ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Концепція впровадження системи «Розумний будинок» на основі технології IoT»

на здобуття освітнього ступеня магістра
зі спеціальності F6 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Андрій АВРАМЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ здобувача)*

Виконав:
здобувач вищої освіти
гр. ІСДМ-62 _____ Андрій АВРАМЕНКО
(ім'я, ПРІЗВИЩЕ)

Керівник: Валентина ДАНИЛЬЧЕНКО
PhD (доктор філософії) *(ім'я, ПРІЗВИЩЕ)*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій
Ступінь вищої освіти магістр
Спеціальність F6 Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедри ІСТ
_____ Каміла СТОРЧАК
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Авраменка Андрія Юрійовича
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Концепція впровадження системи «Розумний будинок» на основі технології IoT.
керівник кваліфікаційної роботи Валентина ДАНИЛЬЧЕНКО, PhD
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 30 » жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи « 26 » грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
- завдання на кваліфікаційну роботу студента
- наукові статті
- технічна література

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
- Аналіз та огляд предметної області.
- Постановка задачі та методологія дослідження.
- Розробка пропонованого алгоритму та засобів реалізації.
- Реалізація, експериментальні дослідження та результати.

- Перелік ілюстративного матеріалу: презентація на слайдах

6. Дата видачі завдання « 30 » жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Затвердження теми кваліфікаційної роботи, ознайомлення з літературними джерелами та складання плану роботи.	30.10.2025	Викон.
2	Написання 1 розділу кваліфікаційної роботи	10.11.2025	Викон.
3	Написання 2 розділу кваліфікаційної роботи	24.11.2025	Викон.
4	Написання 3 розділу кваліфікаційної роботи	29.11.2025	Викон.
5	Висновки, вступ, реферат	28.11.2025	Викон.
6	Перевірка кваліфікаційної роботи на оригінальність тексту	01.12.2025	Викон.
7	Розробка презентації	12.12.2025	Викон.

Здобувач вищої освіти _____ Андрій Авраменко
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Валентина ДАНИЛЬЧЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 79 стор., 26 рис., 11 джерел.

Мета роботи полягає у розробці алгоритмів управління підсистемами автоматизації, безпеки та клімат-контролю на базі концепції Internet of Things для підвищення комфорту, енергоефективності та безпеки мешканців.

Об’єктом дослідження є інтегровані системи автоматизації житлових об’єктів.

Предметом дослідження виступають алгоритми та методи управління підсистемами «Розумного будинку» і їх практична реалізація в умовах використання технологій IoT.

Практичне значення отриманих результатів полягає у можливості застосування запропонованих алгоритмів та сценаріїв у реальних житлових і промислових об’єктах, з подальшою адаптацією до різних умов експлуатації. Розроблені рішення сприяють підвищенню рівня безпеки, комфорту та енергоефективності, що робить їх актуальними для широкого кола сучасних інженерних систем. Унікальність роботи полягає у комплексному підході до об’єднання підсистем комфорту, безпеки та клімат-контролю в єдину інтелектуальну інфраструктуру, побудовану на основі IoT-технологій. Розроблені алгоритми забезпечують адаптивне управління системами житлових приміщень з урахуванням індивідуальних потреб користувачів та змінних зовнішніх умов.

КЛЮЧОВІ СЛОВА: РОЗУМНИЙ БУДИНОК; АВТОМАТИЗАЦІЯ; INTERNET OF THINGS (IOT); ZIGBEE, HOME ASSISTANT.

ABSTRACT

The text part of the Master's qualification thesis: 79 pages, 26 figures, 11 referencs.

The purpose of this research is to develop algorithms for managing automation, security, and climate-control subsystems based on the Internet of Things (IoT) concept, with the aim of enhancing comfort, energy efficiency, and the overall safety of residents. The study focuses on integrated automation systems for residential buildings, examining algorithms and methods for controlling Smart Home subsystems and their practical implementation within IoT-based environments.

The research addresses modern challenges related to the integration of comfort, security, and climate-management technologies into a unified intelligent infrastructure. Special attention is given to the development of adaptive control algorithms capable of responding to dynamic environmental conditions and individual user preferences. The study also evaluates the potential risks and limitations associated with implementing such systems and proposes approaches to minimize them.

The scientific novelty of the work lies in its comprehensive approach to combining multiple subsystems into a cohesive IoT-driven architecture, enabling efficient monitoring and coordinated operation of residential engineering systems. The practical significance of the results is demonstrated through the possibility of applying the proposed algorithms and control scenarios in real residential and industrial environments, with further adaptation to diverse operational conditions. The developed solutions contribute to increasing the level of safety, comfort, and energy efficiency, making them relevant for modern smart infrastructure applications.

KEYWORDS: SMART HOME; AUTOMATION; INTERNET OF THINGS (IOT); ZIGBEE, HOME ASSISTANT.

ЗМІСТ

ВСТУП

Сучасні вимоги до житлових та адміністративних будівель виходять за межі традиційного уявлення про комфорт та базові умови проживання. Окрім наявності в будівлях електро-, водо- та газопостачання, сучасна людина потребує інтеграції інтелектуальних систем, здатних забезпечити автоматизоване керування житловим простором, контроль за станом інженерних мереж для забезпечення рівню безпеки. Тому ідея «Розумного будинку» отримала широке поширення і стала важливою складовою розвитку IT у житловому та комунальному господарстві.

Будь-яка сучасна будівля складається з комплексу систем, які виконують різні функції: від забезпечення енергопостачання до охорони та інформаційного обслуговування. Із зростанням кількості таких систем та ускладненням їх функціонування управління ними стає більш складним та затратним процесом. Традиційні методи ведення господарства, що передбачали участь обслуговуючого персоналу, сьогодні вже не відповідають сьогоденним вимогам, оскільки не гарантують ефективності та швидкості реагування у непередбачуваних ситуаціях.

Особливе місце в архітектурі «Розумного будинку» займають системи безпеки. До їх складу входять комплекси відеоспостереження, охоронні сигналізації, датчики(руху, присутності, положення) та системи контролю доступу. Завдяки можливості інтеграції з мобільними пристроями користувача забезпечується цілодобовий моніторинг стану об’єкта, що підвищує рівень захищеності та знижує ризики нанесення збитків.

Також, не менш важливим елементом є системи клімат-контролю, які дозволяють підтримувати оптимальні параметри, такі як: температура, вологість повітря. Використання інтелектуальних алгоритмів, що забезпечують адаптацію систем до потреб користувачів створюють комфортні умови для проживання та сприяють енергоефективності.

Окрему групу функцій у системі «Розумний будинок» становлять засоби автоматизації побутових процесів, спрямовані на підвищення комфорту користувачів. Серед них - автоматичне керування освітленням залежно від часу доби, дистанційне та запрограмоване відкривання і закривання штор та жалюзі, інтегроване управління побутовою технікою, мультимедійними пристроями та системами поливу. Такі рішення значно знижують рівень рутинних завдань, які виконує людина, створюють комфортні умови проживання та дозволяють гнучко налаштовувати роботу будинку відповідно до індивідуальних потреб.

Інтеграція підсистем безпеки, відеоспостереження, клімат-контролю та побутової автоматизації в єдину інтелектуальну мережу дозволяє комплексно вирішувати завдання управління будівлею. Це забезпечує ефективний розподіл ресурсів, своєчасне реагування на аварійні ситуації та оптимізацію витрат на експлуатацію. Таким чином, система «Розумний будинок» може розглядатися як універсальне рішення, спрямоване на підвищення рівня безпеки, комфорту та надійності житлових і адміністративних об’єктів.

Актуальність теми. Сучасні тенденції розвитку житлових технологій обумовлюють необхідність створення інтегрованих систем, які забезпечують не лише функціонування будівлі, а й покращення якості життя її мешканців. Зростаючий рівень автоматизації дозволяє реалізовувати управління комплексними процесами: контроль мікроклімату, безпеки, освітлення та побутової техніки. Впровадження таких рішень сприяє підвищенню комфорту та ефективності використання ресурсів, а також дозволяє власникам будинків зменшувати операційні витрати на обслуговування та підтримку інженерних систем.

Особливого значення набуває автоматизація повсякденних побутових процесів. Завдяки сучасним технологіям можна реалізувати дистанційне та програмоване управління шторами, освітленням, мультимедійними пристроями, кухонною технікою та системами поливу. Це дозволяє створювати індивідуальні сценарії використання житла, адаптуючи роботу всіх підсистем під конкретні

потреби мешканців. Такі рішення не лише економлять час, але й підвищують ергономічність та зручність проживання.

Інтеграція систем безпеки і відеоспостереження є одним із ключових аспектів сучасних житлових комплексів. Використання датчиків руху, камер, сигналізацій та контролю доступу у складі єдиної мережі забезпечує постійний моніторинг об’єкта, швидке оповіщення про загрози та можливість дистанційного реагування. Це створює додатковий рівень захисту мешканців та їхнього майна, що є критично важливим у сучасних умовах.

Також актуальним є розвиток систем клімат-контролю, які автоматично регулюють температуру, вологість та якість повітря в приміщеннях, підлаштовуючись під зміну зовнішніх умов та індивідуальні налаштування користувачів. Інтелектуальні алгоритми управління дозволяють збалансувати комфорт і енергоефективність, мінімізуючи витрати на енергоресурси.

У зв’язку з цим проведення досліджень щодо розробки алгоритмів інтеграції підсистем автоматизації, безпеки та клімат-контролю у житлові об’єкти з використанням технології Internet of Things є актуальним і дозволяє підвищити ефективність функціонування сучасних «Розумних будинків». Такі дослідження сприяють створенню гнучких і адаптивних систем, здатних забезпечувати комплексний контроль та управління будівлею, підвищуючи рівень комфорту, безпеки та енергоефективності.

Об’єкт дослідження - інтегровані системи автоматизації житлових об’єктів.

Предмет дослідження - алгоритми та методи управління підсистемами «Розумного будинку» та їх практична реалізація.

Мета роботи полягає у розробці алгоритмів управління підсистемами автоматизації, безпеки та клімат-контролю на базі концепції IoT для підвищення комфорту і безпеки мешканців.

Для виконання поставленої мети необхідно вирішення таких завдань:

- дослідження сучасних методів автоматизації побутових і кліматичних систем;
- провести аналіз інтеграції систем безпеки та відеоспостереження у житлові приміщення;
- розробити алгоритми управління системами кондиціонування та опалення;
- визначити принципи побудови єдиної мережі підсистем із використанням технології IoT;
- оцінити потенційні ризики та способи їх мінімізації при реалізації інтегрованих систем.

Наукова унікальність полягає у комплексному підході до інтеграції систем комфорту, безпеки та клімат-контролю у житлових приміщеннях із застосуванням технологій IoT.

Практичне значення полягає у застосуванні розроблених алгоритмів та сценаріїв для впровадження у реальні житлові та промислові об’єкти, з перспективою адаптації під різні умови експлуатації.

РОЗДІЛ 1 Теоретичні основи створення систем «Розумний будинок»

1.1 Основні терміни та історія розвитку систем автоматизованого управління будинком

Ідея «розумного будинку» виникла у 1970-х роках і мала на меті не лише економію електроенергії, а й підвищення комфорту проживання та безпеки мешканців. На початковому етапі система складалася з різних датчиків - руху, освітленості, температури, що дозволяло автоматично регулювати вмикання освітлення та роботу побутових приладів залежно від присутності людей і умов у приміщенні. Згодом концепція розширилася: з'явилися можливості дистанційного керування пристроями та інтеграції різних підсистем в єдину мережу.

Сучасний розумний будинок - це високотехнологічний житловий простір, що забезпечує зручність, безпеку та енергоефективність. Його електронні системи інтегруються в централізовану платформу, яка дозволяє координувати роботу освітлення, клімат-контролю, безпеки, аудіо- та відеосистем, а також мережевих пристроїв. Така інтеграція спрощує управління всіма системами, забезпечує віддалений контроль і адаптацію до індивідуальних потреб мешканців.

Поняття «розумного будинку» було сформульовано Інститутом інтелектуальної будівлі у Вашингтоні у 1970-х: «Будівля, здатна адаптуватися до потреб користувачів та ефективно управляти ресурсами». Першими практичними прикладами стали інтелектуальні будівлі (Intelligent Buildings), де застосовувалися структуровані кабельні мережі, що дозволяли об'єднувати системи зв'язку, безпеки та обліку енергії. Згодом з'явилися мультиплексні технології передачі даних, які дозволяли передавати різну інформацію через один канал одночасно.

Інтерес до розробки інтелектуальних будинків зростав, і вже у 1978 році компанії X10 USA та Leviton запропонували перші рішення для управління

побутовими приладами через електромережу, проте вони були адаптовані для специфіки США і не прижилися у Європі.

Сучасні системи «розумного будинку» виходять за рамки окремих пристроїв і включають комплексну інтеграцію життєзабезпечення, управління кліматом, безпекою та енергетичними ресурсами. Основна відмінність інтелектуальної будівлі полягає в тому, що підсистеми різних виробників працюють як єдиний керований комплекс, здатний реагувати на зміни у навколишньому середовищі та стані будівлі.

«Розумний будинок» (Intelligent Building) передбачає адаптацію до конкретних подій та сценаріїв: система може керувати поведінкою окремих підсистем на основі попередньо заданих алгоритмів. Термін intelligent означає «розумний» та «адаптивний», підкреслюючи здатність будівлі до самостійного управління.

Сучасні проєкти передбачають можливість інтеграції штучного інтелекту для аналізу даних з усіх сенсорів і систем будівлі, що дозволяє автоматично оптимізувати використання ресурсів та підвищувати комфорт мешканців. Системи розумного будинку здатні прогнозувати потреби, адаптувати роботу клімату та освітлення, реагувати на небезпечні ситуації та забезпечувати віддалене управління через мобільні додатки чи веб-інтерфейси.

Під поняттям «розумний будинок» зазвичай мається на увазі інтегроване управління різними інженерними та побутовими системами в єдиній платформі, серед яких:

- клімат-контроль який включає: опалення, вентиляцію та кондиціонування;
- освітлення та управління шторами і жалюзі;
- безпеку (охоронна та пожежна сигналізація, контроль доступу, відеоспостереження);
- комунікаційні системи (Інтернет, телефонія, локальна комп’ютерна мережа);

- електропостачання (резервні джерела, захист від перевантажень, управління освітленням);
- водопостачання та водовідведення;
- додаткові системи за потребою.

Усі ці функції можуть контролюватися як безпосередньо в будинку, так і через віддалений доступ. Наприклад, мешканець може відчиняти або зачиняти двері та вікна дистанційно, вимикати всі світильники однією командою або прокидатися під улюблену музику та з готовим до використання чайником чи кавоваркою. При виїзді з гаражу брама автоматично відкривається за голосовою командою, а після від'їзду система безпеки активується, блокуючи двері. Розумний будинок також здатний запускати полив газону залежно від погодних умов, отриманих з Інтернету.

Незважаючи на високу технологічність, система «розумного будинку» залишається інтуїтивно зрозумілою та простою у використанні, дозволяючи кожному члену родини ефективно користуватися її можливостями. У майбутньому розумні будинки, ймовірно, стануть настільки ж звичними, як і побутові прилади, а на сьогодні близько половини нових будинків у США вже оснащені подібними системами.

Сучасні системи управління будинком часто інтегрують інтелектуальні помічники, наприклад, Apple HomePod (Рис. 1.1) або Samsung SmartThings (Рис. 1.2), які забезпечують зручне голосове управління різними пристроями. Хоча спершу такі технології можуть здаватися незвичними, їх популярність зростає завдяки простоті використання та високій ефективності контролю. Саме тому інтелектуальні помічники часто стають першою автоматизацією, яку споживачі впроваджують у свої будинки.

Рис. 1.1 – Акустична система Apple HomePod з функцією голосового помічника

Рис. 1.2 – Інтерфейс системи Samsung Smart Things

Виробники обладнання для розумного будинку швидко інтегрують свої пристрої з голосовими помічниками, дозволяючи управляти освітленням, мультимедіа, кліматичними системами та іншими підсистемами будинку. Найбільш активно такі системи використовуються у кухні та вітальні, де зручно керувати побутовими приладами та медіа через голосові команди.

Система керування мікрокліматом (Рис. 1.3) забезпечує всебічний контроль над інженерними системами будинку, які визначають якість повітря, його температуру та вологість.

До складу системи мікроклімату входять:

1. вентиляційні установки;

2. кондиціонери повітря;
3. зволожувачі повітря;
4. система теплої підлоги;
5. опалювальні прилади.

Завдяки поєднанню роботи опалення, теплої підлоги, вентиляції та кондиціонування система здатна оптимально регулювати умови в приміщенні. Вона самостійно обирає найбільш ефективний режим роботи кожного елементу, керуючись принципом економії ресурсів, часу та коштів.

Система забезпечує комфортну атмосферу, адаптовану під потреби мешканців. Здорове, свіже повітря та оптимальна температура створюють сприятливе середовище для відпочинку та продуктивної діяльності. Саме тому автоматичне регулювання мікроклімату є важливою складовою сучасного житлового простору.

Рис. 1.3 – Панель керування кліматом

Система управління освітленням (Рис. 1.4) дає змогу автоматизовано вмикати, вимикати та регулювати яскравість різних світлових джерел у квартирі чи будинку відповідно до заздалегідь заданих сценаріїв. Вона забезпечує зручне керування групами світла за таймером, сигналами датчиків руху або рівня освітленості. Інтелектуальне регулювання світла дозволяє ефективно використовувати електроенергію, скорочуючи споживання на 10–40% і продовжуючи термін служби ламп.

Освітлювальні прилади в приміщенні можуть включати не лише природне світло, люстри чи бра, а й спеціальні світлові елементи, які створюють підсвічування певних зон. Такі акценти дозволяють по-новому сприймати простір, підкреслити дизайнерські рішення та реалізувати ефектні архітектурні ідеї.

Рис. 1.4 – Інтерфейс керування системою освітлення

Система безпеки може охоплювати не тільки всі приміщення будівлі, а й прилеглі території. Контроль периметра здійснюється за допомогою спеціальних датчиків та камер відеоспостереження. Інші сенсори та контролери забезпечують безпеку всередині будівлі. У разі несанкціонованого доступу або виникнення аварійної ситуації система відстежує події через сигнали датчиків (наприклад, відкриття дверей, пошкодження вікна, задимлення або зміни об’єму

у приміщенні) та сповіщає відповідальні служби і власника (через SMS, push-повідомлення або e-mail). Доступний також віддалений моніторинг із переглядом відеозаписів через Інтернет.

Система безпеки має декілька режимів роботи: максимальний - за відсутності мешканців; помірний - у нічний час; звичайний - у денний час.

Об’єднання комп’ютерів і пристроїв у локальну мережу (LAN) дозволяє створити єдину інформаційну платформу всередині будівлі, що забезпечує швидкий і стабільний обмін даними між сенсорами, камерами, контролерами і серверами. Для віддаленого доступу та інтеграції з хмарними сервісами застосовується глобальна мережа (WAN), через яку можна контролювати всі підсистеми будинку навіть поза межами приміщення.

Система телефонії і комунікацій забезпечує інтеграцію аудіо- та відеосигналів, виконуючи функції інтеркому та домофону.

Серед найпопулярніших компонентів сучасних систем «Розумного будинку» - смарт-термостати, охоронні системи, «розумні» лампочки, мережеві камери та аудіосистеми для декількох зон. Управління такою системою здійснюється через локальну LAN або через WAN-з’єднання з мобільним пристроєм чи веб-інтерфейсом. Центр керування може підключатися до Інтернету та хмарного сервісу постачальника обладнання, що спрощує налаштування і взаємодію з усіма підсистемами.

Отже, сучасний «Розумний будинок» - це інтегрована інтелектуальна система, яка об’єднує всі інженерні та життєзабезпечувальні підсистеми. До її основних складових належать:

1. Контролер управління системою;
2. Джерела даних про стан системи – різні сенсори;
3. Виконавчі пристрої (замки, відеокамери тощо);
4. Мережа зв’язку LAN і WAN, що об’єднує всі компоненти і забезпечує віддалений контроль.

1.2 Порівняльний аналіз сучасних рішень для систем типу «Розумний будинок»

У сучасних умовах ринок систем «розумного дому» представлений широким спектром технологічних рішень. Кожна з платформ має власні переваги та недоліки, що зумовлює необхідність комплексного аналізу їх сильних і слабких сторін. До найбільш поширених та актуальних рішень належать:

- Home Assistant;
- LG ThinQ ON / Hub;
- Amazon Echo;
- OpenHAB;
- Apple HomeKit / Netatmo;
- Homey;
- Google Home;
- Xiaomi Mi Home.

Ефективна система «розумного будинку» передбачає дотримання таких головних критеріїв:

- доступна для користувача ціна;
- можливість додавання іншого обладнання для розширення функціоналу системи;
- інтерфейс, адаптований до потреб клієнта;
- підтримка обладнання різних виробників;
- використання безкоштовного програмного забезпечення;
- підтримка широкого пулу протоколів взаємодії компонентів;
- наявність спеціальних можливостей для користувачів з особливими потребами;
- добре організована технічна підтримка.

Home Assistant (Рис. 1.5) є однією з найбільш розповсюджених open-source платформ для побудови систем «розумного дому». Платформа

характеризується високою гнучкістю та модульністю, забезпечує підтримку інтеграції з великою кількістю пристроїв різних виробників, а також сумісність із сучасними протоколами, такими як Zigbee, Z-Wave, MQTT, Thread тощо. Завдяки відкритій архітектурі програмного забезпечення користувач має можливість створювати індивідуальні сценарії автоматизації та адаптувати інтерфейс до власних потреб. Система не обмежується певним брендом обладнання та дозволяє масштабувати інфраструктуру залежно від вимог користувача.

Переваги:

- підтримка великої кількості пристроїв різних виробників, які можуть бути пов’язані між собою;
- модульність та масштабованість.

Недоліки:

- складність початкового налаштування;
- необхідність базових технічних знань для ефективної експлуатації;
- відсутність офіційної служби підтримки, орієнтація переважно на спільноту користувачів.

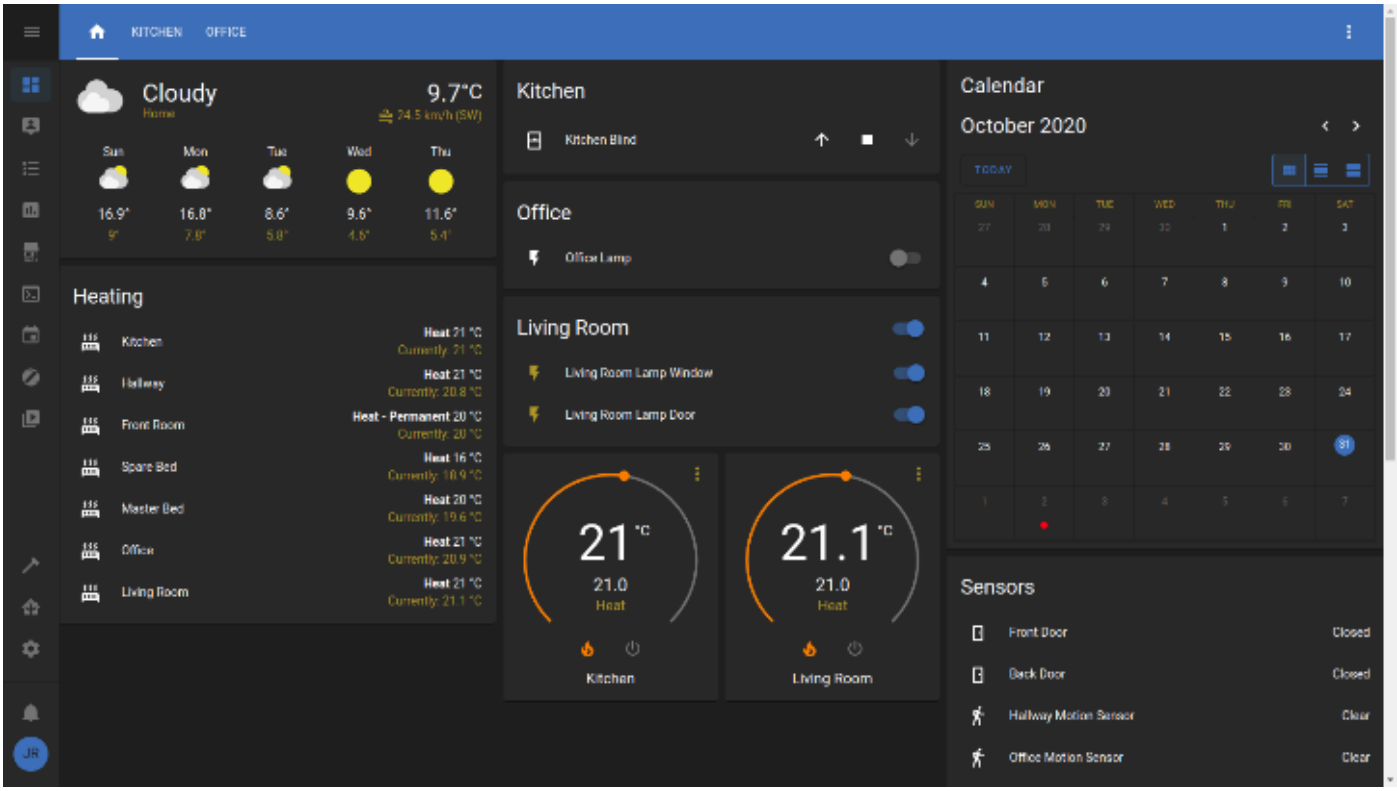


Рис. 1.5 – Інтерфейс платформи Home Assistant

LG ThinQ ON / Hub (Рис. 1.6) є універсальним рішенням для централізованого керування «розумним домом» від компанії LG. Система орієнтована на інтеграцію широкого кола побутової техніки та підтримує стандарти Matter, Zigbee та Thread. Особлива увага приділяється простоті інтерфейсу та зручності використання для кінцевого користувача.

Переваги:

- активна технічна підтримка;
- сумісність з пристроями сторонніх виробників;
- простота налаштувань;
- підтримка сучасних стандартів інтеграції.

Недоліки:

- часткова орієнтація на обладнання LG;
- відносна закритість екосистеми;
- обмежені можливості кастомізації.

Рис. 1.6 – LG Smart Think ON AI

Amazon Echo (Рис. 1.7) є однією з найпопулярніших комерційних платформ, що працює на основі голосового асистента Alexa. Платформа підтримує інтеграцію з великою кількістю пристроїв та має широкий вибір готових навичок (skills) для розширення функціоналу системи.

Переваги:

- сумісність із різними пристроями;
- зручне голосове керування;
- велика кількість інтеграцій та сценаріїв автоматизації;
- стабільна робота через хмарну інфраструктуру Amazon.

Недоліки:

- залежність від Інтернет-з’єднання;
- обмежені можливості локального управління;
- прив’язаність до екосистеми Amazon.

Рис. 1.7 – Акустична система Amazon Echo

OpenHAB (Рис. 1.8) є open-source платформою для побудови систем «розумного дому», що забезпечує високу гнучкість та універсальність. Система підтримує інтеграцію з багатьма пристроями та протоколами і дозволяє створювати складні сценарії автоматизації.

Переваги:

- відкритий код та гнучке налаштування;
- підтримка великої кількості пристроїв і протоколів;
- можливість створення складних сценаріїв автоматизації;
- незалежність від конкретного виробника.

Недоліки:

- складність початкового налаштування;
- потреба у технічних знаннях;

- відсутність офіційної служби підтримки.

Рис. 1.8 – Інтерфейс платформи OpenHAB

Apple HomeKit (Рис. 1.9) у поєднанні з пристроями Netatmo забезпечує безпечне та конфіденційне зберігання даних. Система інтегрується з сертифікованими пристроями та забезпечує стабільну роботу через мобільний додаток Home та голосового асистента Siri.

Переваги:

- високий рівень безпеки та конфіденційності;
- стабільна робота з сертифікованими пристроями;
- зручне керування через Siri та додаток Home;
- підтримка сценаріїв автоматизації.

Недоліки:

- висока вартість сумісного обладнання;
- обмежений вибір пристроїв;
- закрита екосистема з обмеженою кастомізацією.

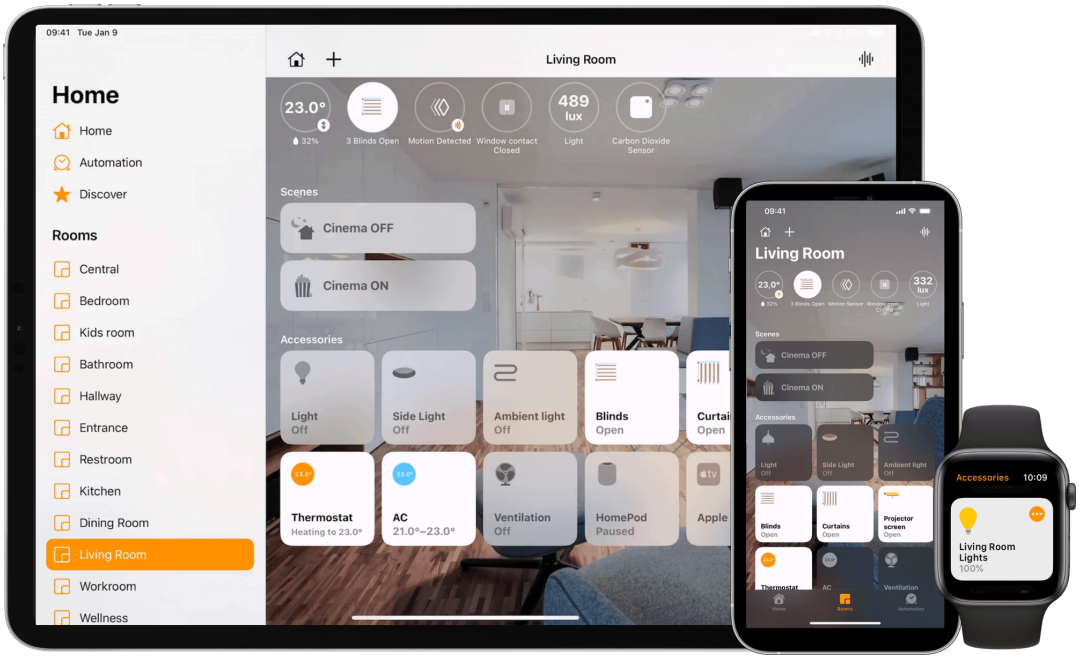


Рис. 1.9 – Інтерфейс платформи Apple HomeKit

Homey (Рис. 1.10) є комерційною платформою, що поєднує простоту використання та широкі можливості інтеграції. Система підтримує численні пристрої та протоколи, має зручний інтерфейс і мобільний додаток для керування.

Переваги:

- підтримка великої кількості пристроїв і протоколів;
- інтуїтивно зрозумілий інтерфейс;
- масштабованість та адаптивність;
- наявність офіційної технічної підтримки.

Недоліки:

- висока вартість платформи та модулів;
- деякі функції доступні лише за передплатою;
- частина сценаріїв складніша для налаштування новачком.

Рис. 1.10 – Контролер розумного будинку Athom Homey Pro

Google Home (Рис. 1.11) інтегрується з сервісами Google та підтримує голосове керування через Google Assistant. Платформа сумісна з багатьма пристроями сторонніх виробників та дозволяє автоматизувати більшість побутових процесів.

Переваги:

- багато сумісних пристроїв;
- потужний голосовий асистент;
- зручна інтеграція з сервісами Google;
- інтуїтивно зрозумілий інтерфейс.

Недоліки:

- залежність від хмарних сервісів;
- обмежена можливість локального управління;
- ризики для конфіденційності даних.

Рис. 1.11 – Розумна колонка Google Home

Mi Home (Рис. 1.12) є платформою для побудови «розумного дому» від компанії Xiaomi. Система поєднує доступність пристроїв із широким вибором продукції власного виробництва. Інтеграція здійснюється через мобільний додаток, а управління можливе як вручну, так і за допомогою сценаріїв автоматизації.

Переваги:

- доступна ціна обладнання;
- широкий асортимент пристроїв власного виробництва;
- підтримка протоколів Zigbee та Wi-Fi;
- зручний мобільний додаток для керування.

Недоліки:

- залежність від хмарної інфраструктури;
- обмежена сумісність із пристроями сторонніх виробників;
- ризики щодо конфіденційності даних.

Рис. 1.12 – Інтерфейс додатку Mi Home

Таблиця 1.1 Порівняння готових апаратно-програмних рішень

Критерій	Home Assistant	LG ThinQ ON	OpenHAB	Apple HomeKit	Google Home	Mi Home

Цінова доступність	Висока	Середня	Висока	Низька	Середня	Висока
Модульність	Висока	Середня	Висока	Середня	Середня	Середня
Масштабованість	Висока	Висока	Висока	Середня	Висока	Середня
Підтримка протоколів	Zigbee, Z-Wave, MQTT, Thread та інші	Matter, Zigbee, Thread	Zigbee, Z-Wave, MQTT, HTTP та інші	Wi-Fi, Thread, Matter	Wi-Fi, Thread, Zigbee (через хаби)	Zigbee, Wi-Fi
Підтримка обладнання різних виробників	Широка	Середня	Широка	Обмежена	Висока	Обмежена
Інтуїтивність інтерфейсу	Середня (залежить від налаштувань)	Висока	Середня	Висока	Висока	Висока
Адаптивність під користувача	Висока	Середня	Висока	Середня	Середня	Середня
Технічна підтримка / ком'юніті	Спільнота	Офіційна підтримка	Спільнота	Офіційна підтримка	Офіційна + спільнота	Офіційна
Відкритість	Повністю відкрита	Частково відкрита	Повністю відкрита	Закрита	Частково	Частково

1.3 Підсистеми комфорту у системах «Розумного будинку»

Підсистеми комфорту є ключовим елементом сучасних систем домашньої автоматизації, спрямованим на створення зручного, безпечного та енергоефективного житлового середовища. Вони забезпечують автоматичне керування кліматом, освітленням, мультимедійними пристроями та іншими елементами побутової інфраструктури, дозволяючи користувачеві оптимізувати умови проживання та зменшити навантаження на ручне управління системою.

Підсистема клімат-контролю є однією з ключових складових розумного будинку, що забезпечує підтримку комфортного мікроклімату в приміщеннях шляхом регулювання температури, вологості та якості повітря. Вона інтегрує різноманітні датчики, зокрема сенсори температури, вологості та рівня CO_2, що дозволяють отримувати точні дані про стан середовища в режимі реального часу. На основі цих показників система автоматично управляє опалювальними приладами, кондиціонерами, вентиляційними установками та іноді зволожувачами чи осушувачами повітря.

Завдяки інтеграції з платформами домашньої автоматизації користувач отримує можливість не лише підтримувати комфортні параметри, а й формувати індивідуальні сценарії клімат-контролю для різних зон приміщення або часу доби. Система дозволяє оптимізувати споживання енергії, запобігати утворенню цвілі чи надмірної сухості повітря, а також підвищувати загальний рівень комфорту та безпеки для мешканців.

Приклади пристроїв та їх функціонал:

Nest Learning Thermostat, Netatmo Smart Thermostat - автоматичне регулювання температури залежно від присутності людей і часу доби, можливість навчання звичок користувачів, дистанційне керування через додаток або голосові асистенти.

Розумні кондиціонери LG ThinQ, Daikin Altherma - дистанційне включення та вимикання, регулювання температури та швидкості обдуву, інтеграція з іншими пристроями для сценаріїв автоматизації.

Xiaomi Mi Temperature & Humidity Sensor - моніторинг температури та вологості, сповіщення при відхиленні від нормальних параметрів, інтеграція з опаленням і кондиціонерами.

Системи типу Home Assistant, OpenHAB та Homey дозволяють формувати автоматизовані сценарії, які враховують погодні умови, час доби та присутність людей у приміщенні, підвищуючи ефективність енергоспоживання та комфорт користувача.

Сучасні підсистеми освітлення є важливою складовою інтелектуального будинку і забезпечують не лише базове освітлення приміщень, а й гнучке управління яскравістю та колірною температурою світла залежно від потреб користувача або заданих сценаріїв. Вони інтегрують розумні лампи, світильники, димери та контролери, які дозволяють змінювати освітлення

автоматично відповідно до часу доби, присутності людей у приміщенні, зовнішнього освітлення або індивідуальних налаштувань.

Завдяки підключенню до платформ домашньої автоматизації користувач отримує можливість створювати комплексні сценарії освітлення, наприклад, «ранкове пробудження», «робочий режим» або «кінотеатр», а також інтегрувати підсистему з іншими компонентами будинку, такими як датчики руху, підсистема клімат-контролю або безпеки. Це дозволяє забезпечити не лише комфорт та ергономіку, а й оптимізувати енергоспоживання, підвищуючи ефективність та екологічність експлуатації системи.

Приклади пристроїв та функції:

Philips Hue, Yeelight, Xiaomi Mi LED Smart Bulb - регулювання яскравості та кольору світла, створення світлових сцен, дистанційне керування через додаток або голосові команди.

Fibaro Motion Sensor, Aqara Motion Sensor - виявлення присутності людей у кімнаті, автоматичне вмикання та вимикання світла, моніторинг освітленості.

Розумні вимикачі Sonoff, Livolo, Aqara - вмикання та вимикання освітлення, інтеграція зі сценаріями «ранок», «вечір», «відсутність вдома».

Підсистема мультимедіа забезпечує централізоване управління аудіо- та відеосистемами, інтегруючи їх в єдину екосистему керування. Вона дозволяє координувати роботу телевізорів, медіаплеєрів, музичних колонок, проекторів та інших мультимедійних пристроїв, забезпечуючи синхронізацію відтворення контенту у різних приміщеннях та автоматизацію сценаріїв на основі потреб користувача.

Завдяки підключенню до платформ домашньої автоматизації користувач може налаштовувати відтворення музики, фільмів або інших медіафайлів відповідно до часу доби, присутності мешканців або попередньо заданих

сценаріїв, наприклад, «вечірній перегляд», «музика під час готування» чи «фонове аудіо в робочому кабінеті». Підсистема мультимедіа також дозволяє інтегрувати голосове управління, дистанційний контроль через мобільні додатки та синхронізацію з іншими підсистемами будинку, такими як освітлення та клімат-контроль, підвищуючи загальний рівень комфорту та ергономічності.

Приклади пристроїв та функціонал:

Amazon Echo, Google Nest Audio, Apple HomePod - відтворення музики, керування голосом, інтеграція з іншими підсистемами.

Системи мультирум Sonos, Bose SoundTouch - синхронізація музики в різних кімнатах, централізоване управління через додаток.

Медіаплеєри та смарт-телевізори - інтеграція з платформами Home Assistant, Homey для автоматизації відтворення контенту.

Підсистема автоматичного регулювання жалюзі та штор забезпечує ефективне використання природного освітлення, контроль інсоляції та підтримку конфіденційності у приміщенні. Вона інтегрує електричні приводи, сенсори освітленості та системи управління в єдину платформу автоматизації, що дозволяє налаштовувати положення жалюзі чи штор залежно від часу доби, рівня природного світла або попередньо заданих сценаріїв.

Завдяки інтеграції з іншими підсистемами інтелектуального будинку користувач може реалізовувати комплексні сценарії, наприклад, автоматичне підняття штор уранці для природного пробудження, затемнення приміщення під час перегляду фільмів або повне закриття в денний час для підтримки приватності. Підсистема також дозволяє дистанційне управління через мобільні додатки, синхронізацію з освітленням та клімат-контролем, що підвищує комфорт, енергетичну ефективність та ергономіку житлового простору.

Приклади пристроїв та функціонал:

Somfy, IKEA FYRTUR, Aqara Smart Curtain - дистанційне відкриття та закриття штор, інтеграція зі сценаріями клімат-контролю та освітлення.

Lutron Serena, Xiaomi Aqara Roller Shade - автоматизація за розкладом або сенсорами освітленості.

Деякі сучасні системи інтелектуального будинку забезпечують контроль рівня вологості повітря та інтеграцію пристроїв для ароматизації, що дозволяє створювати додатковий рівень комфорту і підвищувати якість мікроклімату у приміщенні. Підсистема включає датчики вологості, зволожувачі та осушувачі повітря, а також пристрої для розпилення ароматизаторів або ефірних олій, які інтегруються в платформу управління будинком.

На основі даних сенсорів система автоматично регулює роботу зволожувачів і осушувачів для підтримки оптимальної вологості, що запобігає надмірній сухості або вологості повітря. Ароматизація повітря може бути налаштована за сценаріями, наприклад, під час вечірнього відпочинку, прийому гостей або у робочих зонах для підвищення концентрації. Завдяки інтеграції з іншими підсистемами, такими як клімат-контроль і освітлення, користувач отримує можливість створювати комплексні сценарії, що забезпечують максимальний комфорт, ергономіку та персоналізацію простору.

Приклади пристроїв та функції:

Xiaomi Mi Smart Air Purifier, Dyson Pure Cool - очищення та зволоження повітря, контроль якості повітря через додаток.

Aqara Smart Aroma Diffuser, Stadler Form Jasmine - дистанційне управління ароматизацією, інтеграція зі сценаріями «ранок», «вечір».

Підсистеми комфорту дозволяють реалізовувати комплексні сценарії автоматизації:

1. «Ранковий сценарій» - відкриття штор, увімкнення світла та запуск побутової техніки (кавоварка, мультиварка).

2. «Вечірній сценарій» - зниження освітлення, закриття жалюзі та регулювання температури.

Сучасні підсистеми комфорту взаємодіють із системами управління енергоспоживання та безпеки, що дозволяє автоматично вимикати світло та опалення при відсутності мешканців.

Таким чином, підсистеми комфорту є невід'ємною складовою «розумних будинків», поєднуючи різні гаджети й технології в єдину екосистему, що робить дім безпечним та економним у використанні енергії.

1.4 Підсистеми безпеки інтегровані в систему «Розумний будинок»

Підсистеми безпеки є невід'ємною складовою розумних будинків, забезпечуючи комплексний захист житлового середовища, контроль доступу та попередження небезпечних ситуацій. Вони інтегрують різноманітні датчики, контролери, відеокамери та виконавчі пристрої, з'єднані в одну систему, завдяки чому можна стежити за всім і керувати дистанційно в режимі реального часу.

Системи відеоспостереження забезпечують контроль як зовнішніх, так і внутрішніх зон будинку, фіксують події та дозволяють зберігати архівні записи для подальшого аналізу. Сучасні IP-камери, такі як Xiaomi Mi Home, Arlo або Nest Cam, підтримують високу якість відеозйомки у денний і нічний час, детекцію руху та можливість запису відео. Вбудовані мікрофони та динаміки дозволяють вести двосторонній аудіозв'язок із приміщеннями або зовнішньою територією. Завдяки віддаленому доступу користувач може переглядати відеопотік у режимі реального часу та зберігати записи на центральному сервері або у хмарному сховищі.

Датчики руху та проникнення виконують функцію виявлення несанкціонованого доступу та сповіщення про загрозу. Fibaro Motion Sensor, Aqara Motion Sensor та інші подібні пристрої реагують на рух у кімнаті та

автоматично вмикають світло або запускають сигналізацію. Сенсори відкриття дверей і вікон (Xiaomi, SmartThings чи Netatmo) миттєво інформують користувача про порушення периметру будинку. Під'єднавши ці датчики й сенсори до головного контролера, можна налаштувати автоматичні сценарії безпеки — наприклад, увімкнення сирени, блокування дверей чи надсилання повідомлень на телефон власника.

Сигналізаційні пристрої відіграють ключову роль у попередженні мешканців та охоронних служб про аварійні ситуації, включаючи вторгнення, пожежу, витік газу або води. Розумні сирени Ring, SmartThings або Nest Protect сповіщають про небезпеку звуковим та світловим сигналом. Датчики диму, чадного газу та витоку води від виробників Xiaomi, Fibaro та Netatmo дозволяють віддалено контролювати критичні параметри і активувати захисні сценарії системи. Виконавчі пристрої, такі як реле та розумні замки Yale, Nuki або Aqara Smart Lock, забезпечують автоматичне блокування дверей або активацію сигналізації при виникненні загрози.

Контроль доступу у сучасних системах безпеки дозволяє централізовано керувати правами мешканців та гостей, вести журнал подій і застосовувати біометричні рішення. Розумні замки та біометричні сенсори надають можливість дистанційного відкриття та закриття дверей, а також обмеження доступу до окремих зон будинку.

Підсистеми безпеки також включають контроль за аварійними ситуаціями, такими як витік газу, протікання води чи пожежа. Датчики диму та чадного газу Nest Protect або Xiaomi Aqara Smoke Sensor забезпечують миттєве сповіщення та інтеграцію із сиренами, водяними клапанами або замками для своєчасного реагування. Датчики витоку води Fibaro Flood Sensor та Aqara Water Leak Sensor дозволяють запобігти затопленню, активуючи перекриття водопостачання та надсилання сповіщень власнику.

Інтеграція підсистем безпеки з іншими компонентами інтелектуального будинку, зокрема з підсистемами комфорту та енергоменеджменту, дозволяє формувати комплексні сценарії автоматизації. Наприклад, система може одночасно вимкнути електроприлади, активувати освітлення та заблокувати двері при спрацюванні датчика вторгнення, підвищуючи ефективність захисту та швидкість реагування на загрози. Таким чином, підсистеми безпеки забезпечують цілісну інтегровану систему захисту житлового середовища, яка гарантує комфорт, безпеку та контроль за всіма критично важливими процесами у будинку.

Висновок до розділу 1

Високотехнологічні системи «розумний дім» демонструють постійне зростання популярності завдяки можливості централізованого та інтуїтивного управління інженерними системами будівлі через мобільні додатки, ефективному використанню ресурсів завдяки автоматизації контролю та налаштуванню індивідуальних режимів споживання. Впровадження таких систем забезпечує підвищення рівня комфорту та безпеки мешканців, оптимізацію енергоспоживання та скорочення часу та зусиль, необхідних для управління різними пристроями.

Проведений огляд існуючих готових рішень для організації роботи систем «розумний дім» дозволив виявити їх основні переваги, а також визначити ключові обмеження та проблемні аспекти. Аналіз сучасних методів реалізації показав, що найбільшою увагою потребують підсистеми управління та контролю процесів, а також ефективність передачі даних між датчиками і виконавчими пристроями, що є критично важливим для надійного функціонування інтегрованої екосистеми.

РОЗДІЛ 2 Дослідження застосування технології Internet of Things у проектах «Розумний будинок»

2.1 Особливості використання технології Internet of Things

Інтернет речей (IoT) — одна з ключових концепцій сучасних технологій, яка вже перестала бути лише теорією та активно використовується у різних сферах життя.

У загальному розумінні IoT - це технологічна парадигма, що забезпечує можливість взаємодії фізичних об’єктів («речей») між собою та з навколишнім середовищем без безпосереднього втручання людини. Така взаємодія здійснюється завдяки об’єднанню пристроїв у єдину мережу, що забезпечує обмін інформацією та координацію дій у реальному часі.

Основу функціонування Інтернету речей становлять шість базових принципів:

Anytime, Any Contact (Будь-коли, будь-який контакт) - передбачає безперервну доступність мережі та можливість обміну даними у будь-який час, що забезпечує постійну взаємодію між об’єктами;

Anything, Any Device (Будь-що, будь-який пристрій) - передбачає підключення до мережі будь-яких фізичних об’єктів або пристроїв, незалежно від їх типу, конструкції чи призначення;

Anyone, Anybody (Будь-хто, будь-який користувач) - забезпечує участь у процесі взаємодії будь-якої особи або користувача системи, незалежно від його місцезнаходження чи статусу;

Any Service, Any Business (Будь-яка послуга, будь-який бізнес) - охоплює можливість інтеграції різних сервісів, галузей та бізнес-моделей у межах єдиної цифрової екосистеми;

Any Path, Any Network (Будь-який шлях, будь-яка мережа) - гарантує передачу інформації через різноманітні мережеві інфраструктури, використовуючи різні комунікаційні канали та протоколи;

Any Place, Anywhere (Будь-де, у будь-якому місці) - забезпечує функціонування IoT-систем незалежно від географічного положення пристроїв або користувачів, створюючи глобальне мережеве середовище.

У сукупності ці принципи формують основу концепції Інтернету речей, що забезпечує універсальність, мобільність, масштабованість та інтеграцію цифрових і фізичних систем у єдину інформаційну інфраструктуру (Рис. 2.1).

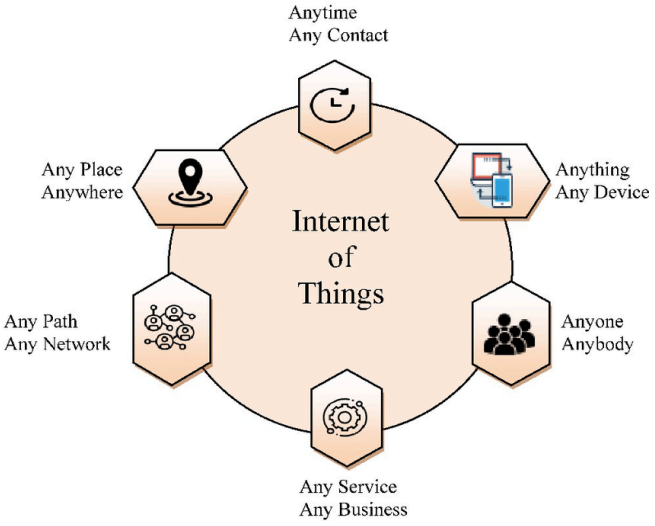


Рис. 2.1 – Принцип IoT

Класична архітектура Інтернету речей (IoT) складається з кількох основних компонентів, що забезпечують повний цикл збору, передавання, оброблення та представлення даних.

IoT-пристрої - це фізичні елементи системи, оснащені сенсорами та виконавчими механізмами, які збирають дані з навколишнього середовища й можуть здійснювати певні дії у відповідь. Такі пристрої бувають персональними, мобільними або вбудованими в різноманітне обладнання.

Шлюзи (Gateways) - проміжна ланка між пристроями та сервером, що приймає дані від сенсорів і передає їм керівні команди. Вони можуть бути

реалізовані у вигляді апаратних маршрутизаторів або програмних рішень, що підтримують різні комунікаційні протоколи.

Серверна частина - компонент, у якому здійснюється зберігання, оброблення та аналітика даних, отриманих від IoT-пристроїв. Сервер може бути фізичним, віртуальним або хмарним, залежно від архітектури системи.

Клієнтська частина - представлена веб- або мобільним застосунком, що забезпечує користувачу доступ до інформації, результатів аналізу та керування пристроями.

Завдяки такій архітектурі, повсякденні предмети - від побутових пристроїв, до складних систем можуть обмінюватися даними без участі людини.

Завдяки розвитку недорогих процесорів і бездротових технологій сьогодні до систем IoT можна підключити майже будь-який предмет — від побутових приладів до безпілотного транспорту. Це дозволяє пристроям обмінюватися даними та поєднувати фізичний і цифровий світи в одну спільну екосистему.

Кількість пристроїв, підключених до мережі, стрімко зростає. Їхня популярність зумовлена підвищенням ефективності роботи систем і зручністю для користувачів (Рис. 2.2).

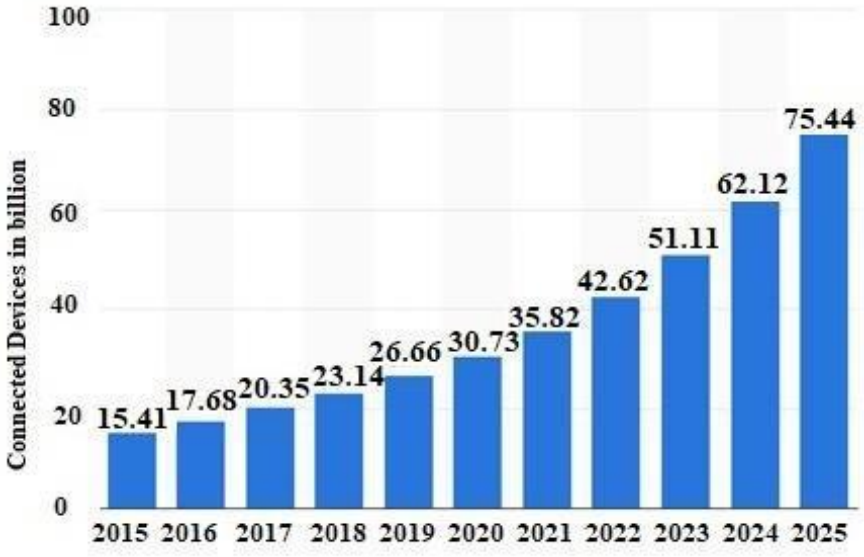


Рис. 2.2 – Статистика зростання кількості підключених пристроїв IoT

Для практичної реалізації концепції Інтернету речей усі навколишні об’єкти та пристрої - побутова техніка, посуд, одяг, продукти, транспортні засоби, промислове обладнання тощо - повинні бути оснащені мініатюрними ідентифікаційними та сенсорними елементами. Якщо є відповідні канали зв’язку, це дозволяє не лише відстежувати місцезнаходження об’єктів у просторі та часі, а й контролювати їхні параметри, але й здійснювати керування ними, а також інтегрувати отримані відомості у глобальну інформаційну систему - своєрідну «розумну планету».

Єдиного загальноприйнятого підходу до архітектури IoT наразі не існує. Різні дослідники пропонують власні варіанти її структури. Зокрема, частина науковців виділяє три рівні архітектури, тоді як інші підтримують чотирирівневу модель. Прихильники другого підходу зазначають, що із розвитком технологій трирівнева структура вже не відповідає сучасним вимогам і не може забезпечити необхідну гнучкість та ефективність роботи систем. Тому поділ на чотири рівні розглядається як більш доцільне рішення подальшого розвитку Інтернету речей.

Таким чином, архітектура пристроїв IoT, що включає чотири основні рівні - сенсори, мережу, оброблення даних та застосування, має вигляд, представлений на Рис. 2.3.

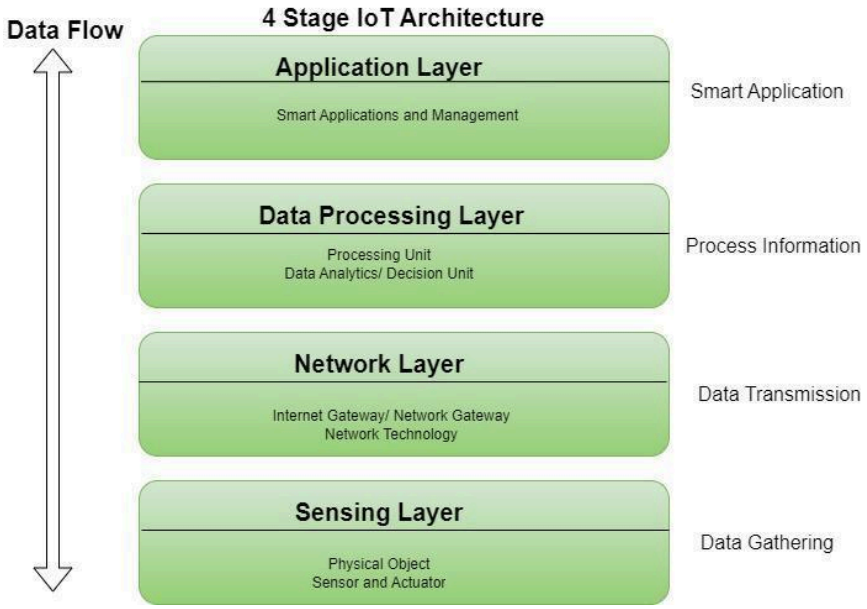


Рис. 2.3 – Рівні та компоненти архітектури IoT

Сенсорний рівень це перший крок у системі, де збираються всі дані з джерел. До його складу входять датчики та виконавчі механізми (актуатори), які розміщуються у фізичному середовищі для отримання інформації про різні фізичні параметри (температура, вологість, рівень шуму). Зв'язок між цими пристроями та наступним рівнем здійснюється через дротові або бездротові комунікаційні протоколи.

Мережевий рівень забезпечує передавання даних і зв'язок між пристроями у межах системи IoT. Він включає технології та протоколи зв'язку, що дозволяють пристроям обмінюватися інформацією між собою та з глобальною мережею Інтернет. До найпоширеніших мережевих технологій належать Wi-Fi, Bluetooth, Zigbee, а також мобільні мережі 4G і 5G. Окрім того, мережевий рівень може містити шлюзи та маршрутизатори, які виступають посередниками між пристроями та Інтернетом. Для забезпечення захисту інформації застосовуються механізми шифрування та автентифікації, що запобігають несанкціонованому доступу.

Рівень оброблення даних охоплює всі програми та пристрої, що збирають, обробляють і аналізують дані, які надходять від IoT-пристроїв.. На цьому етапі сирі дані перетворюються на структуровану інформацію, придатну для подальшого аналізу та прийняття рішень. Одним із прикладів є «озеро даних» (data lake) - централізоване сховище, у якому зберігаються необроблені дані від IoT-пристроїв.

Прикладний рівень є верхнім рівнем архітектури IoT, який безпосередньо взаємодіє з кінцевим користувачем. Його завдання — надавати користувачам зручні інтерфейси та можливість керувати пристроями й працювати з даними. До цього рівня належать мобільні застосунки, вебпортали, панелі моніторингу та інші програмні рішення, що взаємодіють з інфраструктурою IoT. Також прикладний рівень може містити проміжне

програмне забезпечення, яке забезпечує узгоджену взаємодію між різними пристроями та системами. Крім того, він включає аналітичні інструменти та засоби візуалізації даних, які перетворюють отриману інформацію на корисні висновки та рекомендації.

2.2 Аналіз протоколів обміну даними в автоматизованих системах на основі Internet of Things

Сучасні системи домашньої автоматизації умовно поділяють на відкриті та закриті. Відкриті платформи, як-от Home Assistant чи OpenHAB, дозволяють інтегрувати пристрої різних виробників і створювати модульні, масштабовані рішення без додаткових шлюзів чи перехідних пристроїв. Завдяки відкритій архітектурі програмного забезпечення можна налаштовувати індивідуальні сценарії автоматизації та адаптувати інтерфейс під власні потреби. А активна спільнота розробників і користувачів забезпечує підтримку на всіх етапах — від проєктування до монтажу й наладки системи.

Закриті системи, як-от Google Home, Apple HomeKit, LG ThinQ ON та Mi Home, зазвичай використовують для локальних завдань. Вони відрізняються стабільною роботою та легкою інтеграцією в межах однієї екосистеми, але можливості розширення та підключення пристроїв інших виробників обмежені. Такі платформи пропонують готові сценарії автоматизації та зрозумілий інтерфейс, що робить їх зручними для більшості користувачів, проте підвищує залежність від конкретного виробника та його хмарних сервісів.

Для побудови систем домашньої автоматизації використовуються різні протоколи та технології об’єднання пристроїв. Незалежно від складності архітектури, всі системи зводяться до взаємодії великої кількості пристроїв через певні протоколи обміну інформацією між контролерами, датчиками та виконавчими механізмами.

Всі протоколи можна умовно поділити на кілька основних типів:

- Publish/Subscribe - протоколи для асинхронного обміну даними, де пристрої публікують повідомлення, а інші підписуються на них.
- Request/Response - протоколи для запитів і відповідей між клієнтами та серверами.
- Mesh та локальні протоколи - протоколи для бездротових мереж сенсорів і виконавчих механізмів, часто з низьким енергоспоживанням.
- Протоколи для маячків та локальної ідентифікації - використовуються для навігації, тригерів та інтерактивних сценаріїв.

Протоколи типу «Publish/Subscribe» включають:

Zigbee - бездротовий стандарт, що дозволяє будувати енергоефективні та надійні мережі для обміну даними. Він використовує радіочастотний діапазон 2,4 ГГц (залежно від регіону також 868 МГц та 915 МГц) і працює за схемою mesh-мережі, що дозволяє кожному пристрою (сенсору або виконавчому елементу) виступати як ретранслятор сигналу. Такий підхід забезпечує високу стабільність мережі та покриття на великій площі без втрати сигналу.

Переваги**:**

- Низьке енергоспоживання пристроїв;
- Висока надійність завдяки mesh-мережі;
- Масштабованість: легко підключати нові пристрої без суттєвого впливу на роботу системи;
- Широка підтримка у платформах Home Assistant, OpenHAB, Homey, Mi Home.

Недоліки**:**

- Обмежена пропускна здатність, (до 249 кбіт/с);
- Менший радіус прямого сигналу, ніж у Wi-Fi (необхідна наявність повторювачів у великих приміщеннях);
- Необхідність сумісності з певними версіями протоколу для гарантованої взаємодії пристроїв різних виробників.

Z-Wave - бездротовий протокол для домашньої автоматизації, що працює в піддіапазоні радіочастот (приблизно 868–928 МГц, залежно від регіону). Протокол також використовує mesh-структуру, де кожен пристрій може ретранслювати сигнал, що дозволяє збільшити покриття. Особливістю Z-Wave є стандартизований набір команд для управління пристроями, що гарантує сумісність між різними виробниками.

Переваги**:**

- Надійне бездротове з’єднання з низьким енергоспоживанням;
- Висока сумісність між пристроями різних виробників;
- Підходить для контролю різних побутових процесів: світло, тепло, двері;
- Підтримка Home Assistant, OpenHAB та Homey.

Недоліки**:**

- Передає дані повільніше, ніж Wi-Fi;
- Обмежений вибір пристроїв у порівнянні з Zigbee;
- Деякі версії протоколу не сумісні з новими пристроями без оновлення хабу.

MQTT - дозволяє швидко й легко надсилати дані навіть у мережах з обмеженою пропускною здатністю. Він працює за принципом «публікація-підписка» (publish-subscribe), де пристрої публікують дані на сервер (broker), а інші пристрої підписуються на ці дані. Протокол широко використовується у відкритих системах, таких як Home Assistant та OpenHAB.

Переваги**:**

- Надзвичайно низьке споживання ресурсів;
- Підтримка масштабованих систем із великою кількістю пристроїв;
- Швидка передача даних і мінімальна затримка;
- Гнучкість інтеграції в будь-які open-source платформи.

Недоліки**:**

- Потребує центрального брокера для обміну повідомленнями;

- Відсутність власної системи шифрування (потрібно додатково налаштовувати TLS/SSL);
- Менш зручний для непрофесійних користувачів без технічного досвіду.

DDS - протокол обміну даними реального часу без центрального брокера з підтримкою QoS для критичних повідомлень.

Переваги**:**

- Відсутність центрального вузла;
- Висока надійність;
- Підтримка реального часу.

Недоліки**:**

- Складне налаштування.

Протоколи типу «Request/Response» включають:

REST - працює поверх HTTP і широко використовується для зв’язку між пристроями та серверами у IoT. Він дозволяє надсилати та отримувати дані у форматах JSON або XML за допомогою стандартних запитів GET, POST, PUT і DELETE.

Переваги**:**

- Проста реалізація і легке розгортання;
- Висока сумісність із веб-технологіями та мобільними додатками;
- Велика кількість бібліотек та інструментів для різних мов програмування;
- Легко інтегрується з існуючими веб-сервісами та хмарними платформами.

Недоліки**:**

- Відносно великі затримки при обміні даними через HTTP;
- Надмірність даних у запитах та відповідях (наприклад, великий обсяг заголовків);

- Не оптимальний для пристроїв з обмеженими ресурсами та низькою пропускною здатністю мережі;
- Відсутність вбудованих механізмів обміну станами в реальному часі.

CoAP (Constrained Application Protocol) - легкий протокол для обмежених IoT-пристроїв, побудований поверх UDP і призначений для ефективної взаємодії сенсорів, виконавчих механізмів та контролерів у домашніх мережах. Підтримує методи, подібні до REST (GET, POST, PUT, DELETE), та multicast-запити.

Переваги**:**

- Дуже низьке енергоспоживання та невеликі обсяги переданих даних;
- Підтримка multicast для одночасного опитування групи пристроїв;
- Придатний для ресурсозбережених пристроїв (сенсори, контролери);
- Легко інтегрується з REST-сервісами через переклад у HTTP.

Недоліки**:**

- Менша надійність передачі через UDP (пакети можуть втрачатися);
- Необхідність додаткового захисту даних через DTLS для шифрування;
- Менша популярність і підтримка порівняно з HTTP/REST;
- Обмежена функціональність для складних сценаріїв обробки повідомлень.

JMS (Java Message Service) - API і протокол для обміну повідомленнями між Java-додатками, використовується для побудови надійних систем з чергами повідомлень і асинхронною взаємодією.

Переваги**:**

- Надійна доставка повідомлень із гарантованою чергою;
- Підтримка асинхронної взаємодії між серверами і пристроями;
- Інтеграція з Java-екосистемою та корпоративними серверами;

- Підходить для масштабованих систем із великою кількістю пристроїв.

Недоліки**:**

- Не підходить для малопотужних пристроїв або мікроконтролерів;
- Складність налаштування і інтеграції для IoT-проектів на стороні клієнта;
- Велике споживання ресурсів у порівнянні з легкими протоколами (CoAP, MQTT).

XMPP (Extensible Messaging and Presence Protocol) - протокол для обміну повідомленнями в реальному часі, який підтримує наявність стану пристроїв («присутність») та асинхронний обмін даними. Використовується для управління IoT-пристроями та синхронізації станів у мережах «Розумного будинку».

Переваги**:**

- Надійна передача повідомлень у реальному часі;
- Підтримка присутності та стану пристроїв;
- Відкритий стандарт із широкою документацією та бібліотеками;
- Можливість шифрування даних (TLS) і автентифікації.

Недоліки**:**

- Відносно великий обсяг повідомлень через XML-формат;
- Вимагає багато пропускної здатності та обчислювальних ресурсів;
- Складність налаштування для малопотужних пристроїв.

Mesh та локальні протоколи включають:

Thread - протокол бездротового зв’язку, який працює на основі IPv6. Він використовує mesh-мережу для підключення сенсорів, освітлення та інших пристроїв, забезпечуючи стабільну та безпечну передачу даних. Thread активно

використовується у нових відкритих і закритих екосистемах, включно з LG ThinQ, Apple HomeKit та Google Home.

Переваги**:**

- Використання IP-адрес для кожного пристрою, що спрощує інтеграцію з іншими системами;
- Надійність та стабільність завдяки mesh-структурі;
- Енергоефективність для сенсорів та малопотужних пристроїв;
- Підтримка сучасного стандарту Matter для сумісності між різними виробниками.

Недоліки**:**

- Новий протокол, не всі пристрої сумісні;
- Відносно складне налаштування для початківців;
- Необхідність сумісного обладнання для повної інтеграції.

Matter - сучасний відкритий стандарт для взаємодії пристроїв у «розумному домі». Він побудований поверх Thread, Wi-Fi або Ethernet і забезпечує сумісність різних екосистем. Основна мета Matter – стандартизувати комунікацію між пристроями, щоб користувачі могли об’єднувати пристрої Apple, Google, Amazon, LG та інших виробників у єдину систему.

Переваги**:**

- Гарантована сумісність між виробниками;
- Можливість роботи з різними фізичними протоколами (Thread, Wi-Fi, Ethernet);
- Підвищена безпека та надійність;
- Підтримка у нових платформах LG ThinQ, Apple HomeKit, Google Home.

Недоліки**:**

- Новий стандарт – обмежена кількість сертифікованих пристроїв;

- Необхідність оновлення існуючого обладнання для сумісності;
- Частково складне впровадження для користувачів, які не знайомі з технологіями.

Wi-Fi - універсальна технологія бездротового підключення, яка дозволяє об’єднувати пристрої у локальній мережі або підключати їх до Інтернету. Вона широко застосовується у платформах Amazon Echo, Google Home, Mi Home та Homey.

Переваги:

- Широка сумісність з пристроями та мобільними додатками;
- Висока пропускна здатність для обміну даними;
- Швидка інтеграція та легке користування;
- Підтримка дистанційного керування через Інтернет.

Недоліки:

- Високе енергоспоживання для малопотужних пристроїв;
- Залежність від стабільності локальної мережі та Інтернет-з’єднання;
- Можливі конфлікти та перевантаження мережі при великій кількості пристроїв.

Bluetooth та його варіант BLE застосовуються для короткочасного бездротового зв’язку між сенсорами, смартфонами та керуючими пристроями. BLE відрізняється низьким енергоспоживанням і підходить для сенсорів та невеликих виконавчих елементів.

Переваги:

- Низьке енергоспоживання;
- Просте підключення до смартфонів та хабів;
- Підтримка у системах Mi Home, Homey, Amazon Echo;
- Зручне локальне керування.

Недоліки:

- Обмежений радіус дії;
- Відсутність підтримки mesh-мереж у класичному Bluetooth;
- Обмежена кількість одночасних підключень.

Протоколи для маячків та локальної ідентифікації включають:

WebSocket — це протокол, який відкриває постійний канал між клієнтом і сервером для обміну даними. Завдяки цьому повідомлення передаються без повторного з'єднання. У системах «Розумний будинок» його застосовують для миттєвого оновлення інформації про стан сенсорів, камер або контролерів.

Переваги:

- Двостороння комунікація в реальному часі;
- Менше затримок у порівнянні з REST/HTTP;
- Оптимальне рішення для моніторингу, відеоспостереження та push-повідомлень;
- Підтримується більшістю сучасних браузерів і серверів.

Недоліки:

- Не підходить для пристроїв з дуже обмеженими ресурсами;
- Підвищені вимоги до безпеки при відкритих постійних з'єднаннях;
- Потребує спеціального сервера або брокера з підтримкою WebSocket;
- Менш ефективний у мережах з частими розривами зв'язку.

DTLS - криптографічний протокол, створений для забезпечення безпеки передачі даних у з'єднаннях, що використовують UDP. Його основне завдання - забезпечити аналог TLS (SSL) для легких протоколів, таких як CoAP, MQTT-SN чи власні UDP-з'єднання між IoT-пристроями. Завдяки DTLS передача даних у бездротових сенсорних мережах стає захищеною від перехоплення або змін.

Переваги:

- Забезпечує конфіденційність і цілісність даних при використанні UDP;
- Підтримує автентифікацію пристроїв та шифрування з мінімальними затримками;
- Може використовуватись із CoAP, LwM2M та іншими легкими IoT-протоколами;
- Підвищує рівень безпеки у відкритих бездротових мережах.

Недоліки:

- Збільшує навантаження на процесор і споживання енергії малопотужних пристроїв;
- Складність реалізації на мікроконтролерах із обмеженими ресурсами;
- Може спричиняти затримки при повторній аутентифікації або втраті пакетів;
- Не підходить для надзвичайно швидких потоків даних (наприклад, відео в реальному часі).

Різні протоколи мають свої плюси і мінуси. Zigbee та Z-Wave довго працюють від батареї і стабільно передають сигнали, але потрібні хаби для керування. Wi-Fi легко підключається і сумісний з багатьма пристроями, але витрачає більше енергії і чутливий до проблем у мережі.

Таким чином, вибір конкретної платформи домашньої автоматизації залежить від вимог користувача до масштабованості, відкритості системи, наявності готових сценаріїв та необхідності інтеграції обладнання різних виробників. У сучасних умовах перевага відкритих платформ полягає у гнучкості та можливості налаштування системи під індивідуальні потреби користувача, тоді як закриті платформи забезпечують швидке впровадження та стабільність роботи у межах однієї екосистеми.

2.3 Забезпечення інформаційної безпеки при застосуванні технології IoT

Інтернет речей став важливою складовою сучасного суспільства. Швидке зростання кількості підключених пристроїв робить їх привабливою метою для кіберзлочинців і формує новий ландшафт загроз. Часто пристрої випускаються виробниками без належних механізмів забезпечення безпеки, що призводить до їхнього масового залучення в ботнети та використання на користь кіберзлочинних угруповань.

Головним мотивом кіберактивності залишається фінансова вигода: вразливості IoT розглядаються злочинцями крізь призму можливостей монетизації. Тому в дослідженнях поряд із технічними аспектами уразливостей дедалі більше уваги приділяється бізнес-моделям, які використовують кримінальні спільноти - торгівлі доступом, оренді ботнетів, наданню послуг анонімного проксі/VPN тощо. Світовий «чорний ринок» кіберзлочинності пропонує експлойти, модифіковані прошивки, «сервіси» з продажу ботнет-інфраструктур і інші інструменти, що дозволяють перетворювати вразливі пристрої на джерело прибутку для зловмисників.

Серед основних напрямків монетизації зламаних IoT-пристроїв у 2020-х роках виділяються організація DDoS-атак, використання пристроїв як вузлів виходу VPN або проксі, а також розгортання майнінгових рішень на потужних Android-платформах (смарт-телевізорах, приставках тощо). Такі сервіси часто продаються або орендуються іншим учасникам злочинної екосистеми.

Аналітика демонструє швидке зростання активності проти IoT-пристроїв. Навіть прості методи - сканування відкритих портів, використання заводських паролів чи методів брутфорсу - залишаються ефективними через широке розповсюдження незахищених пристроїв і низьку культуру їхнього оновлення. Часто використовувані сімейства шкідливого ПЗ, такі як Mirai, залишаються серед провідних інструментів для створення ботнетів, поряд із іншими варіантами, що застосовують як експлойти, так і методи автоматичного підбору

паролів. Це дозволяє зловмисникам швидко масштабувати мережі заражених пристроїв і зберігати прихований контроль над ними.

Щоб краще зрозуміти структуру цих загроз, варто поглянути на їх загальний розподіл (Рис. 2.4).

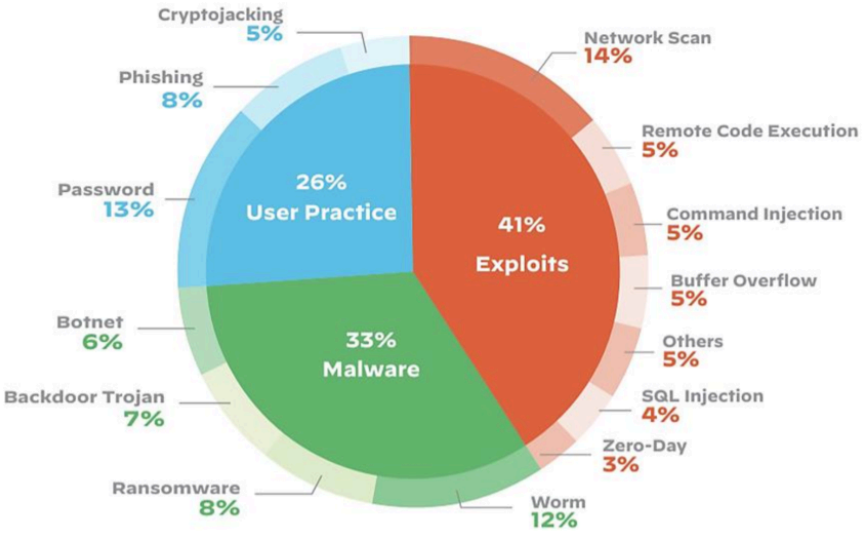


Рис. 2.4 – Діаграма сучасних кіберзагроз

Як ілюструє діаграма, сучасний ландшафт кіберзагроз є комплексним і спирається на три основні стовпи. Найбільшу частку, 41%, становлять експлойти - атаки, що використовують технічні вразливості в програмному забезпеченні пристроїв. Сюди входять як масові сканування мережі (14%) для пошуку слабких місць, так і більш цілеспрямовані атаки, наприклад, віддалене виконання коду (5%) чи SQL-ін'єкції (4%).

Другою за масштабом є категорія шкідливого програмного забезпечення (33%). Саме в ній знаходяться інструменти для створення ботнетів, про які йшлося вище. Зокрема, значну небезпеку становлять мережеві хробаки (12%), здатні до самостійного поширення, та безпосередньо ботнети (6%).

І що особливо важливо в контексті IoT, третя значна частина загроз (26%) пов'язана з практиками самих користувачів. Тут найслабшою ланкою виявляються проблеми з паролями (13%), що прямо перегукується з

використанням заводських чи легко вгадуваних комбінацій. Фішинг (8%) і криптоджекінг (5%) також є поширеними векторами, де людський фактор відіграє вирішальну роль. Таким чином, діаграма наочно демонструє, що вразливості IoT-пристроїв є результатом поєднання технічних недоліків, активності шкідливого ПЗ та людської необережності.

Географічний розподіл джерел атак змінюється з часом і залежить від регіональних відмінностей у поширенні незахищених пристроїв та інфраструктурі. Крім того, окремі сплески активності часто пов’язані зі сплесками виявлених уразливостей або з масштабними кампаніями сканування вразливих моделей пристроїв.

Ключові причини вразливості IoT-сегмента такі: слабкі механізми аутентифікації (наявність заводських паролів або їх незміненість), відсутність або запізніле застосування оновлень прошивки, незашифровані канали передачі даних та недостатня сегментація мережі. Користувачі та організації часто недооцінюють ці ризики: поширені комбінації логінів і паролів на кшталт «admin/admin», «root/root» або «support/support» продовжують бути векторами компрометації.

Отже, до 2025 року IoT-середовище залишається привабливим для кіберзлочинців через поєднання масового розповсюдження пристроїв, низького рівня захищеності виробів і добре налагоджених економічних механізмів на «чорному ринку». Це вимагає від виробників, користувачів і регуляторів посилення заходів безпеки: впровадження захищеної аутентифікації за замовчуванням, регулярного оновлення ПЗ, шифрування каналів зв’язку та мережевої сегментації критичних пристроїв.

2.4 Проблемні аспекти та ризики використання технології «розумного будинку»

Інтеграція технологій «розумного будинку» в сучасний життєвий простір, попри значне підвищення рівня комфорту та автоматизації побутових процесів,

породжує комплекс нових викликів та ризиків. Відносна новизна даної сфери та відсутність уніфікованих стандартів призводять до виникнення низки проблем на етапах проєктування, впровадження та подальшої експлуатації систем. Аналіз сучасного стану ринку дозволяє систематизувати ці проблеми за трьома ключовими напрямами: технологічна фрагментація та сумісність обладнання, економічні аспекти та сукупна вартість володіння, а також загрози кібербезпеці та конфіденційності даних. Кожен із цих аспектів вимагає детального розгляду для формування об'єктивної оцінки потенційних загроз.

Однією з фундаментальних перешкод для гармонійного розвитку ринку є відсутність єдиних стандартів взаємодії пристроїв. Сучасний ринок перенасичений обладнанням від численних виробників, що функціонує на базі різних, часто несумісних між собою, протоколів зв'язку, таких як Zigbee, Z-Wave, Wi-Fi та Bluetooth. Хоча ініціативи, подібні до стандарту Matter, спрямовані на уніфікацію комунікації, на практиці інтегратори змушені поєднувати розрізнені компоненти за допомогою додаткових апаратних шлюзів та програмних платформ. Такий підхід не лише суттєво ускладнює архітектуру системи та збільшує її кінцеву вартість, але й створює додаткові точки відмови, знижуючи загальну надійність. Більше того, це створює залежність функціональності системи від життєвого циклу продуктів окремих виробників, які можуть припинити підтримку свого обладнання, що може частково вивести елементи «розумного будинку» з працездатності.

Економічний аналіз впровадження систем «розумного будинку» повинен враховувати не лише початкові капітальні інвестиції, а й сукупну вартість володіння. Цей показник включає приховані витрати, такі як абонентська плата за доступ до розширених хмарних сервісів (наприклад, архівування відеозаписів), витрати на періодичне технічне обслуговування, а також неминучі затрати на модернізацію обладнання внаслідок його швидкого морального та технологічного старіння. Важливою складовою є і постійне енергоспоживання центральних контролерів, датчиків та мережевих пристроїв.

Таким чином, заявлена виробниками економія ресурсів не є гарантованою і може бути досягнута лише за умови глибокого попереднього аналізу, професійного проєктування системи та розрахунку терміну окупності інвестицій, що підкреслює необхідність залучення кваліфікованих фахівців.

Найбільш значущим та багатогранним ризиком є вразливість систем «розумного будинку» до кіберзагроз. Підключення внутрішньої інфраструктури до глобальної мережі Інтернет перетворює її на потенційну ціль для зловмисників. Основними векторами атак є використання слабких або незмінених заводських паролів, незахищені бездротові мережі, наявність програмних вразливостей у прошивках пристроїв через несвоєчасне оновлення, а також методи соціальної інженерії, спрямовані на отримання облікових даних користувачів. Наслідки успішної кібератаки можуть бути критичними: від порушення приватності через несанкціонований доступ до відеокамер та мікрофонів до прямої загрози фізичній безпеці мешканців шляхом маніпуляцій із системами контролю доступу, сигналізацією чи кліматичним обладнанням. Крім того, скомпрометовані пристрої можуть бути залучені до складу ботнет-мереж для організації масштабних DDoS-атак, що становить загрозу вже для стабільності глобальної інтернет-інфраструктури.

Окремий аспект проблеми безпеки стосується збору та обробки персональних даних. IoT-пристрої безперервно генерують величезні масиви інформації про звички, розпорядок дня, переміщення та навіть розмови користувачів. Ці дані, що є цінним активом для виробників, використовуються для аналітики та таргетованої реклами. Однак їх централізоване зберігання на серверах компаній створює ризик їх витоку внаслідок хакерських атак або недобросовісних дій персоналу. Непрозорі політики конфіденційності та недостатній рівень захисту даних з боку виробників можуть призвести до того, що найбільш чутлива інформація про приватне життя особи стане доступною третім сторонам без її відома та згоди.

Для ефективної мінімізації зазначених ризиків необхідний комплексний підхід, що передбачає розподіл відповідальності між усіма учасниками екосистеми «розумного будинку». Виробники повинні інтегрувати принципи «безпеки через проектування», забезпечуючи регулярний випуск оновлень безпеки та використовуючи надійні механізми автентифікації. Професійні інсталятори зобов'язані проєктувати захищену мережеву архітектуру, зокрема шляхом сегментації мережі та ізоляції IoT-пристроїв в окремому віртуальному сегменті (VLAN). Зі свого боку, кінцеві користувачі несуть відповідальність за дотримання базових правил кібергігієни: використання складних унікальних паролів, своєчасне встановлення оновлень та обережне надання дозволів мобільним додаткам. Тільки разом усі заходи забезпечують потрібний рівень безпеки та надійності для сучасних домашніх автоматизованих систем.

Висновок до розділу 2

У розділі було проведено комплексне дослідження технології Інтернету речей як фундаментальної основи для реалізації проєктів «розумний будинок». Аналіз охопив теоретичні засади IoT, огляд архітектурних рішень, порівняння протоколів передачі даних, а також ідентифікацію ключових загроз інформаційній безпеці та практичних ризиків впровадження.

Дослідження підтвердило, що IoT охоплює багато рівнів і утворює складну систему, що складається з сенсорного, мережевого, обробного та прикладного рівнів. Саме така структурована архітектура дозволяє забезпечити повний цикл функціонування систем «розумного будинку» - від збору даних з фізичного середовища до надання користувачеві зручних інструментів керування та аналітики.

Проведений аналіз протоколів обміну даними виявив ключову проблему сучасного ринку - технологічну різнорідність та відсутність єдиних стандартів. Існує чіткий поділ на відкриті та закриті платформи, а вибір комунікаційних технологій (Zigbee, Z-Wave, Wi-Fi, Thread) являє собою компроміс між енергоефективністю, швидкістю, надійністю та вартістю. Поява нових

стандартів, як-от Matter, свідчить про рух галузі до уніфікації, проте на даному етапі проблема сумісності залишається актуальною.

Було визначено, що забезпечення інформаційної безпеки є критично важливим і водночас найслабшим аспектом сучасних IoT-систем. Стрімке зростання кількості підключених пристроїв створює масштабну поверхню для атак, мотивацією яких переважно є фінансова вигода. Як показало дослідження, загрози є комплексними і включають технічні експлойти, шкідливе програмне забезпечення та помилки користувачів, зокрема використання слабких паролів. Це підтверджує, що вразливості IoT є результатом поєднання недоліків проєктування, активності зловмисників та низького рівня кібергігієни.

Разом з тим, практичне впровадження технології «розумний будинок» супроводжується значними ризиками, що виходять за межі кібербезпеки. До них належать проблеми сумісності обладнання, висока сукупна вартість володіння, що включає приховані витрати на обслуговування та підписки, а також загрози конфіденційності персональних даних, які збираються виробниками.

Таким чином, головний висновок розділу полягає в тому, що попри величезний потенціал технології IoT для автоматизації житлового простору, її успішна та безпечна імплементація стикається з серйозними перешкодами. Ефективне вирішення цих проблем вимагає комплексного підходу та розподілу відповідальності між виробниками, які повинні впроваджувати принципи «безпеки через проектування», інсталяторами та кінцевими користувачами. Результати, отримані в цьому розділі, створюють теоретичну та аналітичну основу для розробки практичних рішень і архітектурних моделей, що будуть розглянуті в наступних частинах роботи.

РОЗДІЛ 3 Проєктування та алгоритмізація системи «Розумний будинок»

3.1 Програмно-апаратні платформи та архітектурні підходи

Сучасні системи «Розумний будинок» базуються на поєднанні апаратних компонентів (сенсорів, виконавчих пристроїв, контролерів) та програмних платформ для управління і обробки даних. Залежно від способу розміщення обчислювальних ресурсів, розрізняють три основні архітектурні підходи до побудови систем автоматизації: хмарний, локальний та змішаний.

Хмарні системи, такі як Microsoft Azure IoT, Google Cloud IoT та IBM Watson IoT, забезпечують централізовану обробку даних і дистанційне керування пристроями через мережу Інтернет.
Вони надають розробникам масштабовану інфраструктуру, вбудовані механізми безпеки, засоби аналітики й зберігання даних у режимі реального часу.

Характерні риси таких платформ:

1. покладаються на інтернет-з’єднання;
2. мають високу масштабованість;
3. зручні для великих проєктів і промислового використання.

Таблиця 3.1 - Аналіз хмарних платформ IoT

Переваги	Недоліки
Глобальний доступ до системи	Повна залежність від Інтернету
Висока масштабованість	Питання захисту даних користувачів
Підтримка мільйонів пристроїв	Абонентна плата та висока вартість інфраструктури
Вбудована аналітика та моніторинг	Збої у хмарного провайдера впливають на роботу системи

Такі рішення частіше застосовуються у «розумних» містах, промисловій автоматизації, великих корпоративних системах

Локальні платформи не потребують постійного підключення до Інтернету, оскільки управління відбувається всередині будинку. Найпоширеніші приклади: Home Assistant, KNX, Loxone.

Їх робота заснована на локальному контролері або сервері, який координує роботу всіх пристроїв через локальні протоколи (ZigBee, Z-Wave, MQTT, Modbus тощо).

Переваги:

1. робота без Інтернету;
2. конфіденційність та безпека даних;
3. відсутність абонплат;
4. висока надійність при правильному резервуванні.

Недоліки:

1. потреба у локальному обладнанні;
2. складність початкового налаштування та адміністрування.

Змішані архітектури - поєднують локальне управління і хмарні сервіси (наприклад, для віддаленого доступу, зберігання відео або повідомлень).

Переваги:

1. система продовжує працювати офлайн;
2. доступ до управління з будь-якого місця.

Недоліки:

1. складніше забезпечити єдину безпеку всіх компонентів;
2. часткова залежність від хмарних сервісів.

В межах даної дипломної роботи обрано локальну архітектуру управління на базі Home Assistant.

Цей вибір обумовлений такими факторами:

1. безперервність роботи - система повністю функціонує без Інтернету;
2. підвищена інформаційна безпека - дані користувачів не передаються у хмару;
3. висока сумісність з великою кількістю розумних пристроїв;
4. масштабованість архітектури - можливість підключення нових підсистем без повної перебудови системи;
5. відсутність регулярних платежів за використання сервісів.

Також Home Assistant підтримує:

1. локальні протоколи ZigBee, Z-Wave, MQTT;
2. інтеграцію камер відеонагляду;
3. керування освітленням, кліматом, системами безпеки;
4. автоматизацію сценаріїв на основі умов і подій.

Таким чином, локальне рішення забезпечує оптимальний баланс надійності, захищеності та економічної вигоди, що є критично важливим для системи автоматизації житлових приміщень.

3.2 Розробка алгоритму функціонування та проєктування системи «Розумний будинок»

У процесі розроблення дипломного проєкту було створено алгоритм функціонування та виконано проєктування автоматизованої системи управління житлом «Розумний будинок». Система має забезпечувати автоматичний контроль та керування інженерними мережами будинку, підвищувати рівень комфорту, енергоефективності та безпеки користувачів.

На основі дослідження вимог до проєктованої системи визначено такі основні принципи її побудови:

- використання центрального серверу управління з частковою автономністю локальних контролерів;

- підтримка дротових і бездротових протоколів зв’язку: **Ethernet / PoE, Wi-Fi, Zigbee**;
- гнучка масштабованість та можливість підключення обладнання різних виробників;
- використання відкритих протоколів взаємодії пристроїв у межах IoT-екосистеми;
- оперативне сповіщення користувача через мобільний застосунок та **Telegram**;

У базовій конфігурації система забезпечує керування такими підсистемами (Рис. 3.1):

- система мікроклімату (опалення, вентиляція, кондиціонування);
- система інтелектуального освітлення;
- система відеоспостереження;
- охоронна сигналізація, датчики відкриття дверей і вікон;
- система пожежної безпеки;
- контроль витоку води та газу;
- система резервного живлення та моніторингу електромережі;
- система віддаленого доступу до управління.

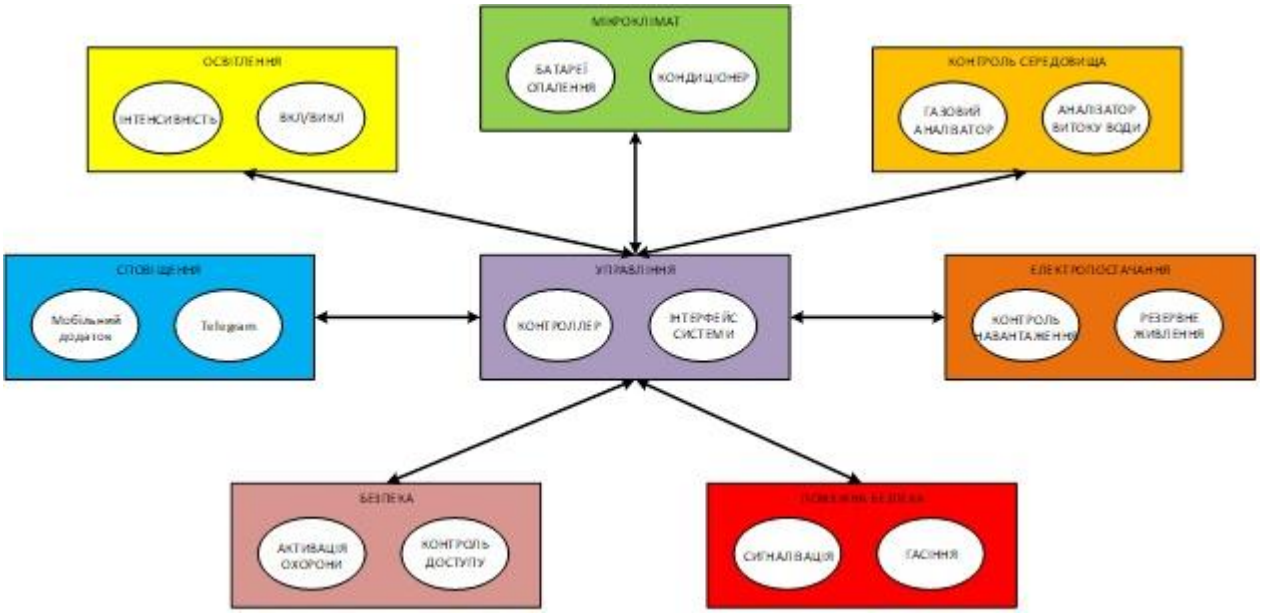


Рис. 3.1 – Структурна схема системи «Розумний будинок»

В якості головного елемента управління обрано **Proxmox VE** - високопродуктивний сервер віртуалізації (Рис. 3.2).

Він забезпечує:

- запуск служб управління та аналітики в окремих віртуальних машинах/контейнерах;
- зберігання відеопотоків від IP-камер;
- постійний контроль станів локальних контролерів і датчиків;
- роботу хмарних сервісів віддаленого доступу.

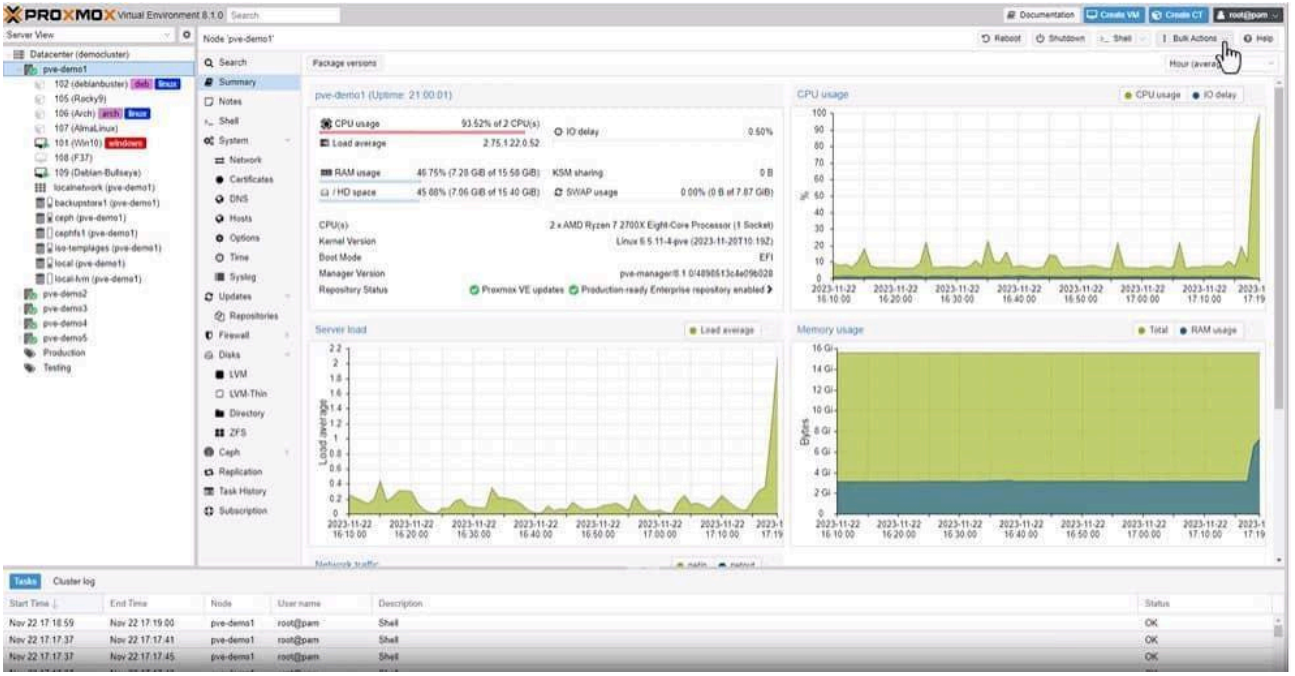


Рис. 3.2 – Інтерфейс Proxmox VE

Комунікація між сервером та периферією здійснюється через IoT-шлюзи з підтримкою Wi-Fi та **Zigbee**, а мережеві камери використовують **PoE з'єднання**, що одночасно забезпечує передачу даних і живлення.

Використовуючи універсальну мову моделювання UML, побудовану структурну схему функціонування системи, яка представлена на Рис. 3.3.

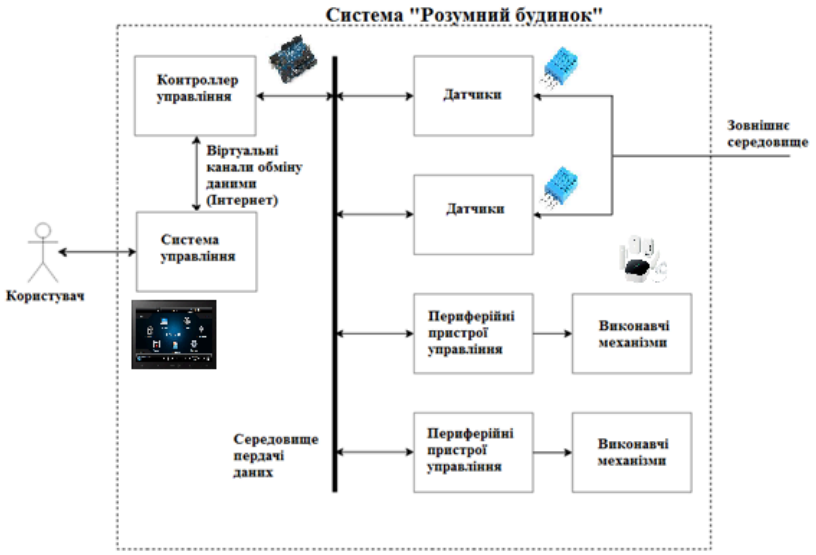


Рис. 3.3 – Структурна схема системи "Розумний будинок"

Система "Розумний будинок" базується на центральному контролері, розгорнутому на сервері Proxmox, який забезпечує роботу всіх сервісів: керування пристроями, відеоспостереження, систем безпеки та клімат-контролю. Для інтеграції та керування бездротовими пристроями використовується **Zigbee 3.0 координатор SMLight SLZB-06P7 з інтерфейсами Ethernet і Wi-Fi** (Рисунок 3.4), який забезпечує надійний зв’язок із датчиками та виконавчими пристроями.

Рис. 3.4 – Zigbee 3.0 координатор SMLight SLZB-06P7

До складу системи входять периферійні пристрої - датчики та виконавчі механізми різного типу: датчики руху, температури, вологості, витоку води, газу,

відкриття вікон і дверей, а також IP-камери, реле, розумні вимикачі тощо. Об’єднання пристроїв відбувається за допомогою універсальних інтерфейсів і протоколів передачі даних, таких як Wi-Fi, Zigbee, Ethernet та PoE, що забезпечує надійну роботу, масштабованість системи та високий рівень захисту мережевої інфраструктури.

Моніторинг параметрів здійснюється на основі показників сенсорів, встановлених у приміщенні. Локальні вузли обробляють дані та виконують регулювання в реальному часі - наприклад, керування вентиляцією, опаленням, зволожувачами, сигналізацією або перекриттям води.

Центральний контролер збирає дані з усіх пристроїв, виконує автоматизовані сценарії, надає доступ до керування системою з будь-якого місця через веб-інтерфейс, мобільний додаток або Telegram-бот, а також забезпечує надсилання сповіщень щодо аварійних подій, тривог чи змін параметрів клімату.

Завдяки такій архітектурі система гарантує зручність користування, підвищену безпеку та енергоефективність житлового простору.

При розробці функціональної моделі система практично буде розділяти Розумний будинок на дві складові:

підсистеми, що потребують постійного моніторингу: безпеки, контролю клімату, аналіз витоку води і газу, освітлення, протипожежна підсистема.

підсистеми, які працюють лише після надсилання керуючих сигналів – включення / виключення освітлення, системи сповіщення.

Загальна функціональна схема взаємодії підсистем та центрального контролера наведена на Рис. 3.5.

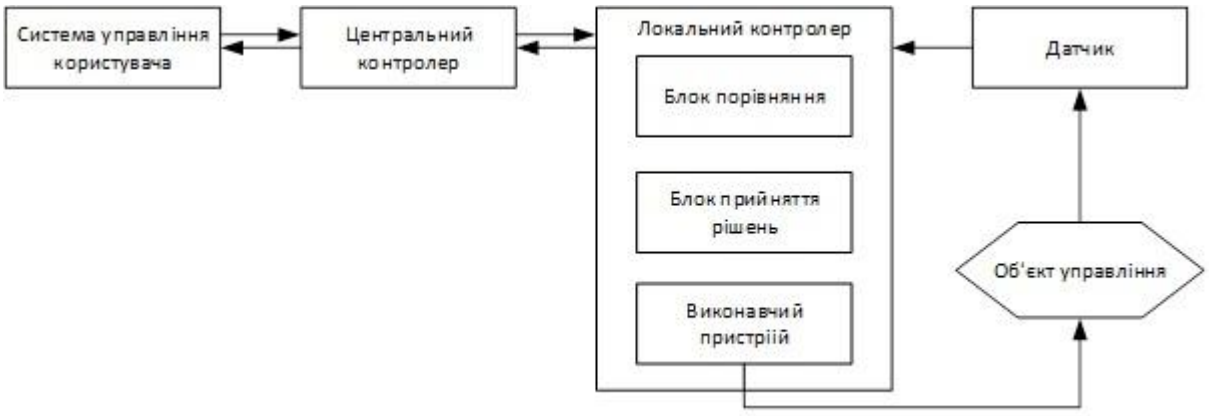


Рис. 3.5 – Функціональна схема системи "Розумний будинок"

Датчики відстежують стан об’єктів і передають інформацію на локальний контролер через певні проміжки часу або у критичних ситуаціях, наприклад, при спрацьовуванні диму. Центральний контролер задає потрібні параметри, а локальний контролер порівнює їх, приймає рішення і керує виконавчими пристроями.

Суть алгоритмічної моделі полягає в розробці алгоритму, який лежить в основі роботи всіх підсистем з виконавчими пристроями.

Як було зазначено вище, для роботи системи в цілому і кожної з підсистем необхідний алгоритм, на підставі якого відбувається вибір тієї чи іншої дії виконавчого приладу, центрального контролера. У системі, всі рішення приймаються на підставі показань датчиків, які перед тестуванням системи повинні бути налаштовані. Залежно від їх показників, система приймає рішення про видачу сигналу на виконавчий механізм, який виконує будь-яку роботу, після чого відбувається сповіщення про подію, що відбулася і запис її в пам'ять.

Алгоритм роботи всієї системи в цілому наведений на Рисунку 3.6.

Таким чином, головна мета роботи системи - це моніторинг заздалегідь заданих параметрів.

Крім того, в даній системі існують підсистеми, які виконують будь-яку дію тільки після прямого надходження керуючого сигналу, що подається або з пульта дистанційного керування, або з іншого пристрою управління.

Алгоритм роботи цих підсистем простий і включає в себе лише перевірку прийнятого сигналу на коректність і виконання команди. Даний алгоритм наведений на Рис. 3.7.

Відповідно до першого алгоритму (Рис. 3.6) працюють такі підсистеми:

- контролю витоку води і газу;
- контролю клімату;
- підсистема пожежної безпеки.
- управління інтенсивності освітлення.

Всі інші підсистеми управляються безпосередньо з пристроєм управління.

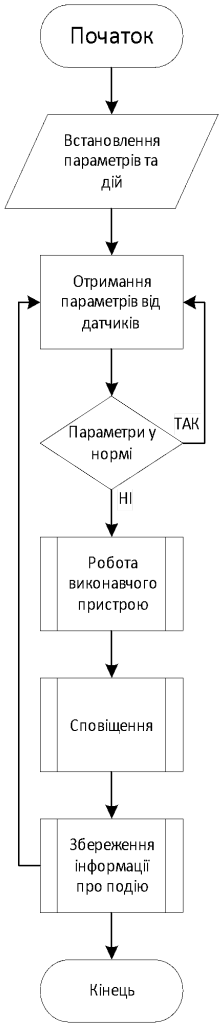


Рис. 3.6 – Алгоритм роботи системи

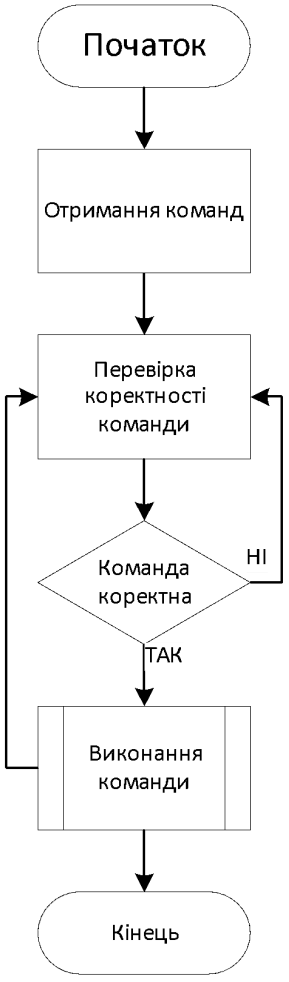


Рис. 3.7 – Алгоритм роботи підсистем, які не потребують порівняння параметрів із заданими

3.3 Розробка алгоритмів функціонування систем клімат-контролю та підсистеми опалення

Система підтримує комфортну температуру в будинку, яку користувач може встановити через веб-інтерфейс або в налаштуваннях у файлі. Програма працює у трьох режимах, з верхньою та нижньою допустимою температурою.

1) **Економічний режим**. Система може працювати в режимі максимального енергозбереження, коли опалення споживає мінімум ресурсів.

2) **Стандартний режим**. Нормальний режим, в який підходить більшості людей.

3) **Режим «тепло»**. Режим коли система підтримує високу температуру, витрачається більше всіх ресурсів.

Всі режими можна перемикати в web інтерфейсі (мобільному застосунку) або за допомогою фізичних кнопок на пульті управління.

Датчики на трубах і радіаторах відслідковують температуру. Якщо труба гарячіша за радіатор — опалення працює, радіатор закритий. Коли обидва тепліші за кімнатну температуру — опалення і радіатор ввімкнені. Якщо холодні — все вимкнено.

Загальна блок-схема управління системою контролю температури приведена на Рис. 3.8.

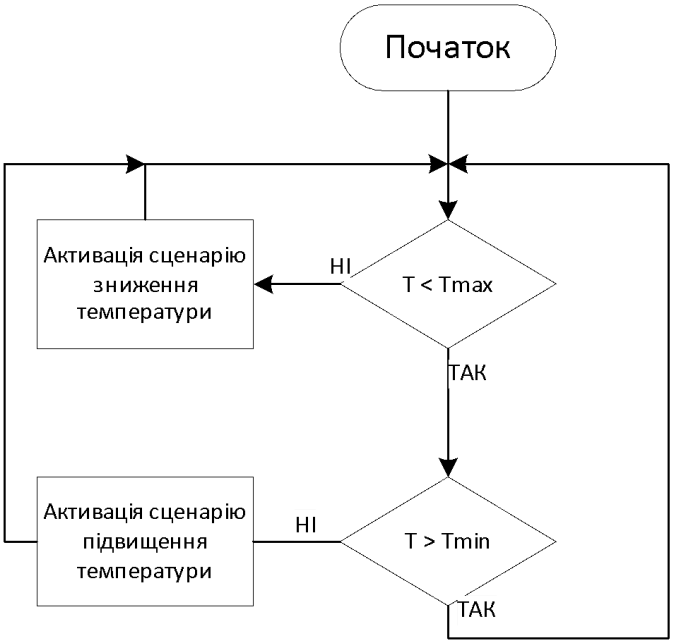


Рис. 3.8 – Загальна блок-схема управління системою контролю температури

Коли температура піднімається вище допустимого рівня, система автоматично запускає сценарій для її зниження. Алгоритм роботи сценарію зниження температури приведено на Рис.3.9.

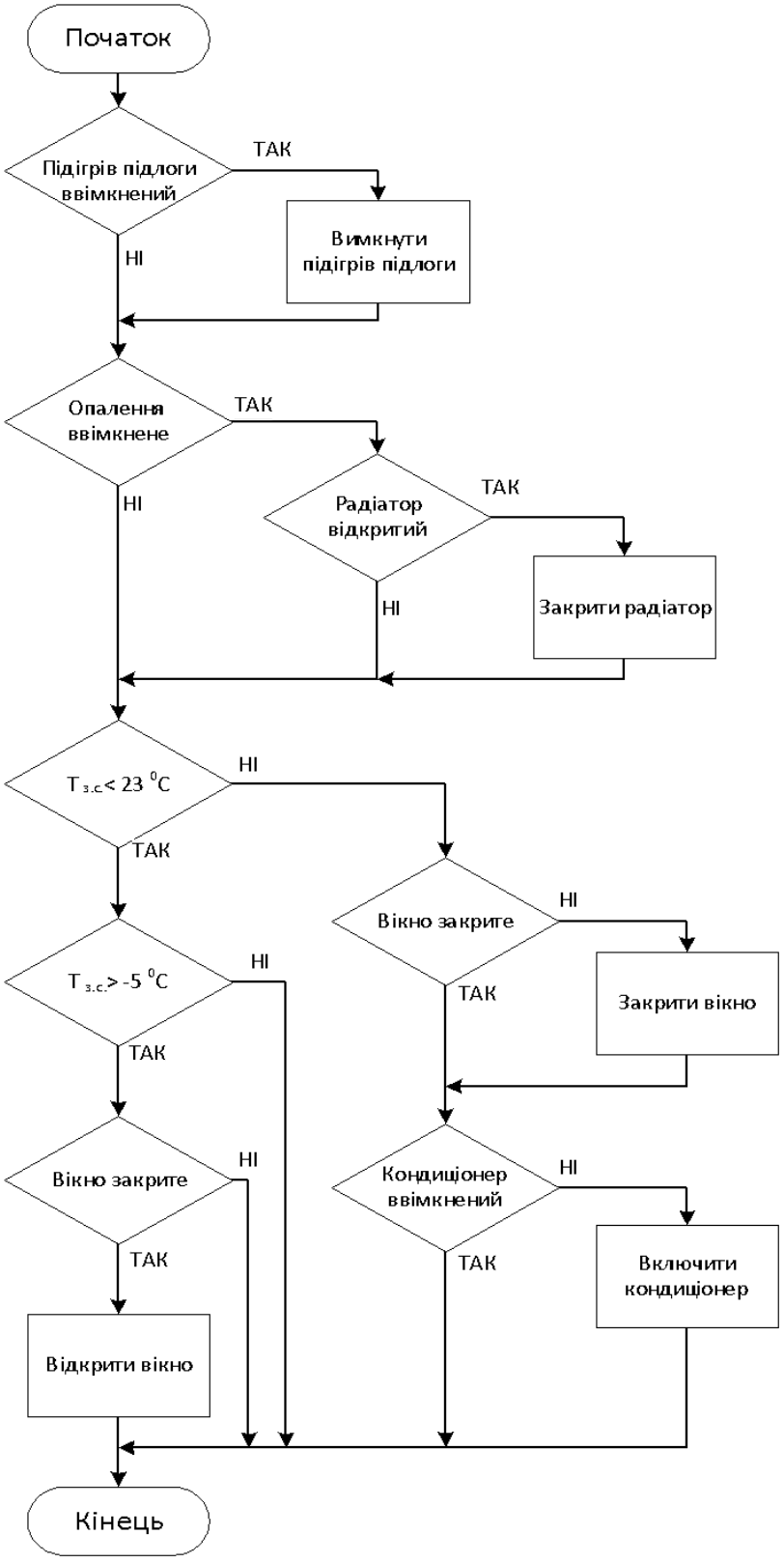


Рис. 3.9 – Алгоритм роботи сценарію зниження температури

У системі клімат-контролю «Розумного будинку» є два основні автоматичні режими: охолодження та нагрівання. Система перемикається між ними залежно від даних сенсорів температури всередині та поза приміщенням.

У разі перевищення температурою у приміщенні верхнього порогу система переходить у режим охолодження (Рис. 3.10). Спершу вимикається підігрів підлоги, якщо він працював, а також опалення — через закриття кульового клапана радіаторів, якщо температура теплоносія достатня. Після цього перевіряється температура зовнішнього повітря: якщо її значення знаходиться в межах від −5 °C до +23 °C, автоматично виконується відкриття вікна за допомогою електричного приводу для природної вентиляції. У випадку, коли температура зовнішнього повітря перевищує +23 °C та вікно при цьому відчинене, керуюча система подає команду на його зачинення. Якщо ж зовнішня температура є високою та опалення відключене, здійснюється увімкнення кондиціонера для охолодження приміщення.

Якщо температура в приміщенні падає нижче допустимого мінімуму, система автоматично переходить у режим нагрівання. На цьому етапі кондиціонер вимикається, якщо він був увімкнений, а вікна зачиняються для збереження тепла. При наявності гарячого теплоносія у системі центрального опалення відкривається кульовий електричний клапан радіатора. Якщо опалення недоступне, кондиціонер вимкнений, а зовнішня температура нижче +10 °C, вмикається підігрів підлоги. Додатково підігрів підлоги запускається, якщо радіатори вже працюють, але температура в кімнаті все ще нижче мінімально встановленого рівня.

В обох режимах, після досягнення комфортної температури у приміщенні, система переходить у режим енергозбереження - автоматично зачиняє вікна, вимикає кондиціонер і вимикає підігрів підлоги, забезпечуючи раціональне використання енергоресурсів без втрати комфорту користувача.

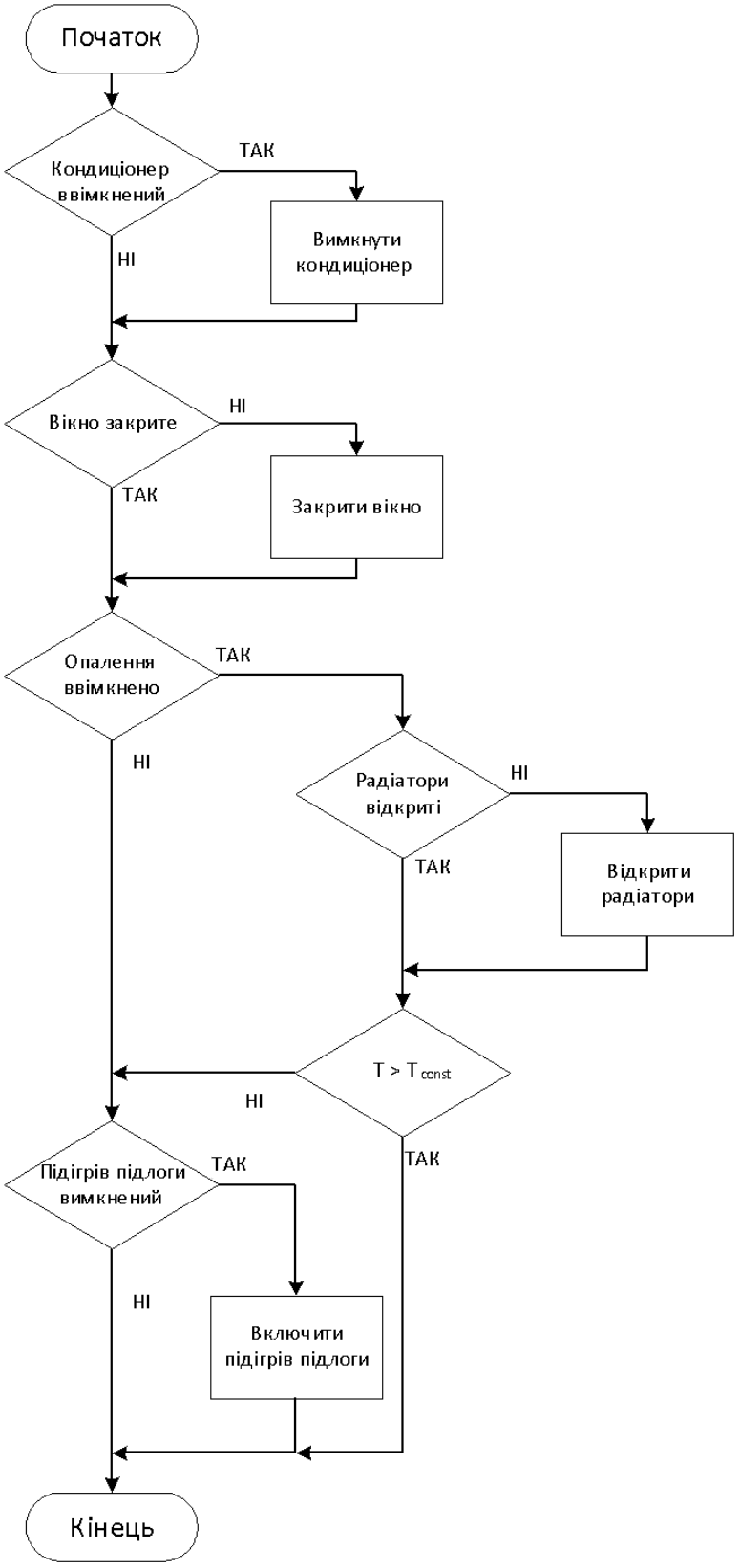


Рис. 3.10 – Алгоритм роботи сценарію підвищення температури.

3.4 Розробка алгоритмів функціонування систем безпеки та відеонагляду

Системи безпеки та відеоспостереження є критично важливими складовими розумного будинку, забезпечуючи персональну безпеку користувачів, захист майна, а також оперативне реагування на позаштатні ситуації.

До складу системи входять наступні підсистеми:

1. Підсистема охорони периметра:
    - датчики відчинення дверей та вікон (геркони);
    - інфрачервоні датчики руху;
    - сенсори розбиття скла.
2. Підсистема інженерної безпеки:
    - датчики витоку води;
    - датчики загазованості;
    - датчики диму та чадного газу.
3. Система відеоспостереження:
    - зовнішні та внутрішні камери;
    - запис відео на NAS-сховище з використанням PoE-інфраструктури;
    - алгоритми детекції руху та аналітика подій.
4. Підсистема сповіщення:
    - мобільний додаток;
    - Telegram-бот;
    - звукові та світлові сирени.

Комунікації системи реалізовані по Wi-Fi, Ethernet та ZigBee протоколам. У разі пошкодження зв’язку передбачено резервування каналів передачі даних.

Алгоритм роботи охоронної підсистеми включає 2 режими:

1. Нормальний режим (користувач вдома):
    - Геркони та датчики руху працюють у фоновому режимі
    - Події тільки логуються у системі
    - Камери ведуть запис за детекцією руху
2. Активований охоронний режим («Охорона»):

Якщо будь-який з охоронних датчиків спрацьовує - система перевіряє статус користувача (за геолокацією та шифрованим ключем).

У разі підтвердження тривоги:

- активується сирена
- починається безперервний запис відео з камер у зоні спрацювання
- користувач отримує миттєве сповіщення Telegram та push-сповіщення мобільного додатку

Таблиця 3.2 - Алгоритми функціонування системи інженерної безпеки

Тип датчика	**Умова спрацювання**	**Дії системи**
Датчик води	Виявлено контакт з рідиною	Закрити електромагнітний клапан водопроводу, надіслати сповіщення, активувати камеру зони
Датчик газу (метан/CO)	Перевищення порогової концентрації	Відкрити вікно (якщо можливо), увімкнути вентиляцію, відправити тривогу
Датчик диму/CO2	Фіксується задимлення	Увімкнути сирену, відправити сповіщення, активувати режим евакуації
Датчик температури	Перегрів системи або різке підвищення	Попередження та логування події

Система відеоспостереження працює у взаємодії з підсистемою охорони та включає такі алгоритми:

- Безперервний запис у режимі тривоги
- Запис за детекцією руху або присутності людини (AI-детекція)
- Аналітика подій: визначення напрямку руху (всередину/назовні), визначення залишених предметів, фіксація розпізнаного обличчя
- Автоматичне створення відеофрагмента при тривозі і надсилання користувачу
- Збереження архіву на мережевому сховищі з доступом через VPN

Висновок до розділу 3

У розділі було виконано проєктування автоматизованої системи «Розумний будинок» із детальним аналізом архітектурних підходів до її реалізації. На основі порівняння хмарних, локальних та змішаних IoT-рішень обґрунтовано вибір локальної архітектури на базі платформи Home Assistant, що забезпечує автономність функціонування, високу безпеку даних та можливість подальшої масштабованості системи.

Розроблено структурну та функціональну моделі системи, побудовано алгоритми взаємодії підсистем і центрального контролера. Визначено класифікацію підсистем за принципом автоматизації: такі, що потребують постійного моніторингу та автоматичного керування, а також підсистеми із керуванням на основі безпосередніх команд користувача.

Окрему увагу приділено розробці алгоритмів функціонування кліматичної підсистеми, що включає опалення, кондиціонування, вентиляцію та керування електроприводами вікон. Запропоновано сценарії автоматичного охолодження

та нагрівання приміщення, що забезпечують енергоефективність та комфортні умови проживання.

Також розроблено алгоритми роботи системи безпеки та відеоспостереження, які забезпечують виявлення загроз, фіксацію подій, автоматичне включення засобів протидії та інформування користувача через мобільні сервіси. Передбачено комплексний захист: контроль периметра, відеонагляд, виявлення пожежонебезпечних ситуацій, витоків води та газу.

Таким чином, створений комплекс алгоритмів забезпечує надійне, адаптивне та інтелектуальне управління всіма критично важливими інженерними системами будинку, підвищує рівень безпеки, комфорту та ефективності використання енергоресурсів, що повністю відповідає поставленим проєктним вимогам.

ВИСНОВКИ

У магістерській роботі було комплексно досліджено концепцію створення системи «Розумний будинок» на основі технологій Інтернету речей (Internet of Things), що на сьогодні є одним із найдинамічніших напрямів цифрової трансформації побутового простору. Розроблена система базується на локальній архітектурі із застосуванням Home Assistant, що забезпечує високий рівень автономності, безпеки даних та можливість масштабування в майбутньому, що підтверджує доцільність такого підходу в умовах постійного зростання кіберзагроз та ризиків залежності від хмарних сервісів.

Виконано аналіз апаратних і програмних платформ, протоколів комунікації та механізмів захисту даних. Встановлено, що найбільш придатними для сучасного житлового середовища є бездротові стандарти Wi-Fi і Zigbee, а також MQTT як ефективний транспорт для передачі сенсорних даних у реальному часі, завдяки його низькому навантаженню на мережу, надійності та підтримці розподіленої архітектури IoT.

Було побудовано структурну модель системи з декомпозицією на основні підсистеми: клімат-контроль, охоронний модуль, відеонагляд, освітлення та аварійний моніторинг небезпечних станів. Для кожної із підсистем розроблено алгоритми функціонування та логіку дій у стандартних і критичних сценаріях, зокрема інтегроване реагування на ризики пожежі, витоку газу, води або спроби проникнення.

Система автоматизації будинку орієнтована на енергоефективність, що є особливо важливим у контексті 2025 року та сучасних умов України - як через економічні виклики, так і через зростання вимог до раціонального використання ресурсів. Використання інтелектуального регулювання температури, оптимізації роботи опалення та кондиціонування, автоматизації освітлення сприяє зменшенню витрат на енергоносії, продовженню ресурсу обладнання та створенню сталого життєвого простору.

Окрема увага приділена інформаційній безпеці, адже IoT-інфраструктура залишається привабливою ціллю для кіберзлочинців. У роботі сформовано принципи побудови захищеної мережевої архітектури: ізоляція IoT-сегменту, використання VPN-доступу, шифрування каналів зв’язку, автентифікація та контроль оновлень ПЗ.

Практична частина проєкту продемонструвала реальну можливість інтегрувати в єдину систему різнорідні пристрої: датчики відкриття, температури, газоаналізатори, камери відеоспостереження, розумні приводи, електронні замки та інші виконавчі модулі. Це дозволяє створити безпечне, адаптивне та високотехнологічне середовище проживання, яке автоматично реагує на зміни умов та потреби користувача.

Загалом, отримані результати підтверджують, що впровадження системи «Розумний будинок»:

- підвищує рівень комфорту, безпеки та енергоефективності житла;
- знижує експлуатаційні витрати;
- забезпечує своєчасне виявлення небезпечних ситуацій;
- зменшує людський фактор у керуванні побутовими процесами;
- має високу гнучкість і можливість подальшої модернізації.

Отже, розроблена в роботі концепція та реалізована модель системи є актуальною, технічно обґрунтованою та перспективною для реального впровадження в умовах розвитку смарт-інфраструктури України у 2025 році. Створена архітектура може стати основою для подальших досліджень і розширення функціоналу, зокрема у напрямках штучного інтелекту, прогнозної аналітики, інтеграції з енергетичними мережами та використання глобального стандарту Matter.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Architecture of Internet of Things [Електронний ресурс]; Режим доступу до ресурсу: https://www.geeksforgeeks.org/computer-networks/architecture-of-internet-of-things-iot/
2. Smart Homes and Their Users: A Systematic Review. – *Journal of Ambient Intelligence and Humanized Computing*, 2020.
3. Home Assistant офіційна документація [Електронний ресурс]; Режим доступу до ресурсу: https://www.home-assistant.io/installation/
4. Governing Documents and Support from The Alliance [Електронний ресурс] Режим доступу до ресурсу: https://csa-iot.org/resources/developer-resources/
5. Технології Інтернету речей. Навчальний посібник / Б. Ю. Жураковський, І. О. Зенів. Київ : Київський політехнічний інститут імені Ігоря Сікорського, 2021. – Електронне видання.
6. Про охорону праці № 2694-XII: Закон України від 14 жовтня 1992 року із змінами та доповненнями у редакція від 05.12.2019 [Електронний ресурс]; Режим доступу: https://zakon.rada.gov.ua/laws/show/2694-12#Text
7. An Overview of Home Automation Systems [Електронний ресурс]; Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7791223/
8. Bear Stone Smart Home Documentation [Електронний ресурс]; Режим доступу до ресурсу: https://github.com/CCOSTAN/Home-AssistantConfig
9. Спосіб організації системи управління «Розумний дім» [Електронний ресурс]; Режим доступу до ресурсу: https://ela.kpi.ua/items/b69a2158-09d4-4265-b9d0-9d6087b218c8
10. An IoT-based smart home prototype: Enhancing energy efficiency, water conservation, and sustainability education [Електронний ресурс]; Режим доступу до ресурсу: https://joease.id/index.php/joease/article/view/148/70

11. ADVANCEMENTS IN AI-DRIVEN IOT SYSTEMS FOR SMART HOME ENERGY EFFICIENCY [Електронний ресурс]; Режим доступу до ресурсу: https://ephijse.com/index.php/SE/article/view/293/369

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інформаційних систем та технологій

«Концепція впровадження системи «Розумний будинок» на основі технології IoT»

Виконав: студент групи ІСДМм-62 Андрій АВРАМЕНКО

Науковий керівник: PhD Валентина ДАНИЛЬЧЕНКО

МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

Мета роботи - розробка алгоритмів управління підсистемами автоматизації, безпеки та клімат-контролю на базі концепції IoT для підвищення комфорту і безпеки мешканців.

Об'єкт дослідження - інтегровані системи автоматизації житлових об'єктів.

Предметом дослідження є - алгоритми та методи управління підсистемами «Розумного будинку» та їх практична реалізація.

Актуальність теми зумовлена сучасними тенденціями розвитку житлових технологій, які потребують створення інтегрованих систем, що забезпечують не лише функціонування будівлі, а й підвищення якості життя її мешканців. Зростаючий рівень автоматизації дозволяє здійснювати ефективне управління комплексними процесами - контролем мікроклімату, безпеки, освітлення та побутової техніки. Впровадження таких рішень сприяє підвищенню комфорту, раціональному використанню ресурсів та дає можливість власникам будинків знижувати операційні витрати на обслуговування інженерних систем.

ЗАВДАННЯ ПРОЕКТУ

1. Дослідити сучасні методи автоматизації побутових і кліматичних систем.
2. Провести аналіз інтеграції систем безпеки та відеоспостереження у житлові приміщення.
3. Розробити алгоритми управління системами кондиціонування та опалення.
4. Визначити принципи побудови єдиної мережі підсистем із використанням технології IoT.
5. Визначити принципи побудови єдиної мережі підсистем із використанням технології IoT.

Порівняння готових апаратно-програмних рішень

Критерій	Home Assistant	LG ThinQ	Amazon Echo	OpenHAB	Apple HomeKit	Homey	Google Home	Mi Home
Цінова доступність	Висока	Середня	Середня	Висока	Низька	Низька	Середня	Висока
Модульність	Висока	Середня	Середня	Висока	Середня	Висока	Середня	Середня
Масштабованість	Висока	Висока	Висока	Висока	Середня	Висока	Висока	Середня
Підтримка протоколів	Zigbee, Z-Wave, MQTT, Thread та інші	Matter, Zigbee, Thread	Wi-Fi, Zigbee (через хаби)	Zigbee, Z-Wave, MQTT, HTTP та інші	Wi-Fi, Thread, Matter	Zigbee, Z-Wave, Wi-Fi, Bluetooth, Matter	Wi-Fi, Thread, Zigbee (через хаби)	Zigbee, Wi-Fi
Підтримка обладнання різних виробників	Широка	Середня	Висока	Широка	Обмежена	Висока	Висока	Обмежена
Інтуїтивність інтерфейсу	Середня	Висока	Висока	Середня	Висока	Висока	Висока	Висока
Адаптивність під користувача	Висока	Середня	Середня	Висока	Середня	Висока	Середня	Середня
Технічна підтримка / ком'юніті	Спільнота	Офіційна підтримка	Офіційна + спільнота	Спільнота	Офіційна підтримка	Офіційна підтримка	Офіційна + спільнота	Офіційна
Відкритість	Повністю відкрита	Частково відкрита	Частково	Повністю відкрита	Закрита	Частково	Частково	Частково

5

Вибір рішення та його обгрунтування

В межах даної дипломної роботи обрано локальну архітектуру управління на базі **Home Assistant**.

Цей вибір обумовлений такими факторами:

- безперервність роботи - система повністю функціонує без Інтернету;
- підвищена інформаційна безпека - дані користувачів не передаються у хмару;
- висока сумісність з великою кількістю розумних пристроїв;
- масштабованість архітектури - можливість підключення нових підсистем без повної перебудови системи;
- відсутність регулярних платежів за використання сервісів.

Також Home Assistant підтримує:

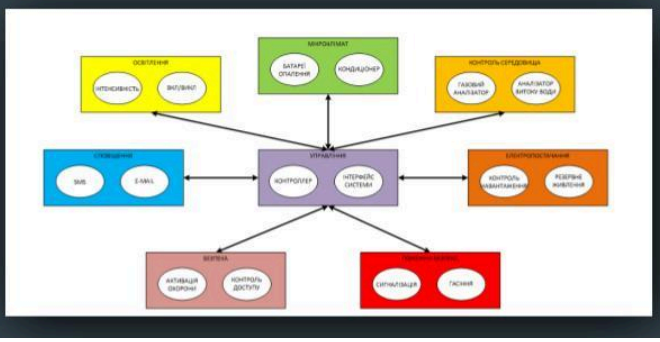
- локальні протоколи ZigBee, Z-Wave, MQTT;
- інтеграцію камер відеонагляду;
- керування освітленням, кліматом, системами безпеки;
- автоматизацію сценаріїв на основі умов і подій.

6

Принципи побудови системи та її модель-схеми

На основі дослідження вимог до проєктованої системи визначено такі основні принципи її побудови:

- використання центрального серверу управління з частковою автономністю локальних контролерів;
- підтримка дротових і бездротових протоколів зв'язку: **Ethernet / PoE, Wi-Fi, Zigbee**;
- гнучка масштабованість та можливість підключення обладнання різних виробників;
- використання відкритих протоколів взаємодії пристроїв у межах IoT-екосистеми;
- оперативне сповіщення користувача через мобільний застосунок та **Telegram**;

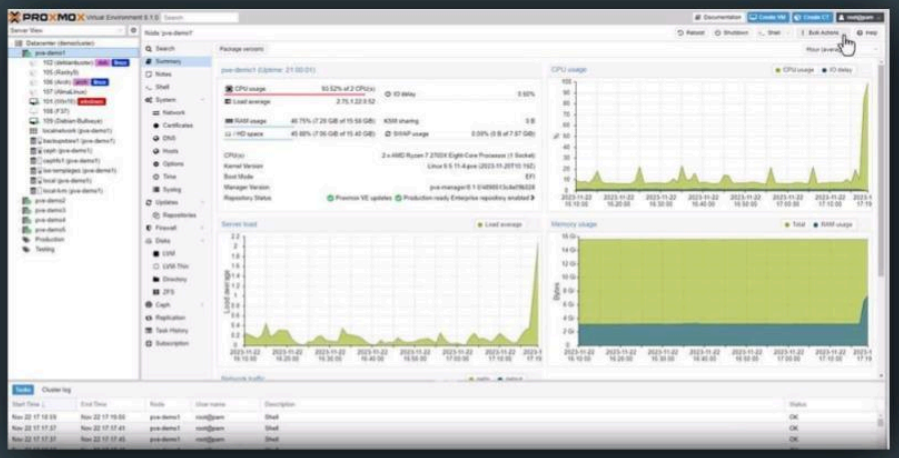


7

Елементи управління

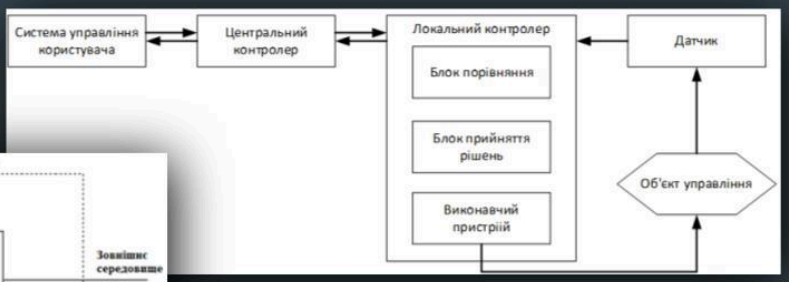
В якості головного елемента управління обрано **Proxmox VE** - високопродуктивний сервер віртуалізації

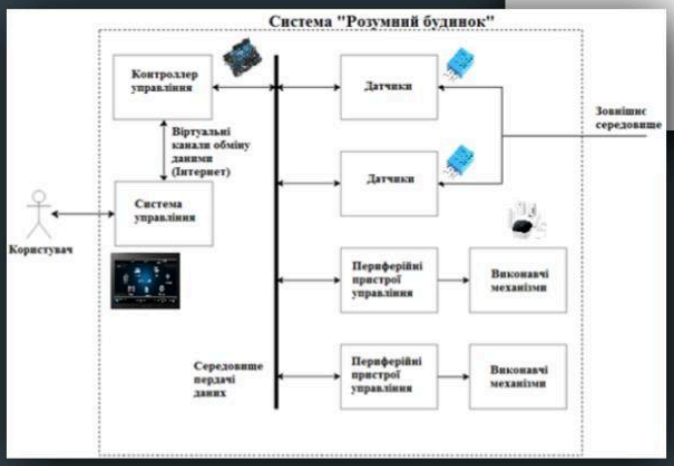
Для інтеграції та керування бездротовими пристроями використовується **Zigbee 3.0 координатор SMLight SLZB-06P7 з інтерфейсами Ethernet і Wi-Fi**



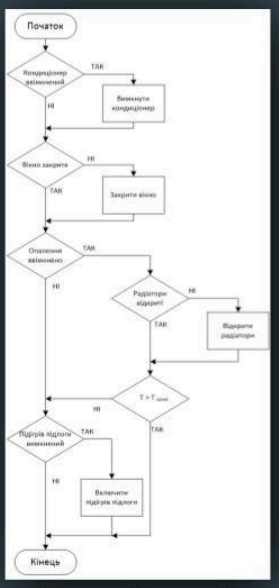
8

Структурна та функціональна схеми системи

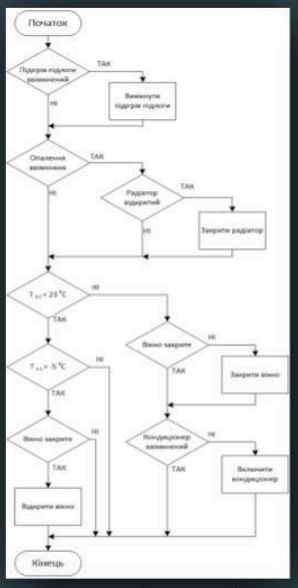




Алгоритми роботи клімат контролю



Алгоритм роботи сценарію підвищення температури



Алгоритм роботи сценарію зниження температури

Алгоритми функціонування систем відеонагляду

Алгоритм роботи охоронної підсистеми включає 2 режими:

Нормальний режим (користувач вдома):

- Геркони та датчики руху працюють у фоновому режимі
- Події тільки логуються у системі
- Камери ведуть запис за детекцією руху

Активований охоронний режим («Охорона»):

- Якщо будь-який з охоронних датчиків спрацьовує - система перевіряє статус користувача (за геолокацією та шифрованим ключем).
- **У разі підтвердження тривоги:**
  - активується сирена
  - починається безперервний запис відео з камер у зоні спрацювання
  - користувач отримує миттєве сповіщення Telegram та push-сповіщення мобільного додатку

Алгоритми функціонування систем інженерної безпеки

Тип датчика	Умова спрацювання	Дії системи
Датчик води	Виявлено контакт з рідиною	Закрити електромагнітний клапан водопроводу; надіслати сповіщення; активувати камеру відповідної зони
Датчик газу (метан/CO)	Перевищення порогової концентрації	Відкрити вікно (якщо можливо); увімкнути вентиляцію; надіслати тривожне сповіщення
Датчик диму / CO_2	Фіксується задимлення	Увімкнути сирену; надіслати сповіщення; активувати режим евакуації
Датчик температури	Перегрів системи або різке підвищення	Надіслати попередження; зафіксувати подію в журналі (логування)

ВИСНОВКИ

1. **Проведено комплексне дослідження концепції системи «Розумний будинок»**, включно з аналізом технологій Інтернету речей, архітектурних підходів, апаратних та програмних платформ, протоколів комунікації та засобів захисту даних.
2. **Розроблено архітектуру локальної IoT-системи на базі Home Assistant**, що забезпечує автономність, безпеку даних, масштабованість та мінімізацію залежності від хмарних сервісів.
3. **Створено структурну модель системи та алгоритми роботи ключових підсистем**, таких як клімат-контроль, охоронна система, відеонагляд, освітлення та аварійний моніторинг небезпечних станів.
4. **Реалізовано практичну інтеграцію різнорідних IoT-пристроїв** (датчиків, камер, приводів, замків, сенсорів небезпеки) в єдине середовище Home Assistant з налаштованою автоматизацією та сценаріями реагування.
5. **Сформовано та впроваджено принципи кіберзахисту IoT-системи**.

АПРОБАЦІЯ:
1. Всеукраїнська науково-практична конференція «Актуальні проблеми кібербезпеки», на тему «СМАРТ-ТЕХНОЛОГІЇ ТА ІНТЕРНЕТ РЕЧЕЙ», ст.36, 24 жовтня 2025 року.
2. III Всеукраїнська науково-технічна конференція «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу», на тему «ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ТА ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМАХ «РОЗУМНОГО БУДИНКУ», 18 листопада 2025 року.

Дякую за увагу!