ВСТУП

На сьогоднішній день вже дуже багато «розумних» будинків створено. Їх створюють для того, щоб людині було комфортно, безпечно та простіше жити.

Комфорт та безпека досягається за рахунок використання високотехнологічних пристроїв та автоматизації. У розумному будинку комфорт забезпечується для всіх користувачів.

У найпростішому випадку система «розумного дому» повинна вміти розпізнавати конкретні ситуації, що відбуваються в будинку, і відповідним чином на них реагувати. Вона повинна вміти працювати за сценаріями, які заздалегідь створюються. Наприклад о шостій ранку увімкнути чайник та закип’ятити воду, щоб коли людина прокинулася, то одразу могла зробити чай або каву і не витрачати зайвий час на очікування. Або коли система збирає безліч даних погоди і враховує інші фактори, щоб зробити правильну та комфортну температуру для перебування. Система також оберігає і оселю і користувачів, якщо станеться якесь лихо, будь-то пожежа чи протік водопроводу вдома, то система повідомить користувачів та спеціальні служби, які негайно допоможуть у ліквідуванні проблеми.

Система «розумного дому» дуже економить час людині та робить життя безпечнішим. А безпечним життя буде, якщо своєчасно буде виявлено небезпеку, яка може статися з кожним. Саме тому, необхідно щоб система «розумного дому» працювала безвідмовно і максимально правильно виконувала сценарії.

Метою цієї роботи є оптимізувати організацію системи «розумного дому», об’єктом дослідження є процес функціонування систем, які використовуються для створення «розумного дому», а предметом дослідження є технології, параметри та характеристики систем управління "розумний дім".

1. Дослідження розвитку та перспектив концепції Інтернету речей.

1.1 Що таке IoT і його розвиток

Епоха Інтернету речей почалася в період з 2008 по 2009 рік.

За цей період кількість пристроїв, підключених до Інтернету, перевищила світове населення.

Людина, якій приписують створення терміну Інтернет речей, - це Кевін Ештон. Працюючи в Procter & Gamble у 1999 році, Кевін використав цю фразу, щоб пояснити нову ідею, пов'язану з підключенням ланцюжка постачання компанії до Інтернету. Кевін згодом пояснив, що Інтернет речей тепер включає додавання «почуттів» до комп'ютери. Його цитували: «У XX столітті комп'ютери були мозком без почуттів – вони знали лише те, що ми їм говорили». Комп'ютери залежали від людей для введення даних та знань за допомогою набору тексту, штрих-кодів і т. д. Інтернет речей змінює цю парадигму. У епоху інтернету речей комп'ютери відчувають речі самі.

Широко визнано, що інтернет речей - це серйозне технологічний прорив, але які його масштаби та важливість? Яке місце це займає у розвитку Інтернету?

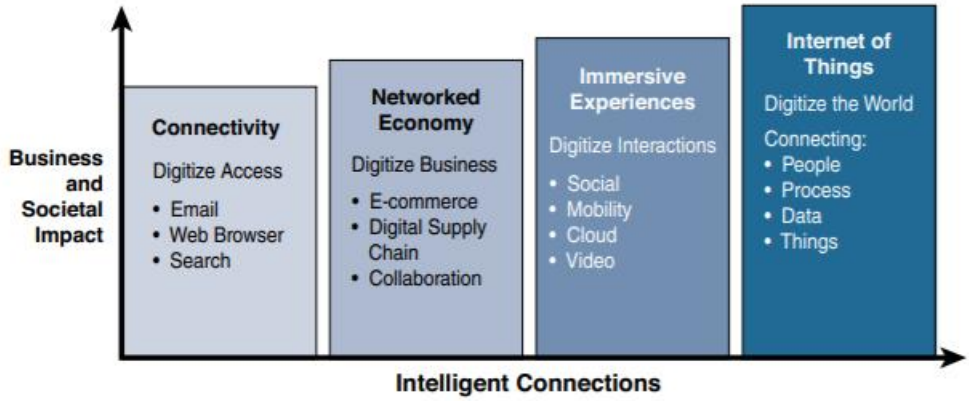

Рисунок 1.1 – Еволюційні фази Інтернету

Еволюцію Інтернету (рис. 1.1) можна поділити на чотири фази. Кожен із цих етапів вплинув на наше суспільство і наше життя. Ці чотири фази визначено у таблиці 1.1.

Таблиця 1.1 – Еволюційні фази Інтернету

Інтернет-фаза	**Визначення**
Підключення (Оцифрований доступ)	Ця фаза підключала людей до електронної пошти, веб-сервісів і пошуку, щоб інформація для кожного була легко доступною.
Мережева економіка (Оцифрувати бізнес)	Ця фаза дозволила вдосконалити електронну комерцію та ланцюг поставок разом із спільним залученням для підвищення ефективності бізнес-процесів.
Захоплюючий досвід (Оцифрування взаємодії)	Цей етап розширив досвід Інтернету, щоб охопити широко поширене відео та соціальні медіа, завжди будучи підключеним до інтернету. Все більше додатків переміщуються в хмару.
Інтернет речей (Оцифрувати світ)	На цьому етапі додається підключення до об’єктів і машин у навколишньому світі, щоб створити нові послуги та досвід.

Кожна з цих еволюційних фаз залежить від попередньої. З кожним наступним етапом все більше цінностей стає доступнішими для бізнесу, уряду та суспільства в цілому.

Початок першої фази припадає на 1990 рік. Спочатку електронна пошта та доступ до Інтернету були розкішшю для університетів і великих компаній. Підключення звичайної людини до Інтернету через комутований модем або навіть базове підключення часто здавалося неймовірним.

Незважаючи на те, що підключення та його швидкість продовжували покращуватися, була досягнута точка, коли підключення більше не було основною проблемою. Тепер увага зосереджена на використанні підключення для ефективності та прибутку. Ця точка і стала початком другого етапу еволюції Інтернету, який називається мережевою економікою.

З мережевою економікою електронна комерція та цифрові ланцюги поставок стали популярними, що спричинило одну з головних проблем за останні 100 років. Постачальники тісно зв'язалися з виробниками і інтернет-магазини зазнали неймовірної популярності. Жертвами цієї зміни стали традиційні роздрібні торговці. Сама економіка стала більш цифровою взаємопов'язаною, оскільки відносини постачальників та споживачів стали більш прямими.

Третя фаза характеризується появою соціальних мереж та широкого розповсюдження їх на різних пристроях. Зараз підключення до інтернету можливо виконати з будь-якого пристрою, будь-то мобільний телефон або планшетів, чи ноутбук або настільний комп'ютер. Підключення з будь-якого девайсу , дає змогу спілкуватися та співпрацювати, а також використовувати соціальні мережі через декілька каналів, за допомогою електронної пошти або текстових повідомлень, голосу та відео. Можна сказати, що спілкування між людьми стало більше цифровим.

Останній етап – Інтернет речей. Незважаючи на всі розмови та висвітлення в ЗМІ про IoT, багато в чому розвиток лише на початку цього етапу. Якщо подумати про те, що 99% інтернет «речей» все ще не пов'язані між собою, можна зрозуміти, що це еволюційна фаза. Машини та об'єкти на цій фазі з'єднуються з іншими машинами та об'єктами, а також з людьми. Бізнес і суспільство вже пішли цим шляхом і відчувають величезне зростання даних і знань. Своєю чергою, тепер це призводить до раніше невідомих ідей, а також до підвищення автоматизації та нової ефективності процесів. IoT готовий змінити світ новими та інноваційними способами, як і минулі етапи Інтернету.

1.2 IoT та оцифрування

IoT і оцифрування – це терміни, які часто використовуються як синоніми. У більшості контекстів ця подвійність є нормальною, але є ключові відмінності, про які слід знати.

На високому рівні IoT зосереджується на підключенні «речей», таких як об’єкти та машини, до комп’ютерної мережі, наприклад Інтернету. IoT – це добре зрозумілий термін, який використовується в індустрії в цілому. З іншого боку, оцифрування може означати різні речі для різних людей, але загалом охоплює зв’язок «речей» з даними, які вони генерують, і бізнес-інсайтами, які випливають з цього.

Наприклад, у торговому центрі, де розгорнуто відстеження місцезнаходження по Wi-Fi, «речами» є пристрої Wi-Fi. Відстеження місцезнаходження по Wi-Fi — це просто можливість знати, де знаходиться споживач у торговельному середовищі через підключення його смартфона до мережі Wi-Fi продавця. Хоча цінність підключення Wi-Fi-пристроїв або «речей» до Інтернету очевидна і цінується покупцями, відстеження місцезнаходження клієнтів Wi-Fi у режимі реального часу надає особливу перевагу бізнесу для власників торгових центрів і магазинів. У цьому випадку це допомагає бізнесу зрозуміти, де зазвичай збираються покупці та скільки часу вони проводять у різних частинах торгового центру чи магазину. Аналіз цих даних може призвести до суттєвих змін у місцях розміщення демонстрацій товарів та реклами, де розміщувати певні типи магазинів, скільки платити за оренду та навіть де розміщувати охоронців і тому подібне.

Оцифрування, як її визначають у найпростішій формі, — це перетворення інформації в цифровий формат. Оцифрування в тій чи іншій формі відбувається вже кілька десятиліть. Наприклад, оцифрована вся фотоіндустрія. Зараз практично у кожного є цифрові камери, як окремі пристрої, так і вбудовані в мобільні телефони. Майже ніхто не купує плівку

і не відносить її на прояву. Цифрування фотографії повністю змінило наш досвід, коли справа доходить до зйомки зображень.

Інші приклади оцифрування включають індустрію прокату відео та транспорт. Раніше люди ходили в магазин, щоб взяти напрокат або придбати відеокасети чи DVD-диски з фільмами. Завдяки оцифрування майже всі передають відеоконтент або купують фільми у вигляді файлів, які можна завантажити з будь-якого кутку світу, де є доступ в інтернет.

Транспортна галузь зараз проходить оцифрування у сфері послуг таксі. Така компанія, як Uber, використовує цифрові технології, щоб люди могли проїхатися за допомогою програми для мобільних телефонів. Ця програма визначає автомобіль, водія та вартість проїзду. Потім водій оплачує вартість проїзду за допомогою програми.

У контексті IoT оцифрування об’єднує речі, дані та бізнес-процеси, щоб зробити мережеві з’єднання більш актуальними та цінними. Хорошим прикладом цього, з яким можуть ознайомитися багато людей, є сфера домашньої автоматизації з популярними продуктами, такими як Nest. З Nest датчики визначають бажані налаштування клімату, а також підключають інші розумні об’єкти, як-от димові сигналізатори, відеокамери та різні сторонні пристрої. У минулому ці пристрої та функції, які вони виконують, керувалися та контролювались окремо і не могли забезпечити цілісний досвід, який тепер можливий. Nest — це лише один із прикладів оцифрування та Інтернету речей, які підвищують актуальність і цінність мережевих інтелектуальних з’єднань і позитивно впливають на наше життя.

Сьогодні компанії дивляться на оцифрування як на відмінну рису для свого бізнесу, а IoT є основним фактором цифровізації. Розумні об’єкти та розширені можливості підключення стимулюють оцифрування, і це одна з головних причин того, що багато компаній, країн та урядів сприймають цю тенденцію зростання.

1.3 Вплив Інтернету речей

Сьогодні близько 22 мільярдів «речей» підключено до Інтернету. Спеціалісти прогнозують, що до 2025 року ця цифра сягне 70 мільярдів. У доповіді уряду Великобританії припускається, що ця цифра може бути ще вищою — у діапазоні 100 мільярдів підключених об’єктів. Крім того нові з’єднання призведуть до 19 трильйонів доларів прибутку та економії витрат. На рисунку 1.2 наведено графічне зображення зростання кількості підключених пристроїв.

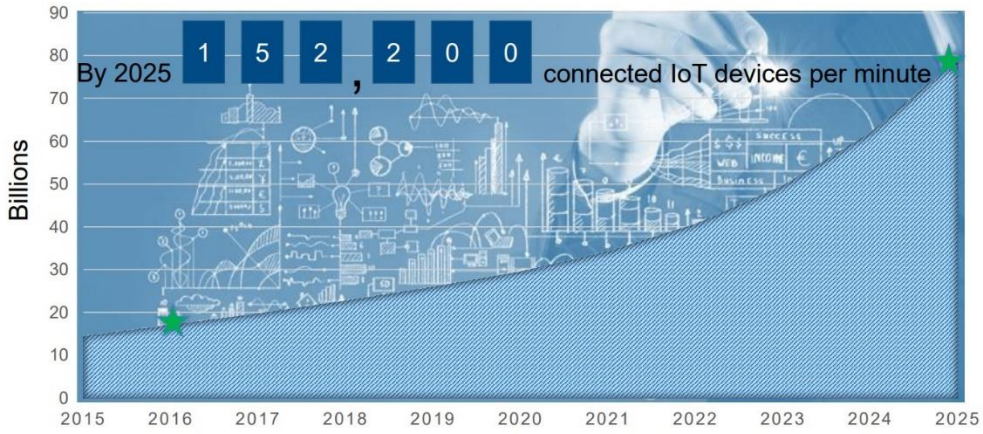

Рисунок 1.2 – зображення зростання кількості підключених пристроїв

Ці цифри означають, що IoT кардинально змінить спосіб взаємодії людей і підприємств із оточенням. Управління та моніторинг смарт-об’єктів за допомогою підключення в режимі реального часу дає змогу на абсолютно новому рівні приймати рішення на основі даних. Це, в свою чергу, призводить до оптимізації систем і процесів і надає нові послуги, які економлять час як людям, так і підприємствам, одночасно покращуючи загальну якість життя.

У літературі та кіно люди фантазували про самокерований автомобіль або автономний автомобіль протягом десятиліть. Хоча ця фантазія зараз стає реальністю з відомими проектами, такими як самокерований автомобіль Google (рис.1.3), IoT також є необхідним компонентом для впровадження повністю підключеної транспортної інфраструктури.

Рисунок 1.3 – самокерований автомобіль від Google

IoT дозволить самокерованим транспортним засобам краще взаємодіяти з транспортною системою навколо них шляхом двостороннього обміну даними, а також надавати важливі дані водіям. Щоб повністю розкрити свій потенціал, автономним транспортним засобам потрібен постійно ввімкнений надійний зв'язок і дані від інших датчиків, пов'язаних із транспортуванням. З'єднані дороги – це термін, пов'язаний з як водієм, так і безпілотними автомобілями, які повністю інтегруються з навколишньою транспортною інфраструктурою.

Основні датчики вже є в автомобілях. Вони контролюють тиск масла, тиск в шинах, температуру та інші умови експлуатації, а також надають дані про основні функції автомобіля. З-за керма водій може отримати доступ до цих даних, а також керувати автомобілем за допомогою такого обладнання, як кермо, педалі тощо. Потреба всієї цієї сенсорної інформації та контролю очевидна. Водій повинен вміти розуміти, керувати та приймати важливі рішення, концентруючись на безпечному водінні. Інтернет речей реплікує цю концепцію в набагато більших масштабах.

Сьогодні ми бачимо автомобілі, що випускаються з тисячами датчиків, щоб вимірювати все: від споживання палива до місця прибуття, які відео

ваша родина дивиться під час поїздки. Оскільки виробники автомобілів намагаються заново винайти відчуття водіння, ці датчики стають підтримкою IP, щоб забезпечити легкий зв'язок з іншими системами як всередині, так і зовні автомобіля. Крім того, розробляються нові датчики та комунікаційні технології, які дозволяють транспортним засобам «спілкуватися» з іншими транспортними засобами, світлофорами та іншими елементами транспортної інфраструктури. Зараз починається реалізація рішення для підключеного транспорту.

Більшість рішень зосереджені на вирішенні сучасних транспортних проблем.

До цих проблем можна віднести:

а) безпека;

б) мобільність;

в) навколишнє середовище.

Кожного року відбувається велика кількість дорожньо-транспортних пригод, у яких гинуть люди і це найперша проблема яку потрібно вирішувати. Саме тому і роблять машини з автопілотом у яких дуже багато датчиків і які набагато швидше зреагують на ситуацію, ніж людина, та зможуть уникнути дорожньо-транспортної пригоди.

Зараз понад мільярд автомобілів на дорогах у всьому світі. Підключені додатки до інтернету у транспортних засобах можуть дозволити системним операторам і водіям приймати більш обґрунтовані рішення, що, у свою чергу, може зменшити затримки в дорозі. Затори спричиняють 5,5 мільярдів годин затримок у дорозі на рік, і скорочення затримок у поїздках є більш важливим, ніж будь-коли раніше. Крім того, зв'язок між громадським транспортом, транспортними засобами аварійного реагування та інфраструктурами управління рухом допомагає оптимізувати маршрути транспортних засобів, ще більше зменшуючи потенційні затримки.

Зараз на дорогах дуже багато машин, будь-то громадський транспорт чи власний автомобіль, увесь цей транспорт виділяє велику кількість

вуглекислого газу (CO2). Саме тому активно розроблюють електромобілі, які збережуть навколишнє середовище.

Протягом багатьох років традиційні фабрики працювали в невигідному становищі, їм заважали виробничі середовища, які «відключені» або, принаймні, «строго закриті» від корпоративних бізнес-систем, ланцюгів поставок, клієнтів і партнерів. Менеджери цих традиційних фабрик, по суті, «працюють наосліп» і не бачать їхньої діяльності. Ці операції складаються з заводів, передніх офісів і постачальників. Отже, усунути проблеми з простоями, проблеми з якістю та першопричини різної неефективності виробництва часто важко.

Основні проблеми, з якими сьогодні стикається виробництво у заводських умовах, включають наступне:

а) прискорення впровадження нових продуктів і послуг для задоволення можливостей клієнтів і ринку;

б) збільшення виробництва, якості та безперебійної роботи заводу при зниженні вартості;

в) пом'якшення незапланованих простоїв (на які витрачається в середньому щонайменше 5% виробництво);

г) захист заводів від кіберзагроз;

д) зменшення високих витрат на прокладку кабелів і перепрокладку (до 60% витрат на розгортання);

е) підвищення продуктивності та безпеки працівників.

Ще один рівень ускладнення до цих проблем полягає в тому, що їх часто потрібно вирішувати на різних рівнях виробничого бізнесу. Наприклад, виконавче керівництво шукає нові шляхи виробництва більш рентабельним способом врівноважуючи зростаючі витрати енергії та матеріалів. Розробка продукту має час вийти на ринок як головний пріоритет. Керівники заводів повністю зосереджені на підвищенні ефективності та оперативності роботи заводу. За заводом доглядає відділ

контролю та автоматизації мереж, елементів керування та додатків, і тому вимагає повної видимості всіх цих систем.

Промислові підприємства по всьому світу переоснащують свої заводи передовими технологіями та архітектурами, щоб вирішити ці проблеми та підвищити гнучкість та швидкість виробництва. Ці вдосконалення допомагають їм досягти нових рівнів загальної ефективності обладнання, швидкості реагування ланцюга поставок і задоволеності клієнтів. Починає відбуватися конвергенція операційних технологій та архітектур на базі фабрик із глобальними IT-мережами, і це називається підключеною фабрикою.

Як і у випадку з рішеннями IoT для підключених доріг, про які йшлося раніше, на заводах вже існує велика кількість базових датчиків. Проте з IoT ці датчики не тільки стають більш досконалими, але й досягають нового рівня підключення. Вони стають розумнішими та мають здатність спілкуватися, в основному за допомогою Інтернет-протоколу (IP) через інфраструктуру Ethernet.

На додаток до датчиків, пристрої на заводі стають розумнішими у своїй здатності передавати та отримувати велику кількість інформаційних та діагностичних даних у реальному часі. З'єднання Ethernet стає все більш поширеним і поширюється за межі лише основних контролерів на заводі до таких пристроїв, як роботи на заводі. Крім того, до виробничого середовища додається більше пристроїв із підтримкою IP, включаючи відеокамери, діагностичні смарт-об'єкти та навіть персональні мобільні пристрої.

Інше місце, де IoT робить важливий вплив, — це простір розумних підключених будівель. Протягом останніх кількох десятиліть будівлі ставали дедалі складнішими, системи накладалися одна на одну, що призвело до складних перетинів структурних, механічних, електричних та IT-компонентів. З часом ці операційні мережі, які підтримують середовище будівлі, перетворилися на складні системи; однак, здебільшого, вони

розгортаються та керуються як окремі системи, які практично не взаємодіють одна з одною.

Функція будівлі полягає в тому, щоб забезпечити робоче середовище, яке забезпечує комфорт, ефективність і безпеку працівників. Робочі місця повинні бути добре освітлені і підтримуватися при комфортній температурі. Щоб забезпечити безпеку працівників, необхідно ретельно керувати системою пожежної сигналізації та пожежогасіння, а також системою дверної та фізичної охоронної сигналізації. Хоча інтелектуальні системи для сучасних будівель розгортаються та вдосконалюються для кожної з цих функцій, більшість із цих систем наразі працюють незалежно одна від одної — і вони не завжди враховують, де насправді перебувають мешканці будівлі та скільки з них перебуває в будівлі. Однак у багатьох будівлях починають розгортати датчики по всій будівлі для виявлення присутності. Це, як правило, датчики руху або датчики, прив'язані до відеокамер. Датчики виявлення руху чудово працюють, якщо всі пересуваються в переповненій кімнаті, і можуть автоматично вимикати світло, коли всі підуть, але що робити, якщо людина в кімнаті знаходиться поза полем зору датчика? Неприємно перебувати у владі нерозумного датчика на стіні, який хоче вимкнути світло, бо вважає, що нікого немає.

Аналогічно, датчики часто використовуються для управління системою опалення, вентиляції та кондиціонування повітря (HVAC). Датчики температури поширені по всій будівлі і використовуються для впливу на контроль над потоком повітря в кімнаті системою управління будівлею (BMS).

Іншим цікавим аспектом розумної будівлі є те, що це полегшує та зменшує вартість для керування ними. Враховуючи величезні витрати, пов'язані з експлуатацією таких складних конструкцій, не кажучи вже про те, скільки людей проводять часу на робочому місці всередині будівлі, менеджери все більше цікавляться способами зробити будівлі більш ефективними та дешевшими в управлінні. Інколи люди звертаються до своїх

менеджерів і просять змінити план приміщення, наприклад, просять збільшити площу приміщення, на якому вони працюють, і їх часто просять довести свою правоту. Але докази ефективності та використання підлоги на робочому місці, як правило, в кращому випадку є кумедними. Коли датчики розумних будівель і виявлення заповнюваності поєднуються з потужністю аналізу даних, стає легко продемонструвати використання плану поверху та довести свою правоту. Крім того, керівник будівлі може використовувати подібний підхід, щоб побачити, де підлога використовується неефективно, і використовувати цю інформацію для оптимізації доступного простору. Це призвело до епохи автоматизації будівель, уповноваженої IoT.

Хоча існує багато технічних рішень для догляду за системами будівництва, донедавна вони потребували окремих накладних мереж, кожна з яких відповідала за своє завдання. Намагаючись об'єднати ці системи в єдину структуру, було розроблено систему автоматизації будівлі (BAS), щоб забезпечити єдину систему управління системою HVAC, освітленням, пожежною сигналізацією та системою виявлення, а також контролем доступу. Усі ці системи можуть підтримувати різні типи датчиків і підключень до BAS. Потрібно з'єднати їх разом, щоб будівлею можна було керувати узгоджено.

Перш ніж ви зможете об'єднати гетерогенні системи, вони повинні з'єднатися на мережевому рівні та підтримувати загальний рівень сервісів, що дозволяє інтегрувати програми. Цінність конвергентних мереж добре задокументована. Наприклад, на початку 2000-х Cisco та кілька інших компаній виступали за конвергенцію голосу та відео в єдиних IP-мережах, які використовувалися спільно з іншими IT-додатками. Економія від масштабу та операційна ефективність були настільки величезними, що VoIP та технології спільної роботи зараз є нормою. Однак наближення до IP та загальної структури послуг для будівель відбувалося повільніше.

Наприклад, де-факто, комунікаційний протокол, відповідальний за автоматизацію будівлі, відомий як BACnet (Мережа автоматизації та

керування будівлі). Коротше кажучи, протокол BACnet визначає набір послуг, які дозволяють зв'язок на основі Ethernet між пристроями будівлі, такими як HVAC, освітлення, контроль доступу та системи виявлення пожежі. Ті самі комутатори Ethernet будівлі, що використовуються для IT, також можуть використовуватися для BACnet. Ця стандартизація також робить можливим точку перетину IP-мережі (якою керує IT-відділ) за допомогою пристрою шлюзу. В додаток, ACnet/IP було визначено для того, щоб «речі» в будівельній мережі могли спілкуватися через IP, що дозволило ближче консолідувати систему управління будівлею в єдиній мережі.

Іншою багатообіцяючою технологією IoT у розумних підключених будівлях, яка набуває широкого поширення, є «цифрова стеля». Цифрова стеля – це більше, ніж просто система управління освітленням. Ця технологія охоплює кілька різних мереж будівлі, включаючи освітлення, HVAC, жалюзі, CCTV (замкнуте телебачення) і системи безпеки, і об'єднує їх в єдину IP-мережу.

Центральне місце в технології цифрових стель займає система освітлення. Ринок освітлення в даний час переживає серйозний зсув у бік світлодіодів (LED). У порівнянні з традиційним освітленням, світлодіоди пропонують менше споживання енергії та набагато триваліший термін служби. Нижчі вимоги до живлення світлодіодних світильників дозволяють їм працювати від живлення через Ethernet (PoE), що дозволяє підключати їх до стандартних мережевих комутаторів.

У середовищі цифрової стелі кожен світильник або освітлювальний прилад безпосередньо під'єднані до мережі, забезпечуючи контроль та живлення над тією ж інфраструктурою. Цей перехід на світлодіодне освітлення означає, що єдина конвергентна мережа тепер може охоплювати світильники, які є частиною консолідованого управління будівлею, а також елементи, якими керує IT-мережа, підтримуючи голосові, відео та інші програми для передачі даних.

Подивившись на стелю в офісній будівлі, можна помітити, що кількість світильників легко перевищує кількість фізичних дротових портів — на значний відрив. Очевидно, що підтримка більшої кількості портів Ethernet і щільності IP-адрес вимагає деякої перебудови мережі, а також вимагає тихого безвентиляторного комутатора з підтримкою PoE на стелі. З огляду на це, довгостроковий бізнес-обґрунтування підтримки зниження витрат на електроенергію від світлодіодних світильників у порівнянні з традиційними люмінесцентними або галогенними лампами настільки значущий, що додаткові початкові інвестиції в мережу майже не мають значення. Бізнес-обґрунтування цифрової стелі стає ще міцнішим, коли будівля ремонтується або будується нова споруда. У цих випадках економічність прокладки кабелів CAT 6/5e у стелі порівняно з електричною проводкою з номінальною потужністю до кожного освітлення є значною.

Цінність енергозбереження світлодіодного освітлення на стелі з підтримкою PoE очевидна. Однак наявність сенсорного пристрою з підтримкою IP на стелі в кожній точці, де люди можуть бути присутніми, відкриває абсолютно новий набір можливостей. Наприклад, більшість сучасних світлодіодних стельових світильників підтримують датчики присутності. Ці датчики забезпечують збір даних про присутність з високою роздільною здатністю, які можна використовувати для вмикання та вимкнення освітлення, і ці ж дані можна об’єднати з розширеною аналітикою для керування іншими системами, такими як HVAC та безпека. На відміну від традиційних датчиків, які використовують елементарне виявлення руху, сучасні датчики освітлення інтегрують різноманітні технології визначення присутності, включаючи Bluetooth з низьким споживанням енергії (BLE) і Wi-Fi. Оскільки майже кожна людина сьогодні носить розумний пристрій, який підтримує BLE і Wi-Fi, все, що датчик повинен зробити, це виявити BLE або Wi-Fi-маяки з сусіднього пристрою. Коли хтось йде біля світла, місцезнаходження людини визначається, і бездротова система може надсилати інформацію, щоб керувати потоком повітря від системи HVAC в

цю зону в режимі реального часу, максимізуючи комфорт офісного працівника.

Інтелектуальне освітлення IoT не тільки забезпечує оптимізовані рівні освітлення на основі фактичної зайнятості та використання будівлі, але й дозволяє детально контролювати температуру, керувати виявленням диму та вогню, відеокамерами та контролювати доступ до будівлі. IoT дозволяє всьому цьому працювати через єдину мережу, що вимагає менше часу на встановлення та меншу загальну вартість володіння системою.

1.4 Конвергенція IT та ОП

Донедавна інформаційні технології (IT) та операційні технології (OT) здебільшого жили в окремих світах. IT підтримує підключення до Інтернету разом із відповідними даними та технологічними системами та зосереджено на безпечному потоці даних в організації. OT відстежує та контролює пристрої та процеси у фізичних операційних системах. Ці системи включають складальні лінії, комунальні мережі, виробничі приміщення, системи доріг та багато іншого. Як правило, IT не бере участь у виробництві та логістиці середовищ OT.

Зокрема, IT-організація відповідає за інформаційні системи бізнесу, такі як електронна пошта, файли та служби друку, бази даних тощо. Для порівняння, OT відповідає за пристрої та процеси, що діють на промислове обладнання, такі як заводські машини, лічильники, виконавчі механізми, пристрої автоматизації розподілу електроенергії, системи SCADA (диспетчерського контролю та збору даних) тощо. Традиційно OT використовував виділені мережі зі спеціалізованими протоколами зв'язку для підключення цих пристроїв, і ці мережі працювали повністю окремо від IT-мереж.

Управління ОТ пов'язане з життєвою силою компанії. Наприклад, якщо мережа, що з’єднує машини на заводі, виходить з ладу, машини не можуть функціонувати, і виробництво може зупинитися, що негативно вплине на бізнес приблизно на мільйони доларів. З іншого боку, якщо сервер електронної пошти (керований ІТ-відділом) виходить з ладу на кілька годин, це може дратувати людей, але навряд чи це вплине на бізнес приблизно на тому ж рівні. Таблиця 1.2 висвітлює деякі відмінності між мережами ІТ та ОТ та їх різні проблеми.

Таблиця 1.2 – відмінності між мережами ІТ та ОТ

Критерій	**Промислова мережа ОТ**	**ІТ-мережа підприємства**
Оперативний фокус	Підтримка роботи бізнесу 24x7	Керування комп’ютерами, даними та системою зв’язку співробітників у безпечний спосіб
Пріоритети	1. Доступність 2. Цілісність 3. Безпека	1. Безпека 2. Цілісність 3. Доступність
Типи даних	Дані моніторингу, контролю та нагляду	Голосові, відео, транзакційні та масові дані
Безпека	Контрольований фізичний доступ до пристроїв	Пристрої та користувачі, автентифіковані в мережі

Продовження таблиці

Критерій	**Промислова мережа ОТ**	**ІТ-мережа підприємства**
Наслідки невдачі	Порушення мережі ОТ безпосередньо впливає на бізнес	Це може вплинути на бізнес залежно від галузі, але можливі обхідні шляхи
Оновлення мережі (програмне або апаратне забезпечення)	Тільки під час експлуатаційного обслуговування вікон	Часто вимагає відключення вікна, коли працівників немає на місці; вплив можна пом’якшити
Уразливість безпеки	Низький: мережі ОТ ізольовані і часто використовують власні протоколи	Високий: потрібне безперервне виправлення хостів, а мережа підключена до Інтернету та потребує пильного захисту

Із розвитком Інтернету речей і протоколів, заснованих на стандартах, таких як IPv6, світ ІТ і ОТ зближується або, точніше, ОТ починає приймати мережеві протоколи, технології, транспорт і методи ІТ-організації та ІТ організація починає підтримувати оперативні вимоги, які використовуються ОТ. Коли ІТ та ОТ починають використовувати одні й ті ж мережі, протоколи та процеси, є очевидна економія на масштабі. Конвергенція не тільки зменшує обсяг необхідної капітальної інфраструктури, але й мережі стають легшими в експлуатації, а гнучкість відкритих стандартів дозволяє швидше розвиватися та адаптуватися до нових технологій.

Однак, як видно з таблиці 1.2, конвергенція ІТ і ОТ до єдиної консолідованої мережі створює кілька проблем. Між цими двома

організаціями існують принципові культурні та пріоритетні відмінності. IoT змушує ці групи працювати разом, коли в минулому вони діяли досить автономно. Наприклад, організація OT збентежена, коли IT планує зупинку на вихідні для оновлення програмного забезпечення без урахування вимог виробництва. З іншого боку, IT-група не розуміє поширеності власних або спеціалізованих систем і рішень, розгорнутих OT.

Візьмемо приклад розгортання якості обслуговування (QoS) в мережі. Коли IT-команда розгортає QoS, голосовий і відеотрафік майже повсюдно обробляється з найвищим рівнем обслуговування. Однак, коли система OT використовує одну й ту саму мережу, можна навести дуже вагомі аргументи, що трафіку OT в реальному часі слід надавати більший пріоритет, ніж навіть голосові, оскільки будь-які порушення в мережі OT можуть вплинути на бізнес.

З об’єднанням OT та IT, вдосконалюються обидві системи. OT більше дивиться на IT-технології з відкритими стандартами, такими як Ethernet та IP. У той же час IT стає більш діловим партнером OT, краще розуміючи бізнес-результати та операційні вимоги.

Загальна перевага спільної роботи IT та OT — це більш ефективний і прибутковий бізнес завдяки скороченню простоїв, нижчих витрат за рахунок економії масштабу, скорочення запасів і кращого часу доставки. Якщо конвергенція IT/OT керується правильно, IoT повністю підтримується обома групами. Це забезпечує сценарій «найкращого з обох світів», коли надійні промислові системи управління базуються на відкритій, інтегрованій та безпечній технологічній основі.

1.5 Проблеми Інтернету

Хоча майбутнє з підтримкою IoT створює вражаючу картину, воно не обходиться без значних проблем. Багато частин Інтернету речей стали

реальністю, але потрібно подолати певні перешкоди, щоб IoT став повсюдним у промисловості та нашому повсякденному житті. У таблиці 1.3 висвітлено кілька найбільш значущих проблем і проблем, з якими зараз стикається Інтернет речей.

Таблиця 1.3 – проблеми IoT

Проблема	**Опис**
Масштаб	У той час як масштаб IT-мереж може бути великим, масштаб OT може бути на кілька порядків більшим. Наприклад, одна велика електрична компанія в Азії нещодавно почала впроваджувати інтелектуальні лічильники на основі IPv6 у своїй електричній мережі. Якщо в цьому комунальному підприємстві працюють десятки тисяч співробітників (які можна вважати IP-вузлами в мережі), то кількість лічильників у зоні обслуговування становить десятки мільйонів. Це означає, що масштаб мережі, якою керує компанія, збільшився більш ніж у 1000 разів! Розділ 5, «IP як мережевий рівень IoT», досліджує, як розробляються нові підходи до проектування для масштабування мереж IPv6 до мільйонів пристроїв.

Продовження таблиці

Проблема	**Опис**
Безпека	Оскільки все більше «речей» зв’язуються з іншими «речами» та людьми, безпека стає все більш складною проблемою для IoT. Ваша поверхня загроз тепер значно розширена, і якщо пристрій зламано, його підключення викликає серйозну проблему. Зламаний пристрій може служити відправною точкою для атаки на інші пристрої та системи. Безпека IoT також поширена майже в усіх аспектах IoT.
Конфіденційність	Оскільки датчики стають все більш плідними в нашому повсякденному житті, велика частина даних, які вони збирають, буде специфічною для окремих людей та їх діяльності. Ці дані можуть варіюватися від інформації про стан здоров’я до моделей покупок і транзакцій у роздрібних закладах. Для підприємств ці дані мають грошову оцінку. Зараз організації обговорюють, кому належать ці дані та як окремі особи можуть контролювати, чи надаватимуться вони спільному доступу та з ким.

Продовження таблиці

Проблема	**Опис**
Великі дані і аналітика даних	Інтернет речей і його велика кількість датчиків спровокують потік даних, які необхідно обробляти. Ці дані нададуть важливу інформацію та розуміння, якщо їх можна обробляти ефективно. Однак проблема полягає в тому, щоб оцінити величезні обсяги даних, які надходять з різних джерел у різних формах, і робити це вчасно.
Сумісність	Як і будь-яка інша нова технологія, різні протоколи та архітектури борються за частку ринку та стандартизацію в рамках IoT. Деякі з цих протоколів та архітектур засновані на власних елементах, а інші є відкритими. Останні стандарти IoT допомагають мінімізувати цю проблему, але часто існують різні протоколи та реалізації для мереж IoT.

1.6 Висновки

У цьому розділі було досліджено поняття Інтернету речей. Що це таке та як працює, етапи створення та розвиток.

У цьому розділі також наведено історичний погляд на Інтернет речей, а також поточний погляд на Інтернет речей як наступну еволюційну фазу Інтернету.

Також описано на прикладах де і для чого використовуються Інтернет речі.

У цьому розділі визначено ряд концепцій і термінів IoT. Обговорюються відмінності між IoT та оцифруванням, а також зближення між IT та OT. Також описано проблеми, з якими стикається IoT.

2. Огляд систем «розумний дім».

2.1 Що таке «розумний дім»

Поняття «розумний дім» спочатку було лише у фантастичних творах та оповіданнях, але згодом у XX-сторіччі після того, як широко почали вводити електрику у будівлі та почався розвиток інформаційних технологій ідея «розумного дому» почала матеріалізовуватись. Вперше про віддалені прилади контролю судами та транспортними засобами у 1898 році можна віднести до розробки Ніколою Тесла [].

У побуті електронні прилади почали з’являтися у 1915-1920 роках, але на той час була проблема з енергозбереженням при використанні нових технологій, тому лише багаті люди могли собі дозволити використовувати нові технології. Першим з’явився пилосос, згодом тостер та холодильник, посудомийка, а у 1935 році пральна машина та у 1945 мікрохвильова піч. Усі ці електронні пристрої робили життя людей простішим, за рахунок економії часу та сил.

Після винаходів електронних приладів, люди почали думати як ще більше спростити життя та насолоджуватися їм. Тому почали з’являтися ідеї «розумного дому». Спочатку це були ідеї, бо були не достатньо розвинуті технології . Але з часом американський інженер Еміль Матіас у 1950 році створив концепцію першого розумного будинку (рис.2.1). За автоматизацію процесів відповідали кнопки, але на той час це виглядало дивним і не задалося перспективним проектом. Згодом у 1966 році американський інженер Джеймс Сазерленд створив комп’ютер Echo IV (рис.2.2). За допомогою комп’ютера можна було керувати домашнього кліматичною технікою, також він був здатний включати або виключати деякі прилади, а також друкувати списки покупок. Але у цього проекта не було перспективи на той час [].

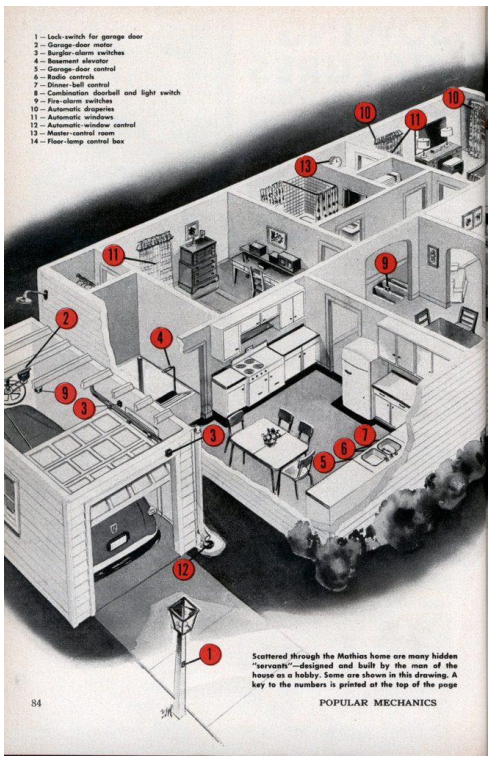

Рисунок 2.1 – Розумний будинок Еміля Матіаса

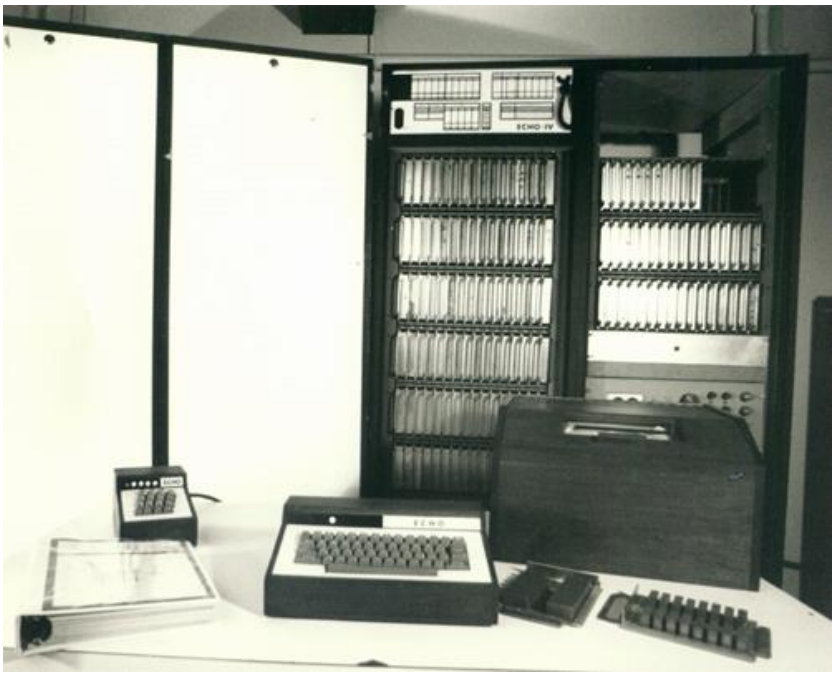

Рисунок 2.2 – Комп’ютер Echo IV Джеймса Сазерленда

Лише у 1975 році був створений перший протокол для управління домашніми пристроями який звався X10. Цей стандарт був розроблений шотландською компанією Pico Electronics (рис.2.3). Для цього протоколу

середовищем передачі даних була електронна мережа. Також було створено безпровідне керування на різних радіочастотах, у Європі стандартом було 433 МГц, а у США 310 МГц. Завдяки цій системі з'явилася можливість включати або виключати прилади, також можна було змінювати яскравість освітлення. Через низьку ціну та легкість у використанні та встановлені ця система доволі швидко розповсюджувалася. З цього часу і почали з’являтися «розумні будинки».

Рисунок 2.3 – Логотип компанії Pico Electronics

Під поняттям «розумним будинком» можна описати систему, яка повинна чітко розпізнавати ситуації, що відбуваються в будівлі і відповідним чином зреагувати на ту чи іншу ситуацію. Наприклад одна система може керувати станом інших систем по заздалегідь запрограмованим алгоритмам. Головна особливість «розумної» будівлі є об'єднання малих підсистем в єдину керовану систему. Головна ознака «розумного дому» полягає у тому, що людина завдяки одному пристрою може керувати усім домом, задати бажану комфортну обстановку однією командою, а уже автоматичне обладнання починає виконувати алгоритми та забезпечує комфортний стан всередині домашньої оселі завдяки підтримки потрібної температури повітря, полу, води з крану, м’якого освітлення як всередині будинку так і ззовні та багато іншого. []

2.2 Ідея «розумного дому»

Поняття «розумний дім» можна описати як "розумно побудований дім". Це означає, що будівля повинна бути спланована та побудована так, що всі сервіси могли комунікувати один з одним з мінімальними витратами (з точки зору фінансів, часу і трудомісткості), а їх обслуговування не займало багато часу и сил[].

Ідея технології «smart» для будинку з’явилася в середині XX століття, але саме поняття «розумний дім» виникло у 1984 році. Цю технологію можна описати як автоматизована система управління домашніми пристроями без участі людини. Людина може керувати цією системою за допомогою спеціального програмного забезпечення та доступу в інтернет, щоб мати змогу як і локально так і віддалено керувати будь-якою системою будинку. Програмне забезпечення може бути встановлено на будь-який девайс, будь то смартфон на Android або планшет на Apple. Встановлення «розумних» модулів можна робити як і при початку побудови будинку так і потім після завершення будівництва. Користувач системи може налаштувати функції «розумного дому» один раз. Після першого налаштування вони будуть працювати автоматично. Також можна в будь-який момент вносити корекції в роботу системи або ввімкнути або вискнути будь-який пристрій коли це буде потрібно.

Концепція «розумного дому» має містити такі положення:

а) інтегрована система управління будинком. Система у якої є можливість забезпечити комплексну роботу усіх систем у будинку. До цих систем можна віднести: опалення, водопостачання, освітлення, контролю доступу, вентиляції, пожежної безпеки, кондиціонування та безліч інших;

б) відсутність персоналу, який мав би обслуговувати «розумний дім», та передача контролю і прийняття рішень підсистемам інтегрованої системи

управління будинком. В цих підсистемах і відбуваються усі алгоритми та дії на різні ситуації, за рахунок того, що ці підсистеми є «розумом» будівлі;

в) наявність функції відключення і передачі управління людині будь-якою підсистемою «розумного дому» якщо є така необхідність, але також у людини, яка користується системою «розумного дому», повинен бути зручний доступ для управління і відображення всіх підсистем і частин «розумного дому»;

г) забезпечення роботи окремих підсистем, якщо відмовить загальна керуюча система або будь-яка інша частина системи;

д) мінімізація вартості обслуговування і модернізації системи «розумного дому». Досягти цього можна за допомогою використання загальних стандартів у побудові системи та підсистем, автоматичне конфігурування і додавання нових модулів і пристроїв при їх виявленні у системі;

е) наявність в будинку готового комунікаційного середовища для підключення до нього модулів та пристроїв системи. Можна використовувати слабкострумові лінії та силові лінії або радіоканал для комутації модулів та пристроїв системи.

2.3 Склад «розумного дому»

Система «розумного дому» складається з великої кількості компонентів:

а) центральний контролер (хаб), на якому знаходяться алгоритми роботи системи;

б) термостати, датчики, що зчитують середовище оселі (деякі встановлюються на цоколі будівлі);

в) панель керування для активації, управління обладнанням;

г) група підконтрольного обладнання: побутова техніка, розумні розетки, електрокрани, електрозамки, жалюзі на вікнах, автоматика розумного опалення, освітлення;

д) елементи живлення: реле, запобіжники, акумулятори.

Центральний контролер (рис.2.4) – це мозок всього дому. Завдяки ньому з’єднуються усе інше обладнання, яке використовується в системі «розумного дому». Хаб може бути як автономним, так і може залежати від інтернету, тобто якщо не буде доступу в інтернет, то система може працювати не повноцінно.

Рисунок 1.4 – Приклад зображення контролера

Датчики (рис.2.5) – це пристрої, які реєструють факт виникнення будь-якої події і перетворюють цю подію в електричний сигнал. Для розумного дому можуть застосовувати такі типи датчиків[]:

а) Датчик освітленості

б) Датчики вимірювання вологості повітря, тиску і температури

в) Датчики руху

г) Датчики розбиття скла

д) Датчики вимірювання чистоти та якості повітря

е) Датчики витоку води

ж) Датчик відкриття дверей та вікон

з) Датчик охорони периметра

и) Датчик дощу

Рисунок 2.5 – Приклад зображення датчиків

До панелей керування можна віднести планшети, мобільні телефони, комп'ютери та ноутбуки, спеціальні кнопки або універсальні пульти. Зазвичай використовують планшети або телефони на операційній системі IOS або Android, інколи на Windows. Завдяки спеціальним кріпленням можна закріпити панелі в декількох місцях у будинку, для зручності користування.

Після встановлення системи, частиною неї стануть мобільні гаджети, домашній комп’ютер. За допомогою програмного забезпечення можна буде здійснювати контроль через WiFi або мобільну мережу віддалено від дому у будь який час.

2.4 Базові можливості «розумного дому»

На сьогоднішній день «розумний дім» здатен виконувати безліч функцій, але можна виділити основні, які завжди майже скрізь використовуються. До базових можливостей можна віднести:

а) керування освітленням;

б) забезпечення безпеки;

г) регуляція температури;

д) водопостачання.

Для того щоб регулювати освітленням у будинку існує декілька способів:

а) дистанційний;

б) локальний;

в) за допомогою датчика руху;

г) управління по подіям;

д) за розкладом.

Дистанційний спосіб (рис.2.6) має свої різновиди.

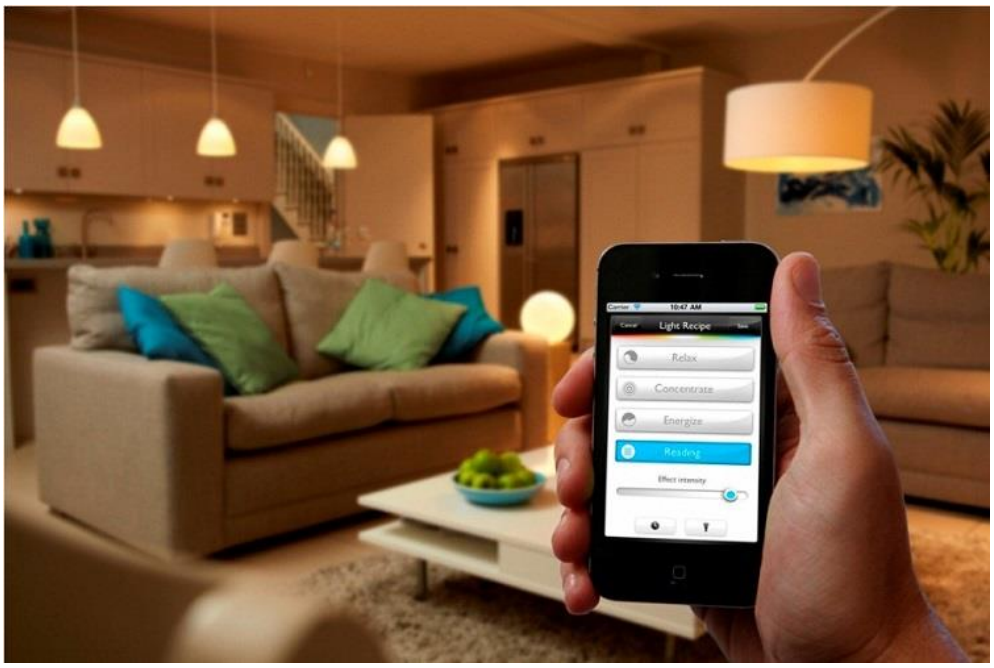

Рисунок 2.6 – Приклад дистанційного керування

Пульт керування. За допомогою цього пристосування регулювати освітлення можна з будь-якого куточка будинку. Можна спокійно почитати книгу при світлі в ліжку, а потім не встаючи одним натисканням кнопки на пульті вимкнути освітлення в кімнаті і лягти спати. А якщо виходячи з ванної, ви забули вимкнути освітлення, це можна буде вдіяти не повертаючись. При виході з будинку можна одним кліком відключити всі освітлювальні прилади. Група світильників може включати від 1 до більш ніж 200 одиниць. Пульти можуть бути кнопковими або з сенсорними дисплеями. Є можливість створення центрального пульта і додаткових, в формі брелків з основним набором функцій. Подібні системи використовуються в сценічному освітленні або освітленні нічного клубу, де потрібно одночасно налаштовувати безліч різнопланових світильників.

Управління за допомогою стаціонарного комп'ютера. Завдяки спеціальному програмному забезпеченню, можна керувати освітлювальними процесами в будинку за допомогою комп'ютерного пристрою.

Управління за допомогою комп'ютера з будь-якої точки світу. Доступ до центрального пристрою можна отримати через проміжний сервер. Ця можливість корисна людям, які постійно виїжджають з дому у відрядження або подорожі. Таким чином, можна перевірити вимкнене світло і провернути інші маніпуляції.

Дистанційне керування за допомогою мобільного телефону. Контроль над освітленням проводиться за допомогою спеціальних додатків на мобільному телефоні. Такі програми є на iPhone і Android.

Настінний контролер візуально схожий з класичним вимикачем, але це зовсім інший пристрій. Він не підключений до електричної мережі, його живить батарея. Контролер передає сигнали асоційованим вимикачів. Кнопки настінного контролера можна запрограмувати на кілька груп світильників. Такий апарат зручний на виході з дому, одним кліком можна вимкнути все світло в приміщенні.

Локальний контроль над освітленням здійснюється безпосереднім натисканням на вимикач. Цей тип управління можна поєднувати з дистанційним або іншими для ситуативного зручності.

Датчики руху (рис2.7) добре заощадять електрикою тим, хто забуває вимикати світло у ванній або вбиральні. Цей прилад фіксує рух в зоні видимості і виконує запрограмовані команди (включає / вимикає світло). Датчик руху може реагувати як на рух безпосередньо, так і на звук. У першому випадку він оснащений приймачем інфрачервоних променів. Людське тіло випромінює тепло і апарат на це реагує. Дана система абсолютно нешкідлива для людини і тварин в будинку. Для того щоб датчик не реагував на розігріті предмети, він оснащується декількома фотоелементами, а не одним. Акустичний прилад реагує на звуки. Такими датчиками оснащуються вуличні прожектори стежить світла.

Рисунок 2.7 – Приклад датчика руху

Контроль освітлення по подіям на увазі включення і виключення світла внаслідок певних змін у навколишньому середовищі. Регулюючим показником може виступати освітленість.

Вечірньої пори, коли рівень освітлення падає до зазначеного рівня, датчик зреагує і світло включиться, зворотний процес відбудеться в ранковий час.

Його можна встановити як всередині приміщення, так і до світильника, який знаходиться з зовнішньої сторони будинку. Цей прилад можна запрограмувати і на інші події. Наприклад, на відкривання / закривання дверей. Найчастіше він використовується в вуличному освітленні.

Управління світлом за часом дозволяє задати розклад, за яким світло будуть включатися і вимикатися. Рамки активності освітлення можна задати виходячи з розпорядку дня господарів будинку. Світло буде включатися і вимикається в зазначені проміжки часу. Цей спосіб управління освітленням можна використовувати в якості захисту від зловмисників у відсутності господарів. Буде створюватися ілюзія присутності. Також такий варіант використовується в рекламі, наприклад в рекламних світлових коробах.

Забезпечити безпеку у розумному домі можна за допомогою встановлення різних типів датчиків, які зможуть виявити небезпеку та повідомити як власників так і органи безпеки для вчасного реагування.

Датчики встановлюються не тільки всередині приміщення, але і по периметру.

Здійснювати контроль за периметром будинку, вчасно реагувати на несанкціоноване проникнення на територію – все це можливо завдяки правильному встановленні датчиків та сенсорів.

Датчики руху дозволяють зафіксувати перетинання периметру, який охороняється, і вчасно зреагувати на небезпечну ситуацію. Сенсори діляться на такі різновиди:

а) інфрачервоні;

б) ультразвукові;

в) радіохвильові;

г) комбіновані.

Кожен тип сенсорів має свої переваги і недоліки. Комбіновані різновиди детекторів є найбільш чутливими. Вони використовують кілька технологій одночасного виявлення і це виключає ризик того, що сенсор помилково спрацює.

Найчастіше зловмисники намагаються проникнути в будинок через вікна. І не важливо на якому поверсі квартира, потрапити до неї через вікно можна завдяки спеціальному обладнанню, тому для запобігання проникнення через вікно допоможуть датчики відкриття (рис.2.7). Вони можуть своєчасно сповістити господарів та органи охорони про проникнення всередину будинку. Принцип дії таких сенсорів у тому, що вони складаються з двох елементів я якщо один від одного віддаляться, то спрацює тривога та відправиться повідомлення як господарям так і органам безпеки.

Рисунок 2.7 – Приклад датчика відкриття

Також завдяки датчикам розбиття скла(рис.2.8) можна посилити систему безпеки. Такі сенсори відстежують механічні та акустичні коливання і відправляють інформацію про проникнення. Детектори розбиття скла діляться на:

а) електроконтактні;

б) п'єзоелектричні;

в) акустичні.

Якщо в будинку є сейф, захистити його від злому допоможуть датчики вібрації.

Рисунок 2.8 – Приклад датчика розбиття скла

Камери відеоспостереження це дуже важливий елемент систем безпеки. Їх встановлюють як зовні так і всередині будинку. Зовнішні слідкують за тим, що відбувається на території будинку, а за допомогою внутрішніх можна в режимі реально часу переконатися, що у будинку все добре. Також можна слідкувати за домашніми улюбленцями та близькими людьми, які потребують додаткової уваги, наприклад старі люди або діти.

Ще один приклад використання відеокамер це використання їх з домофоном. Камери, підключені до системи безпеки, дозволяють отримати візуальну і звукову інформацію про те, що відбувається за вхідними дверима.

Найчастіше охоронні системи об'єднують з комплексами протипожежної безпеки. Використовуючи спеціальний сповіщувач, можна попередити раптову пожежу і поширення вогню. Датчики диму(рис.2.9) – одні з головних елементів пожежної сигналізації.

Рисунок 2.9 – Приклад датчика диму

Витрати на опалення це основна частина витрат, пов’язаних з експлуатацією приміщень, тому з’явилася необхідність максимально оптимізувати рівень енергоспоживання та енерговитрат.

Функціонує розумній комплекс опалення завдяки:

а) термостатичним голівкам і вентилям;

б) температурним датчикам;

в) термостатам;

г) радіаторам та програматорам.

Завдяки цьому комплексу власник дому може віддалено керувати температурою. Підготувати комфортну температуру перед тим як прийти додому, щоб не чекати, поки температура стане комфортна.

Система водопостачання також дуже важлива. Вона вирішує завдання захищеності житла від комунальних аварій. Така функція дозволяє жити комфортно і не витрачати зайвий час на проблеми побуту.

Автоматизація водопостачання одна із необхідних систем для розумного дому. Її встановлення принесе багато корисного в «розумний дім». Перебуваючи далеко від дому, можна не переживати про протік води будь-де у будинку. Також можна налаштувати автоматичне включення води для наповнення ванни водою з температурою яка потрібна в будь-який час. Можливостей, які надає автоматизація системи водовідведення, існує величезна кількість. До них можна віднести:

а) контроль якості води. Датчики періодично вимірюють показники чистоти води;

б) контроль систем на протоку. При отриманні від датчика сигналу про протікання система блокує подачу води. У алгоритмі захисту від протікання води «розумного дому» можна запрограмувати відправку повідомлення про ситуацію яка сталася і отримати на телефон;

в) наповнення ванній підігрітою до заданої температури водою і підтримання цієї температури;

г) управління сенсорної сантехнікою;

д) підтримка потрібного рівня води, якщо на ділянці або в будинку є басейн;

е) автоматичний полив згідно заданих сценаріїв в залежності від вологості грунту, часу, ріку і доби.

Нагрівання води може проводитися в будь-якій котельні. Автоматизація системи опалення та водопостачання дозволяє здійснювати безперебійну та ефективну роботу системи.

І керувати усією системою можна з смартфону або планшету.

2.5 Технології для автоматизації «розумного дому»

Один з перших протоколів які з’явилися ще в 70-х роках минулого століття – це x10. Цей стандарт є відкритим. Він використовує в якості

середовища передачі силову електропроводку і тому прокладати додаткові кабелі не потрібно для пристроїв, які працюють з цим стандартом[].

Так як це найперший протокол який створили для автоматизації, тому для нього виготовлено велику кількість різноманітних модулів. Наприклад модулі управління освітленням, опаленням та вентиляцією та іншими модулями. Також досі випускається багато різних вимикачів, датчиків, які можуть працювати спільно з виконавчими модулями, але для роботи необхідно додатково інсталювати спеціальні контролери. Ще можна використовувати комунікаційні модулі, які потрібні для роботи з комп'ютером та з іншими протоколами.

Для роботи бездротових пультів, перемикачів та інших пристроїв був розроблений протокол використання радіоканалу. Бездротові пристрої передають по радіоканалу пакети даних, а для передачі використовується частота 310 МГц в США і 433 МГц в Європі.

Але цей протокол був створений давно, тому має ряд суттєвих недоліків. Цей протокол досить повільний, для передачі адреси та команди може зайняти 3/4 секунди. Інші більш сучасніші протоколи працюють швидше. Також у мережі X10 можна передавати тільки одну команда та в конкретний момент часу, якщо в один і той же час буде йти передача більше ніж однієї команди, то це призведе до колізії. Колізія – це коли команда не буде правильно прийнята або будуть виконані неправильні дії.

Через нові блоки живлення, які використовуються з новими девайсами на зразок комп'ютера або телевізора, можуть не доходити команди, а все через конденсатори в блоках живлення. Деякі модулі X10 некоректно працюють або не працюють взагалі, якщо керують пристроєм з низькою споживаної енергією менше 50 Ватт, наприклад, флуоресцентними лампами.

Рисунок 2.10 – Логотип стандарту «KNX»

KNX (рис.2.10) - це відкритий стандарт для автоматизації комерційних та побутових будівель.

KNX – це польова шина для автоматизації будівель. На ринку автоматизації будівель KNX є наступником польових шин European Installation Bus (EIB), BatiBus та European Home Systems (EHS). Технічно KNX – це подальший розвиток EIB за рахунок додавання механізмів конфігурації та засобів передачі, які спочатку були розроблені для BatiBus та EHS. [] KNX сумісний з EIB.

Після того, як у 1991 році на ринку були запропоновані перші продукти відповідно до цього стандарту, існувало майже 4000 груп продуктів з безліччю різних продуктів від більш ніж 200 компаній. Ці продукти охоплюють різні галузі та додатки в будівлі, зберігаючи при цьому взаємозамінність продуктів, тому вони можуть працювати разом у системі, розробленій з KNX. KNX тепер є першим стандартом відкритого світу для автоматизації будинку та будівель. Це регулюється в Європі з 1994 року [] EN 50090. Стандартизація ISO була проведена як стандарт ISO / IEC 14543-3.

KNX керує освітленням і жалюзі або затіняючими пристроями, опаленням будівлі, а також системами замикання та сигналізації. Віддалений моніторинг та управління будівлею також можливі за допомогою EIB (KNX). Управління відбувається через самого користувача або через комп'ютер з

відповідним програмним забезпеченням. Спочатку протокол був орієнтований на комерційні будівлі, але KNX все частіше використовується в житлових будинках і, зокрема, в приватних будинках. KNX не може слідувати тенденції до передачі більшої кількості інформації з камер, датчиків, голосу та засобів масової інформації. Їх можна і потрібно передавати лише через паралельні мережі.

У той час як сильна сторона KNX в децентралізованому кабельному розведенні економічно корисна в комерційних будинках, централізована кабельна розводка більш поширена в невеликих будинках (прокладання всіх ліній датчиків і виконавчих механізмів до однієї або двох центральних точок). Тенденція до використання IP-рішень у будівництві будівель (VoIP) назавжди змінила ринок. Зростання тенденції до використання логіки (сервер, візуалізація) забезпечує сильне збільшення кількості ПЛК.в будівництві. Деякі виробники ПЛК пропонують шлюзи до KNX для з'єднання обох світів. KNX в даний час в основному встановлюється в нових житлових та функціональних будинках, але може бути модернізований при модернізації старих будівель. Мережі KNX вже стандартно інтегровані у будівлі недорогих збірних будинках.

Тим не менш, піонери у розробці EIB/KNX вже висловили сумніви щодо майбутньої життєздатності KNX у спеціальній літературі. У довгостроковій перспективі KNX зможе уникнути загальної тенденції до створення мереж лише на рівні IP; можливості конкуруючих систем надто різноманітні. Вищі швидкості передачі, особливо у медіа- секторі (мультирум), у разі вимагають інших мережевих концепцій . Істотною особливістю та перевагою цієї технології є і буде дуже безпечна та відкрита шинна архітектура KNX.

Протокол KNX можна переглянути, ґрунтуючись на мережевій моделі OSI. Це децентралізована однорангова мережа з керуванням подіями. Мережа KNX підтримує стандартний протокол передачі даних, який реалізований у різних середовищах передачі:

а) кабель із крученою парою;

б) лінія електропередачі;

в) мережа IP (EIB.net);

г) радіоканал.

Передача здійснюється модуляцією напруги в мережі, а логічний нуль надсилається як імпульс, з амплітудою приблизно ± 6 В. Відсутність імпульсу інтерпретується як логічна одиниця. Інформація надсилається пакетами з 8 байтів. Переадресація синхронізується з бітами запуску та зупинки. Також є біт контролю парності.

Для вирішення зіткнень інформації в мережі використовується метод CSMA / CA. Цей метод гарантує випадковий, безперебійний доступ пристроїв до шини, без істотного зниження його максимальної пропускної здатності. Повідомлення з найвищим пріоритетом будуть передані в першу чергу.

Рисунок 2.11 – Логотип стандарту «Zigbee»

Zigbee (рис.2.11) - це специфікація на базі IEEE 802.15.4 для набору протоколів зв'язку високого рівня, що використовуються для створення персональних мереж з невеликими цифровими радіоприймачами.

ZigBee - це специфікація для бездротових мереж з низьким обсягом даних та низьким енергоспоживанням, таких як домашня автоматизація, сенсорні мережі, світлотехніка. Пристрої ZigBee обмінюються даними в мережі або спеціальної мережі . Це означає, що якщо зв'язок у мережі ZigBee виходить з ладу, замість нього використовується інший шлях у мережі. ZigBee орієнтований на мережі малого радіусу дії до 100 м у приміщенні та до 300 м у зоні прямої видимості. []

Назва ZigBee походить від зигзагоподібного танцю бджіл.

Специфікація є розробкою ZigBee Alliance, заснованої наприкінці 2002 року. В даний час це асоціація, що об'єднує понад 230 компаній, що сприяють глобальному розвитку цієї технології. Перша специфікація ZigBee вийшла у 2004 році. Версія, відома тепер як ZigBee 2004, вважається застарілою і 2006 року була замінена повністю переробленою версією. У 2007 році з'явилася ще одна гілка специфікації ZigBee-ZigBee Pro. Він призначений для додатків, яким необхідно використовувати як низькі швидкості передачі даних, так і мінімізоване споживання енергії.

Специфікація ZigBee надає розробнику три різні типи пристроїв (ZigBee Devices). З цими пристроями налаштовано бездротову персональну мережу ZigBee (WPAN). Пристрій ZigBee може виконувати три ролі:

а) кінцевий пристрій (ZigBee End Device, ZED);

б) маршрутизатор (маршрутизатор ZigBee, ZR);

в) координатор (координатор ZigBee, ZC).

До кінцевих пристроїв можна віднести модулі керування або рецептори. Пристрої в основному працюють від батарейок. Вони можуть бути реалізовані як кінцеві пристрої ZigBee та вимагають лише деяких функцій специфікації ZigBee. Вони не беруть участі в маршрутизації в мережі і можуть переходити до сплячого режиму. Ви входите в систему на вибраному маршрутизаторі і таким чином приєднуєтеся до мережі ZigBee. Вони можуть спілкуватися лише з маршрутизатором, через який вони підключилися до мережі. Якщо дані надсилаються на такий кінцевий

пристрій, і він знаходиться в сплячому режимі, маршрутизатор зберігає ці пакети, поки кінцевий пристрій не «прокинеться» та не запросить ці пакети.

Маршрутизатор ZigBee беруть участь у маршрутизації пакетів по мережі. Вам потрібен ширший набір функцій і, отже, трохи більше апаратних ресурсів. Маршрутизатор ZigBee приєднується до мережі шляхом входу в маршрутизатор в мережі. Маршрутизація в мережі здійснюється або по дереву, яке формується таким чином (профіль стека ZigBee), або за допомогою динамічної маршрутизації у вигляді комірчастої мережі (профіль стека ZigBee PRO). Якщо радіомодуль підключається до мережі через маршрутизатор, йому призначається 16-бітова коротка адреса . У разі пористих мереж це відбувається випадково. Конфлікти, що виникають при вирішенні, необхідно розпізнавати, а потім вирішувати.

Координатор ZigBee запускає мережу із зазначеними параметрами. Після запуску він виконує ті самі завдання, що маршрутизатор ZigBee.

Системні вимоги та пристрої визначаються для конкретної програми у профілях ZigBee. Кожен пристрій реалізує кілька кластерів. Приклади профілів: Домашня автоматизація, Автоматизація будівель та Охорона здоров'я.

ZigBee Light Link - використовується для управління освітлювальною технікою всіх видів, у цьому профілі передбачено управління колірними складовими, яскравістю та просте включення та вимикання ламп. Для простоти немає потреби в координаторі і, отже, у центрі довіри для розподілу ключів. Зв'язок завжди шифрується за допомогою ключа мережі. Мережевий ключ передається в зашифрованому вигляді на радіомодуль, що приєднується до мережі за допомогою головного ключа. Це також є головне слабке місце Light Link. Майстер-ключ ідентичний всім сертифікованих Light Link продуктів ZigBee і повідомляється виробнику ZigBee Alliance після проходження сертифікації. Це означає, що була спроба зберегти майстер-ключ у секреті. Проте це вже давно відомо.[] Надалі не планується змінювати майстер-ключ на сертифікованих продуктах. Інший недолік

секретності майстер-ключа полягає в тому, що приватні користувачі, наприклад, не можуть створювати власні продукти, такі як перемикачі або контролери для сертифікованих продуктів Light-Link, поки майстер-ключ не відомий. Що стосується управління освітленням, то з погляду безпеки ключова проблема не така вже й велика. Загалом, серйозної шкоди завдати не можна, і діапазон передачі ZigBee Light Link також досить малий, тому потенційний зловмисник повинен підійти дуже близько до обладнання.

ZigBee Home Automation - також можна використовувати для керування освітлювальної техніки, але він використовується для загального управління пристроями в невеликих будинках. Передача також шифрується мережевим ключем. Тут також мережевий ключ зашифрований і передається головним ключем при вході в мережу. У цьому випадку головний ключ відомий, але доступ до мережі можна заблокувати за допомогою центру керування безпекою та, наприклад, дозволити лише натисканням кнопки протягом кількох секунд. Однак і тут збитки від ненавмисного доступу можуть бути більшими. Якщо, наприклад, змінити значення температури для кондиціонерів, холодильників або опалювальних систем, це може мати значні наслідки.

Рисунок 2.12 – Логотип стандарту «Z-Wave»

Z-Wave (рис.2.12) - це запатентований бездротовий протокол.

Z-Wave - це протокол бездротового зв'язку, що використовується в основному в мережах розумного будинку, що дозволяє інтелектуальним пристроям підключатися та обмінюватися керуючими командами та даними один з одним.

Завдяки двосторонньому зв'язку через мережу та підтвердження повідомлень протокол Z-Wave допомагає зменшити проблеми з живленням та забезпечує недорогий бездротовий зв'язок для домашньої автоматизації, пропонуючи альтернативу Wi-Fi з меншим енергоспоживанням та альтернативу Bluetooth з більшим радіусом дії.

Мережа Z-Wave складається з пристроїв Інтернету речей (IoT) та первинного контролера, також відомого як концентратор розумного будинку, який є єдиним пристроєм у мережі Z-Wave, який зазвичай підключено до Інтернету. Коли концентратор Z-Wave отримує команду від програми розумного будинку на смартфоні, планшеті або комп'ютері користувача, він направляє команду на цільовий пристрій через мережі, що налічують до 232 пристроїв, включаючи концентратор.

Використовуючи технологію мережі з маршрутизацією від джерела, сигнали Z-Wave можуть проходити через інші пристрої Z-Wave, щоб досягти пристрою, яким користувач має намір керувати. Кожна мережа Z-Wave вміщує максимум чотири переходи.

Протокол Z-Wave працює в низькочастотному діапазоні 908,42 МГц у США та діапазоні 868,42 МГц у Європі. Хоча можливі перешкоди в роботі іншої домашньої електроніки, наприклад, бездротових телефонів, протокол дозволяє уникнути перешкод у діапазоні 2,4 ГГц, в якому працюють Wi-Fi і Bluetooth.

Z-Wave пропонує швидкість передачі невеликих пакетів даних із пропускною здатністю 9,6 кбіт/с, 40 кбіт/с або 100 кбіт/с. Рівні Z-Wave PHY та MAC засновані на глобальному стандарті радіозв'язку ITU-T G.9959, а протокол використовує модуляцію GFSK та манчестерське кодування. Він також включає шифрування AES 128, IPv6 та багатоканальну роботу.

З точки зору ідентифікації та авторизації, кожна мережа Z-Wave ідентифікується ідентифікатором мережі, а кожен кінцевий пристрій ідентифікується ідентифікатором вузла. Унікальний мережний ідентифікатор не дозволяє, наприклад, одному будинку, обладнаному Z-Wave, керувати пристроями в іншому будинку, обладнаному аналогічним чином.

Зв'язок між пристроями знаходиться в діапазоні від 98 до 328 футів; Радіус дії серії 500 становить 130 футів, а серія 700 - 328 футів. Оскільки стіни та інші щільні будівельні матеріали обмежують діапазон, рекомендується розміщувати пристрої Z-Wave на відстані 50 футів або менше для досягнення максимальної потужності сигналу.

Використання ретранслятора Z-Wave - додаткового пристрою Z-Wave між іншими пристроями - або пристроїв у мережі з живленням від мережі, а не батарейок, також може посилити сигнал і допомогти йому досягти пункту призначення. Максимальна дальність із чотирма стрибками оцінюється в 600 футів.

Що стосується терміну служби батарейок, деякі пристрої Z-Wave серії 700 можуть працювати до 10 років від батарейки типу «таблетка», в той час як багато інших пристроїв з батарейним живленням служать рік або довше.

Вся технологія Z-Wave обернено сумісна.

Щоб носити бренд Z-Wave, продукти для розумного будинку мають пройти сертифікацію Z-Wave. Це включає виконання ряду вимог і, що найважливіше, сумісність з усіма іншими пристроями, сертифікованими Z-Wave.

Рисунок 2.13 – Логотип технології 1-Wire

1-Wire (рис 2.13) - протокол передачі даних, який працює в обидві сторони та використовуючи однин дріт.

Даний протокол описує послідовний інтерфейс Dallas Semiconductor Corp. (сьогодні Maxim Integrated), який обходиться одним дротом передачі даних (DQ), який використовується як як джерело живлення, так і як лінія передачі та прийому. Термін 1-Wire вводить в оману, тому що також потрібне заземлення (GND). У разі пристроїв у формі кнопки заземлення досягається за рахунок ізоляції половин корпусу один від одного. Фактично завжди використовуються два фізичні з'єднання проводів (GND, DQ).

Доступні інтегровані модулі для вимірювання температури, моніторингу батареї, годинника реального часу, невелика пам'ять і т. д. Технологія була розроблена для зв'язку між компонентами пристрою, наприклад, Б. для запису стану батареї в мобільному пристрої збору даних (MDE).

Пристрої у формі кнопок поширені як механічно особливо прості чинники аутентифікації, які стосуються користувача, особливо у касах

Режим зв'язку в цьому протоколі - асинхронний і напівдуплексний, а також "гострий". У цьому режимі надсилаються мультибайтні дані і передача йде від молодшого байта до старшого.

На шині має бути лише один пристрій, який відсилатиме команди. Також до загальної шини підключаються пристрої, які приймають команди і відповідають на них.

Протокол 1-Wire хороший тим, що не складний в реалізації і для зв'язку потрібно всього два або три дроти. Це шина даних, земля і живлення. Але у цьому протоколі є і недоліки - він досить чутливий до часу та перешкод. Також 1-Wire не здатен передавати великий обсяг даних та не має високої швидкості обміну даними [].

Протокол 1-Wire описує фізичний, канальний, мережевий і транспортний рівні взаємодії.

На фізичному рівні даються описи методів зв'язку, вимоги до шини даних і живленню.

Канальний рівень описує способи читання і передачі бітів по протоколу.

Мережевий рівень визначає методи адресації до різних пристроїв на лінії.

Транспортний рівень описує функціональні команди, які використовують пристрої 1-Wire.

Рисунок 2.14 – домофонний ключ

До пристроїв, що використовують інтерфейс 1-Wire можна віднести домофонний ключ (рис 2.14). Цей ключ в більшості випадків працює через цей протокол. Принцип дії такий: мікроконтролер, який встановлений у

замок запитує унікальний код у ключа, а якщо цей код міститься в списку дозволених пристроїв, то мікроконтролер відкриє замок.

Використовується 1-Wire й у пристроях для ідентифікації та авторизації. Наприклад у ключах та картках пропуску. Також і у багато яких датчиках. Наприклад датчики температури або вологості, освітлення та інші датчики.

Рисунок 2.15 – Логотип технології Bluetooth

Bluetooth (рис.2.15) - це відкритий стандарт бездротової технології передачі даних з фіксованих і мобільних електронних пристроїв на короткі відстані. Bluetooth був представлений в 1994 як бездротовий замінник кабелів RS-232.

Bluetooth обмінюється даними з різними електронними пристроями та створює персональні мережі, що працюють у неліцензованому діапазоні 2,4 ГГц. Робочий діапазон залежить від класу пристрою. Bluetooth використовують різні цифрові пристрої, включаючи MP3-плеєри, мобільні та периферійні пристрої, а також персональні комп'ютери.

Пристрої Bluetooth управляються за допомогою радіочастотної топології, відомої як «зіркоподібна топологія». Група пристроїв, синхронізованих таким чином, утворює пікомережу, яка може містити один провідний пристрій і до семи активних ведених пристроїв з додатковими веденими пристроями, які не беруть активну участь в мережі. (Цей пристрій також може бути частиною однієї або декількох пікомереж як ведучого або

веденого.) У пікомережі фізичний радіоканал спільно використовується групою пристроїв, які синхронізовані із загальним годинником і стрибкоподібною перебудовою частоти. шаблон, при цьому провідний пристрій надає посилання на синхронізацію.

Пристрої в пикосеті використовують певний шаблон стрибкоподібної перебудови частоти, який алгоритмічно визначається провідним пристроєм. Базовий шаблон стрибкоподібної перебудови – це псевдовипадкове впорядкування 79 частот у діапазоні ISM. Шаблон стрибкоподібної перебудови може бути адаптований для виключення частини частот, що використовуються пристроями, що заважають. Метод адаптивного перемикання покращує співіснування технології Bluetooth зі статичними (без перемикання) системами ISM, такими як мережі Wi-Fi, коли вони розташовані поблизу пікомережі.

Фізичний канал (або бездротовий зв'язок) поділяється на тимчасові одиниці, відомі як слоти. Дані передаються між пристроями з підтримкою Bluetooth у пакетах, які розміщуються у цих слотах. Стрибкоподібна перебудова частоти відбувається між передачею або прийомом пакетів, тому пакети, що становлять одну передачу, можуть відправлятися різних частотах в діапазоні ISM.

Фізичний канал також використовується як транспорт для одного або декількох логічних каналів, які підтримують синхронний та асинхронний трафік, а також широкомовний трафік. Кожен тип посилання має певне призначення. Наприклад, синхронний трафік використовується для передачі аудіоданих в режимі гучномовця, а асинхронний трафік може нести інші форми даних, які можуть витримувати велику мінливість часу доставки, наприклад друк файлу або синхронізацію вашого календаря між телефоном і комп'ютером.

Одна із складнощів, часто пов'язаних з бездротовою технологією, - це процес підключення бездротових пристроїв. Користувачі звикли до процесу

підключення дротових пристроїв, вставляючи один кінець кабелю в один пристрій, а інший кінець додатковий пристрій.

Технологія Bluetooth використовує принципи запиту та сканування запитів. Скануючі пристрої прослуховують на відомих частотах пристрою, які активно опитують. Коли запит отримано, скануючий пристрій надсилає відповідь з інформацією, необхідною запитувачу, щоб визначити та відобразити природу пристрою, який розпізнав його сигнал.

Рисунок 2.16 – Логотип технології Wi-Fi

Wi-Fi (рис.2.16) - означає Wi з бездротовим доступом delity. Він заснований на сімействі стандартів IEEE 802.11 і в першу чергу є технологією локальної мережі (LAN), призначену для забезпечення широкосмугового покриття всередині будівлі.

Сучасні системи Wi-Fi підтримують пікову швидкість передачі даних фізично 54 Мбіт/с і зазвичай забезпечують покриття всередині приміщення на відстані до 100 футів.

Wi-Fi став де-факто стандартом широкосмугового підключення «останньої милі» у будинках, офісах та громадських точках доступу. Системи зазвичай можуть забезпечувати зону покриття лише близько 1000 футів від точки доступу.

Wi-Fi пропонує значно вищі пікові швидкості передачі даних, ніж системи 3G, насамперед тому, що він працює з більшою смугою пропускання 20 МГц, але системи Wi-Fi не призначені для підтримки високошвидкісної мобільності.

Однією з значних переваг Wi-Fi над WiMAX та 3G є широка доступність кінцевих пристроїв. Переважна більшість ноутбуків, що поставляються сьогодні, мають вбудований інтерфейс Wi-Fi. Інтерфейси Wi-Fi тепер також вбудовуються в різні пристрої, включаючи кишенькові комп'ютери (КПК), бездротові телефони, мобільні телефони, камери та медіаплеєри.

Всі мережі WiFi являють собою системи TDD на основі конкуренції, в яких точка доступу та мобільні станції змагаються за використання одного й того ж каналу. Через роботу із загальним носієм всі мережі Wi-Fi є напівдуплексними.

Існують постачальники обладнання, які продають конфігурації ніздрюватої мережі Wi-Fi, але ці реалізації включають технології, не визначені в стандартах.

Стандарти WiFi визначають фіксовану смугу пропускання каналу 25 МГц для 802.11b та 20 МГц для мереж 802.11a або g.

Радіосигнали - це ключі, які уможливлюють створення мереж Wi-Fi. Ці радіосигнали, що передаються антенами WiFi, вловлюються приймачами WiFi, такими як комп'ютери та стільникові телефони, оснащені картками WiFi. Щоразу, коли комп'ютер приймає будь-який із сигналів у межах діапазону мережі Wi-Fi, який зазвичай становить 300-500 футів для антен, карта WiFi зчитує сигнали і, таким чином, створює інтернет-з'єднання між користувачем та мережею без використання шнур.

Точки доступу, що складаються з антен і маршрутизаторів, є основним джерелом передачі та прийому радіохвиль. Антени працюють сильніше і мають довшу радіопередачу з радіусом 300-500 футів, які використовуються в громадських місцях, у той час як слабкіший, але ефективний

маршрутизатор більше підходить для будинків з радіопередачею 100-150 футів.

Стандарт 802.11 визначається декількома специфікаціями WLAN. Він визначає бездротовий інтерфейс між бездротовим клієнтом та базовою станцією або між двома бездротовими клієнтами.

У сімействі 802.11 є кілька специфікацій:

а) 802.11 - це відноситься до бездротових локальних мереж і забезпечує передачу зі швидкістю 1 або 2 Мбіт / с в діапазоні 2,4 ГГц з використанням розширеного спектра з стрибкоподібною перебудовою частоти (FHSS), або розширеного спектра прямої послідовності (DSSS).

б) 802.11a – це розширення стандарту 802.11, яке відноситься до бездротових локальних мереж та працює зі швидкістю 54 Мбіт/с у діапазоні 5 ГГц. 802.11a використовує схему кодування з мультиплексування з ортогональним частотним поділом каналів (OFDM) на відміну від FHSS або DSSS.

в) 802.11b - високошвидкісний Wi-Fi 802.11 є розширенням стандарту 802.11, який відноситься до бездротових локальних мереж і забезпечує швидкість передачі даних до 11 Мбіт/с (з відкатом до 5,5, 2 та 1 Мбіт/с залежно від сили сигналу) 2.4- Діапазон ГГц. У специфікації 802.11b використовується лише DSSS. Зверніть увагу, що 802.11b насправді був поправкою до вихідного стандарту 802.11, доданим у 1999 році, щоб дозволити бездротовій функціональності бути аналогічною дротовим з'єднанням Ethernet.

г) 802.11g - відноситься до бездротових локальних мереж і забезпечує 20+ Мбіт/с у діапазоні 2,4 ГГц.

Ось технічне порівняння трьох основних стандартів Wi-Fi (табл.2.1).

Таблиця 2.1 – Порівняння трьох основних стандартів

Особливість	Wi-Fi (802.11b)	Wi-Fi (802.11a / g)
Основне застосування	Бездротова мережа	Бездротова мережа
Діапазон частот	2,4 ГГц ISM	2,4 ГГц ISM (g) 5 ГГц U-NII (a)
Пропускна здатність каналу	25 МГц	20 МГц
Напів/Повний дуплекс	Напів	Напів
Радіотехніка	Пряма послідовність Розширений спектр	OFDM (64 канали)
Пропускна здатність	<= 0,44 біт / с / Гц	≤ = 2,7 біт / с / Гц
Модуляція	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Відсутній	Згортковий код
Шифрування	Додатково - RC4m (AES в 802.11i)	Додатково - RC4 (AES в 802.11i)
Мережа	Власність постачальника	Власність постачальника
Протокол доступу	CSMA / CA	CSMA / CA

Безпека була одним із основних недоліків WiFi, хоча зараз стають доступними більш досконалими системами шифрування. Шифрування через WiFi не є обов’язковим і визначено трьома різними методами. Ці методи наведені тут:

а) Wired Equivalent Privacy (WEP), 40- або 104-бітне шифрування на основі RC4 зі статичним ключом;

б) WiFi Protected Access (WPA). Це новий стандарт від WiFi Alliance, який використовує 40- або 104-бітний ключ WEP, який змінює ключ для кожного пакету. Ця змінюючись ключева функція називається протоколом цілісності временного ключа (TKIP);

в) IEEE 802.11i / WPA2. IEEE виконує стандарт 802.11i, заснований на більш надійному методі шифрування, який називається Advanced Encryption Standard. WiFi Alliance позначає продукти, відповідні стандарту 802.11i, як WPA2. Однак для реалізації 802.11i потрібно оновлення обладнання.

2.6 Актуальність «розумного дому»

Технології розвиваються з кожним днем, і «розумний будинок» стає все більше актуальнішим. У минулому розумні будинки вважалися частиною розкішного способу життя, але вони стали важливою частиною нашого життя. Основні переваги актуальності «розумного будинку»:

а) ефективність. За допомогою однієї сенсорної кнопки або програми мобільного телефону можна керувати численними гаджетами або системами. За допомогою інтелектуального пристрою є змога керувати опаленням та охолодженням, а також вмикати та вимикати світло одним дотиком до екрану смартфону з будь-якої точки вашого будинку. Це не лише ефективна процедура, а й економія електроенергії;

б) зручність. Наявність розумного будинку дозволяє мати справу з багатьма електронними пристроями і системами з дому або по всьому світу. Відкрийте штори, увімкніть світло та стежте за безпекою;

в) комфорт: розумний будинок зробить ваше життя комфортним; вам не потрібно пересуватися вдома для виконання різних функцій. За допомогою смарт-пристроїв ви можете виконувати всі домашні операції через програми, зручно влаштувавшись на дивані або в ліжку;

г) душевний спокій. Розумний будинок також є важливим способом дати душевний спокій, можна використовувати інтелектуальний пристрій

для перевірки дверей, вікон, датчиків розливу води і т. д. Крім того, також можна перевірити, чи правильно закриті двері гаража за допомогою програми. Більше не потрібно турбуватися про те, щоб піти перевірити;

д) кастомізація. Розумні будинки також дозволяють мати електронні речі у тому вигляді, в якому вони подобаються. Можна налаштувати автоматичне малювання відтінків у певний час, відрегулювати яскравість внутрішнього та зовнішнього освітлення на ваш вибір. Так само можна налаштувати кожен електронний елемент за своїм бажанням, і, крім того, можна встановити час для різних варіантів, які будуть реалізовані.

Крім цих переваг, є ще кілька важливих причин, чому потрібно робити будинки «розумними»:

а) безпека. Тероризм та інші дрібні злочини зараз дуже поширені, і в цю епоху кожен хоче захистити свій будинок. Розумні будинки дозволять вам захистити свій будинок, а також дозволять вам легко контролювати безпеку через свої смартфони;

б) рахунки за комунальні послуги. Світ з кожним днем дорожчає, і люди дуже стурбовані своїми рахунками за комунальні послуги. Розумний будинок допоможе заощадити електроенергію та скоротити рахунки за електроенергію та воду. Часто спостерігається, що світло залишається включеним через те, що ліньки вставати і вимикати його. Розумний будинок дозволить вимикати світло та інші електронні пристрої, навіть коли людина перебуває в ліжку та збираєтеся спати. Це заощадить величезну суму грошей;

в) рятувальна сигналізація для дому. Пожежа і крадіжка - це лише пара подій, які можуть знищити будинок або підірвати життя друзів та сім'ї. Пристрої розумного будинку можуть інформувати про такі події за допомогою сигналів тривоги та повідомлень, яких може бути достатньо, щоб урятувати життя.

2.6 Висновки

Ще на початку 20 століття з’явилися перші згадки про «розумний дім». «Розумний будинок» описували у фантастичних творах, але реалізовувати цю ідею почали лише в середині 20 століття. Але спочатку розвивалися інші технології і без їх розвитку не було б і «розумного дому».

Сьогодні «розумний дім» ні для кого не новизна, як це було колись. Зараз майже кожний може зробити свій дім «розумним». Для цього необхідно просто вибрати технологію та ціль, для чого саме потрібен «розумний дім».

«Розумний дім» принесе лише користь. Завдяки цій технології жити стане краще, комфортніше та безпечніше.

Люди проходячи додому не будуть відволікатися на якісь дрібні речі, вони прийдуть і зможуть відразу відпочивати, а якщо щось потрібно змінити в приміщенні, то достатньо лише взяти смартфон у руки та змінити те, що викликає дискомфорт, будь то температура або рівень освітленості. Технології які ще колись бачили у кіно або читали в книжках стали реальними.

3. Вибір та оптимізація системи «розумного дому».

3.1 Вибір системи

Проаналізувавши ринок систем можна виділити три основні технології які використовуються для організації систем «розумного дому». До цих технологій відносяться:

а) Zigbee;

б) WiFi;

в) Z-Wave.

Усі ці технології показали себе дуже добре з усіх сторін і багато задоволених користувачів та спеціалістів рекомендують саме ці протоколи для побудови «розумного дому».

Протокол Zigbee дуже популярний для побудови «розумного дому».

Розглянемо систему «розумного дому» на технології ZigBee (рис.3.1) від Aqara.

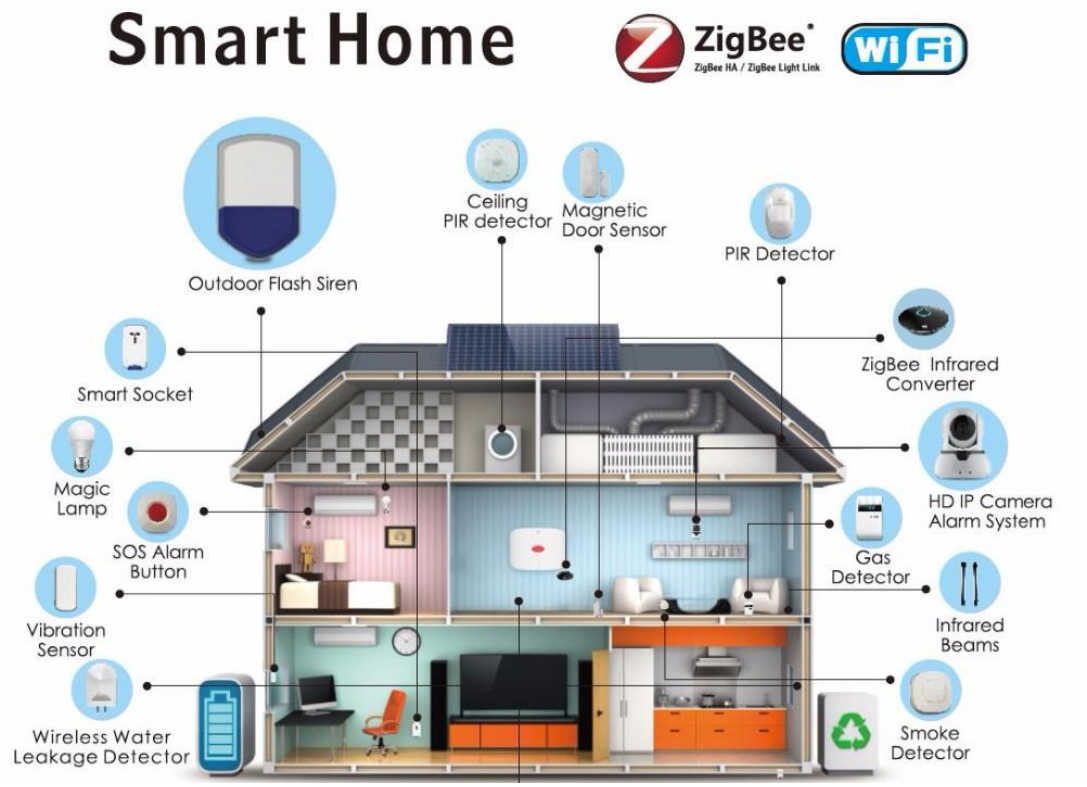

Рисунок 3.1 – система «розумного дому» на технології ZigBee

На малюнку 3.1 можна побачити основні компоненти які входять у склад «розумного дому». До цих компонентів відносяться:

а) сенсор вібрації;

б) розумні розетки;

в) детектори диму;

г) детектор газу;

д) датчики руху та присутності;

е) детектор витоку води;

ж) IP камера;

з) датчик відкриття дверей.

Деякі із цих компонентів працюють через технологію WiFi. Це IP камера, для контролю безпеки вдома, та безпровідний датчик витоку води.

За об'єднання всіх цих компонентів в єдину систему «розумного дому» відповідає шлюз ZigBee. До нього можна підключитися через спеціальний додаток на Android або IOS.

Максимальна швидкість передачі даних у цій системі 250 кб/с.

Час затримки передачі інформації може займати до 240мс, а середнє значення близько 100мс. Залежить від кількості даних які передаються.

Ще один фактор який дуже впливає на роботу ZigBee це те, що протокол працює у навантаженому каналі 2.4 ГГц. У цьому каналі працює WiFi. Чим більше навколо системи «розумного дому» буде WiFi мереж тим гірше може працювати система. Також технологія Bluetooth працює на такому ж каналі, але її вплив не на стільки великий.

3.2 Оптимізація за допомогою зміни основного контролера

Зараз у системі, яку розглянуто вище, використовується контролер який працює у каналі 2.4 ГГц.

Для покращення зв'язку та вирішення деяких проблем буде розглянуто роутер 4G WI-FI ZIGBEE MULTIROUTER SM-4Z (рис.3.2). Як можна

зрозуміти з назви даний роутер має вбудований модуль ZigBee і до нього можна без усіляких проблем приєднати уже створену систему «розумного дому».

Рисунок 3.2 – роутер 4G WI-FI ZIGBEE MULTIROUTER SM-4Z

У цього роутера є підтримка 4G мережі, що дасть змогу працювати через мобільну мережу у разі зникнення основного каналу зв’язку через глобальну мережу інтернет. Підтримує даний роутер гігабітну мережу та є 3 лан порти для підключення та спеціальний лоток для сім карти. Також є наявність двох каналів WiFi 2.4 ГГц та 5 ГГц. Додатково є USB порт для встановлення прошивки на роутер.

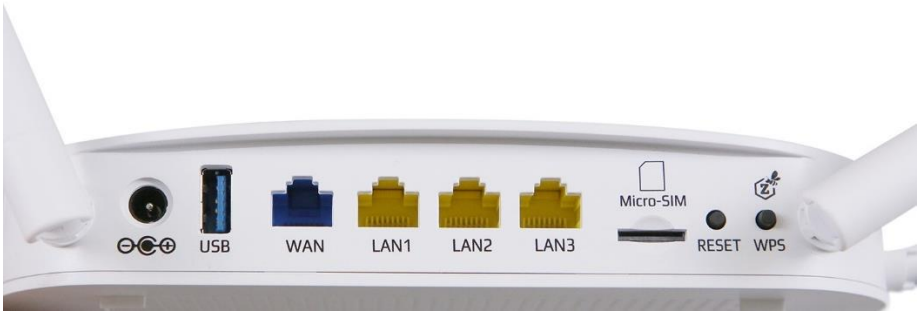

Рисунок 3.3 – порти на роутері 4G WI-FI ZIGBEE MULTIROUTER SM-4Z

У даного роутера 256 мб оперативної пам’яті. Великий обсяг оперативної пам'яті потрібен для надійної роботи всіх підключених пристроїв, у тому числі якщо ви просто використовуєте Wi-Fi, роутер легко переносить до десятка пристроїв, які приймають і передають дані, не починає збоїти при їх передачі.

Підключитися та налаштувати роутер можна як у програмі, так і веб-версії. Програма існує як для iOS, так і для Android. Скануєте QR-код (рис.3.4) і отримуєте доступ.

Рисунок 3.4 – QR-код на роутері

Підключитися можна і через браузер після вводу у рядок адреси 192.168.1.1. Після вводу паролю можна потрапити на стартове вікно (рис.3.5)

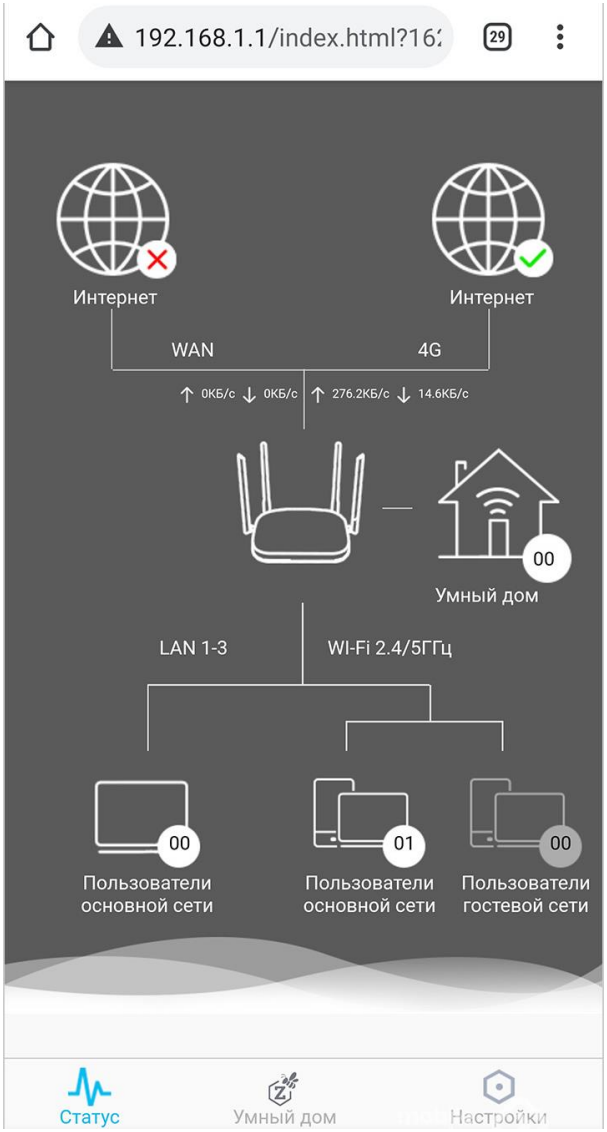

Рисунок 3.5 – стартове вікно після вводу паролю

Є можливість вибору роботи WiFi у двох діапазонах або одному (рис.3.6). Та і як у звичайних роутерах назначити пароль для точки доступу та і саму назву точки доступу.

Рисунок 3.6 – налаштування WiFi

Після налаштування WiFi можна ввімкнути функцію перемикання контролю потоку. Тобто коли зникне доступ до глобальної мережі інтернет через WAN порт, роутер автоматично перейде на використання 4G мережі для доступу в інтернет (рис.3.7). Також є можливість обмежити роботу в роумінгу, а також встановити обмеження на обсяг даних, що передаються.

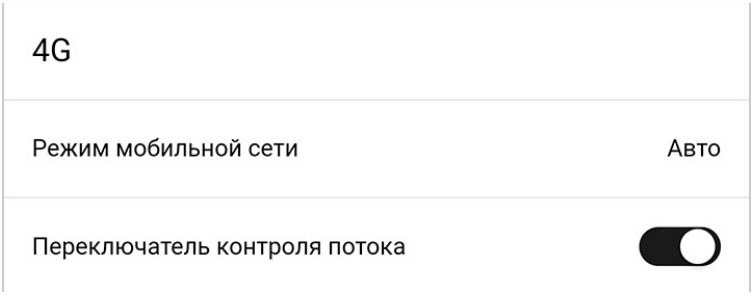

Рисунок 3.7 – налаштування резервного каналу

Додаток для керування роутером називається MultiRouter (рис.3.8). Завантажити його можна в через додаток Play Market. Для IOS є аналогічний додаток. Завантажити його можна через додаток Apple Store.

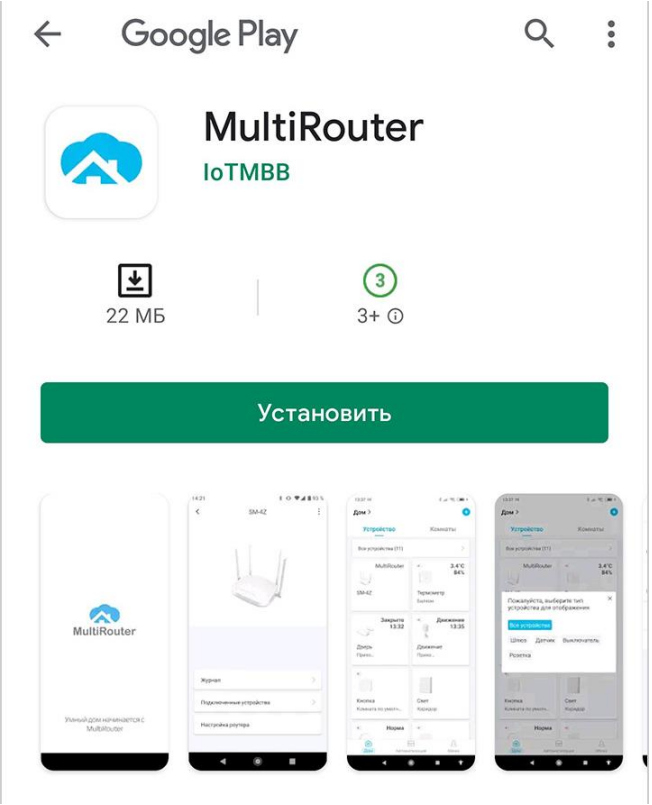

Рисунок 3.8 – додаток для мобільного пристрою

Через даний додаток можна почати додавати необхідні елементи для системи «розумного дому» (рис.3.9). Є можливість додати датчики різних типів. Наприклад:

а) датчик витоку води;

б) датчик вібрації;

в) датчик температури;

г) датчик диму.

Роутер виступає шлюзом у даному випадку.

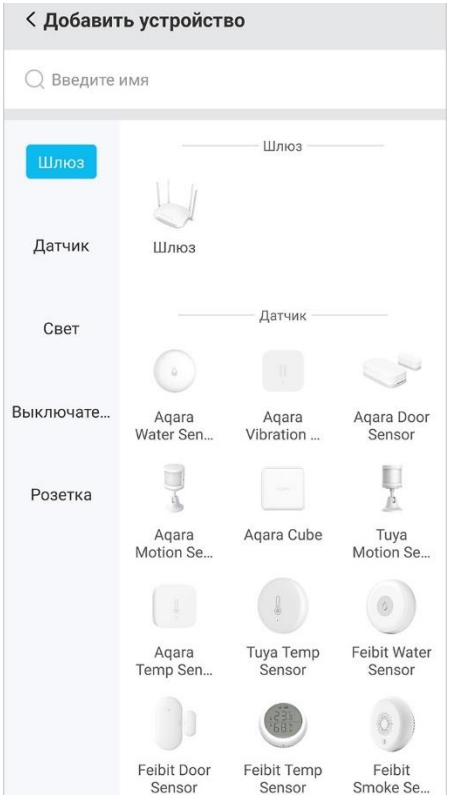

Рисунок 3.9 – додавання нового пристрою системи «розумний дім»

Після додавання пристрою він з’явиться у вкладці «розумний дім» (рис.3.10).

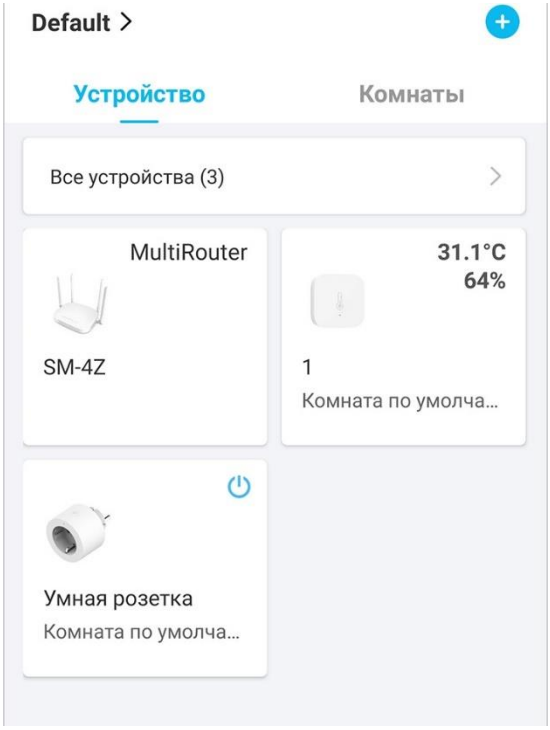

Рисунок 3.10 – відображення пристроїв у вкладці «розумний дім»

Є можливість створення сценаріїв автоматизації (рис.3.11). Тобто можна створити сценарій при якому якийсь із елементів системи «розумного дому» виконував певні дії. Можна налаштувати час виконання та графік, у які дні тижня або взагалі кожного дня. Також через те, що у даного роутера є підтримка сім карти, є можливість відправляти SMS повідомлення.

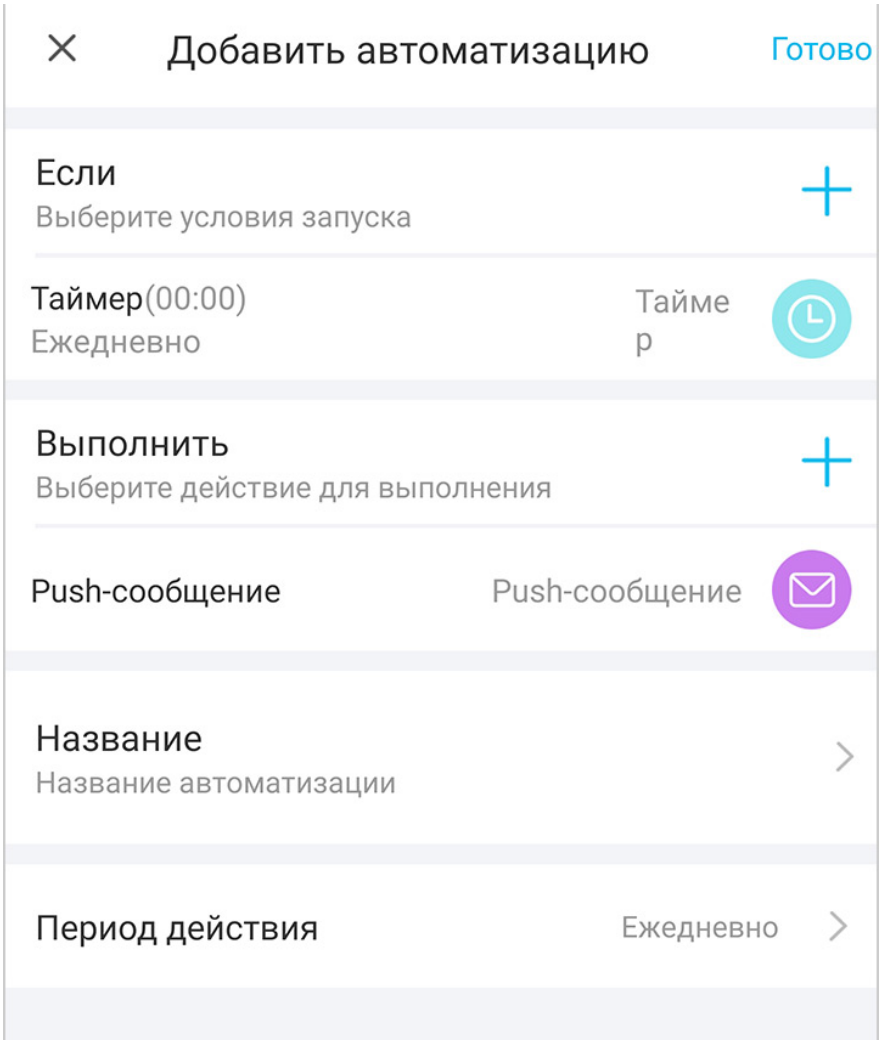

Рисунок 3.11 – створення сценарію для автоматизації процесу

Також є цікава функція, коли пропадає світло у всьому будинку роутер зможе відправити SMS повідомлення про те, що напруга зникла та керувати елементами системи «розумного дому» не має можливості. Ця функція наявна за рахунок конденсатора, енергії якого вистачить для відправки SMS повідомлення у разі зникнення напруги.

Підводячи підсумки даного рішення можна сказати, що при використанні роутера 4G WI-FI ZIGBEE MULTIROUTER SM-4Z у якості шлюзу для системи «розумного дому» на базі ZigBee від Aqara та точки доступу для користування WiFi на каналі 5 ГГц можна досягти оптимізації часу затримки передачі інформації максимальної з 240мс до 200, а середнє значення зі 100мс до 80мс. Тобто максимальна затримка зменшиться на 17%, а середня на 20%.

За рахунок того що канал зв'язку 2.4 ГГц буде вже не на стільки навантажений робота системи «розумного дому» буде більш стабільніша.

Також буде присутній резервний канал зв'язку який знадобиться у разі обриву основної лінії зв'язку і можливість відправки SMS повідомлення при зникненні напруги.

3.3 Оптимізація за допомогою використання протоколу Z-Wave

ZigBee це відносно не дорога технологія, але ця технологія має декілька недоліків, які можуть впливати на роботу системи «розумного дому». До цих недоліків можна віднести:

а) використовує діапазон 2,4 ГГц, де сильні перешкоди від Wi-Fi, Bluetooth, мікрохвильових печей;

б) вкрай погана сумісність між пристроями ZigBee різних виробників через занадто м'які умови сертифікації, що висуваються консорціумом ZigBee Alliance;

в) проблеми з безпекою через недотримання виробниками вимог сертифікації.

Також максимальна швидкість передачі даних 250кб\с. Для таких частин «розумного дому» як освітлення чи опалення буде достатньо такої швидкості, навіть якщо будуть сильні перешкоди через навантажений діапазон 2.4 ГГц, а ось частина системи «розумного дому» які відповідають за безпеку, захисту від диму, газу, протікання води, датчиків відкриття

дверей та інші, повинні працювати бездоганно та без збоїв і відпрацьовувати як найшвидше.

На ринку технологій для «розумного дому» є протокол Z-Wave. Він був розроблений для домашньої та офісної автоматизації. Працює в діапазоні до 1 ГГц. Тобто ця технологія працює не в навантаженому каналі і тому робота системи «розумного дому» буде завжди стабільною.

Для оптимізації важливих компонентів системи «розумного дому» буде використано контролер розумного будинку Z-Wave Vera Secure - MCVEVERA_SECURE (рис.3.12).

Рисунок 3.12 – контролер Z-Wave Vera Secure - MCVEVERA_SECURE

Дане рішення цікаве тим, що контролер має підтримку не тільки протоколу Z-Wave, але і ZigBee та Bluetooth. Тобто не потрібно буд тримати додатковий контролер для автоматизації для протоколу ZigBee.

Також є вбудований резервний канал 3G, а також є внутрішня батарея ємкістю на 2400mAh. Тобто у разі зникнення напруги та доступу в інтернет, система «розумного дому» все одно буде працювати.

Для оптимізації потрібно змінити деякі частини системи «розумного дому». Потрібно підібрати датчик диму, газу, витоку води та відкриття дверей. Усі ці датчики повинні спрацьовувати без збоїв через навантажений діапазон. Головною перевагою Z-Wave є те, що будь-які датчики можуть працювати разом, майже усі датчики сумісні між собою.

У якості датчика диму буде обрано HEIMAN SMOKE SENSOR Z-WAVE PLUS (рис.3.13).

Рисунок 3.13 – датчик диму HEIMAN SMOKE SENSOR Z-WAVE PLUS

У якості датчика газу буде обрано Z-WAVE HEIMAN GAS SENSOR (рис.3.14).

Рисунок 3.14 – датчик газу Z-WAVE HEIMAN GAS SENSOR

У якості датчика протоку води буде обрано Z-WAVE NEO COOLCAM FLOOD SENSOR (рис.3.15).

Рисунок 3.15 – протоку води Z-WAVE NEO COOLCAM FLOOD SENSOR

У якості датчика відкриття дверей буде обрано Z-WAVE NEO COOLCAM DOOR/WINDOW SENSOR (рис.3.16).

Рисунок 3.16 – датчик відкриття дверей Z-WAVE NEO COOLCAM DOOR/WINDOW SENSOR

Після встановлення та налаштування системи «розумного дому», а саме:

а) додавання нового контролеру;

б) заміна старих датчиків на нові;

в) додавання старої та нової системи у контролер.

Можна зробити висновки, що система захисту від протікання води, витоку газу, появи диму та відкриття дверей «розумного дому» почне працювати стабільніше за рахунок використання іншого протоколу, який працює в діапазоні до 1 ГГц. У той час коли пропускна здатність у протоколу ZigBee варується від 5кб\с до 40 кб\с і дуже залежить від того, на скільки навантажений діапазон 2.4 ГГц, в середньому це значення близько 25кб\с, то у Z-Wave пропускна здатність починається з 40кб\с і може досягати 100кб\с.

Тобто мінімальна пропускна здатність збільшиться на 38%, а максимальна на 60%.

Також перевагою цієї системи є наявність резервного каналу зв’язку через наявність вбудованого модулю 3G, а також можливість підтримки роботи системи «розумного дому» за рахунок наявності резервного каналу живлення, який знаходиться в середині контролера на 2400mAh.

3.4 Висновки

У даному розділі було розглянуто два варіанти оптимізації системи «розумного дому» на базі протоколу ZigBee. У першому варіанті було розглянуто оптимізацію за рахунок зміни головного контролера який працює виключно з протоколом ZigBee і використанні контролера як роуетра з каналом WiFi 5 ГГц і відмовитися від каналу 2.4ГГц для WiFi для оптимізації часу затримки, яка стала краще на 17-20%. Також завдяки використанню цього контролера у системи «розумного дому» з’явився резервний канал зв’язку.

У другому варіанті було розглянуто оптимізацію системи «розумного дому» за рахунок зміни контролера з підтримкою не лише ZigBee, а і Z-Wave та Bluetooth. Було запропоновано змінити основні датчики , які відповідали за безпеку появи диму, газу, витоку води та відкриття дверей які раніше працювали з протоколом ZigBee, на датчики які працюють з протоколом Z-Wave. За рахунок цього мінімальна пропускна здатність збільшилася на 38%, а максимальна на 60%. Також завдяки використанню цього контролера у системи «розумного дому» з’явився резервний канал зв’язку 3G та резервний канал живлення з ємкістю 2400mAh.

ВИСНОВОК

В даній магістерській дисертації було розроблено два способи оптимізації організації системи «розумний дім». В ході дослідження було виконано наступні завдання: досліджено основні поняття системи «розумний дім»; досліджено існуючі протоколи для побудови систем «розумного дому» ; оптимізовано організацію за рахунок зміни обладнання, яке працює з тим же протоколом; оптимізовано організацію частини системи за рахунок зміни протоколу.

Оптимізація системи управління «розумного дому» на базі технології ZigBee у першому випадку була досягнута за рахунок зменшення часу затримки на 17-20%. Досягти цього результату вдалося завдяки зміні центрально контролера на роутер 4G WI-FI ZIGBEE MULTIROUTER SM-4Z. Він виступає як роутер і як контролер «розумного дому». Протокол ZigBee працює в діапазоні 2.4 ГГц, як і WiFi, тому заміна на цей роутер дає змогу використовувати діапазон 5 ГГц для WiFi та зменшити навантаження каналу 2.4 ГГц для протоколу ZigBee і покращення стабільності роботи. Також у цій системі «розумного дому» з’явилась можливість використовувати резервний канал зв’язку 4G, у разі зникнення основного каналу. А також реалізовано можливість відправки SMS у разі зникнення напруги.

У другому випадку оптимізація системи управління «розумного дому» на базі технології ZigBee була досягнута за рахунок збільшення пропускної здатності деяких важливих датчиків, мінімальна пропускна здатність збільшилася на 38%, а максимальна на 60%. Досягти цього результату вдалося завдяки використанні протоколу Z-Wave та заміні центрально контролера на Z-Wave Vera Secure - MCVEVERA_SECURE, а також заміни датчиків диму, газу, витоку води та відкриття дверей. Також у даній системі є резервний канал зв’язку 3G та резервне внутрішнє живлення на 2400 mAh.