологія WPA2-PSK забезпечує захист передаваних даних шляхом використання шифрування та автентифікації пристроїв за допомогою пароля доступу. Це дозволяє запобігти несанкціонованому підключенню сторонніх користувачів до мережі та підвищує надійність функціонування IoT-системи. Крім того, використання захищених бездротових мереж є важливою складовою забезпечення стабільної роботи датчиків, виконавчих механізмів та серверного обладнання в умовах постійного обміну даними.

Створені SSID налаштовані відповідно до структури супермаркету та зон розміщення IoT-пристроїв. Після завершення налаштування точки доступу забезпечили стабільне підключення сенсорів і коректний обмін інформацією із центральним сервером системи керування.

Для забезпечення стабільного та безперебійного бездротового з’єднання IoT-пристроїв у межах супермаркету використано дві точки доступу Wi-Fi. Використання декількох точок доступу дало змогу рівномірно розподілити навантаження між мережевими вузлами, підвищити якість покриття бездротового сигналу та забезпечити надійний зв’язок між IoT-пристроями і центральним сервером системи керування. Такий підхід є особливо важливим для середовищ із великою кількістю підключених пристроїв, оскільки дозволяє уникнути перевантаження мережі та зменшити ризик втрати даних під час їх передавання.

IoT-пристрої, розташовані у зоні 1, підключені до першої точки доступу. До цієї групи входять датчики руху, освітлення, а також інші сенсори, встановлені у відповідній частині приміщення супермаркету. Розміщення окремої точки доступу для цієї зони дозволило забезпечити стабільний рівень

сигналу, знизити вплив перешкод та мінімізувати можливі затримки під час передавання інформації до сервера. Крім того, таке рішення позитивно впливає на швидкість реагування систем автоматизації, зокрема систем освітлення та контролю безпеки (рис. 3.15).

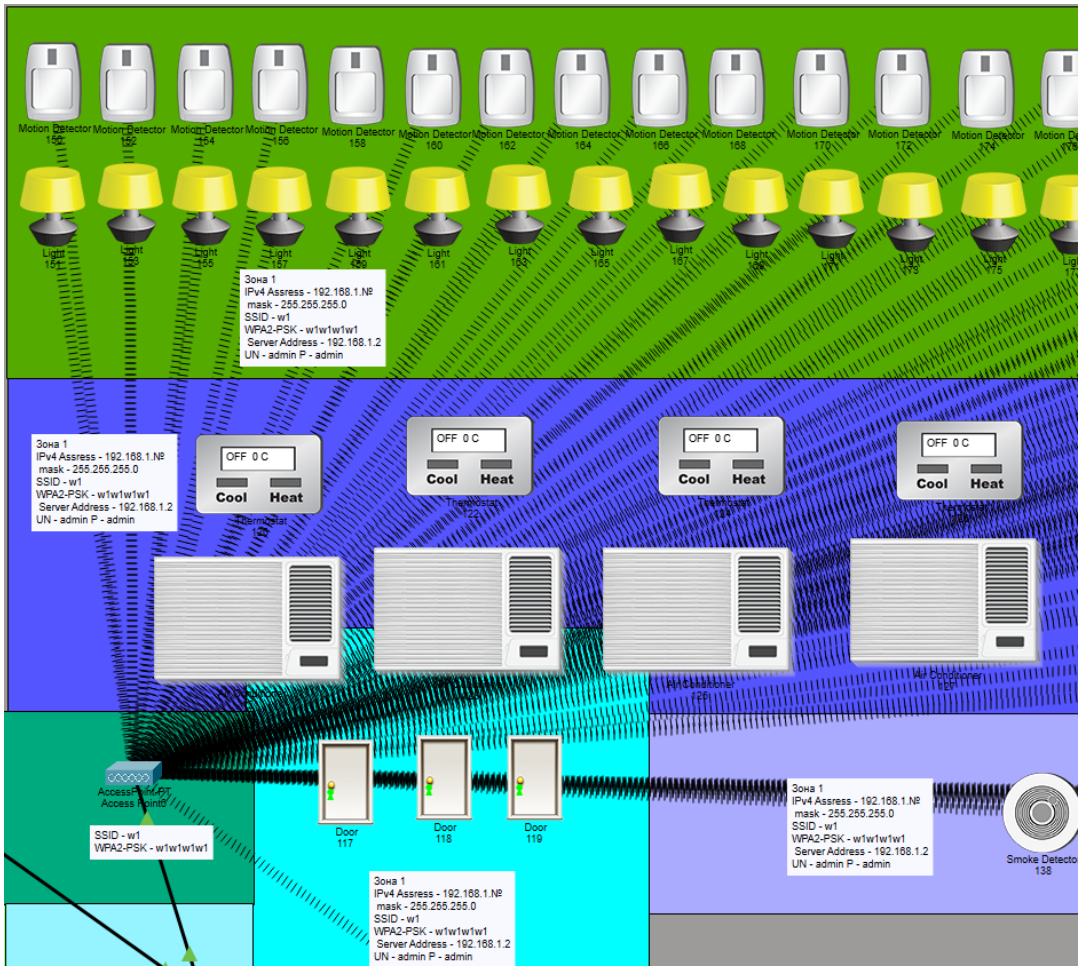

Рисунок 3.15 – IoT-пристрої, розташовані у зоні 1

IoT-пристрої, що знаходяться у зонах 2 та 3, підключені до другої точки доступу. До цієї частини мережі входять датчики температури, диму, дверей, сигналізації та інші пристрої моніторингу, необхідні для забезпечення належного функціонування супермаркету. Об’єднання цих зон в межах однієї точки доступу дозволяє ефективніше використовувати ресурси мережі, спрощує процес адміністрування та забезпечує стабільну взаємодію між усіма компонентами IoT-інфраструктури. Незважаючи на підключення до різних точок доступу, усі пристрої працюють в одній локальній мережі, що забезпечує

централізований обмін даними та можливість єдиного керування всією системою (рис. 3.16).

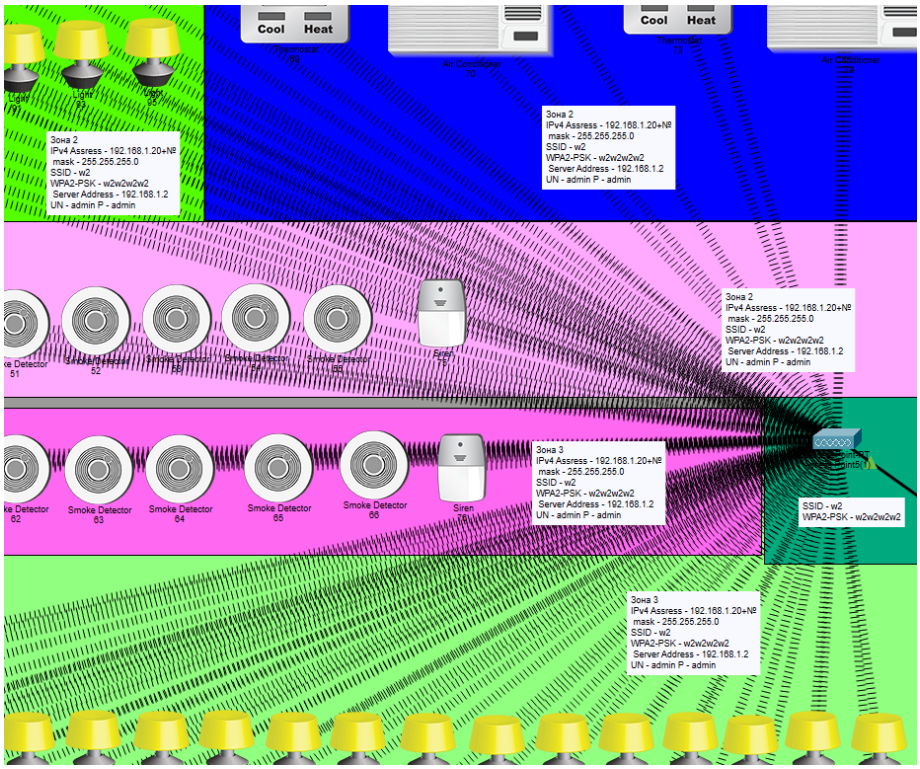

Рисунок 3.16 – IoT-пристрої, що знаходяться у зонах 2 та 3

Під час налаштування бездротової мережі для обох точок доступу задані основні параметри мережі, зокрема SSID, типи шифрування та паролі доступу. Після завершення налаштування усі IoT-пристрої підключені до відповідних бездротових мереж та протестовані на коректність обміну даними із сервером (рис. 3.17).

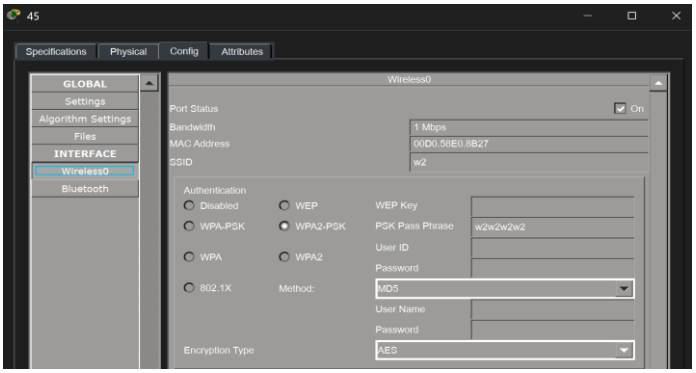

Рисунок 3.17 – Підключення IoT-пристроїв до бездротових мереж

На рисунку 3.17 показано налаштування підключення IoT-пристрою до бездротової мережі. У процесі конфігурації вибрано відповідну бездротову мережу, вказано параметри підключення та введено пароль доступу, необхідний для автентифікації пристрою в мережі. Після успішного підключення IoT-пристрій отримує можливість передавати дані до центрального сервера та взаємодіяти з іншими компонентами системи.

Для взаємодії пристроїв із сервером на IoT Server попередньо активовано службу реєстрації IoT-пристроїв та створено облікові дані для авторизації. Після цього на кожному датчику виконувалося налаштування параметрів підключення, зокрема IP-адреси сервера, логіна та пароля доступу. Після успішної авторизації пристрої автоматично реєструвалися на сервері та відображалися у списку підключених IoT-пристроїв (рис. 3.18).

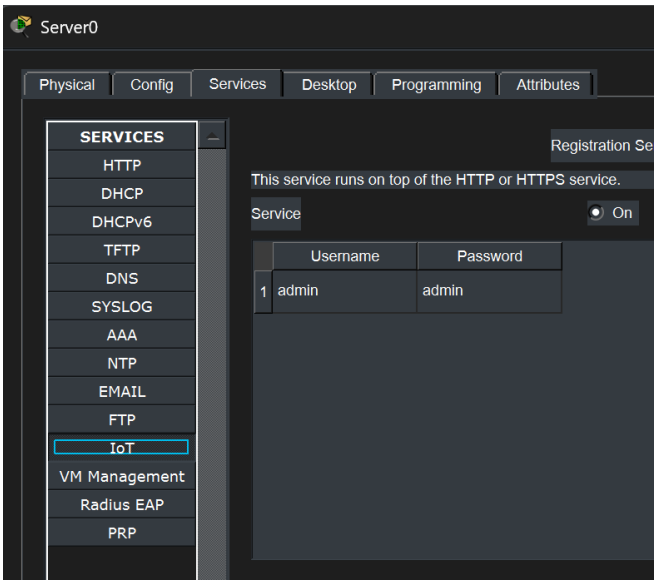

Рисунок 3.18 – Активовано службу реєстрації IoT-пристроїв

У межах реалізованого проєкту до IoT-сервера підключені датчики руху, температури, освітлення, диму та дверні сенсори, розміщені у відповідних функціональних зонах супермаркету. Кожен із датчиків виконує окрему функцію моніторингу навколишнього середовища та передає отримані дані до сервера в режимі реального часу. Наприклад, датчики руху використовуються для автоматичного керування освітленням, температурні сенсори для контролю

кліматичних умов у приміщеннях і морозильних камерах, а датчики диму та дверні сенсори для підвищення рівня безпеки об’єкта (рис. 3.19).

Рисунок 3.19 – Підключення IoT-пристроїв до IoT-сервера

Передавання даних у режимі реального часу забезпечує можливість постійного централізованого моніторингу стану всієї системи та оперативного реагування на зміну параметрів середовища. У разі виникнення нестандартних ситуацій сервер може автоматично надсилати команди виконавчим пристроям, наприклад активувати сигналізацію, увімкнути освітлення або змінити режим роботи систем кондиціонування. Завдяки цьому IoT-інфраструктура забезпечує автоматизацію основних процесів супермаркету, підвищує ефективність роботи обладнання та покращує рівень безпеки приміщення.

3.4.5 Налаштування IoT-пристроїв

Додано IoT-пристрої, зокрема датчики температури, диму та освітлення, які використовуються для моніторингу стану середовища (рис. 3.20).

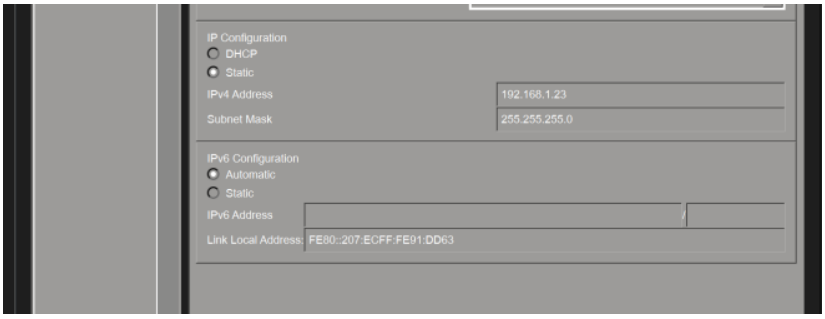

Рисунок 3.20 – Налаштування IoT-пристроїв

Як видно з рисунку 3.20, IoT-пристрої підключені до комутатора серверного сегмента та використовують статичні IP-адреси в діапазоні від 192.168.1.20 до 192.168.1.254. Це забезпечує стабільність зв’язку та спрощує керування пристроями.

На рисунку 3.21 продемонстровано доступ до веб-інтерфейсу сервера, що свідчить про повноцінне функціонування мережевих сервісів та готовність системи до експлуатації.

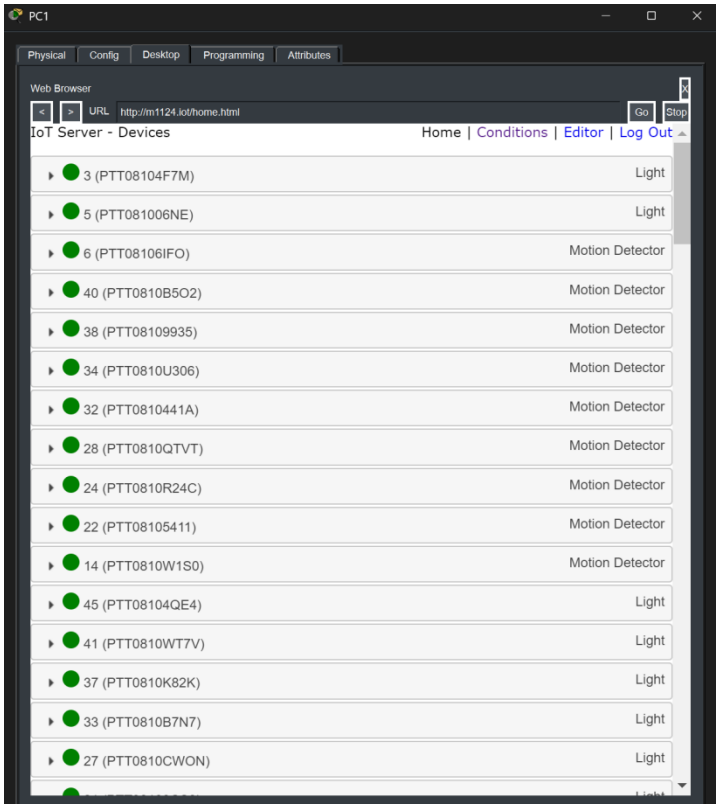

Рисунок 3.21 – Веб-інтерфейс сервера

3.4.6 Параметри налаштування роботи IoT-датчиків

У межах розробленої IoT-інфраструктури реалізовано систему взаємодії датчиків і виконавчих пристроїв на основі подієво-орієнтованих сценаріїв автоматизації. Такий підхід забезпечує автоматичне реагування системи на зміни параметрів навколишнього середовища без необхідності постійного втручання персоналу. Кожен IoT-датчик у системі не лише виконує функцію моніторингу, але й бере участь у формуванні логічних сценаріїв керування

відповідними виконавчими пристроями. Це дозволяє підвищити ефективність роботи інфраструктури, оптимізувати енергоспоживання та забезпечити стабільне функціонування всіх підсистем супермаркету (рис. 3.22).

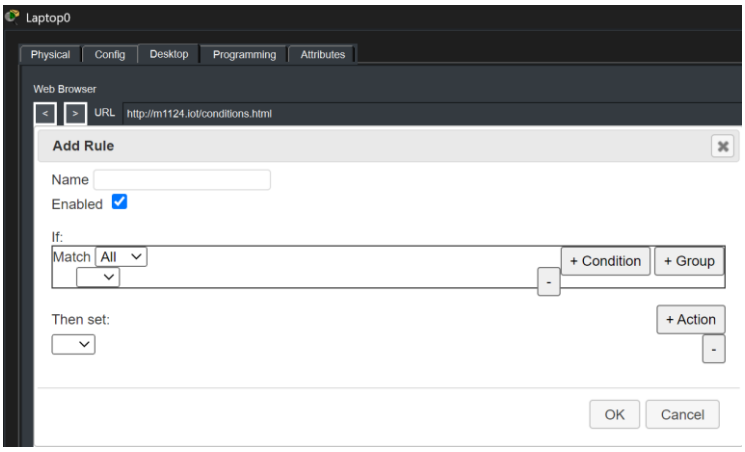

Рисунок 3.22 – Налаштування роботи датчиків

Одним із основних сценаріїв є взаємодія датчика руху та системи освітлення. У разі виявлення руху в певній зоні торгового залу датчик надсилає сигнал до системи керування, після чого автоматично активуються освітлювальні прилади. Додатково в роботу включається датчик освітленості, який аналізує рівень природного освітлення у приміщенні. Якщо рівень світла є недостатнім, система вмикає освітлення на необхідному рівні яскравості. У випадку достатнього природного освітлення інтенсивність штучного освітлення може бути зменшена або освітлення взагалі не активується. Такий механізм дозволяє суттєво оптимізувати енергоспоживання та підвищити ефективність використання електроенергії (рис. 3.23).

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	z3s1p1	4 On is true	Set 3 Status to On
Edit Remove	Yes	z3s1p2	4 On is false	Set 3 Status to Off
Edit Remove	Yes	z3s2p1	6 On is true	Set 5 Status to On
Edit Remove	Yes	z3s2p2	6 On is false	Set 5 Status to Off

Рисунок 3.23 – Налаштування сценаріїв роботи датчиків руху

Для підвищення рівня безпеки в супермаркеті реалізовано автоматизовану систему пожежного реагування. У випадку спрацювання любого датчика диму або виявлення підвищеної концентрації газів система миттєво активує всі сирени та звукові оповіщувачі незалежно від їхнього розташування. Одночасно інформація про аварійну ситуацію передається на центральний IoT-сервер, що дозволяє здійснювати централізований моніторинг стану системи та оперативно реагувати на надзвичайні ситуації. Такий принцип організації забезпечує швидке інформування персоналу та відвідувачів про можливу небезпеку і підвищує загальний рівень пожежної безпеки об’єкта (рис. 3.24).

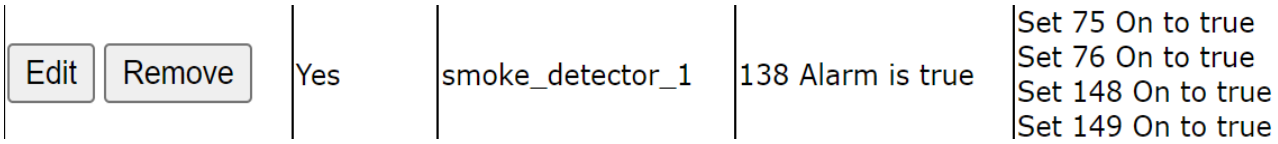

Рисунок 3.24 – Налаштування сценаріїв роботи датчиків диму

Окремий блок автоматизації реалізовано для холодильного обладнання та систем контролю температури. У межах цього сценарію використовується взаємодія термостата та охолоджувальної системи, роль якої виконує кондиціонер або холодильний компресор. Температурні датчики постійно здійснюють моніторинг умов зберігання продукції та порівнюють поточні значення з установленими нормативними параметрами. У разі перевищення допустимого температурного порогу система автоматично активує охолодження, забезпечуючи підтримання стабільного мікроклімату у холодильних приміщеннях.

Для різних категорій продукції встановлено окремі температурні діапазони зберігання. Для охолоджених продуктів, зокрема молочних виробів, м’яса та риби, підтримується температура в межах від +2° С до +6° С. Для замороженої продукції встановлено температурний режим від -18° С до -12° С, що забезпечує належні умови тривалого зберігання. Овочі та фрукти

короткотривалого зберігання утримуються при температурі від +4° С до +10° С, а готова кулінарна продукція у межах від +2° С до +5° С (рис. 3.25).

Edit	Remove	Yes	term_1	126 Temperature > 6.0 °C	Set 127 On to true
Edit	Remove	Yes	term_1(1)	126 Temperature < 2.0 °C	Set 127 On to false
Edit	Remove	Yes	term_2	120 Temperature > 10.0 °C	Set 121 On to true
Edit	Remove	Yes	term_2(1)	120 Temperature < 4.0 °C	Set 121 On to false
Edit	Remove	Yes	term_3	124 Temperature > -12.0 °C	Set 125 On to true
Edit	Remove	Yes	term_3(1)	124 Temperature < -18.0 °C	Set 125 On to false

Рисунок 3.25 – Налаштування сценаріїв роботи датчиків температури

У разі відхилення температури від заданих меж термостат автоматично передає сигнал на виконавчий пристрій, який активує систему охолодження. Після досягнення необхідного температурного режиму система переходить у режим підтримки стабільних параметрів. Такий підхід дозволяє автоматизувати контроль кліматичних умов, забезпечити відповідність умов зберігання продукції санітарним нормам та мінімізувати ризик псування товарів.

3.5 Результати тестування системи

У ході тестування розробленої IoT-інфраструктури супермаркету виконано комплексну перевірку коректності взаємодії всіх компонентів системи, зокрема IoT-датчиків, серверного обладнання, бездротової мережі та виконавчих пристроїв. Основна увага приділялася швидкості реагування системи на події, стабільності передавання даних та правильності виконання реалізованих сценаріїв автоматизації в різних умовах роботи.

Під час моделювання роботи торгового приміщення встановлено, що датчики руху коректно виявляють присутність людей у відповідних зонах та автоматично ініціюють активацію систем освітлення. Одночасно система враховує показники датчиків освітленості, що дозволяє адаптувати роботу освітлювальних приладів залежно від рівня природного освітлення. Отримані

результати підтверджують правильність реалізації сценарію енергозбереження та ефективність автоматизованого керування освітленням (рис. 3.26).

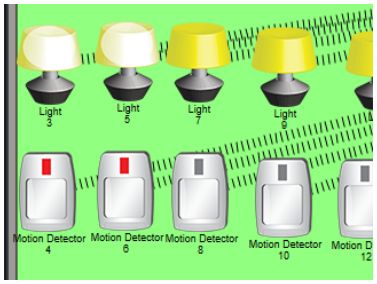

Рисунок 3.26 – Демонстрація роботи датчиків руху

Окремо протестовано роботу системи пожежної безпеки. Під час спрацювання датчиків диму система автоматично активувала всі підключені сирени та засоби оповіщення незалежно від їхнього розташування в межах супермаркету. Інформація про подію миттєво передавалася на IoT-сервер, що забезпечувало централізовану реакцію на потенційно небезпечні ситуації та можливість оперативного інформування персоналу про виникнення загрози (рис. 3.27).

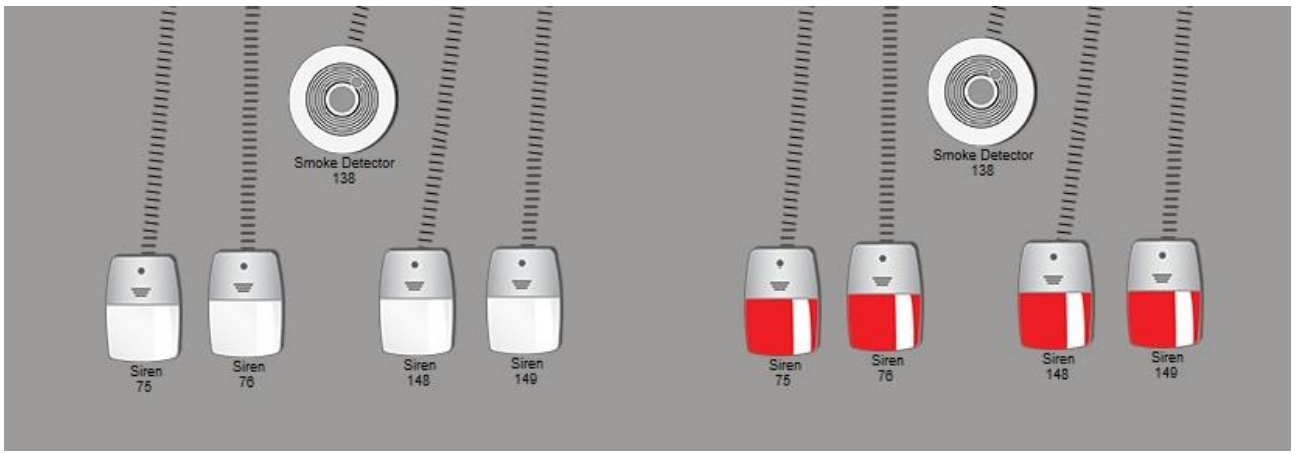

Рисунок 3.27 – Демонстрація роботи датчиків диму

Також перевірено функціонування температурних датчиків у холодильних і морозильних зонах. У процесі тестування підтверджено, що показники температури безперервно передаються в режимі реального часу до

керуючого сервера, який аналізує отримані дані та автоматично взаємодіє з кондиціонерами й холодильними установками для підтримання необхідного температурного режиму. У разі відхилення температурних показників від установлених меж система своєчасно активує охолоджувальне обладнання та стабілізує умови зберігання продукції (рис. 3.28).

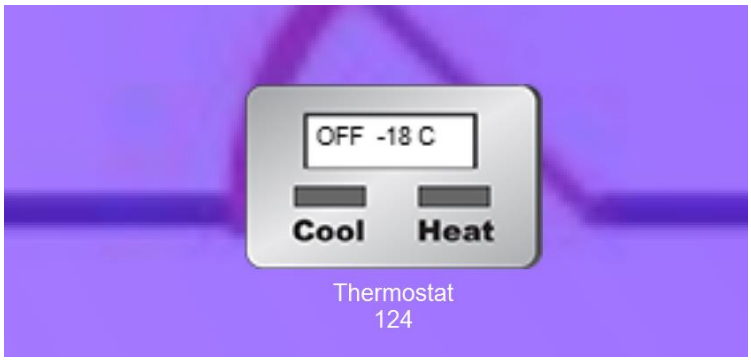

Рисунок 3.28 – Демонстрація роботи датчиків температури

Результати тестування підтвердили стабільність роботи мережевої інфраструктури, коректність взаємодії між IoT-пристроями та сервером, а також ефективність реалізованих механізмів автоматизації. Реалізована система забезпечує безперервний моніторинг стану супермаркету, оптимізацію використання ресурсів і підвищення рівня безпеки об’єкта.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи досягнуто поставленої мети, що полягала у проєктуванні та моделюванні IoT-інфраструктури супермаркету з використанням сучасних програмних засобів.

Проведено аналіз предметної області Інтернету речей. Розглянуто основні принципи побудови IoT-систем, їх архітектуру, складові елементи та сфери застосування. Проаналізовано існуючі рішення у сфері автоматизації комерційних об’єктів, що дозволило обґрунтувати актуальність впровадження IoT-технологій у супермаркетах

Здійснено вибір та обґрунтування засобів розробки. Для створення цифрової моделі супермаркету використано середовище AutoCAD, що забезпечило точне відтворення плану приміщення. Моделювання мережевої інфраструктури реалізовано в Cisco Packet Tracer, який дозволив створити віртуальну IoT-систему та дослідити її роботу в умовах, наближених до реальних

Виконано практичну реалізацію проєкту. Побудовано цифрову модель супермаркету з урахуванням функціонального зонування, реалізовано фізичний та мережевий рівні системи, інтегровано IoT-пристрої, зокрема датчики руху, освітленості, температури та диму. Налаштовано взаємодію між пристроями, реалізовано автоматизовані сценарії керування освітленням, кліматом і системами безпеки. Проведено тестування роботи системи, що підтвердило її працездатність та ефективність.

У результаті виконання кваліфікаційної роботи проаналізовано сучасні IoT-технології та підходи до автоматизації комерційних об’єктів. Розроблено IoT-інфраструктуру супермаркету на основі датчиків і мережевих пристроїв, спроєктовано цифрову модель об’єкта та реалізовано мережеву модель у середовищі Cisco Packet Tracer. Проведено тестування системи.

Отримані результати підтверджують, що впровадження в супермаркеті IoT-інфраструктури дозволяє підвищити рівень автоматизації, забезпечити

ефективне використання ресурсів, покращити безпеку та створити комфортні умови для відвідувачів і персоналу.

Перспективами подальших досліджень є розширення функціональних можливостей системи, інтеграція з хмарними сервісами, впровадження аналітики на основі штучного інтелекту та реалізація повноцінної фізичної системи на базі реального обладнання.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз продуктивності безпечних протоколів Інтернету речей для зв’язку в мікромережах у режимі реального часу URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X20305707 (дата звернення: 12.02.2026).

2. Вісник Університету «Україна» Серія Інформатика, обчислювальна техніка та кібернетика. URL: https://visn-it.uu.edu.ua/old_site/files/2020/17.pdf (дата звернення: 12.02.2026).

3. Інтернет - Інтернет речей та смарт технології. URL: https://surl.li/loafrl (дата звернення: 12.02.2026).

4. Інтернет речей: нові виклики для інформаційної безпеки URL: https://surli.cc/glupmu (дата звернення: 12.02.2026).

5. Інтернет речей: перспективи розвитку та можливості використання URL: https://duikt.edu.ua/ua/news-1-570-11324-internet-rechey-perspektivi-rozvitku-ta-mozhlivosti-vikoristannya_kafedra-informaciynih-sistem-ta-tehnologiy (дата звернення: 13.02.2026).

6. Ітернет речей як складова індустрії 4.0: проектний підхід URL: https://www.researchgate.net/publication/350662788_INTERNET_RECEJ_AK_SKLADOVA_INDUSTRII_40_PROEKTNIJ_PIDHID (дата звернення: 13.02.2026).

7. Комп’ютерна графіка AutoCad навчальний посібник URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi83/0063446.pdf (дата звернення: 18.03.2026).

8. Лекція 1. Основи Інтернету Речей. Школа автоматики. URL: http://edu.asu.in.ua/mod/book/tool/print/index.php?id=112 (дата звернення: 14.02.2026).

9. Огляд протоколів Інтернету речей та проблем їхньої безпеки крізь призму загального стеку Інтернету речей URL: https://www.sciencedirect.com/science/article/abs/pii/S2542660520300986 (дата звернення: 11.03.2026).

10. Повний посібник з датчиків Інтернету речей URL: https://halodetect.com/uk/blog/iot-sensors/ (дата звернення: 12.03.2026).

11. Проблеми безпеки інтернету речей URL: https://surl.li/ddohbl (дата звернення: 12.05.2026).

12. Революція IoT: як технології трансформують сучасний бізнес - IAMPM. IAMPM - IAMPM - курси для нетехнічних спеціальностей в IT. URL: https://iampm.club/ua/revolyucziya-iot-yak-tehnologiyi-transformuyut-suchasnij-biznes/ (дата звернення: 21.02.2026).

13. Система AutoCad. Основні принципи роботи AutoCad. Креслення простих геометричних елементів. URL: https://surl.li/bjwzkk (дата звернення: 18.03.2026).

14. Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу україни і світу URL: https://duikt.edu.ua/uploads/p_2626_35882840.pdf (дата звернення: 21.02.2026).

15. Що таке Internet of Things (IoT)? - STUD-POINT. STUD-POINT. URL: https://stud-point.com/blog/it_life/shcho-take-internet-of-things-iot/ (дата звернення: 12.02.2026).

16. DSpace ПВНЗ "МЕГУ імені академіка Степана Дем'янчука": Технології інтернет речей Apache Tomcat/9.0.65. URL: http://library.megu.edu.ua:8180/jspui/handle/123456789/4212 (дата звернення: 21.02.2026).

17. Internet of Things: A General Overview between Architectures, Protocols and Applications. MDPI. URL: https://www.mdpi.com/2078-2489/12/2/8 (date of access: 18.02.2026).

18. IT-Enterprise. Internet of Things, IoT. IT-Enterprise - цифрова трансформація бізнес-процесів, ERP| it.ua. URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot (date of access: 18.02.2026).