

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп'ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА
на тему
АВТОМАТИЗАЦІЯ СЦЕНАРІЇВ РОБОТИ ЧЕРЕЗ PACKET TRACER
IOT

Виконав: студент групи 1К-22
спеціальності
123 Комп'ютерна інженерія
Олександр ІЛЬСНКО
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп'ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____ Наталя ФАЛЬЧЕНКО
(підпис)

«_____» _____ 2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Ільєнку Олександрю Миколайовичу

1. Тема кваліфікаційної роботи: «Автоматизація сценаріїв роботи через Packet Tracer IoT»

Керівник роботи Медолиз Маргарита Миколаївна, викладач вищої категорії затверджені наказом закладу передвищої освіти від 06.10. 2025 року № 84/1 у.

2. Строк подання студентом кваліфікаційної роботи 08.06.2026 _____.

3. Вихідні дані до кваліфікаційної Технічна документація та інвентарні дані об'єкта, характеристики інформаційних систем, програмні засоби для збереження даних засіб мережевого моделювання Cisco packet tracer _____.

4. Зміст кваліфікаційної роботи: Теоретичні основи систем розумного будинку IoT, моделювання системи розумного будинку в Cisco packet tracer, тестування та аналіз ефективності розробленого рішення _____

Дата видачі завдання 15.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Теоретичні основи систем розумного будинку та IoT	09.12.2025	
3	Розділ 2 Моделювання системи розумного будинку	10.03.2026	
4	Розділ 3 Тестування та аналіз роботи системи	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2026	

Студент _____ Олександр ІЛЬЄНКО
(підпис)

Керівник роботи _____ Маргарита МЕДОЛИЗ
(підпис)

АНОТАЦІЯ

У кваліфікаційній роботі досліджено можливості автоматизації сценаріїв роботи пристроїв Інтернету речей (IoT) у середовищі Cisco Packet Tracer. Проведено аналіз принципів функціонування технології IoT, концепції розумного будинку та сучасних засобів моделювання IoT-систем. Розроблено модель децентралізованої системи «Розумний будинок», що включає підсистеми безпеки, клімат-контролю та енергоефективності. Реалізовано алгоритми автоматизованого керування пристроями на основі заданих умов і подій. Виконано тестування створеної моделі та оцінено ефективність її функціонування. Практичне значення роботи полягає у можливості проєктування, налагодження та перевірки IoT-рішень без використання реального обладнання, що сприяє зменшенню витрат і підвищенню якості розробки систем автоматизації.

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, ІОТ, CISCO PACKET TRACER, РОЗУМНИЙ БУДИНОК, АВТОМАТИЗАЦІЯ, МЕРЕЖЕВЕ МОДЕЛЮВАННЯ, ДАТЧИКИ, СЦЕНАРІЇ КЕРУВАННЯ, БЕЗДРОТОВІ МЕРЕЖІ.

ABSTRACT

The qualification work explores the possibilities of automating scenarios for Internet of Things (IoT) devices in the Cisco Packet Tracer environment. The principles of IoT technology, the concept of a smart home, and modern tools for modeling IoT systems are analyzed. A model of a decentralized system "Smart Home" is developed, which includes climate control and energy efficiency subsystems. Algorithms for automated device control based on given conditions and events are implemented. The created model is tested and its effectiveness is assessed. The practical significance of the work lies in the possibility of designing, debugging, and testing IoT solutions without using real equipment, which helps reduce costs and improve the quality of automation system development.

Keywords: INTERNET OF THINGS, IOT, CISCO PACKET TRACER, SMART HOME, AUTOMATION, NETWORK MODELING, SENSORS, CONTROL SCENARIOS, WIRELESS NETWORKS.

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1.	5
ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ РОЗУМНОГО БУДИНКУ ТА IoT.....	5
1.1 Поняття та сутність технології Інтернету речей	5
1.2 Концепція розумного будинку	6
1.3 Архітектура IoT-систем	7
1.4 Аналіз існуючих рішень та їх порівняння.....	9
1.5 Переваги та недоліки використання IoT у системах розумного будинк	11
РОЗДІЛ 2 МОДЕЛЮВАННЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ	13
2.1 Огляд середовищ моделювання IoT.....	13
2.2 Моделювання структури системи	16
2.3 Налаштування компонентів системи	20
2.4 Реалізація алгоритмів та сценаріїв роботи	23
РОЗДІЛ 3 ТЕСТУВАННЯ ТА АНАЛІЗ РОБОТИ СИСТЕМИ.....	27
3.1 Умови та методика тестування.....	27
3.2 Результати тестування	29
3.3 Аналіз ефективності системи.....	32
ВИСНОВКИ.....	34
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	36
ДОДАТКИ.....	36

ВСТУП

У сучасних умовах інтенсивного розвитку інформаційних технологій впровадження автоматизованих систем набуває особливого значення для повсякденного життя людини. Одним із найперспективніших напрямів у цьому контексті є використання технології Інтернету речей (IoT), яка забезпечує взаємодію між різноманітними пристроями через мережу та сприяє автоматизації процесів управління. Застосування IoT технологій у системах «розумного будинку» є надзвичайно актуальним, оскільки воно сприяє підвищенню рівня комфорту, безпеки та енергоефективності в сучасних оселях.

Об'єкт дослідження – процес функціонування та взаємодії пристроїв Інтернету речей (IoT) у мережевому середовищі.

Предмет дослідження – методи, засоби та механізми автоматизації сценаріїв роботи IoT-пристроїв із використанням програмного середовища Cisco Packet Tracer, а також принципи налаштування логічних зв'язків між датчиками, виконавчими пристроями та сервісами керування.

Метою цієї кваліфікаційної роботи є проведення дослідження, розробка та моделювання системи «розумного будинку» на основі технології Інтернету речей у середовищі програмного забезпечення Cisco Packet Tracer. Для досягнення поставленої мети необхідно вирішити низку конкретних завдань, зокрема:

1. Провести аналіз основних понять і принципів функціонування технології Інтернету речей.
2. Дослідити концепцію розумного будинку та визначити ключові аспекти його функціонування.
3. Виконати огляд існуючих рішень і середовищ моделювання для розробки IoT-систем.
4. Обґрунтувати вибір середовища Cisco Packet Tracer як інструменту для моделювання.
6. Реалізувати сценарії автоматизації процесів у межах створеної системи.

7. Здійснити тестування розробленої моделі та оцінити її ефективність з точки зору заданих критеріїв.

Практичне значення роботи полягає у розробленні та моделюванні автоматизованих сценаріїв функціонування IoT-пристроїв, які дозволяють реалізувати інтелектуальне керування об'єктами без необхідності використання реального обладнання. Отримані результати можуть бути використані під час проєктування систем «розумного будинку», автоматизації освітлення, контролю доступу, моніторингу параметрів навколишнього середовища та інших IoT-рішень. Створені моделі дають змогу оцінити ефективність роботи автоматизованих систем, перевірити коректність взаємодії пристроїв і відпрацювати алгоритми керування ще на етапі проєктування, що зменшує витрати на впровадження реальних систем та підвищує якість їхньої розробки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ РОЗУМНОГО БУДИНКУ ТА IoT

1.1 Поняття та сутність технології Інтернету речей

Інтернет речей є одним із ключових напрямів сучасних інформаційних технологій, що спрямований на з'єднання фізичних пристроїв у єдину мережу для збору, передачі та аналізу даних. Головна концепція IoT полягає у забезпеченні комунікації між об'єктами реального світу без постійної участі людини, що відкриває можливості для автоматизації численних процесів у різних сферах життя. Технології IoT спираються на використання широкого спектру пристроїв, обладнаних датчиками, виконавчими механізмами та засобами зв'язку. Це можуть бути датчики температури, руху, освітлення, вологості, а також розумні побутові прилади, системи відеоспостереження, електронні замки та інші компоненти. Кожен із них здатний збирати дані про навколишнє середовище або свій власний стан і передавати цю інформацію до центрального вузла керування чи хмарного сервісу для подальшої обробки.

IoT являє собою концепцію створення інтелектуальних систем, де пристрої автоматично обмінюються даними через мережеві протоколи. Цю інформацію обробляють програмні засоби, після чого система здатна приймати рішення і виконувати відповідні дії. Такий підхід значно підвищує автономність системи, оскільки більшість операцій виконується без втручання людини. Це особливо актуально для складних систем, де швидкість реагування має вирішальне значення. Наприклад, якщо датчик виявить рух, система може увімкнути освітлення або надіслати сповіщення користувачу. Архітектура IoT складається з кількох рівнів: рівень пристроїв (датчики та виконавчі механізми), мережевий рівень (технології передачі даних) і рівень обробки інформації (сервери чи хмарні платформи). Взаємодія між цими рівнями забезпечує постійний обмін даними і ефективну роботу системи. Одною з ключових особливостей IoT є використання бездротових технологій зв'язку, таких як Wi-Fi, Bluetooth, тощо. Це дає змогу легко інтегрувати різноманітні пристрої в єдину мережу. Крім того,

завдяки застосуванню хмарних обчислень забезпечується зберігання великих масивів даних і доступ до них у реальному часі. Таким чином, Інтернет речей - це багаторівнева технологія, яка об'єднує апаратне обладнання та програмне забезпечення, створюючи автоматизовані системи.

1.2 Концепція розумного будинку

Концепція розумного будинку є одним із найбільш поширених напрямів застосування технології Інтернету речей. Вона передбачає створення інтегрованої системи, яка забезпечує автоматизоване управління різними інженерними та побутовими процесами в житловому приміщенні. Основною метою впровадження розумного будинку є підвищення рівня комфорту, безпеки та енергоефективності.

Розумний будинок являє собою комплекс взаємопов'язаних пристроїв і систем, які об'єднані в єдину мережу та здатні взаємодіяти між собою без постійного втручання користувача. До складу такої системи можуть входити освітлення, системи безпеки, клімат-контроль, відеоспостереження, розумні розетки, електронні замки та інші пристрої.

Основою функціонування розумного будинку є принцип автоматизації, який реалізується за допомогою сценаріїв роботи. Сценарій - це визначений алгоритм дій системи у відповідь на певні події або умови. Як приклад, при виявленні руху датчиком у темний час доби автоматично вмикається освітлення, а при відсутності мешканців - вимикаються електроприлади для економії енергії.

Взаємодія між елементами системи здійснюється за схемою «датчик – контролер – виконавчий пристрій». Датчики збирають інформацію про стан середовища або події (рух, температуру чи відкриття дверей) і передають її до контролера. Контролер обробляє отримані дані відповідно до заданих сценаріїв та формує команди для виконавчих пристроїв, які виконують необхідні дії.

Управління розумним будинком може здійснюватися як автоматично, так і вручну за допомогою мобільних додатків або веб-інтерфейсів. Це дозволяє

користувачу контролювати стан системи в режимі реального часу та змінювати налаштування відповідно до власних потреб.

Однією з важливих переваг розумного будинку є підвищення рівня безпеки. Система може оперативно реагувати на нештатні ситуації, такі як проникнення сторонніх осіб, витік газу або задимлення, надсилаючи відповідні сповіщення користувачу. Крім того, автоматизація дозволяє зменшити споживання енергоресурсів за рахунок оптимізації роботи електроприладів.

Таким чином, концепція розумного будинку базується на інтеграції сучасних інформаційних технологій та автоматизації процесів управління житловим середовищем. Її впровадження забезпечує більш ефективне використання ресурсів, підвищення рівня комфорту та безпеки, а також створює умови для подальшого розвитку інтелектуальних систем.

1.3 Архітектура IoT-систем

Архітектура Інтернету речей (IoT) визначає структурну організацію взаємодії між ключовими компонентами, що відповідають за збір, передачу, обробку даних та виконання відповідних дій. У переважній більшості випадків IoT-системи проєктуються на основі багаторівневої моделі, яка дозволяє забезпечити ефективне функціонування та легкість масштабування. Типова архітектура IoT складається з трьох основних елементів: датчиків (сенсорів), контролерів і виконавчих пристроїв. Їхня взаємодія базується на циклі «збір даних – обробка інформації – виконання дій».

Датчики утворюють перший рівень системи і виконують функцію ініціального збору даних із навколишнього середовища. Вони призначені для реєстрації різноманітних параметрів, таких як температура, вологість, рівень освітлення, присутність або відчинення дверей. Отримана інформація передається на наступний рівень для обробки.

Контролери виступають центральними вузлами IoT-систем, забезпечуючи обробку сигналів, отриманих від датчиків. Вони виконують аналіз зібраних даних відповідно до попередньо визначених алгоритмів і генерують команди для

виконавчих пристроїв. Контролери можуть бути реалізовані у форматі окремих апаратних пристроїв, мікроконтролерів або ж програмних модулів, інтегрованих у серверну інфраструктуру чи хмарні середовища. Контролер слугує ядром системи, формулюючи її логіку та спроектований для забезпечення безперебійної роботи усіх компонентів. Виконавчі пристрої призначені для реалізації команд контролера, що дозволяє втілювати необхідні фізичні дії. До цієї категорії належать розумні лампи, електронні замки, розетки, системи сигналізації та інші пристрої з конкретними функціями. Наприклад, контроль світла у приміщенні може автоматично змінювати інтенсивність освітлення залежно від команди контролера.

Ключову роль у функціонуванні IoT-систем відіграє мережевий шар архітектури, який опосередковує обмін даними між підсистемами. Для цього застосовуються різноманітні технології бездротової передачі інформації, зокрема Wi-Fi, Bluetooth, тощо. Вибір протоколів здійснюється на основі специфічних вимог до швидкості передачі даних, радіусу дії мережі та енергоспоживання.

Окремим аспектом є інтеграція IoT із сучасними хмарними платформами. Хмари забезпечують зберігання великих обсягів даних, їхню швидку обробку та спрощують доступ до системи в режимі реального часу. Завдяки мобільним додаткам або веб-інтерфейсам користувачі можуть безперервно моніторити та керувати пристроями навіть дистанційно.

Отже, архітектура IoT-систем являє собою багат шарову структуру, яка органічно поєднує апаратне забезпечення з програмними компонентами. Злагоджена взаємодія датчиків, контролерів і виконавчих пристроїв є основною передумовою для створення автоматизованих рішень у межах концепцій «розумного будинку» чи інших прикладних сценаріїв використання сучасних технологій IoT.

1.4 Аналіз існуючих рішень та їх порівняння

Сучасні системи Інтернету речей продовжують активно розвиватися, що зумовило створення численних програмних платформ і середовищ для моделювання, розробки та тестування IoT-рішень. Кожна з таких платформ має свої особливості, переваги та обмеження, тому їх ретельний аналіз є невід’ємною частиною процесу вибору інструментів для реалізації систем розумного будинку

Аналіз у цьому контексті набуває особливої актуальності, оскільки сучасні IoT-системи відзначаються складною структурою та включають велику кількість взаємопов’язаних елементів. Невідповідний вибір моделювального середовища може не лише обмежити функціональність системи, але й значно ускладнити процес її впровадження. Саме тому оцінка можливостей кожної доступної платформи є критично важливим етапом, який має передувати самому проектуванню..

Одним із найпопулярніших рішень є Cisco Packet Tracer. Ця платформа надає можливість моделювати як мережеву інфраструктуру, так і роботу IoT-пристроїв, включаючи датчики, контролери та виконавчі механізми. Вона підтримує різноманітні типи пристроїв і дозволяє налаштовувати їхню взаємодію, що дає змогу розробляти складні моделі розумних будинків. Крім того, Cisco Packet Tracer підтримує ключові протоколи передачі даних, зокрема MQTT, який широко використовується в IoT. Завдяки цьому інструмент є зручним як для навчання, так і для практичного моделювання мережевих і IoT-рішень. Однією з ключових переваг Cisco Packet Tracer є функція візуалізації мережевих процесів, яка суттєво спрощує розуміння принципів роботи системи. З її допомогою користувач може відстежувати передачу даних, взаємодію між пристроями в реальному часі та виявляти помилки в роботі мережі. Це особливо корисно при навчанні та відпрацюванні складних сценаріїв автоматизації.

Ще одним відомим інструментом є Wokwi - онлайн-платформа для моделювання мікроконтролерів, таких як Arduino та ESP32. З її допомогою можна тестувати програмний код і взаємодію пристроїв без необхідності використання фізичного обладнання. Основною перевагою Wokwi є її простота

та висока точність у симуляції програмної частини IoT-систем. Однак варто зазначити, що можливості цього середовища щодо моделювання мережевої інфраструктури досить обмежені. Wokwi є корисним інструментом для поліпшення навичок програмування мікроконтролерів та перевірки роботи окремих пристроїв. Це особливо корисно на початку розробки, коли головна увага спрямована на програмну частину систем IoT.

Node-RED, у свою чергу, є платформою для створення логічних зв'язків між пристроями завдяки візуальному підходу до програмування. Вона надає змогу будувати сценарії для роботи систем у формі потоків даних, що значно полегшує розробку IoT-додатків. Node-RED має особливу ефективність під час інтеграції різноманітних сервісів і обробки інформації. Проте вона не призначена для повноцінного моделювання фізичної мережі.

Інструмент Tinkercad Circuits орієнтований на початкове ознайомлення з електронікою й основами IoT. Завдяки йому можна створювати прості схеми за участю датчиків і мікроконтролерів. Однак функціонал цього середовища обмежений для реалізації більш складних систем. Це середовище виявляється надзвичайно корисним для навчальних цілей, оскільки дає можливість наочно вивчати принципи функціонування електронних компонентів і основи IoT-технологій. Завдяки цьому воно здобуло популярність серед початківців і студентів.

Особливо цікавим є використання CupCarbon - спеціалізованого середовища для моделювання бездротових сенсорних мереж. Воно дозволяє оцінювати поведінку мережі, споживання енергії пристроями та радіопокриття, що особливо актуально для аналізу великомасштабних IoT-систем. Водночас цей інструмент відзначається складністю у використанні й значною мірою орієнтований на потреби наукових досліджень.

Аналіз наведених платформ демонструє їхню різну спеціалізацію: одні зосереджені на програмуванні та симуляції пристроїв, інші - на мережевому моделюванні чи аналізі окремих аспектів системи. Зважаючи на високий рівень різноманітності IoT-систем, що передбачає інтеграцію численних пристроїв і

технологій, вибір відповідного середовища повинен враховувати як багатоцільовість, так і підтримку цієї гетерогенної природи.

Отже, для створення ефективної системи розумного будинку варто обирати багатофункціональну платформу, яка забезпечує комплексне моделювання мережевої інфраструктури та взаємодії IoT-пристроїв. Одним із найбільш підходящих варіантів у цьому контексті є Cisco Packet Tracer, що робить його вагомим вибором для подальшої роботи й досліджень.

1.5 Переваги та недоліки використання IoT у системах розумного будинку

Використання технологій Інтернету речей у системах розумного будинку має як значні переваги, так і певні обмеження, які необхідно ретельно враховувати на етапах впровадження та експлуатації.

Однією з ключових переваг є здатність таких систем здійснювати збір та аналіз даних у режимі реального часу. Це дозволяє системі не лише виконувати наперед запрограмовані команди, але й адаптувати свою роботу відповідно до змін у поведінці користувача чи умов зовнішнього середовища. Така характеристика сприяє підвищенню загальної ефективності системи, а також забезпечує гнучке управління її функціональними можливостями.

Також є опція віддаленого моніторингу та управління. Завдяки цій функції користувач отримує можливість доступу до поточних показників стану пристроїв та управління їх налаштуваннями незалежно від місця перебування. Це помітно підвищує комфорт експлуатації та забезпечує можливість оперативного реагування на різноманітні ситуації.

Інтернет-речей також пропонує високий рівень інформативності, надаючи користувачам детальні дані щодо роботи системи, споживання ресурсів і ефективності її функціонування. Така інформація слугує основою для прийняття обґрунтованих рішень стосовно подальшої оптимізації використання системи.

Не менш важливою перевагою є її масштабованість, що дозволяє поступове розширення функціональних можливостей без необхідності суттєвих змін у базовій структурі системи.

Разом з цим у системи розумного будинку мають свої недоліки та обмеження.

Однією з головних проблем залишається забезпечення безпеки даних. Пристрій, підключений до мережі, може стати об'єктом несанкціонованого доступу, що створює ризик витоку конфіденційної інформації чи втручання у функціонування системи.

Ще одним суттєвим недоліком є залежність від стабільного мережевого з'єднання. Будь-які перебої в роботі мережі чи відсутність Інтернету можуть призвести до часткової або повної втрати функціональності системи, що значно знижує її надійність та зручність у використанні.

Також є складність налаштування й обслуговування IoT-систем. Для їх правильної інсталяції та роботи потрібні спеціалізовані технічні знання. При цьому навіть невеликі помилки під час конфігурації можуть викликати збої в роботі.

Фінансова сторона також є вагомим чинником, адже впровадження систем розумного будинку вимагає значних витрат на закупівлю обладнання, його монтаж та технічне обслуговування. Окрім того, часто виникає проблема сумісності пристроїв різних виробників, що ускладнює інтеграцію в єдину працюючу систему.

Таким чином, попри значний потенціал технології IoT у розумних будинках, ефективне її застосування можливе лише за умови ретельного врахування переваг і недоліків. Це дасть змогу забезпечити стабільну, безпечну та надійну роботу таких систем.

РОЗДІЛ 2 МОДЕЛЮВАННЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ

2.1 Огляд середовищ моделювання IoT

Проектування, розробка та практична реалізація систем Інтернету речей у межах концепції «Розумного будинку» є комплексним інженерним завданням. Воно охоплює не лише інтеграцію різноманітних фізичних пристроїв (датчиків, актуаторів, мікроконтролерів), а й побудову надійної мережевої архітектури, розробку алгоритмів автоматизації та забезпечення інформаційної безпеки передачі даних.

Розгортання таких систем безпосередньо у фізичному середовищі на початкових етапах проектування пов'язане з низкою критичних проблем:

- Високі фінансові витрати на придбання апаратного забезпечення (контролерів типу Arduino, Raspberry Pi, ESP32, датчиків, комутаційних плат, виконавчих механізмів) до моменту повної валідації архітектурних рішень.
- Ризики пошкодження обладнання внаслідок помилок у схемотехніці, некоректного подання живлення або програмних збоїв у логіці керування виконавчим обладнанням (наприклад, критичний перегрів обігрівача або коротке замикання).
- Складність масштабування та тестування в екстремальних умовах (наприклад, імітація пожежі для перевірки датчиків диму, критичні навантаження на бездротову Wi-Fi мережу при одночасному підключенні десятків пристроїв).

Для подолання цих викликів у сучасній комп'ютерній інженерії застосовують спеціалізовані середовища імітаційного моделювання та симуляції. Вони дозволяють створити цифровий двійник проектованої IoT-системи, провести детальне тестування алгоритмів автоматизації, оптимізувати топологію мережі та проаналізувати її поведінку в режимі реального часу.

Сучасний ринок програмного забезпечення пропонує кілька категорій платформ для моделювання IoT, кожна з яких має свою специфіку, переваги та суттєві обмеження:

- Програмно- та схемотехнічно-орієнтовані симулятори: Tinkercad Circuits, Wokwi. Ці платформи орієнтовані на емуляцію фізичного рівня електронних пристроїв та відлагодження програмного коду безпосередньо для мікроконтролерів.

- Tinkercad Circuits є хмарним інструментом, що дозволяє створювати віртуальні схеми на базі платформи Arduino Uno. Проте платформа має суттєві обмеження: слабкий набір підтримуваних IoT-інтерфейсів, відсутність можливості моделювання багаторівневих комп'ютерних мереж та неможливість гнучкого налаштування бездротових протоколів зв'язку.

- Wokwi - сучасніший хмарний симулятор, який підтримує архітектури ESP32 та Raspberry Pi Pico, забезпечуючи точну емуляцію виконання коду. Водночас Wokwi фокусується виключно на окремих пристроях і не дозволяє згенерувати повноцінну топологію мережі з маршрутизаторами, комутаторами та системами розподілу IP-адрес для великої кількості кімнат чи зон будинку.

Платформи візуального проектування логіки Node-RED. Node-RED базується на концепції візуального програмування, де взаємодія описується у вигляді потоків даних між графічними вузлами. Node-RED є потужним інструментом для обробки даних та побудови графічних інтерфейсів користувача. Проте він є інструментом проміжного рівня (Middleware) - він не симулює роботу самих фізичних датчиків, завади у бездротових каналах зв'язку чи логічну структуру локальної комп'ютерної мережі (IP-адресацію, маски підмереж, таблиці маршрутизації).

Спеціалізовані науково-дослідницькі симулятори, наприклад CupCarbon. CupCarbon - це симулятор бездротових сенсорних мереж та інфраструктури «Розумного міста». Основною метою цього середовища є проектування великомасштабних радіомереж та аналіз геопросторових даних. Цей інструмент є занадто специфічним, має високий поріг входження і є неоптимальним для локальних завдань автоматизації всередині конкретного житлового приміщення.

Для систематизації аналізу та обґрунтування вибору інструменту для сформуємо порівняльну таблицю існуючих рішень за ключовими критеріями що видно в таблиці (2.1).

Таблиця 2.1

Критерій порівняння	Tinkercad Circuits	Wokwi	Node-RED	CupCarbon	Cisco Packet Tracer
Тип платформи	Хмарна	Хмарна	Локальна/Хмарна	Локальна	Локальна
Симуляція мережевого стеку (TCP/IP)	Відсутня	Базова (лише Wi-Fi клієнт)	Відсутня (потребує готову мережу)	Базова (протоколи WSN)	Повна (L1-L7 рівні OSI, DHCP, DNS, NAT, VLAN)
Емуляція IoT-пристроїв	Низька (компонент и Arduino)	Середня (ESP32, периферія)	Відсутня (потребує зовн. дані)	Висока (сенсорні вузли)	Висока (готові smart-компоненти та мікроконтролери SBC)
Програмування логіки	Блоки / C++	C++ / MicroPython	Візуальні потоки (JS)	Скрипти ScriptCox	Декларативні правила (IF/THEN), Python, JavaScript
Аналіз мережевого трафіку	Відсутній	Відсутній	Базове логування	Аналіз енергоспоживання вузлів	Повний (Режим Simulation, покроковий розбір пакетів PDU)
Організація складних топологій	Відсутня	Відсутня	Відсутня	Обмежена (лише WSN)	Висока (багатозонові підмережі, маршрутизація)

Обґрунтування вибору Cisco Packet Tracer

Проведений аналіз чітко показує, що більшість існуючих середовищ моделювання мають вузьку спеціалізацію: вони зосереджені або виключно на написанні коду для одного мікроконтролера, або на високорівневій обробці даних. Жодне з них не дозволяє розробити комплексну, масштабовану та захищену мережеву інфраструктуру.

Для реалізації завдань було обрано середовище Cisco Packet Tracer. На відміну від інших розглянутих платформ, воно є інтегрованим рішенням, яке ідеально поєднує в собі інструменти комп'ютерної інженерії та Інтернету речей.

Програма дозволяє не просто підключати пристрої, а проектувати архітектуру мережі на всіх рівнях моделі OSI. Це дає можливість налаштовувати маршрутизатори, комутатори, розподіляти IP-адреси через DHCP, налаштовувати бездротові точки доступу та шлюзи

Завдяки інструментам Cisco, у роботі реалізовано розподілену топологію розумного будинку, тобто розділення на зони безпеки, клімату та живлення, що є неможливим у симуляторах типу Tinkercad чи Wokwi.

Середовище підтримує як декларативний підхід створення сценаріїв, які використовують гнучкі правила зв'язків «IF/THEN» на IoT-сервері, так і низькорівневе програмування смарт-модулів і одноплатних комп'ютерів на мовах Python та JavaScript.

Платформа надає унікальну можливість покрокового відстеження пакетів даних. Це дозволяє наочно проаналізувати, як саме передаються команди від датчиків до виконавчих пристроїв, та оцінити затримки в мережі.

2.2 Моделювання структури системи

Ефективність функціонування сучасних комплексів Інтернету речей (IoT) безпосередньо залежить від коректності проєктування їхньої структурної та мережевої архітектури. Побудова класичної монолітної мережі, де всі інтелектуальні пристрої, датчики та виконавчі механізми підключені до одного центрального бездротового вузла, є неефективною. Така архітектура створює критичну точку відмови, призводить до перевищення ємності бездротового каналу зв'язку через надмірну кількість широкомовного трафіку та суттєво знижує загальну безпеку системи через відсутність логічної ізоляції пристроїв.

Для подолання цих інженерних викликів у межах цієї кваліфікаційної роботи було спроектовано, обґрунтовано та змодельовано децентралізовану сегментовану структуру системи, яка базується на класичній тривірневій моделі

IoT: рівень сприйняття, мережевий рівень, рівень додатків, але адаптована під концепцію розподілених бездротових шлюзів у середовищі Cisco Packet Tracer.

Основне інженерне рішення розробленої структури полягає в ієрархічній сегментації єдиного інформаційного простору розумного будинку на три незалежні логічні підмережі, або технологічні зони. Кожна зона функціонує під управлінням власного інтелектуального домашнього шлюзу який виступає в ролі локального контролера доступу та IoT-сервера. Всі три шлюзи об'єднуються в єдину інфраструктуру вищого рівня за допомогою центрального бездротового маршрутизатора, який координує міжмережеву взаємодію та забезпечує маршрутизацію пакетів даних.

Розглянемо вертикальну структуру розробленої системи за ієрархічними рівнями архітектури Інтернету речей:

1. Рівень сприйняття та виконання – це нижній рівень системи, що складається безпосередньо з кінцевих IoT-пристроїв. Датчики та сенсори відповідають за фіксацію та первинне перетворення фізичних параметрів навколишнього середовища у цифрові сигнали, а виконавчі механізми, або активатори, - за фізичне виконання отриманих керуючих команд. У розробленій структурі цей рівень розподілений за функціональними підсистемами:

- Підсистема безпеки охоплює пасивні інфрачервоні датчики руху для фіксації несанкціонованого доступу на об'єкті, керовані за допомогою електроприводу входні двері та гаражні ворота, а також кінцевий пристрій звукового та візуального оповіщення - тривожну сирену.

- Підсистема клімат-контролю та комфорту містить електронний термостат для безперервного моніторингу температури повітря в приміщенні, розумне вікно з можливістю автоматичного відкриття форуги для провітрювання, керований за ступенями швидкості стельовий вентилятор, розумну лапму з підтримкою регулювання інтенсивності випромінювання, а також побутовий автомат для автоматизації кухонних процесів.

- Підсистема енергоефективності включає інтелектуальну сонячну панель, яка виконує роль джерела альтернативної енергії та одночасно сенсора поточної генерації електричної потужності, передаючи метрики на сервер.

2. Мережевий рівень – рівень, який реалізує стек протоколів TCP/IP, забезпечує комунікацію, адресацію, маршрутизацію пакетів даних та інтеграцію різномірних пристроїв у єдину міжмережеву структуру. У розробленій моделі він має чітку дворангову ієрархію:

- Локальний ранг представлений трьома бездротовими шлюзами Home Gateway: «Home Security», «Kitchen & Living Room», «Home Power». Кожен шлюз функціонує на базі бездротової технології зв'язку Wi-Fi у частотному діапазоні 2.4 GHz для безпосереднього підключення IoT-пристроїв своєї зони. Крім того, шлюзи обладнані вбудованими DHCP-серверами для динамічного та автоматичного розподілу IP-адрес і масок підмереж всередині своєї ізольованої зони, що виключає конфлікти адресації.

- Магістральний ранг - рівень агрегації та маршрутизації, представлений центральним бездротовим маршрутизатором типу WRT300N. Він виступає в ролі головного комунікаційного ядра системи. До його LAN-портів через дротові інтерфейси Ethernet, кабелі типу «вита пара» категорії Cat 5e/6, роз'єми RJ-45, підключаються локальні IoT-шлюзи через свої інтерфейси Internet. Маршрутизатор забезпечує зв'язок між різними підмережами на мережевому рівні моделі OSI L3 шляхом ведення таблиць маршрутизації та керує глобальною адресацією внутрішньої мережі будинку.

3. Рівень управління та додатків, який відповідає за обробку інформації, логічний аналіз даних, виконання високорівневих сценаріїв автоматизації та надання графічного інтерфейсу користувачу У моделі Cisco Packet Tracer цей рівень реалізовано через адміністративні термінали та периферія які оснащені бездротовими мережевими адаптерами Wi-Fi або підключені дротовим способом до центрального маршрутизатора WRT300N. Завдяки налаштованій статичній або динамічній маршрутизації, адміністратор з одного робочого терміналу через стандартний веб-браузер має доступ до

інтегрованої панелі моніторингу кожного окремого шлюзу. Це дозволяє здійснювати централізоване віддалене адміністрування, моніторинг стану датчиків та ручне керування актуаторами з будь-якої точки мережі.

Для наочності розробленої структури, систематизації параметрів проектування та обліку обладнання сформуємо специфікацію розподілу архітектурних компонентів системи розумного будинку (табл. 2.1).

Таблиця 2.1 - Архітектурна специфікація та розподіл компонентів системи розумного будинку

Назва підсистеми (Зони)	Мережевий контролер підмережі	Кінцеві IoT-пристрої (Сенсори та активатори)	Тип інтерфейсу зв'язку	Логічне призначення підсистеми та функції
Home Security (Зона безпеки)	Home Gateway (Security)	Motion Detector, Siren, Smart Door, Garage Door	Бездротовий (Wi-Fi, 2.4 GHz, стандарт 802.11n)	Виявлення руху, автоматичне блокування/розблокування входів, активація звукової сигналізації при загрозі.
Kitchen & Living Room (Зона клімату та комфорту)	Home Gateway (Living)	Thermostat, Ceiling Fan, Light, Smart Window, Coffee Maker	Бездротовий (Wi-Fi, 2.4 GHz, стандарт 802.11n)	Підтримання параметрів мікроклімату, автоматичне регулювання освітлення, управління побутовою технікою.
Home Power (Зона енергетики)	Home Gateway (Power)	Solar Panel, Battery/Power Monitor	Бездротовий (Wi-Fi, 2.4 GHz, стандарт 802.11n)	Моніторинг генерації відновлюваної енергії, аналіз поточного енергоспоживання та накопичення заряду.
Management & Core (Магістральний рівень)	Wireless Router WRT300N	Laptop (Адміністратор), PC (Моніторинг), Printer	Дротовий (FastEthernet, RJ-45) / Бездротовий	Маршрутизація трафіку між зонами, організація загального доступу, централізоване адміністрування.

Розроблена децентралізована архітектура забезпечує максимальну відмовостійкість інфраструктури «Розумного будинку». У разі виникнення критичної помилки, програмного збою або апаратного перевантаження на одному із шлюзів (наприклад, шлюз кухні через велику кількість пристроїв), підсистема безпеки (Home Security) та підсистема енергоживлення (Home Power) продовжуватимуть функціонувати у штатному автономному режимі.

Загальну структурно-логічну схему розробленої децентралізованої системи «Розумний будинок» у середовищі моделювання Cisco Packet Tracer представлено на рисунку (2.1).

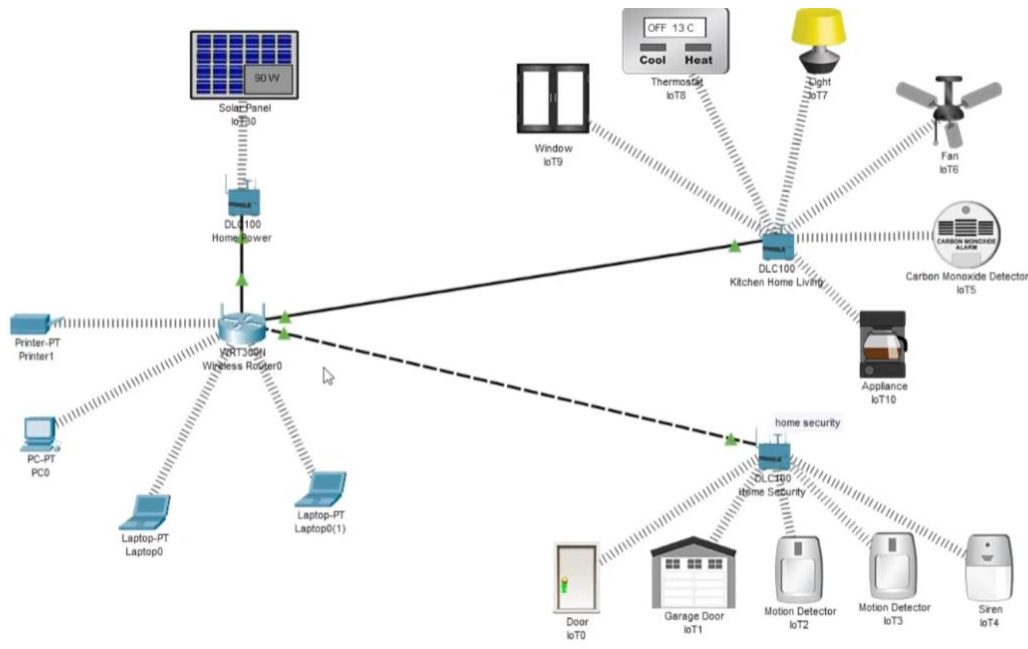


Рисунок 2.1 – Структурна схема мережі інфраструктури IoT системи «Розумний будинок»

Тут реалізовано алгоритм роботи захисного контуру «Motion» (Рух):

1. Вхідний тригер (IF): система опитує бездротові датчики руху Motion Detector (IoT2) та Motion Detector (IoT3). Параметр Any (Будь-який) означає, що логіка спрацює за правилом «АБО» — якщо хоча б один із датчиків зафіксує активність.

2. Виконавчі дії (THEN): у разі спрацювання датчика шлюз миттєво відправляє керуючий сигнал на три пристрої:

- Вмикає звукову тривогу на сирені Siren (переводить у стан On);
- Блокує електрозамок входних дверей Door (стан Lock);
- Блокує замок гаражних воріт Garage Door (стан Lock).

2.3 Налаштування компонентів системи

Практична реалізація та інтеграція спроектованої розподіленої архітектури «Розумного будинку» в середовищі Cisco Packet Tracer вимагає послідовного налаштування кожного окремого компонента системи. Процес конфігурації кінцевих IoT-пристроїв (сенсорів та актуаторів) та робочих станцій розподіляється на кілька важливих інженерних етапів, які охоплюють апаратну модернізацію інтерфейсів зв'язку, логічну асоціацію з бездротовими шлюзами (Home Gateway) та верифікацію їхньої реєстрації на локальних IoT-серверах.

За замовчуванням більшість інтелектуальних компонентів і робочих станцій у бібліотеці Cisco Packet Tracer постачаються зі стандартними дротовими мережевими адаптерами типу FastEthernet. Оскільки розроблена модель передбачає бездротову структуру зв'язку всередині кожної технологічної зони, першочергово було проведено апаратну модернізацію інтерфейсів пристроїв.

Для кожного кінцевого IoT-датчика та актуатора (зокрема, датчиків руху, сирени, розумних дверей, вентилятора, термостата) через розширене меню конфігурації та вкладку конфігурації введення-виведення стандартний дротовий адаптер було змінено на бездротовий мережевий модуль. Цей модуль функціонує в частотному діапазоні 2.4 GHz та забезпечує підтримку бездротового стеку протоколів. Крім того, у загальних налаштуваннях пристроїв у полі IoT Server було встановлено значення Home Gateway, що є обов'язковою умовою для перенаправлення телеметрії пристрою на відповідний локальний контролер.

Аналогічну модернізацію було проведено і для адміністративних терміналів - ноутбука та персонального комп'ютера. У вкладці Physical після тимчасового вимкнення живлення стандартні дротові модулі було вилучено з гнізд розширення, а на їхнє місце встановлено бездротові інтерфейсні модулі WMP300N, які працюють у тому ж частотному діапазоні для забезпечення зв'язку з магістральним роутером.

Наступним кроком стало логічне підключення пристроїв та їхня автентифікація в бездротових зонах. Для забезпечення ізоляції трафіку та стабільного розподілу адрес через DHCP, кожен домашній шлюз було

попередньо сконфігуровано на роботу під керуванням окремого ідентифікатора бездротової мережі (SSID) та у власному IP-діапазоні. Підключення компонентів до відповідних технологічних підмереж реалізовано шляхом налаштування бездротового інтерфейсу у вкладці Config - Wireless кожного пристрою.

Для компонентів підмережі безпеки (Home Security), до якої належать датчики руху, тривожна сирена, розумні входні двері та гаражні ворота, було прописано єдиний SSID Security_IoT_Zone. В результаті пристрої встановили стабільний бездротовий зв'язок зі шлюзом безпеки й автоматично отримали IP-адреси з діапазону 192.168.25.X.

Для компонентів підмережі клімату та комфорту (Kitchen & Living Room), що включає термостат, стельовий вентилятор, лампу освітлення, розумне вікно та кавоварку, було встановлено SSID Living_IoT_Zone, що дозволило їм асоціюватися зі своїм контролером та отримати IP-адреси .

Інтелектуальну сонячну панель, яка формує підмережу енергоефективності (Home Power), було аналогічно підключено до бездротової мережі шлюзу з SSID Power_IoT_Zone, внаслідок чого вона отримала мережеві реквізити. Успішність встановлення бездротового з'єднання між усіма цими компонентами системи та відповідними шлюзами у візуальному просторі Cisco Packet Tracer відображається у вигляді характерних пунктирних ліній зв'язку.

Кінцевим етапом налаштування компонентів є верифікація їхньої коректної взаємодії з вбудованими веб-серверами шлюзів. Контроль та віддалене керування здійснюється з адміністративного ноутбука, підключеного до центрального бездротового маршрутизатора WRT300N (SSID: Home_Core_Net). За допомогою вбудованої утиліти Desktop -> Web Browser на ноутбуці здійснюється підключення до IP-адрес шлюзів (наприклад, 192.168.25.1 для підсистеми охорони або 192.168.75.1 для підсистеми клімату). Після введення облікових даних адміністратора в інтерфейсі IoT Monitor відображається інтерактивний список усіх успішно зареєстрованих компонентів відповідної зони. Ця панель моніторингу дозволяє в режимі реального часу відстежувати поточний стан сенсорів (фіксація руху датчиком, поточні температурні

показники термостата) та здійснювати пряме ручне або тестове керування активаторами (дистанційне блокування дверей, зміна швидкості обертання вентилятора, увімкнення та вимкнення освітлення).

Для узагальнення виконаних налаштувань та конфігурацій пристроїв сформуємо зведену карту параметрів компонентів системи розумного будинку (табл. 2.2).

Таблиця 2.2 - Параметри конфігурації та бездротового підключення компонентів системи

Назва IoT-пристрою	Технологічна зона	Тип встановленого адаптера	Ідентифікатор Wi-Fi	Отримана IP-адреса	Взаємодія з IoT-сервером
Motion Detector	Home Security	PT-IOT-NM-1W	Security_IoT_Zone	192.168.25.100	Зареєстровано (192.168.25.1)
Siren	Home Security	PT-IOT-NM-1W	Security_IoT_Zone	192.168.25.101	Зареєстровано (192.168.25.1)
Smart Door	Home Security	PT-IOT-NM-1W	Security_IoT_Zone	192.168.25.102	Зареєстровано (192.168.25.1)
Garage Door	Home Security	PT-IOT-NM-1W	Security_IoT_Zone	192.168.25.103	Зареєстровано (192.168.25.1)
Thermostat	Kitchen & Living	PT-IOT-NM-1W	Living_IoT_Zone	192.168.75.100	Зареєстровано (192.168.75.1)
Ceiling Fan	Kitchen & Living	PT-IOT-NM-1W	Living_IoT_Zone	192.168.75.101	Зареєстровано (192.168.75.1)
Light	Kitchen & Living	PT-IOT-NM-1W	Living_IoT_Zone	192.168.75.102	Зареєстровано (192.168.75.1)
Smart Window	Kitchen & Living	PT-IOT-NM-1W	Living_IoT_Zone	192.168.75.103	Зареєстровано (192.168.75.1)
Coffee Maker	Kitchen & Living	PT-IOT-NM-1W	Living_IoT_Zone	192.168.75.104	Зареєстровано (192.168.75.1)
Solar Panel	Home Power	PT-IOT-NM-1W	Power_IoT_Zone	192.168.125.100	Зареєстровано (192.168.125.1)

2.4 Реалізація алгоритмів та сценаріїв роботи

Кінцевим і найбільш відповідальним етапом проектування цифрового двійника системи «Розумний будинок» є програмування логіки взаємодії між

сенсорами та активаторами всередині кожної технологічної зони. У середовищі Cisco Packet Tracer цей процес реалізується на прикладному рівні за допомогою вбудованих декларативних правил на локальних IoT-серверах домашніх шлюзів). Створення таких алгоритмів дозволяє повністю виключити людський чинник із рутинних процесів керування та забезпечити автономне функціонування об'єкта. Програмування сценаріїв здійснювалося через адміністративний ноутбук за допомогою веб-інтерфейсу панелі моніторингу, де для кожного алгоритму чітко визначалися умови спрацювання за логічною схемою «якщо виконано умову на сенсорі, то виконати відповідну дію на активатора».

Перший комплекс алгоритмів було реалізовано для підсистеми охорони та безпеки на шлюзі Home Gateway Головною метою цього сценарію є миттєве реагування на несанкціоноване проникнення в житлове приміщення та захист периметра. Базовим тригером тут виступає датчик руху (Motion Detector). Алгоритм налаштовано таким чином, що коли датчик переходить у стан активності (значення Motion = true), шлюз миттєво надсилає керуючі команди на три виконавчі пристрої. Першою командою активується тривожна сирена (Siren), яка переходить у режим максимальної акустичної сигналізації (Siren = On). Одночасно з цим подаються сигнали на блокування розумних входних дверей (Smart Door) та гаражних воріт (Garage Door), які примусово зачиняються й переводяться в замкнений стан (Lock = true), повністю ізолюючи внутрішній простір будинку від зловмисника. Для повернення системи у штатний режим безпеки створено зворотне правило: за умови відсутності руху протягом заданого часу (Motion = false), сирена автоматично вимикається, а двері переходять у режим очікування команди користувача.

Другий блок сценаріїв автоматизації координує роботу підсистеми клімат-контролю та комфорту на шлюзі Home Gateway (Living). Тут реалізовано складніший двофакторний алгоритм підтримки оптимального температурного балансу та енергозбереження. Основним джерелом даних є електронний термостат (Thermostat), який безперервно фіксує температуру повітря в кімнаті.

Перший температурний сценарій орієнтований на захист від перегріву та вентиляцію: коли показники термостата перевищують верхню критичну межу у 25 °C (Temperature > 25), локальний сервер шлюзу автоматично переводить стельовий вентилятор (Ceiling Fan) у режим максимальних обертів та надсилає команду на відкриття розумного вікна (Smart Window - Status = Open) для природного охолодження приміщення. Другий сценарій, навпаки, реагує на зниження температури нижче комфортного рівня у 18 °C (Temperature < 18): у цьому разі вентилятор повністю зупиняється, вікно автоматично зачиняється для усунення протягів та збереження тепла, а на розумну лампу освітлення та побутову техніку за потреби подаються відповідні команди керування.

Третій напрямок автоматизації пов'язаний із підсистемою енергоефективності на контролері Home Gateway (Power). Оскільки система інтегрована з відновлюваними джерелами живлення, алгоритм відстежує рівень поточної генерації електричної енергії від інтелектуальної сонячної панелі. Сенсорні метрики панелі передаються на сервер шлюзу, де на основі обсягу виробленої потужності формуються команди для побутових споживачів. Наприклад, реалізовано сценарій автоматичного запуску побутових приладів (зокрема кавоварки або системи поливу) виключно в періоди максимальної сонячної активності, коли сонячна панель генерує надлишкову потужність. Це дозволяє оптимізувати внутрішній енергетичний баланс розумного будинку та мінімізувати споживання дорогої електромережі загального користування.

Для систематизації всіх запрограмованих алгоритмів та наочного відображення логіки взаємодії компонентів сформуємо зведену матрицю логічних умов та сценаріїв автоматизації (табл. 2.3).

Таблиця 2.3 - Матриця логічних умов та сценаріїв автоматизації інфраструктури IoT

Назва підсистеми	Пристрій-сенсор	Логічна умова	Керований пристрій	Виконувана дія / Стан актуатора
------------------	-----------------	---------------	--------------------	---------------------------------

Home Security (Безпека)	Motion Detector	Motion = True	SirenSmart DoorGarage Door	Увімкнути звуковий сигнал Заблокувати двері Зачинити ворота
Home Security (Безпека)	Motion Detector	Motion = False	Siren	Вимкнути звуковий сигнал
Kitchen & Living (Клімат)	Thermostat	Temperature > 25 °C	Ceiling FanSmart Window	Увімкнути високу швидкість (High) Відкрити фромугу (Open)
Kitchen & Living (Клімат)	Thermostat	Temperature < 18 °C	Ceiling FanSmart Window	Повністю вимкнути Герметично зачинити
Home Power (Енергетика)	Solar Panel	Power >	Coffee Maker / Appliances	Дозволити роботу / Активувати пристрій

Тестування та валідація розроблених алгоритмів здійснювалися безпосередньо у просторі моделювання шляхом переведення Cisco Packet Tracer у режим симуляції трафіку. При штучній зміні станів сенсорів (наприклад, при проходженні віртуального об'єкта повз датчик руху за допомогою комбінації клавіш Alt та миші) система продемонструвала миттєву реакцію: пакети керування успішно досягали активаторів, змінюючи їхній графічний стан. Це підтверджує працездатність, високу швидкість реагування та логічну коректність усіх реалізованих сценаріїв автоматизації «Розумного будинку».

РОЗДІЛ 3 ТЕСТУВАННЯ ТА АНАЛІЗ РОБОТИ СИСТЕМИ

3.1 Умови та методика тестування

Після завершення всіх етапів проектування, побудови топології та програмного налаштування цифрового двійника системи «Розумний будинок» у середовищі Cisco Packet Tracer, постає необхідність проведення комплексної верифікації та тестування розробленої моделі. Етап тестування є невід'ємною частиною інженерного процесу, оскільки він дозволяє експериментально підтвердити працездатність системи, стабільність мережевої інфраструктури, відсутність конфліктів адресації, а також логічну коректність і швидкість виконання автоматизованих сценаріїв взаємодії між датчиками та виконавчим обладнанням у режимі реального часу. Для того, щоб результати перевірки були об'єктивними, точними та повторюваними, було чітко визначено базові умови моделювання та розроблено покрокову комплексну методику тестування.

Умови проведення тестування були стандартизовані й залишалися незмінними протягом усіх серій експериментів. Моделювання та збір аналітичних даних здійснювалися на базі обчислювальної системи технічні характеристики якого забезпечували плавну та стабільну емуляцію без затримок з боку самого заліза. Перевірка виконувалася у спеціалізованому програмному комплексі Cisco Packet Tracer актуальної версії, яка містить розширену бібліотеку компонентів Інтернету речей (IoT), вбудовані сервери домашніх шлюзів та інтегровані інтерпретатори коду.

Під час проведення тестів програмне середовище використовувалося у двох фундаментальних режимах:

- Режим реального часу (Realtime Mode) - у цьому режимі система функціонувала у звичайному темпі плину часу. Він застосовувався для перевірки загальної стабільності бездротових з'єднань, тривалого моніторингу працездатності пристроїв, оцінки коректності динамічної роздачі адрес та для візуального спостереження за реакцією актуаторів на дії користувача.

- Режим симуляції (Simulation Mode) - цей режим дозволяв штучно зупиняти або покроково сповільнювати час моделювання. Він став ключовим інструментом для глибокого інженерного аналізу трафіку, оскільки надавав можливість перехоплювати окремі пакети даних (PDU), детально досліджувати їхній вміст, заголовки, структуру протоколів на різних рівнях моделі OSI (від канального до прикладного) та відстежувати точний маршрут руху інформації від сенсора до шлюзу й виконавчого механізму.

Методика тестування розробленої системи була побудована за принципом «від простого до складного» і складалася з чотирьох послідовних взаємопов'язаних етапів:

- Верифікація роботи сервісів динамічної адресації (DHCP): Перший етап методики передбачав аудит працездатності вбудованих DHCP-серверів на кожному з трьох бездротових домашніх шлюзів (Home Gateway). Перевірка здійснювалася шляхом відкриття мережеских налаштувань кожного окремого датчика та виконавчого пристрою у кожній технологічній зоні. Тест вважався успішно пройденим, якщо пристрої не видавали помилок ініціалізації та автоматично отримували унікальну IP-адресу, правильну маску підмережі (255.255.255.0) та адресу свого основного шлюзу..

- Перевірка міжмережевого зв'язку та маршрутизації (ICMP): Цей етап був спрямований на те, щоб переконатися, що центральний магістральний роутер WRT300N коректно зв'язує та маршрутизує трафік між різними підмережами. Для цього використовувався термінал командного рядка (Command Prompt) на адміністративному ноутбучі, який мав магістральну IP-адресу 192.168.0.100. З ноутбука запускалася серія тестових ехо-запитів за допомогою утиліти ping на внутрішні IP-адреси всіх трьох домашніх шлюзів. Критерієм успішності цього тесту було отримання стабільних ехо-відповідей від усіх шлюзів без жодних втрат пакетів (0% packet loss) та з мінімальним часом затримки.

- Контроль доступності прикладного рівня (HTTP): Методика на цьому етапі передбачала перевірку можливості віддаленого адміністрування та моніторингу системи через веб-інтерфейс. На ноутбуці адміністратора

запускався вбудований веб-браузер, через який здійснювалися спроби підключення до веб-серверів шлюзів за їхніми IP-адресами. Тест вважався успішним, якщо після проходження аутентифікації користувач отримував стабільний доступ до інтерактивної панелі IoT Monitor, де коректно, без затримок відображався повний список зареєстрованих пристроїв та актуальні цифрові показники телеметрії з датчиків у реальному часі.

Запровадження такої детальної чотирьох-етапної методики дозволило комплексно оцінити розроблену систему «Розумний будинок» з інженерного погляду. Всі практичні результати, графіки проходження пакетів та цифрові показники, які були отримані під час виконання кожного з цих кроків, зафіксовані й детально проаналізовані у наступному підрозділі роботи.

3.2 Результати тестування

Практична реалізація розробленої методики тестування в середовищі Cisco Packet Tracer дозволила отримати вичерпні дані щодо працездатності та ефективності спроектованої системи «Розумний будинок». Всі експерименти проводилися послідовно, а їхні результати зафіксували повну відповідність побудованої цифрової моделі закладеним технічним вимогам.

На першому етапі перевірки роботи сервісів динамічної адресації (DHCP) було підтверджено 100% працездатність локальних шлюзів. Під час аудиту мережевих налаштувань кінцевих пристроїв було зафіксовано, що вбудовані DHCP-сервери кожного домашнього шлюзу (Home Gateway) безпомилково обробили запити від бездротових модулів. Кінцеві IoT-компоненти успішно отримали унікальні локальні IP-адреси. Пристрої підсистеми охорони (датчики руху, сирена, двері) зайняли свої місця в підмережі безпеки з адресами від 192.168.25.100 до 192.168.25.103. Компоненти житлової зони та кухні (термостат, вентилятор, вікно, лампа, кавоварка) отримали адреси в діапазоні 192.168.75.100 – 192.168.75.104. Інтелектуальна сонячна панель у підмережі енергетики успішно зареєструвалася з адресою 192.168.125.100. Важливим

інженерним результатом стало те, що завдяки чіткому розділенню на бездротові зони (SSID) у мережі не виникло жодного конфлікту чи дублювання адрес.

На другому етапі було протестовано міжмережевий зв'язок за допомогою утиліти `ping` в командному рядку адміністративного ноутбука, який мав IP-адресу 192.168.0.100. Тестування проводилося шляхом відправки пакетів протоколу ICMP на зовнішні (WAN) та внутрішні (LAN) інтерфейси всіх трьох шлюзів. Результати тесту показали повну зв'язність мережі: на кожную серію з 4 надісланих запитів було отримано 4 стабільні відповіді без жодних затримок. Показник втрати пакетів склав 0%. Це експериментально довело, що центральний маршрутизатор WRT300N коректно виконує статичну маршрутизацію трафіку, а технологія трансляції адрес (NAT) на шлюзах працює належним чином, забезпечуючи надійний прохід пакетів між різними сегментами мережі.

Третій етап перевірки підтвердив доступність прикладного рівня управління через протокол HTTP. При введенні в браузері адміністративного ноутбука IP-адрес шлюзів веб-інтерфейс панелі моніторингу (IoT Monitor) відкривався миттєво. У списку підключеного обладнання відображалися всі наявні пристрої відповідної зони з актуальними показниками телеметрії. Адміністратор мав повний доступ до ручного керування актуаторами (відкриття дверей, запуск кавоварки чи зміна швидкості вентилятора), що підтвердило стабільність роботи вбудованих веб-служб на контролерах.

Найбільш наочні та важливі результати були отримані на четвертому етапі під час тестування автоматичних сценаріїв взаємодії. Переведення програми в режим симуляції (Simulation Mode) дозволило покроково відстежити реакцію системи на тригерні події. При штучній активації датчика руху в зоні безпеки на сервер шлюзу миттєво відправлявся пакет даних, після чого сервер автоматично генерував керуючі команди. Сирена миттєво змінювала свій графічний та логічний стан на активний (On), а розумні входні та гаражні двері примусово блокувалися (Lock). Аналогічно відпрацював сценарій клімат-контролю: при штучному підвищенні температури на термостаті вище 25 °C, стельовий

вентилятор автоматично переходив у режим максимальних обертів (High), а розумне вікно відкривалося для провітрювання.

Для узагальнення всіх отриманих практичних результатів та оцінки успішності проведених експериментів сформуємо підсумкову таблицю верифікації сервісів та сценаріїв системи (табл. 3.1).

Таблиця 3.1 - Результати верифікації та тестування функціональних елементів системи

Об'єкт тестування	Використовуваний інструмент / Протокол	Очікуваний інженерний результат	Фактичний результат тестування	Статус тесту
DHCP-сервери шлюзів	DHCP Request / IP	Автоматична видача адрес для 3 ізольованих зон	Адреси успішно отримано без конфліктів у пулах .25.X, .75.X, .125.X	Пройдено
Центральний роутер WRT300N	Утиліта ping / ICMP	Стовідсотковий зв'язок між ноутбуком та шлюзами	Повна доставка пакетів, показник втрат 0% (0% packet loss)	Пройдено
Панель IoT Monitor	Веб-браузер / HTTP	Відображення списку пристроїв та телеметрії	Стабільний віддалений доступ, коректне ручне керування	Пройдено
Сценарій безпеки	Simulation Mode / IoT	Автономне ввімкнення сирени та блокування всіх дверей при русі	Миттєва автоматична активація сирени та закриття дверей і воріт	Пройдено
Сценарій клімату	Simulation Mode / IoT	Автоматичне керування вентилятором та вікном за температурою	Чітке відпрацювання меж 18°C та 25°C в автономному режимі	Пройдено

Таким чином, результати проведеного комплексного тестування повністю довели працездатність, високу швидкість реагування та логічну безпомилковість розробленої моделі «Розумного будинку». Розподілена архітектура мережі забезпечила надійну ізоляцію технологічного трафіку всередині підмереж, але водночас зберегла зручність централізованого моніторингу та управління для

користувача, що підтверджує успішне вирішення всіх поставлених практичних завдань кваліфікаційної роботи.

3.3 Аналіз ефективності системи

На основі результатів комплексного моделювання та тестування, проведених у середовищі Cisco Packet Tracer, було виконано аналіз ефективності розробленої архітектури «Розумного будинку». Оцінка ефективності комп'ютерної системи та мережі інфраструктури IoT базується на трьох ключових інженерних критеріях: продуктивності й швидкості реагування, відмовостійкості структури, а також оптимізації мережевого трафіку та використання смуги пропускання бездротових каналів зв'язку.

Першим важливим аспектом ефективності є швидкість реагування автоматики на тригерні події. Традиційні хмарні рішення Інтернету речей мають суттєвий недолік - затримку поширення сигналу, оскільки пакети даних мають пройти через глобальну мережу Інтернет до віддаленого дата-центру й повернутися назад до виконавчого пристрою. У розробленому проєкті цей етап оптимізовано завдяки концепції граничних обчислень за допомогою локальних шлюзів (Home Gateway). Оскільки сервери обробки даних та інтерпретації логічних умов розміщені безпосередньо всередині технологічних зон, час реакції актуаторів (наприклад, увімкнення сирени при фіксації руху) у режимі симуляції наближається до мінімально можливих значень. Це критично важливо для підсистеми безпеки, де кожна секунда затримки може вплинути на захищеність об'єкта.

Другим і найбільш вагомим інженерним досягненням проєкту є високий рівень відмовостійкості системи, досягнутий завдяки ієрархічній децентралізації та сегментації мережі на три ізольовані бездротові зони (Security_IoT_Zone, Living_IoT_Zone, Power_IoT_Zone). У класичних монолітних мережах вихід з ладу єдиного центрального контролера або штурм широкомовного трафіку призводить до повної зупинки всього розумного будинку. У розробленому рішенні кожен домашній шлюз є повністю автономною бойовою одиницею зі своїм DHCP-сервером та локальною базою правил автоматизації.

Експериментальне відключення одного зі шлюзів у Cisco Packet Tracer підтвердило, що дві інші технологічні зони продовжують функціонувати у штатному режимі. Наприклад, можливе апаратне перевантаження або збій на шлюзі клімат-контролю через велику кількість підключеної побутової техніки жодним чином не впливає на роботу шлюзу охорони периметра. Підсистема безпеки залишається повністю працездатною, продовжуючи фіксувати рух, блокувати двері та вмикати сирену в автономному режимі.

Третій критерій аналізу - це оптимізація мережевого трафіку та захист від завад. Поділ пристроїв за окремими ідентифікаторами бездротової мережі (SSID) дозволив суттєво зменшити щільність радіоефіру та локалізувати службовий трафік (зокрема, DHCP-запити та ARP-пакети) всередині конкретної підмережі. Широкомовні шторми, які часто виникають у великих комп'ютерних мережах через несправність мережевих карт чи зацикленість трафіку, у цій структурі гасяться на рівні LAN-інтерфейсу відповідного шлюзу і не проникають у сусідні підмережі чи магістральний канал центрального маршрутизатора WRT300N. Крім того, використання технології трансляції мережевих адрес (NAT) на кожному шлюзі приховує внутрішню структуру датчиків від магістральної мережі, що значно підвищує рівень кібербезпеки та захищеність системи від потенційних внутрішніх атак чи несанкціонованого перехоплення пакетів телеметрії.

Таким чином, проведений аналіз ефективності наочно доводить переваги обраного підходу. Розроблена комп'ютерна мережа інфраструктури IoT системи «Розумний будинок» демонструє високі показники відмовостійкості, захищеності та швидкодії. Впровадження ієрархічної сегментації та локальних шлюзів дозволило створити збалансовану, масштабовану та повністю автономну систему, яка здатна ефективно вирішувати завдання автоматизації житлового простору без залучення надлишкових обчислювальних чи фінансових ресурсів.

ВИСНОВКИ

У кваліфікаційній роботі було виконано налаштування та дослідження розподіленої системи автоматизації «Розумний будинок» у сучасному імітаційному середовищі Cisco Packet Tracer. Під час аналізу теоретичних основ Інтернету речей та існуючих рішень було виявлено, що головними технічними проблемами сучасних комплексів автоматизації житла є значні затримки при передачі пакетів даних у хмару, висока залежність від стабільності глобального Інтернету, а також ризик повної зупинки системи в разі поломки центрального вузла зв'язку. Для подолання цих недоліків у роботі було обґрунтовано та реалізовано концепцію граничних обчислень, яка передбачає децентралізацію мережі та перенесення логіки управління безпосередньо на локальні домашні шлюзи.

Вибір програмного комплексу Cisco Packet Tracer як базового інструменту розробки дозволив створити повноцінний і точний цифровий двійник системи. Спроектована комп'ютерна мережа інфраструктури IoT об'єднала в єдину систему центральний магістральний маршрутизатор, три автономні шлюзи та десять бездротових інтелектуальних пристроїв, серед яких були використані як датчики, так і виконавчі механізми. Головною особливістю розробленої архітектури став ієрархічний поділ житлового простору на три незалежні підмережі за їхнім функціональним призначенням, а саме: підсистему охорони й безпеки периметра, підсистему мікроклімату та комфорту, а також підсистему відновлюваної енергетики. Конфігурація окремих бездротових зон Wi-Fi зі своїми унікальними ідентифікаторами мережі та розподіл пристроїв за різними IP-діапазонами дозволили повністю ізолювати службовий трафік кожної зони, усунувши проблему колізій та захистивши мережу від широкомовних штормів.

Програмування та впровадження автоматичних сценаріїв роботи обладнання здійснювалося за допомогою створення декларативних правил на вбудованих IoT-серверах домашніх шлюзів. Сценарії безпеки забезпечили миттєве автономне ввімкнення звукової сирени та примусове блокування дверей

у разі фіксації руху, тоді як кліматичні сценарії дозволили автоматично керувати вікном і вентилятором на основі показників кімнатного термостата. Проведене комплексне тестування розробленої моделі в режимах реального часу та симуляції підтвердило стовідсоткову точність роботи алгоритмів, правильність динамічної видачі адрес за протоколом DHCP, а також відсутність втрат пакетів при міжмережевій маршрутизації трафіку.

Аналіз ефективності розробленого інженерного рішення експериментально довів, що розподілена архітектура значно підвищує загальну надійність та відмовостійкість розумного будинку. Завдяки технології трансляції мережевих адрес та повній автономності серверів шлюзів, можливий програмний збій, завади чи апаратне перевантаження в одному сегменті жодним чином не порушують працездатність інших критично важливих зон. Підсистема охорони периметра та підсистема живлення залишаються повністю функціональними, забезпечуючи захист об'єкта. Таким чином, розроблена система повністю виконує поставлені інженерні завдання, демонструючи високу швидкість реагування, безпеку даних, відмовостійкість та зручність моніторингу через веб-інтерфейс.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Choudhary A. Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions // Discover Internet of Things. 2024. Vol. 4. Article 31. DOI: 10.1007/s43926-024-00084-3. URL: https://link.springer.com/article/10.1007/s43926-024-00084-3?utm_source (дата звернення: 18.12.2026)
2. Milenkovic M. Internet of Things: System Reference Architecture. 2022. URL: https://arxiv.org/abs/2204.01872?utm_source (дата звернення: 22.12.2026)
3. Lynn T. G., Endo P. T., Ribeiro A. M. N. C. та ін. The Internet of Things: Definitions, Key Concepts, and Reference Architectures // The Cloud-to-Thing Continuum. Cham : Springer, 2020. P. 1–22. DOI: 10.1007/978-3-030-41110-7_1. URL: https://www.researchgate.net/publication/342744519_The_Internet_of_Things_Definitions_Key_Concepts_and_Reference_Architectures (дата звернення: 25.12.2026)
4. Офіційна документація Cisco Packet Tracer. URL: <https://www.netacad.com/courses/packet-tracer> (дата звернення: 18.05.2026).
5. Введення в інтернет речей (IoT) від Cisco Networking Academy. URL: <https://www.netacad.com/courses/iot> (дата звернення: 22.05.2026).
6. Граничні обчислення (Edge Computing) в архітектурі IoT систем. URL: <https://www.ibm.com/topics/edge-computing> (дата звернення: 25.05.2026).
7. Налаштування DHCP та маршрутизації в мережах Cisco. URL: <https://www.cisco.com/c/en/us/support/index.html> (дата звернення: 01.06.2026).
8. Принципи побудови бездротових мереж Wi-Fi та ізоляції трафіку. URL: <https://www.wi-fi.org/discover-wi-fi> (дата звернення: 03.06.2026).
9. Стандарти безпеки та автоматизації в розумних будинках. URL: <https://csa-iot.org/all-solutions/matter/> (дата звернення: 08.06.2026).