Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Клименко Валерія Вікторівна,
студентка групи РЗ-181

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

Розробка безпечної бездротової мережі для керування елементами розумного будинку

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма:
Кібербезпека

Керівник:
Стопакевич Олексій Аркадійович,
к.т.н., доцент

Одеса – 2022

Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ
_____
д.т.н.,проф. А.А.Кобозєва
«___» 2022р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Клименко Валеії Вікторівні

1.Тема роботи: *Розробка безпечної бездротової мережі для керування елементами розумного будинку*.
керівник роботи Стопакевич Олексій Аркадійович*, к.т н., доцент*,
затверджені наказом ректора від „17” 05.2022р. №168-в.
2. Зміст роботи*: аналіз проблемної області, постановка задачі, аналіз вразливостей систем розумного будинку, розробка проекту системи безпеки датчиків розумного будинку, охорона праці*.
3. Перелік ілюстративного матеріалу: *структурна схема DS18B20, алгоритм передачі пакету, шифрування на мережевому рівні, шифрування на рівні програми, архітектура стека ZigBee, робочі частотні діапазони, поєднання каналів Wi-Fi та ZigBee, рівні роботи Frame Counter, тестовий стенд головного серверу, інтерфейс зчитування значень з датчику температури.*

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання рийняв
Охорона праці	Ярова І.А.	19.05.2022	

5. Дата видачі завдання "_____"_____20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*15-11-2021*	*виконано*
2	*Обґрунтування вибору рішення. Збір даних*	*15-12-2021*	*виконано*
3	*Аналіз вразливостей систем розумного будинку*	*11-01-2022*	*виконано*
4	*Розробка проекту системи безпеки датчиків розумного будинку*	*20-02-2022*	*виконано*
5	*Підготовка тексту роботи*	*11-04-2022*	*виконано*
6	*Підготовка презентації та доповіді*	*15-05-2022*	*виконано*
7	*Попередній захист*	*17-06-2022*	*виконано*
8	*Нормоконтроль, рецензування*	*29-06-2022*	*виконано*

Здобувач вищої освіти _____ *Клименко В.В.*

Керівник роботи _____ *Стопакевич О.А.*

ЗАВДАННЯ

на розробку розділу “Охорона праці”

Клименко Валерії Вікторівні, група РЗ-181

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Тема роботи: *Розробка безпечної бездротової мережі для керування елементами розумного будинку*

Зміст розділу:

1 Аналіз умов праці і вибір основних заходів виробничої безпеки.

2 Аналіз пожежної безпеки і вибір заходів та засобів пожежної безпеки.

Керівник роботи	Консультант з охорони праці
_____ (Стопакевич О.А.)	_____ (Ярова І.А.)
«____» _____ 2022 р.	«____» _____ 2022 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему “Розробка безпечної бездротової мережі для керування елементами розумного будинку” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 – Кібербезпека, спеціалізація, освітня програма: Кібербезпека, містить 10 рисунків, 1 таблицю, 37 літературних джерел за переліком посилань. Робота виконана на 47 сторінках основного тексту.

Метою роботи є підвищення та модернізація рівня безпеки систем «Розумний будинок».

У роботі проведено аналіз безпеки протоколу ZigBee для системи «Розумний будинок», описані загрози безпеці системи та заходи їх усунення.

У результаті виконання кваліфікаційної роботи було розроблено проект захищеного вузла розумного будинку для забезпечення комфортних кліматичних умов усередині приміщення.

Результати даної роботи можуть бути використані при побудові захищеної мережі систем розумного будинку у мережі ZigBee.

ZIGBEE, РОЗУМНИЙ БУДИНОК, ЗАСОБИ ЗАХИСТУ, ДАТЧИКИ, ДАТЧИКИ ТЕМПЕРАТУРИ, ШИФРУВАННЯ, БЕЗПЕКА.

ANNOTATION

Qualification work on "Development of a secure wireless network for smart home control" for the first (bachelor's) level of higher education in 125 - Cybersecurity, specialization, educational program: Cybersecurity, contains 10 figures, 1 table, 37 references at the list of links. The work is performed on 37 pages of main text.

The aim of the work is to increase and modernize the level of security of "Smart Home" systems.

The paper analyzes the security of the ZigBee protocol for the Smart Home system, describes the security threats to the system and measures to eliminate them.

As a result of the qualification work, a project of a protected unit of a smart home was developed to provide comfortable climatic conditions indoors.

The results of this work can be used to build a secure network of smart home systems in the ZigBee network.

ZIGBEE, SMART HOUSE, PROTECTION EQUIPMENT, SENSORS, TEMPERATURE SENSORS, ENCRYPTION, SECURITY.

ЗМІСТ

ВСТУП

Зараз все більше людей хочуть спростити своє життя і не витрачати час для виконання повсякденних дрібних завдань на кшталт включення чайника або вимикання світла в усьому будинку та вирішення цього система розумного будинку. Хоча насправді можливостей у нього набагато більше, а саме:

- опалення;
- пожежна сигналізація ;
- система контроля доступу;
- система виявлення витоку води, газу чи аварії в електромережі;
- відеоспостереження та сигналізація;
- керування освітленням;
- контроль за енергоспоживанням та інше.

Розумний будинок - це комплекс побутових пристроїв, які об'єднані в одну мережу та керуються за допомогою бездротової мережі. У розумному будинку всі системи працюють злагоджено, дозволяючи об'єднати всі комунікації в одну і поставити їх під управління штучного інтелекту, що програмується та настроюється під усі потреби користувача.

Враховуючи що при використанні пристроїв розумного будинку збирається про них та про їх власника інформація, яка у свою чергу має бути захищена, розумний будинок має свої методи забезпечення безпеки. Однак у кожній з них є низка вразливостей. Моє завдання в даній дипломній роботі мінімізувати ці ризики та бажано з мінімальними витратами.

1 АНАЛІЗ ПРОБЛЕМИ

1.1 Аналіз сучасного стану системи «розумний дім»

«Розумний дім» являє собою зв'язок між домашніми пристроями, які з'єднані однією мережею та настроєні під потреби конкретної людини, яка керує цими пристроями та отримує від них інформацію за допомогою смартфона або окремого пристрою. Існує декілька систем, які поділяються за певними ознаками:

- дротові;
- бездротові;
- централізовані;
- децентралізовані;
- з відкритим протоколом;
- із закритим протоколом.

Всі пристрої "Розумний будинок", які пов'язані дротовою системою, здійснюють цей зв'язок за допомогою шини, яка передає дані між датчиками і пристроями будинку. Дротовий сигнал є надійним і має високу швидкість відгуку, за умови правильного проектування. На відміну від бездротових систем, у дротової є великий вибір елементів, що управляють, а також інтегрованих систем. Ще однією перевагою провідної системи є відносно висока тривалість служби. Особливістю такої системи виступає той факт, що про неї потрібно подбати на етапі проектування будинку або квартири, у крайньому випадку її можна встановити під час капітального ремонту, але це може бути більш труднішим в реалізації і внаслідок дорожче.

Бездротові системи працюють за допомогою радіоканалу. Це дає змогу встановити «Розумний дім», коли ремонт вже зроблений і не є в планах. Система може бути як вбудованою, так і накладною. Також така система потребує менше часу на її встановлення, знижує кількість необхідних дротів і не потребує, в більшості випадках, проекту. Кожен вимикач являє собою також радіопередавач, він має зв’язок з іншими вимикачами і дає змогу створювати різні сценарії освітлення. Ціновий діапазон різноманітний. Так як бездротова система працює

по радіоканалу вона потребує якісний радіозв’язок. Система менш надійна і швидкість відгуку також може бути гіршою. Мінімізувати ці недоліки можливо шляхом вибору якісного обладнання з великим ступенем захищеності цієї системи.

Ці дві системи: дротову та бездротову, також можна використовувати одночасно, наприклад доповнити вже встановлену заздалегідь дротову систему елементами бездротової, якщо немає можливості провести додаткові дроти і загалом облегшити доповнення потрібними пристроями свій «Розумний будинок».

Централізоване управління являє собою центральний модуль, а саме програмований контролер, який здійснює управління усіма «розумними» пристроями. Централізоване управління використовується і в дротовій, і в бездротових системах. Має можливість встановлення тяжких сценаріїв роботи пристроїв і їх широкий вибір. Перевага централізованої системи полягає в тому, що при поломці одного з компонентів, система продовжить свою роботу без нього, але якщо зі строю вийде центральний модуль, уся система припинить роботу. Основні компанії, що виробляють централізовану систему:

- Z-WAVE;
- Bechoff;
- AMX та інші.

Децентралізоване управління в системі «Розумний будинок» має сервер на який всі пристрої відправляють дані, але при виході зі строю головного серверу кожен пристрій може працювати автономно, тому така система вважається надійною. Пристрої в такій системі не залежать один від одного і мають енергонезалежну пам’ять. Основні компанії, що виробляють децентралізовану систему:

- Gira;
- ABB;
- HDL;
- Jung та інші.

Відкриті протоколи передачі даних – це протоколи, які були створені компаніями або окремими особами та надані для загального користування. Сам по собі протокол передачі даних є якоюсь угодою на основі якої відбувається обмін даних між пристроями або програмами. Найбільш відомими відкритими протоколами є:

– TCP/IP;
– UDP;
– FTP;
– HTTP;
– SSH;
– NTP.

Закритий (пропрієтарний) протокол передачі. Інформація про такі протоколи доступна лише її творцям або особам, які купили ліцензію. Прикладами таких протоколів є транспортний протокол Вентурі (VTP) та Kerberos.

1.2 Аналіз роботи бездротових мереж

У системі "Розумний дім" є три основні ланки:

– датчики;
– актуатори;
– центральний контролер.

Датчики збирають інформацію про стан навколишньої середи. Актуатори керують пристроями та відповідають за можливість зміни стану навколишньої середи. Центральний контролер у свою чергу приймає інформацію від датчиків та керує роботою актуатора. Він є сполучною ланкою між системою домашньої автоматизації та мережею провідної або бездротової. За наявності веб-сервера керувати своїм "Розумним будинком" можна з будь-якого браузера.

Розповсюдження отримали такі технології бездротових мереж як ZigBee, KNX, Z-Wave, Wi-Fi та Bluetooth. Але підключення датчиків та актуаторів до Wi-Fi може здійснюватися лише якщо вони підтримують цю мережу.

KNX є популярним, але не дешевим варіантом протоколу зв'язку. Він складний у проектуванні та монтажі, але в ньому досить багато функцій. Цей протокол здійснює передачу даних декількома способами: через радіоканал, електричну мережу або виту пару. Часто використовую саме шину (виту пару) впроваджуючи її в проект ще під час будівництва. KNX можна використовувати як децентралізовану мережу, де модулі взаємодіють між собою. При цьому система повинна мати джерело живлення. Актуатори для даного протоколу зв'язку відрізняються своїм різноманіттям, що дозволяє власнику розумного будинку впровадити в нього не тільки базовий функціонал. KNX – це досить важкий протокол для встановлення, тому в основному його установкою займаються лише спеціалісти.

Wi-Fi – найпоширеніший протокол передачі даних. Його використовують майже у всіх розумних будинках. Цей стандарт зв'язку дуже зручний, коли в будинку вже встановлено автоматизовану систему і потрібно керувати нею з телефону або іншого пристрою. Деякі пристрої мають можливість працювати автономно без участі автоматизованої системи, маючи зв'язок з Wi-Fi. На відміну від KNX, Wi-Fi не підходить для складних систем автоматизації, бо швидкість не така якісна як у інших протоколів та модулі зв’язку невиправдано дорогі.

Протокол зв'язку ZigBee використовує радіоканал і добре підходить для впровадження в систему розумного будинку. Датчики в даному стандарті мають низьке енергоспоживання та гарний відгук. Модулі ZigBee в основному знаходяться в режимі сну і моментально спрацьовують, коли це необхідно. ZigBee підтримує комірчасту топологію мережі, в якій окремі елементи можуть взаємодіяти один з одним і працювати як комутатор. Така система стійка до відмови, тому вихід з робочого стану одного або декількох складових не несе за собою серйозних наслідків. Комірчаста топологія дає можливість організувати збільшену область роботи бездротової мережі. ZigBee ділиться на три типи елементів мережі: координатори, маршрутизатори та кінцеві пристрої. Координатори займаються керуванням мережі. Маршрутизатори здійснюють зв'язок між пристроями. А кінцеві пристрої розпочинають процес передачі даних.

Процес монтажу системи ZigBee досить простий, проте якщо використовувати пристрої ZigBee різних виробників, може виникнути проблема сумісності.

Протокол бездротової мережі Z-Wave, як і ZigBee має комірчасту топологію мережі та низьке енергоспоживання. Проте в технічній частині вони відрізняються і мають різну стандартизацію. Всі пристрої Z-Wave базуються на модулях Sigma Designs, тому, на відміну від ZigBee, вони сумісні один з одним.

Bluetooth працює з усіма рівнями OSI. Цей стандарт зв'язку називається Bluetooth Low Energy і має низьке енергоспоживання та таку ж пропускну здатність. Передача даних здійснюється невеликими пакетами і з'єднання пристроїв один з одним відбувається тільки коли надсилаються або приходять дані. У Bluetooth Low Energy досить велика швидкість передачі даних та відгуку пристрою, так само він більшу частину часу перебуває в пасивному режимі, швидко реагуючи на появу задачі. Крім цього, у даного стандарту є технологія названа маячками, яка дозволяє визначити точне розташування пристрою або його близькість. Смартфон та розумний пристрій за допомогою Bluetooth мають можливість зв'язуватися один з одним безпосередньо, що є великою перевагою цього стандарту. Недоліками Bluetooth Low Energy полягають у тому, що він використовує діапазон частот 2,4 ГГц і є проблемою з частими перешкодами, загасанням сигналу та малим радіусом дії.

1.3 Аналіз принципів захисту системи від злому

Якими б зручними не були технології розумного будинку, у них є негативна сторона. Зі зростанням популярності та кількості систем розумного будинку зростатиме і кількість зламів цих систем. Більшість систем мають проблеми, пов'язані з безпекою. Однією з таких проблем є те, що технолігії розумного будинку розвиваються досить швидко і, як виявилося, набагато швидше, ніж система безпеки для них.Підключаючи "розумні" пристрої до інтернету, користувач покладається на роботу сервера та якість з'єднання, і якщо обладнання вразливе, злочинець може його зламати. Центром розумного будинку найчастіше є контролер, за допомогою якого користувач звертається до пристроїв своєї

автоматизованої системи. Пристрої передають свої дані та дані про виконання свого завдання. Метою злому може стати як хмарний сервер, так і будь-який розумний пристрій. Були випадки, коли система "Розумний дім" від деяких компаній, дозволяла будь-кому отримати доступ до резервних копій програмної частини контролера і в результаті завантажувати їх на хмарний сервер. У резервній копії контролера зберігається багато даних про власника, такі як паролі, розташування, електронної адреси. І все це знаходиться без шифрування, за винятком пароля від панелі адміністратора, який хешується, однак, маючи всі резервні копії, пароль можна підібрати. Користуючись цією вразливістю, зловмисник має можливість проникнути в систему і дати собі права суперкористувача, що дасть повний контроль над розумним будинком, якого немає навіть у його власника.

Інша ситуація: користувач за допомогою свого пристрою надсилає контролеру команду синхронізації. Контролер має серійний номер за яким йому призначається файл конфігурації. Він завантажує потрібний файл, змінюючи параметри системи за даними цього файлу. Загроза полягає в тому, що файл конфігурації проходить через не захищене з'єднання, через що є ризик заміни файлу. Друга загроза - це серійний номер, дізнавшись його нападник, може відправити контролеру свій файл конфігурації і той його пропустить. Файл конфігурації містить ім'я та пароль користувача. Пароль звичайно захищений, але, як виявилося, не надійно. І цьому також сприяє те, що введення складного пароля розробниками не передбачено. Таким чином, дізнавшись, по необережності користувача, серійний номер, зловмисник може керувати системою розумного будинку.

Ще однією вразливістю є поширене явище серед розробників, коли вони розробляючи програму для розумного будинку, залишають собі "чорний хід", за допомогою якого можна отримати повний доступ над пристроєм і контролювати його. Незважаючи на те, що виробники стверджують, що це потрібно для технічної підтримки, такий прийом є навмисною вразливістю, що йде в розріз із захистом інформації.

Принцип захисту систем розумного будинку, крім створення надійних паролів та передачі даних, полягає у перевірці сторонніх додатків та пристроїв. Існує спеціальний список вимог до системи, якому повинні слідувати розробники під час роботи над нею і в кінцевому підсумку має вийти програма або пристрій із коректною та безпечною системою авторизації. Вона повинна перешкоджати несанкціонованому доступу.

Щоб запобігти несанкціонованому втручанню в систему, обмін даними між сервером і пристроєм повинен бути зашифрованим і використовувати ключ.

Існує стандарт Thread, який використовує IPv6 та був заснований на стандарті IEEE 802.15.4. Головний плюс цього стандарту – це високий рівень його безпеки, в тому числі при знаходженні в мережу великої кількості пристроїв. Thread прозорий, тому користувачі мають можливість перегляду всіх підключених до системи пристроїв. Достатня кількість систем може підтримувати цей стандарт, не потребуючи аппартаних змін, здійснюючи лише регулярне оновлення програмного забезпечення.

2 РОЗРОБКА СТРУКТУРИ СИСТЕМИ «РОЗУМНИЙ ДІМ»

2.1 Вибір та опис системи датчиків та виконавчих пристроїв системи «розумний дім»

Для того, щоб розумний будинок міг справно керувати станом окремих частин приміщення, йому необхідно визначати поточний стан речей. Для цього датчики можна розділити в середньому на три складові:

- сенсор;
- мікропроцесор із пристроєм передачі інформації;
- система живлення.

Система "Розумний дім" може поєднувати в собі безліч різних датчиків.

2.1.1 Сенсори температури

В теперішній час у датчиків температури загалом використовується 2 сенсора: DS18B20 та TMP36.

DS18B20 цифровий датчик з широким діапазоном вимірювання температури (-55 – 125) з програмованою точністю від 9 до 12 біт. Кожен датчик при виготовленні отримує свою унікальну адресу, що дозволяє на одній шині даних використовувати велику кількість датчиків (до 264). З'єднання відбувається по шині 1-Wire. Також незаперечним плюсом є можливість підключення живлення двома способами (режим прямого живлення та режим паразитного живлення). Зі структурної схеми (див. рис. 2.1) видно, що за режими живлення датчика відповідають 2 блоки: POWER SUPPLY SENSE;PARASIT POWER CIRCUIT.

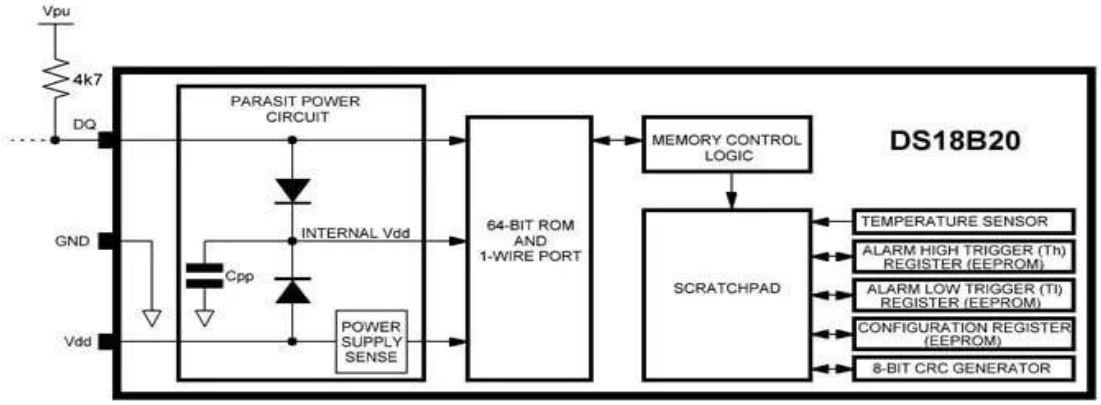

Рисунок 2.1 – Структурна схема DS18B20

Далі слідує блок у якому міститься унікальна адреса пристрою “64-BIT ROM AND 1-WIRE PORT”. Модуль “MEMORY CONTROL LOGIC” використовується для зв'язку шини 1-Wire із внутрішньою пам'яттю датчика SCRATCHPAD. Ця пам'ять взаємодіє з певними регістрами:

- TEMPERATURE SENSOR відповідає за зчитування температури;
- ALARM HIGH TRIGGER та ALARM LOW TRIGGER – регістри, які дозволяють задати верхню та нижню межу спрацьовування сигналів тревоги у разі виходу температури за заздалегідь зазначені межі;
- CONFIGURATON REGISTER – регістр, який потрібен для налаштування точності вимірювань температурного датчика. Він може бути налаштований на зміну температури з точністю від 9 до 12 біт, при цьому точність вимірювання 0.5oC, 0.25oC, 0.125oC і 0.0625oC відповідно;
- 8-BIT CRC GENERATOR – регістр, що генерує контрольну суму для підвищення захисту даних.
- технічні характеристики DS18B20:
- напруга живлення від 3 до 5,5;
- максимальний струм споживання до 4 мА;
- максимальний час вимірювання температури (при 12-бітовій роздільній здатності) 750 мс;
- діапазон вимірювання температури -55 – 125;
- максимальна помилка вимірювання температури +-0,2.

TMP36 – аналоговий датчик вимірювання температури з можливістю калібрування точності вимірювань. Особливість даного датчика полягає в тому, що напруга на виході пропорційна температурі. З цього випливає особливість - вимірювання відбувається логічно зрозумілим способом (де 0 В - мінімальна межа температури, а напруга живлення датчика - максимальна), але мікроконтролер повинен включати блок АЦП, що підвищує вартість кінцевого продукту.

Технічна характеристика TMP36: напруга живлення від 1,8; струм споживання 50 мкА; діапазон температур від -55 до +150; точність виміру температури +-2.

2.1.2 Датчики газу

Невід'ємною частиною безпеки будинку є визначення витоку газу. Найчастіше застосовуються дачі серії MQ:

- MQ-2 – сенсор зрідженого газу, водню, метану, диму, алкоголю, пропану та чадного газу;
- MQ-3 – сенсор пари алкоголю;
- MQ-4 – сенсор виявлення метану, пропану;
- MQ-5 та MQ-6 – призначені для виявлення бутану, пропану;
- MQ-7 - чутливий до чадного газу;
- MQ-8 – спеціалізується з водню H2.

MQ-2 найпоширеніший серед датчиків газу із серії MQ. Даний датчик газу є хімічним резистором, так як при виявленні витоку відбувається зміна опору чутливого матеріалу при вступі газу в контакт з таким матеріалом. При цьому концентрація газу вимірюється при використанні ланцюга дільника напруги. Концентрація, яку датчик MQ-2 може виявити від 200 до 10000 ppm.

Що стосується внутрішньої структури, то датчик MQ-2 знаходиться під двома шарами тонкої сітки з нержавіючої сталі. Таку сітку ще називають антивибуховою, так як вона служить для того, щоб нагрівальний елемент в датчику не викликав вибуху при пошуку легкозаймистого газу. Крім цього сітка забезпечує захист датчика та фільтрує зважені частки. У результаті всередину проходять лише газоподібні елементи. Зв'язок сітки з корпусом забезпечує мідне затискне кільце. Датчик має зіркоподібну структуру, яка складається з чутливого елемента та шести з'єднувальних ніжок. Дві ніжки відповідають за нагрівання чутливого елемента, інші вихідні сигнали. У разі потрапляння певного газу на чутливий елемент його опір змінюється. Вимірюючи цей опір датчик визначає обсяг газу повітря.

Технічні характеристики MQ-2:

- робоча напруга 5;
- споживана потужність <800 мВт;
- вимірювання концентрації 200 – 10000 ppm.

2.2 Вибір бездротового модулю зв’язку

Бездротова технологія для систем розумного будинку є зручним рішенням завдяки можливості швидкого розгортання мережі, мобільності та легкості налаштування. Основними протоколами для бездротової мережі є ZigBee, Wi-Fi та Bluetooth.

Wi-Fi модуль ESP-01 – найпопулярніший модуль серії ESP8266. Зв'язок із пристроями виконується через UART за допомогою введення команд.

Технічні характеристики Wi-Fi модуля:

- Wi-Fi 802.11 b/g/n;
- режими WiFi: клієнт, точка доступу;
- вихідна потужність – 19,5 дБ;
- напруга живлення – 1.8 -3.6 В;
- струм споживання – 220 мА;
- портів GPIO: 4;
- тактова частота процесора – 80 МГц;
- має певний обсяг пам'яті коду, тому може використовуватися без мікроконтролера;
- оперативна пам'ять – 96 КБ;
- розміри – 13×21 мм.

Серед модулів Bluetooth найпопулярнішим є модуль HM-10 Bluetooth 4 BLE. Технічні характеристики HM-10:

- напруга живлення від +2.5V до +3.3V, необхідний максимальний струм 50mA;
- струм споживання в активному стані близько 9mA, і в стані сну 50 - 200uA;

- вихідна потужність RF: -23dbm, -6dbm, 0dbm, 6dbm;
- Bluetooth Version 4.0 BLE;
- швидкість послідовного порту за замовчуванням 9600 бод;
- PIN за замовчуванням 000000, стандартне ім'я HMSoft;
- заснований на чіпі CC2540 або CC2541.

Реалізацією протоколу ZigBee займається модуль XBee. Однак XBee не самостійний пристрій, для його керування потрібен зовнішній мікроконтролер, на відміну від ESP-01. Мікроконтролер займається виправленням модуля за допомогою AT-команд або впорядкованих структур даних. Є варіант використання XBee-модуля без зовнішнього мікроконтролера - це робота із зовнішніми датчиками, які зчитують аналогові значення або мають виходи у вигляді двох станів — «ввімкнене/вимкнено». XBee має 2 види портів: цифрові та мультиплексуванні аналогові. Для керування зовнішніми пристроями, крім цифрових виходів, можна використовувати 2 виводи ШІМ. Під час самостійної роботи модуль XBee може передавати дані за розкладом, надсилаючи їх у разі зміни стану сигналу на цифровому порту або через певні проміжки часу. Є кілька варіантів реалізації модуля без застосування зовнішнього процесора:

- тривожна кнопка із автономним харчуванням;
- активна радіочастотна мітка з використанням батарейного живлення для об'єктів, що переміщуються повільно;
- віддалена активація до 8 цифрових портів та 2 канали з ШІМ-керуванням;
- віддаленої зміни параметрів, наданих датчиком у вигляді напруги;
- зв'язок із будь-якими сенсорами по UART-інтерфейсу.

Але за умови автономного використання XBee не може використовуватися в пристроях, де потрібна обробка даних на віддаленому об'єкті. Внутрішня прошивка модулів не розрахована на підрахунок кількості імпульсів, облік реального часу, накопичення аналогових відліків у внутрішній пам'яті тощо. Для цього вже потрібний зовнішній мікроконтролер. Його потужність і розрядність визначається додатком користувача. Для управління XBee-модулем за допомогою

мікроконтролера і доступом до всіх ресурсів модуля включається режим API. За допомогою режиму API можна створювати мережеві вузли ZigBee.

У цій дипломній роботі розглядатиметься протокол ZigBee та концепція децентролізованого управління розумним будинком. Тому що він легко розширюється, мало споживає електроенергії та надає прийнятні швидкості передачі даних. Децетралізована система буде використовуватися за рядом її переваг: головний сервер виступає тільки в ролі формування задачі для датчика, далі завдання відправляється на датчик і у разі виходу з ладу головного сервера датчик продовжує працювати автономно. Децетралізована система дозволяє датчикам зв'язуватися між собою та приймати ті чи інші рішення. Для розуміння переваг розглянемо наступний сценарій. У приміщенні присутній датчик температури та контролер підігріву підлоги. За допомогою сервера встановлюються завдання для датчика та контролера, завдання полягають у тому, що, якщо датчик показує температуру вище заданої, тепла підлога відключається, якщо нижче – вмикається. Сервер тут відповідає за прийом та передачу інформації з датчиків. При виході його з експлуатації датчик і контролер можуть працювати автономно і відсилати один одному інформацію безпосередньо. У результаті, коли з датчика температури надходить інформація про зміну температури, контролер отримує її і діє відповідно до закладеного завдання.

2.3 Концепція безпеки та побудова топології мережі ZigBee

ZigBee може виступати у трьох режимах: як роутер, як кінцевий пристрій та як ретранслятор.

Таблиця 2.1 – Дані для різної конфігурації мережі

№	Кількість ретрансляцій	Шифрування	Напрямок передачі	Швидкість, кбіт/с
1	1	Ні	Роутер – роутер	35
2	1	Так	Роутер – роутер	19

3	1	Ні	Роутер – кінцевий пристрій	25
4	1	Так	Роутер – кінцевий пристрій	16
5	1	Ні	Кінцевий пристрій – роутер	21
6	1	Так	Кінцевий пристрій – роутер	16
7	4	Ні	Роутер – роутер	10
8	4	Так	Роутер – роутер	5

У теорії ZigBee дозволяє побудувати мережу з 65535 пристроїв, так як під адресу відводиться 2 байти. Але специфікації вказані інші непрямі обмеження. Таким чином, реальна мережа може існувати не більше ніж з 300 пристроїв. При більшій кількості пристроїв помітно зростає службовий трафік, внаслідок чого падає загальна швидкість передачі даних. Головне обмеження для більшої кількості пристроїв – великі затримки їх виявлення, прокладання маршрутів та обмеження ОЗУ для зберігання збільшених таблиць маршрутизації. Максимальне число пересилання пакетів ZigBee до 30 хопів. Цього достатньо, щоб покрити невеликий район.

При надсиланні команди на виявлення вузлів у мережі створюється тимчасова затримка, щоб усі вузли надіслали відповідь і при отруєнні не заважали один одному. Стандартна затримка дорівнює 6 с, при цьому мінімальна затримка – 3,2 с, а максимальна – 8. Час затримки залежить від кількості пристроїв у мережі.

У момент передачі повідомлення кінцевий пристрій вказується параметр максимального числа ретрансляцій. Стандартне значення становить 50 мс на відправлення та 100 мс на обробку даних. З цього випливає, що максимальна кількість ретрансляцій дорівнює 8. Якщо після відправки повідомлення модуль не отримує відповіді протягом 1,6 с, то він робить ще 2 спроби, за підсумком загальний час передачі пакета може займати до 4,8 с. У разі надсилання повідомлення на пристрій, що знаходиться в режимі сну, до цього часу додається ще й час пробудження. Ниже приведен алгоритм передачи пакета (див. рис. 2.2).

Мережа ZigBee - це передача даних, стійка до перешкод, різноманітних збоїв, багатопроменевого згасання та відмов. Також її можна охарактеризувати гарантованою та безпечно передачею. Підхід до моделі безпеки в мережах ZigBee є таким, що є можливість зниження ціни пристроїв, знижуючи при цьому вимоги до рівня безпеки. Конфіденційність в даній мережі забезпечується шляхом захисту ключових даних, проте основою є все ж таки довірчі відносини. Вони потрібні під час початкової установки ключів, а також при обробці інформації щодо безпеки. Це означає, що обмін даними відбувається лише між довіреними сторонами. Ключі в ZigBee є найважливішою частиною архітектури безпеки системи. Тому вони не повинні передаватися не захищеними каналами. За можливим виключенням приєднання до мережі нового пристрою, в момент приєднання.

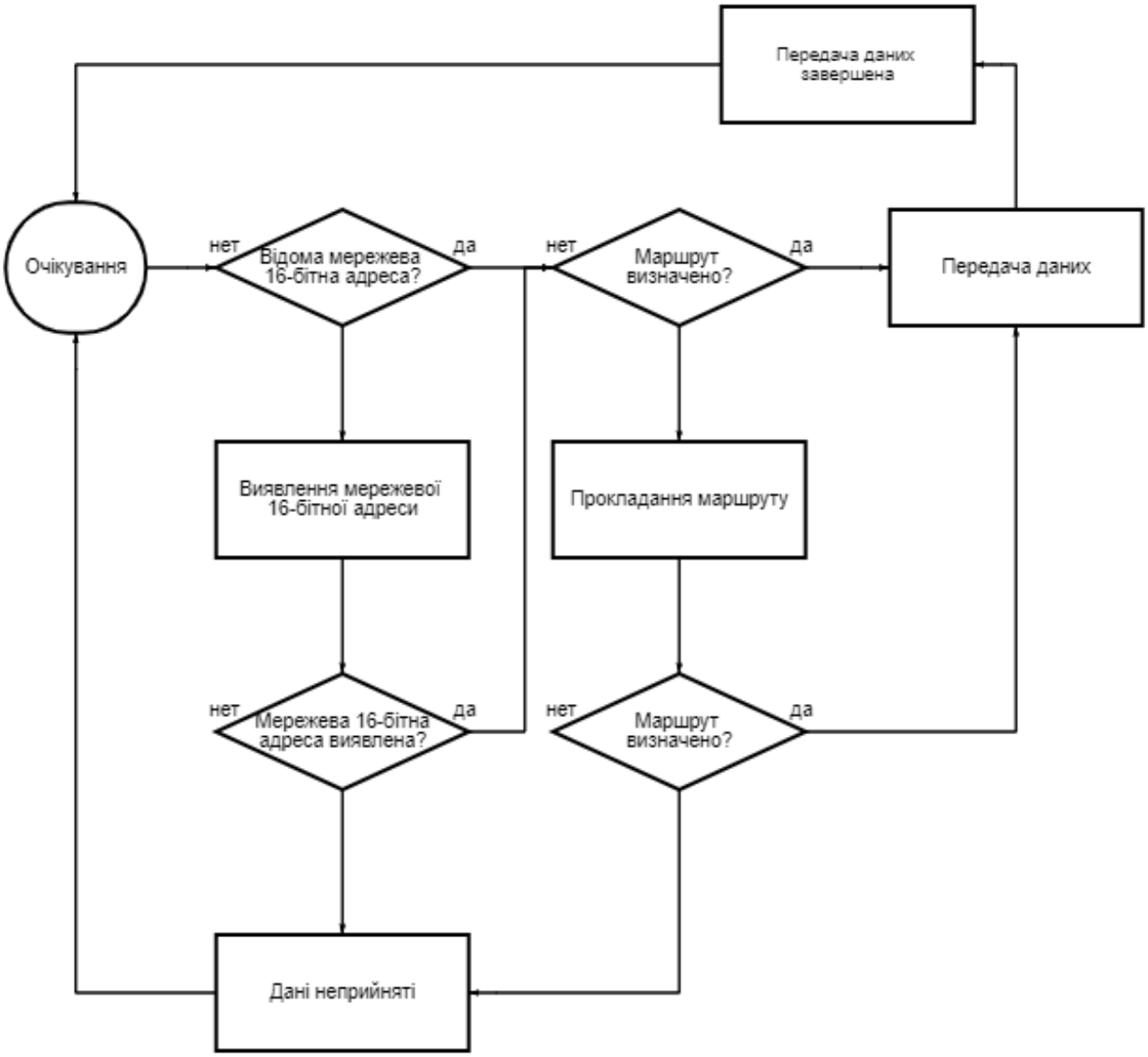

Рисунок 2.2 – Алгоритм передачі пакету

Оскільки мережі, що створюються, можуть бути фізично доступними для зовнішніх пристроїв, а робоче середовище може виявитися непередбачуваним, передбачаються особливі заходи безпеки. ZigBee не передбачає брандмауера між об'єктами додатків, тому в разі одночасного запуску декількох додатків, які використовують для зв'язку один приймач, вони повинні бути взаємно довіреними. Завдяки відкритій моделі довіри забезпечується розділення ключа. Для того щоб несанкціонований трафік міг бути усунений, все корисне навантаження на шарі, що його створює зобов'язана шифруватися, це рішення мінімізує ризик появи шкідливих пристроїв.

Криптографічний захист даних у мережах ZigBee реалізується за допомогою кількох механізмів:

– шифрування засноване на 128-бітному AES алгоритмі;
– 2 типи ключів шифрування;
– підтримка центру довіри;
– механізми перевірки справжності та цілісності повідомлення.

Є три режими безпеки за якими працюєте мережа ZigBee:

– локальний;
– стандартний;
– підвищений.

У локальному режимі безпеки ключ шифування повинен бути заздалегідь встановлений на всіх пристроях, що знаходяться в мережі. Сандартний режим додає додаткові операційні можливості та підтримує шифрування на рівні програм. Підвищений режим надає можливість автентифікації.

Модулі XBee використовують стандартний режим безпеки. При цьому кінцеві пристрої працюють на локальному режимі, маючи можливість підключатися та взаємодіяти з вузлами мережі зі стандартом режиму безпеки.

Безпека ZigBee передбачає її роботу на мережному рівні та на рівні програми. Інформація, під час своєї передачі по каналу шифрується AES алгоритмом з довжиною ключа 128 біт. У цьому випадку ключ є мережним та опціональним зв'язковим. З модуля витягти ключ неможливо. Взаємодіяти між собою можуть ті вузли ZigBee, які мають однаковий ключ. Ключі шифрування – це 128-бітна послідовність, яка може формуватися модулем самостійно або завантажуватися в нього вручну. Розсилку ключів шифрування та авторизацію вузлів, що підключаються до мережі ZigBee з безпекою здійснює центр довіри, він координатор.

На мережному рівні безпеки ключ застосовується для шифрування даних і додаткової інформації верхнього рівня. Останнє - це, пов'язана з інформацією про профіль, кластер і кінцеві точки мережі ZigBee, налаштування над корисними даними. Безпека на мережному рівні (див. рис. 2.3), крім захисту корисного

навантаження, займається шифруванням, пов'язаних зі службовими мережевими операціями, даних. Приклад таких даних є прокладання маршруту і команди рівнів APS. Мережева безпека не впливає на MAC-рівень. Адреси MAC-урівню не шифруються, тому будь-який пристрій 802.15.4, що працює в мережі ZigBee з увімкненою безпекою, може коректно прийняти інформацію, але доступу до даних за MAC-заголовком у нього не буде.

Рисунок 2.3 – Шифрування на мережевому рівні

Безпека на рівні прикладних програм дає можливість шифрувати корисні дані за допомогою ключа шифрування. Такий ключ знають лише відправник та одержувач пакету. Таке шифрування є необов'язковими, часто він використовується при надсиланні конкретного пакета. Також шифрування на рівні програми не може застосовуватися до широкомовних розсилок.

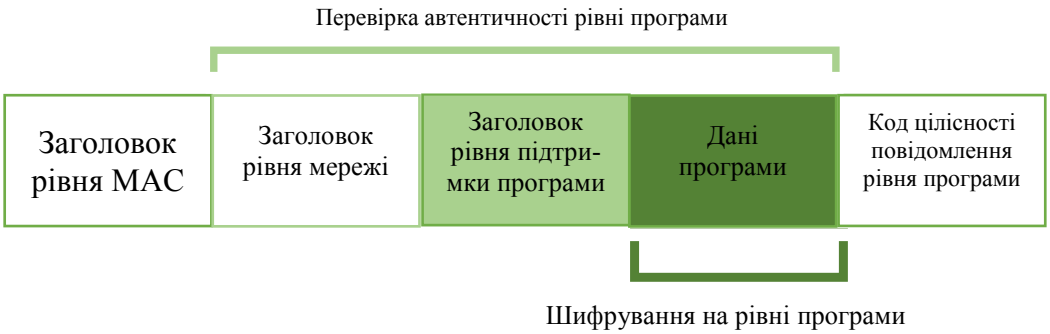

Рисунок 2.4 – Шифрування на рівні програми

Формування безпеки мережі ZigBee відбувається таким чином, що координатор відповідає за вибір мережевого ключа шифрування. Мережевий ключ спочатку заданий в координаторі або вибраний ним рандомнім чином.

Також він формує та роздає зв'язковий ключ, який також може вибиратися рандомно або бути заздалегідь заданим у модулі. При підключенні до мережі нового пристрою йому видається ключ, під час самого підключення. Якщо у програми ключ встановлений примусово, його передача приходить у зашифрованому вигляді. Інакше передача ключа виконується у відкритому вигляді. Однак використовувати відкриту відправку мережного ключа шифрування, оскільки це просто небезпечно. Для максимально надійності системи всі вузли повинні використовуватися в мережі тільки з заздалегідь встановленим зв'язковим ключем.

3 ЗАХИСТ МЕРЕЖІ ZIGBEE

3.1 Практичні вразливості мережі ZigBee

Архітектура стека ZigBee показана на рис. 3.1.

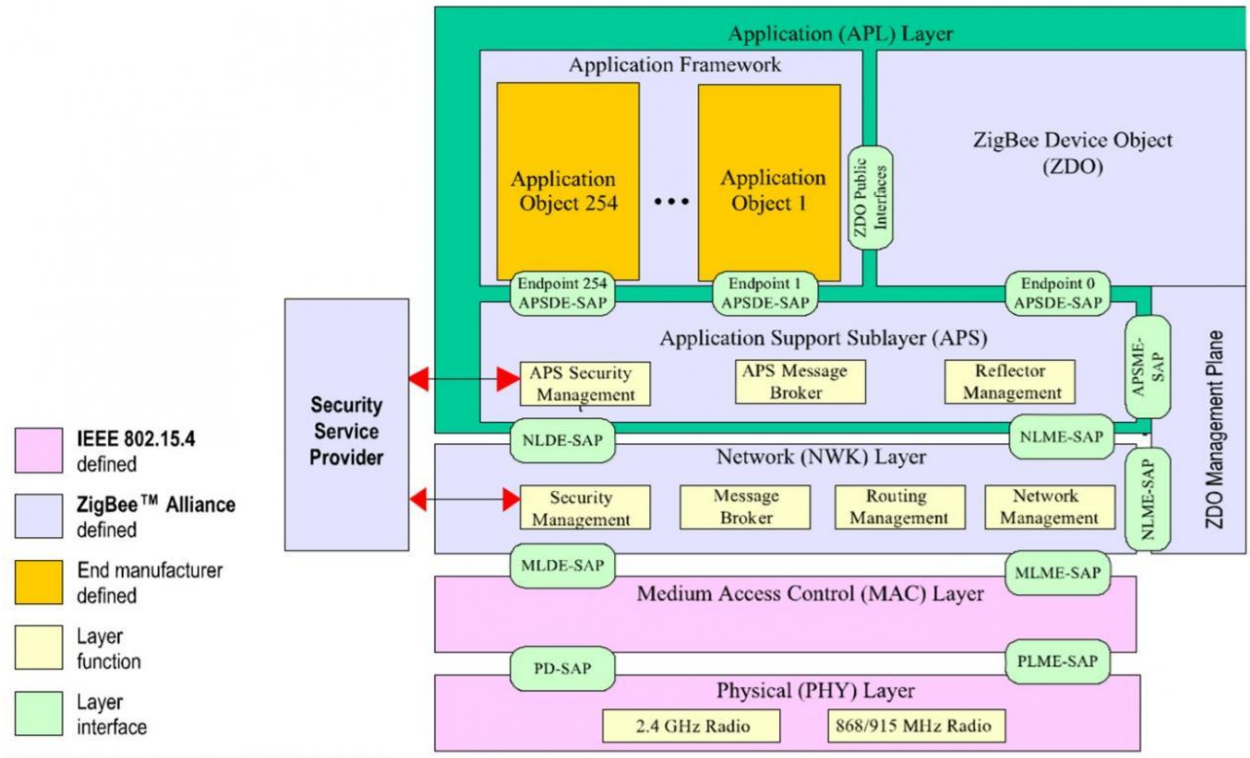

Рисунок 3.1 – Архітектура стека ZigBee

ZigBee може працювати у трьох частотних діапазонах (див. рис. 3.2)

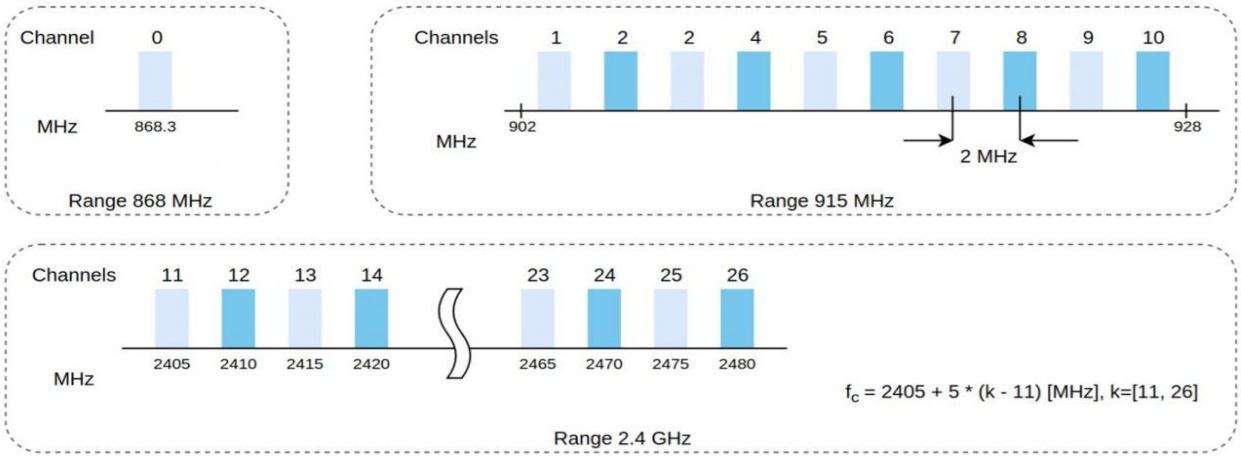

Рисунок 3.2 – Робочі частотні діапазони

Оскільки ZigBee працює на тих же частотах, що й Wi-Fi, рекомендується вказувати частоту роботи ZigBee між каналами Wi-Fi (див. рис. 3.3).

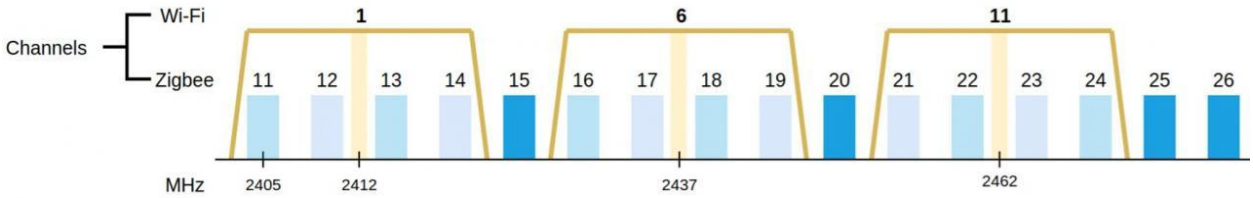

Рисунок 3.3 – Поєднання каналів Wi-Fi та ZigBee

Крім цього, стандарт IEEE 802.14.4 використовує ED (Energy Detection), яка використовується в координаторі розумного будинку для вибору каналу з меншими перешкодами.

Як вказувалося в другому розділі ZigBee для передачі інформації, використовує 128-бітний AEC ключ шифрування на рівнях NWK та/або APL. Але цей ключ шифрування використовується лише якщо пристрої узгоджені або належать одному виробнику. Для зворотної сумісності пристрою різних вендорів використовується стандарт IEEE 802.15.4, що дає низку додаткових вразливостей. Найголовніша з них – використання стандартного ключа шифрування Pre-configured global link key – дефолтний ключ для ZigBee. Його значення – 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39, що означає ZigBeeAlliance09. Він використовується для шифрування network key. Цей ключ необхідний для додавання нового пристрою до мережі, але це відбувається тільки тоді, коли ми вводимо головний сервер у режим додавання нового пристрою, що відбувається при запуску певної команди або натискання певної кнопки (для більшої безпеки рекомендується використовувати фізичну кнопку). При переході головного сервера в режим додавання нового пристрою відводиться невеликий час для обміну стандартними ключами шифрування. Виходячи з цього, якщо зловити момент сполучення нового пристрою, можна додати в мережу свій пристрій. Це зроблено для спрощення розгортання мережі користувачами, проте дає доступ у мережі зловмиснику. Якщо головний сервер не знаходиться в режимі сполучення, додати новий пристрій також неможливо. Але для більшої безпеки цей ключ слід замінити. Мережа може складатися з трьох видів пристроїв:

- роутер;
- координатор;
- кінцевий пристрій.

Кінцевим пристроєм є наші датчики та сенсори, у ролі роутера та координатора виступає головний сервер. Однак, кожен пристрій ZigBee може виступати роутером, координатором і кінцевим пристроєм в одному "обличчі". Координатор використовується для організації та побудови мережі, а також є центром довіри. Саме він вибирає ключі шифрування для рівнів NWK та APL та відповідає за підключення нових вузлів.

Одним із видів вразливості ZigBee є використання дефолтного link key під час підключення нових пристроїв. Про її рішення розповідається вище. Ще однією атакою є replay attack, вона ґрунтується на повторному використанні перехоплених ідентифікаторів сесії або іншої інформації для авторизації цільової системи. Прикладом такої атаки може бути копіювання даних про транзакцію, що передаються в систему фінансів з подальшим їх використанням зловмисником для здійснення платежу. Для цього злочинцю потрібно змінити дані про отримувача грошей сумі переказу у вихідному документі. Захист від таких атак здійснюється шляхом шифрування каналу передачі даних та видачі унікальних тимчасових ідентифікаторів відкритого сеансу. Теоретично на кожному рівні є Frame Counter (захист від відтворення), який повинен перешкоджати replay attack, але на практиці це не зовсім так.

Суть роботи Frame Counter полягає в тому, що кожен вузол у мережі ZigBee має 32-розрядний лічильник кадрів, що збільшується при кожній передачі пакетів даних. Кожен вузол також відстежує попередній 32-бітний лічильник кадрів кожного пристрою (вузла), якого він підключений. Пакет відкидається, якщо вузол отримує пакет від сусіднього вузла з тим самим меншим значенням лічильника кадрів, ніж він отримав раніше. Цей механізм забезпечує захист від відтворення, відстежуючи пакети та відкидаючи їх, якщо вони вже були отримані вузлом. Максимальне значення лічильника кадрів може бути 0XFFFFFFFF, але

якщо максимальне значення досягнуто, передача не може бути виконана. Лічильник кадрів скидається до 0 лише при оновленні ключа мережі.

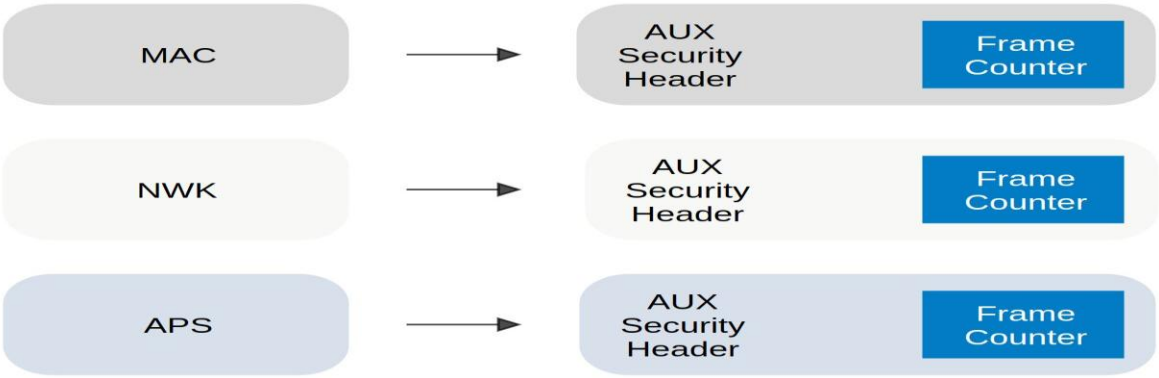

Рисунок 3.4 – Рівні роботи Frame Counter

Атака типу PAN ID. Її суть полягає у розгортанні злочинцем помилкового координатора. У результаті підданий координатор замінює PAN ID на інший пристрій. При цьому пристрої можуть бути прив'язаними до попереднього PAN ID. Це може призвести до неспрацьовування датчиків. Вирішенням проблеми є додавання резервної лінії зв'язку для критично важливих датчиків (у нашому випадку це датчик задимлення та контролер нагрівання теплої підлоги). Оскільки обидва ці модулі працюють від мережі змінного струму, то за резервну лінію зв'язку краще взяти протокол X10. Він дозволяє обмінюватись інформацією за допомогою електромережі. Дана лінія зв'язку буде резервна, в основному використовуватиметься ZigBee.

3.2 Вибір та програмування емуляторів датчиків та виконавчих пристроїв

Як було вказана вище головною проблемою безпеки в системі розумний будинок є підключення пристрою для відстеження показання датчиків та формування завдань для цих датчиків. Мною було розроблено алгоритм безпечного сполучення будь-якого пристрою з головним сервером. Принцип роботи: перед початком пари з пристроєм необхідно на головному сервері затиснути кнопку, що відповідає за підключення нових пристроїв. Після натискання користувач дається певної кількості часу на підключення, якщо час закінчився або введено неправильний ключ більше 5 разів, то повторити спробу

можна буде тільки після закінчення встановленого часу. Таким чином, ми захищаємо систему від грубого підбору паролів (Brute force).

Наведемо програмну реалізацію захищеного підключення будь-якого пристрою з головним сервером:

```
#define CONNECT_BUTTON 6
#define temp_1 7
#define temp_2 8
#define temp_err 9
bool prevState;//прошлое состояние кнопки
uint32_t timer;//когда мы нажали послений раз кнопку
uint32_t timer_connect;//когда мы начали процес подключения
bool set_connect;//определяет подключены или нет
int t=25;
String key_lock = "052dt42stb";
const char *ssid = "yourNetworkName";
const char *password = "yourNetworkPassword";
const char *temp = "t587";
const char *floar = "f179";
const char *inp = "p";
char *name = "NULL";
int prevtemp=25;
char *statetemp_char;//температура в чар
void setup()
{
  Serial.begin(115000);//скорость обмена информации с
модулями
  pinMode(CONNECT_BUTTON, INPUT_PULLUP);
  Serial.print("Connecting");
  Serial.println();
  Serial.println("Connected, IP address: 8.8.8.8");
}
bool butt(int pin)
{
  bool state;
  bool button = !digitalRead(pin);
  if (button && !prevState && millis() - 100 > timer)
  {
    timer = millis();
    prevState = true;
    state = 1;
  }
  if (!button && prevState && millis() - 100 > timer)
  {
```

```
    timer = millis();
    prevState = false;
    state = 0;
  }
  return state;
}
void loop()
{
  if (butt(CONNECT_BUTTON))
  {
    timer_connect = millis();
    while (set_connect==false)
    {

          set_connect = true;
    Serial.println("Connect");
      }
  }
  if(set_connect){
  if(butt(temp_1)) t++;
  if(butt(temp_2)) t--;
  if(butt(temp_err)) t=t+10;
  if(prevtemp!=t){
  if(prevtemp-t>5 || prevtemp-t<-5){
  Serial.println("ERROR Temp");
  prevtemp=t;
  }
  else{
  Serial.println(t);
  prevtemp=t;
  }
  }
  }
}
```

Був розроблений тестовий стенд (див. рис. 3.5) в емуляторі Proteus, де є такі складові частини:

- U1 – мікроконтролер Arduino Nano;
- екран, необхідний відстеження стану;
- 4 кнопки для зміни стану всередині емуляції (підключення, збільшення або зменшення температури та помилка).

Кнопка підключення (connect) необхідна для стикування головного пристрою з гаджетом. Саме ця кнопка при натисканні виділяє певний час для введення ключа.

Оскільки цей тестовий стенд (див. рис. 3.5) розгорнутий всередині емуляції, то доступу до гаджета у нас не передбачено, тому, при натисканні на кнопку connect, з буфера пам'яті підставляється автоматичний ключ. Клавіші регулювання температури необхідні для штучної зміни значень температури. Оскільки всередині емуляції неможливо вимірювати температуру були реалізовані фізичні кнопки, що відповідають за це. Кнопка помилки температури (error temperature) необхідна для введення помилки у показанні температури. Оскільки в реальних умовах температура не може змінюватися різко, то був реалізований механізм порівняння температури з попереднім значенням. Це необхідно для виявлення підроблених даних температури або поломки датчика температури.

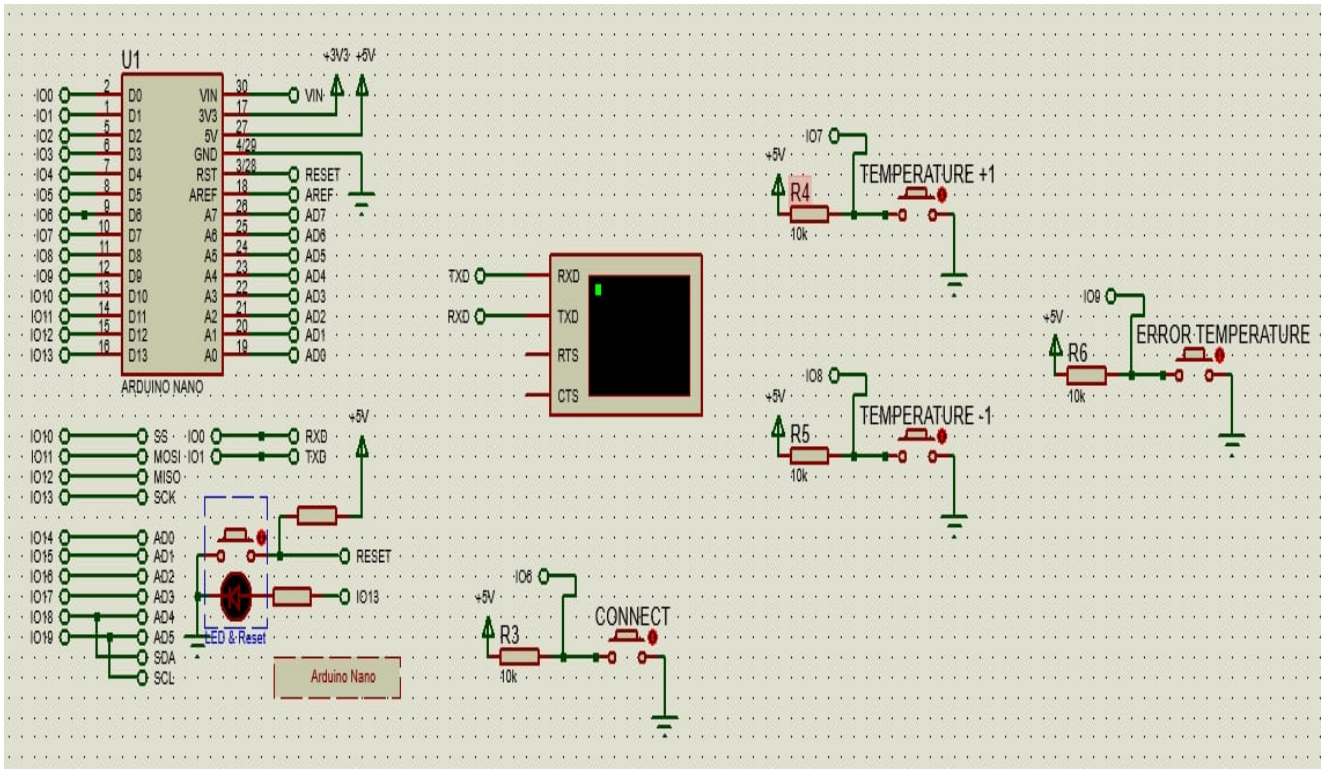

Рисунок 3.5 – Тестовий стенд головного серверу

Оскільки емульоване середовище накладає велику кількість обмежень, був розроблений прототип датчика температури, який зв'язується безпосередньо з головним сервером. А для виведення діючих значень розроблено програму з інтерфейсом (див. рис. 3.6):

```
using System;
```

```
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.IO.Ports;
namespace WindowsFormsApp1
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        private  void  buttonConnect_Click(object  sender,
EventArgs e)
        {
            if (buttonConnect.Text == "Подключиться")
            {
                try
                {
                    serialPort.PortName = "COM5";
                    serialPort.Open();
                    buttonConnect.Text = "Отключиться";
                }
                catch
                {
                    MessageBox.Show("Ошибка Подключения");
                }
            }
            else if (buttonConnect.Text == "Отключиться")
            {
                serialPort.Close();
                buttonConnect.Text = "Подключиться";
            }
        }
        private void label1_Click(object sender, EventArgs
e)
        {
        }
        private void serialPort_DataReceived(object sender,
SerialDataReceivedEventArgs e)
```

```
        {
            string temp = serialPort.ReadLine();
            label1.Text = "Температура дома "+temp;
            chart1.Series[0].Points.AddY(temp);
        }
        private void Form1_Load(object sender, EventArgs e)
        {
        }
        private void chart1_Click(object sender, EventArgs
e)
        {
        }
    }
}
```

Рисунок 3.6 – Інтерфейс зчитування значень з датчику температури

Приклад реалізації датчика температури:

```
#include <OneWire.h>
OneWire ds(51);
float prevTemp=0;
float max=0.1;
void setup(){
  Serial.begin(9600);
}

void loop(){
  byte data[2];
  ds.reset();
  ds.write(0xCC);
  ds.write(0x44);
  delay(1000);
  ds.reset();
  ds.write(0xCC);
  ds.write(0xBE);
  data[0] = ds.read();
  data[1] = ds.read();
  float temperature =  ((data[1] << 8) | data[0]) * 0.0625;
```

```
if(prevTemp==0){
    prevTemp=temperature;
  }

if(abs(prevTemp-temperature)<max){
  Serial.println(temperature);
  prevTemp=temperature;
}
else if(abs(prevTemp-temperature)>max){
  Serial.println("ERROR Temperature");
  delay(5000);
  //prevTemp=temperature;
}
}
```

4 ОХОРОНА ПРАЦІ

В цьому розділі розглядається аналіз умов праці та пожежна безпека на робочому місці інженера-проектувальника систем «Розумний будинок».

Згідно ГОСТу 12.0.003-74 у якому визначені фізичні небезпечні та шкідливі виробничі фактори було виділені ті фактори які присутні на робочому місці інженера-проектувальника систем «Розумний будинок»:

- підвищена чи занижена температура повітря робочої зони;
- підвищений рівень шуму на робочому місці;
- підвищений рівень електромагнітних випромінювань;
- підвищена напруженість електричного поля;
- підвищена напруженість магнітного поля;
- відсутність або нестача природного світла;
- недостатня освітленість робочої зони;
- підвищена яскравість світла;
- знижена контрастність.

В наш час технології безперервно і стрімко розвиваються і професії пов’язані з ІТ стали дуже поширеними. Серед них багато сидячої роботи за комп’ютером. Тому важливо забезпечити безпечні умови праці для робітників, що працюють увесь, або майже увесь час сидячи. Безпечні та комфортні умови праці забезпечують продуктивну роботу та якісне виконання працівниками конкретної задачі. Безпека на робочому місці потрібна для того щоб запобігти травмам та хворобам працівників на робочих місцях, що в свою чергу також дає змогу підприємству працювати якісно. У цьому процесі важливим елементом є ергономіка робочого місця, що являє собою науку про зручність та організацію робочого простору для ефективної та комфортної праці, опираючись на психофізичні особливості організму людини. Вона знижує втомленість працівника, збільшує ефективність бізнес-процесу та зберігає здоров’я людей. Ергономіка забезпечує зниження навантаження на тіло людини, а нам відомо, що чим більше людина втомлюється, тим гіршою буде її продуктивність, що не

вигідно ні працівнику, ні компанії в якій вона працює. Робоче місце повинно бути організоване відповідно стандартів, методичних вказівок та технічних вимог.

Не дивлячись на те, що робота за комп'ютером може здатися цілком безпечною, на відміну від підприємств з більш підвищеною небезпекою, в ній теж є свої нюанси, яких потрібно дотримуватись.

Стандарт висоти письмового та комп'ютерного стола 72-75 см, при такій висоті у людини є достатньо міста для ніг. Монітор розміщується на відстані 45-60 см, клавіатура на 10-15 см і вона повинна дозволяти повністю розмістити лікті на столі. Відстань від підлоги до верхнього краю клавіатури 0,7-0,8 м. Відстань від підлоги до центру екрана 0,8-1,9 м. Якщо недостатньо простору для розміщення усіх необхідних для роботи інструментів, це можна компенсувати розміщенням поряд тумб, стелажу та/або полиць. Усе це повинно бути розташовано по принципу «усе під рукою», що дозволить витрачати менше енергії та направити її на виконання робочого плану.

Якщо людина проводить за ПК більш ніж 6 годин на добу, є ризик розвитку захворювання опорної системи. Для того щоб мінімізувати ризики потрібно обладнати робоче місце спеціальним ортопедичним кріслом для роботи за комп'ютером. Воно оснащене спеціальним валиком у нижній частині спинки, який забезпечує підтримку попереку та повторює анатомічну будову тіла. Спинка крісла у робочому положенні фіксується під прямим кутом 90-95°. Кут між спиною та спинкою крісла 10°-30°. Відстань від підлоги до сидіння крісла 0,375-0,5 м. Кут зору 15°-25°. Інформація про ергономіку описана у ГОСТі 12.2.032-78.

Для приміщення з ПК існують певні вимоги до вологості, температури та рівню пилу. Температура повинна бути 21-25 °С, відносна вологість – 40-60%, рівень аероіонів – от 400-600 до 50 000 (оптимальний – 1500-5000). Це є оптимальними умовами для комфортного теплового балансу температури тіла людини. На терморегуляцію організму людини також впливає вологість повітря. Занадто низька вологість, яка менша 20%, викликає пересихання слизових оболонок, а саме дихальних шляхів та очей, а вища 85% ускладнює терморегуляцію. Також дуже важливою є оптимальна вологість, якщо вона вища

за норму, то слабкішим стає електростатичне та електромагнітне поле, рівень випромінювання яких в приміщеннях з комп'ютером завжди високий.

Що стосується пилу в приміщеннях з ПК, він є не менш важливим, тому що організм людини погано реагує на велику запиленість. Пил в офісі відрізняється від природнього, він містить частки шкіри людини, будівельних матеріалів, клею, тканей меблів, а також бактерії та віруси. Такий пил може визвати як алергічну реакцію, так і захворювання дихальних шляхів. Проблемою офісів з комп'ютерами полягає в тому, що через електромагнітне випромінювання пил не осідає на поверхні, він електризується від монітору та висить у повітрі, тому потрапляє на слизові оболонки людини та в легені. Через це вологе прибирання в офісі з ПК повинно проводитися від 3х разів на тиждень. Також приміщення повинно провітрюватися. Усі заходи безпеки стосовно робочих місць з ПК описані у обов'язкових санітарно-епідеміологічних правилах та нормах – СанПіН 2.2.2/2.4.1340-30 «Гігієнічні вимоги до персональних електронно-обчислювальних машин та організації роботи».

Чи не найбільш важливим є освітлення приміщення та безпосередньо робочого місця, бо більшу частину інформації людина отримує через органи зору, від ступеня втоми очей залежить настрій та самопочуття людини.

Насамперед в приміщенні повинно бути штучне та природне освітлення. Для працівника робоче місце за комп'ютером повинно бути не менше 6 м², а об'єм – більше 20 м³. Має значення й обробка приміщення, а саме її коефіцієнт відображення. Нормою для стін є 0,5-0,6, для стелі 0,7-0,8, для підлоги 0,3-0,5. Для цього застосовують дифузно-видбивні комплектуючі. Орієнтуватися тільки на природнє освітлення забороняється, але воно є оптимальним, бо більш сприятливе для зору людини. Робоче місце необхідно розмішувати біля вікна. Штучне освітлення використовують, коли природнього недостатньо. Воно поділяється на загальне, яке використовує систему освітлення стелі, робоче – освітлення на робочому місці здійснюється за допомогою настінних, настільних світильників, та тих, що ставляться на підлогу. Існує документація ДБН В.2.5-28:20018 , в якій прописані норми та нормативи, які враховуються при організації

освітлення при роботі з ПК. Для офісів спільного призначення з використанням комп'ютеру норма освітленості згідно з ДБН 300-500 лк. Щоб отримати оптимальне освітлення робочого місця, а саме коефіцієнта освітленості потрібно потужність потоку світла розділити на площу. Яскравість освітлення поверхонь, які знаходяться у полі зору повинна бути до 200 кд/м². Яскравість відблисків на екрані монітора не повинна перевищувати 40 кд/м².

Рівень шуму на робочому місці з комп'ютером неповинен перевищувати норм зазначених у СанПіН 2.2.4/2.1.8.562-96. Він складає не більше ніж 50 дБА. Знизити рівень шуму в приміщенні можна за допомогою звукопоглинаючих матеріалів з максимальним коефіцієнтом поглинання звуку в області частот 63-8000 Гц для обробки стін та стелі робочого приміщення. Джерелами шуму виступають:

- звуки, які доносяться з сусідніх приміщень або вулиці;
- технічні звуки. виникають у процесі функціонування обладнання. щоб мінімізувати шум від нього потрібно використовувати більш якісні пристрої.
- шум джерелом якого є людина. для зменшення шуму в приміщенні існують правила, які встановлює підприємство, порушуючи їх співробітник отримує попередження чи штраф.

На робочому місці працівника розміщуються монітор, клавіатура та системний блок. Коли дисплей включений створюється висока напруга на електронно-променевій трубці в декілька кіловат. Забороняється працювати за комп'ютером, якщо одяг або руки вологі, а також протирати його увімкненому стані. Потрібно завжди слідкувати за цілісністю проводки, відсутності пошкоджень та наявність заземлення приекранного фільтра. В процесі роботи ПК на корпусах моніторів наведені токи статичної електрики, які при доторканні можуть призвести до розрядів. Вони хоч і не становлять небезпеки для людини, але можуть призвести до поломки комп'ютера.

Пожежна безпека – комплекс заходів направлених на попередження виникнення випадкової або навмисної пожежі, обмеження та усунення його, якщо

він виник та мінімізація наслідків цього явища. Для досягнення потрібного рівня безпеки про роботі з комп'ютером, у виробничому приміщенні повинні бути аптечки першої медичної допомоги, системи автоматичної пожежної сигналізації і вогнегасники. Якщо в приміщені працюють багато комп'ютерів, там повинен бути службовий вимикач, що дозволяє в разі необхідності вимкнути усе живлення кімнати. Пожежна безпека забезпечується пожежною профілактикою та активним пожежним захистом.

Переважна більшість людей гине через токсичність продуктів горіння, а саме отруєнням чадним газом, він більш інтенсивне реагує з гемоглобіном ніж кисень і у людини виникає кисневе голодування та порушення координації рухів. Оксид вуглецю має велику концентрацію в продуктах горіння, тому й створює підвищену небезпеку. Основним токсичними продуктами горіння є оксид сірки та вуглецю, газоподібні кислоти, а саме синильна та соляна, аміак, альдегіди альфатичні. Чадний газ при концентрації 8-10% приводить до смерті через декілька хвилин.

Температура, яка перевищує 100 °С під час пожежі призводить до втрати свідомості людини і подальше загибелі через декілька хвилин. Така температура може викликати опіки шкіри. Небезпечною температурою вважається від 55 °С. До того ж вона викликає опіки другого ступеня при тривалості впливу 20 с, температура 70 °С завдає шкоди за 1 с.

Для забезпечення пожежної безпеки потрібно проводити бесіди з працівниками стосовно правил пожежної безпеки та не допускати дій, які можуть стати причиною пожежі. Також потрібне встановлення планів евакуації персоналу, технічне обслуговування вогнегасників. Зазвичай причинами пожежі на підприємствах з ПК стають електроприлади, куріння в невстановлених місцях, використання легкозаймистих речовин, порушення технологій, порушення правил використання електроприладів, закрите вентиляційний отвір в електроапаратурі та інше.

Потрібно слідкувати за чистотою приміщення. Сміття та горючі відходи потрібно регулярно утилізувати у спеціально виділене для цього місце.

Евакуаційні виходи, коридори, двері, сходини повинні бути порожніми, нічим не заставлені. Мебель та дроти не повинна бути перешкодою для евакуації людей в разі пожежі. Розташування електричних дротів повинно бути таким щоб вони не пошкоджувались і виключити ризик ураження робітників електричним струмом. По закінченню роботи потрібно вимкнути усі електроприлади та перевірити приміщення.

Для тушіння пожежі у приміщеннях використовують вогнегасники, які призначені для початкової стадії розвитку пожежі. Безпосередньо у приміщеннях з комп'ютерами використовують вогнегасник вуглекислотний ОУ-5, який призначений для гасіння різноманітних матеріалів, електричних установок, які знаходяться під напругою, ПК та оргтехніки. Хід дій такий, що при пожежі потрібно піднести вогнегасник якомога ближче до вогню , направити розтруб у вогнище, зірвати пломбу, далі відкрити вентиль, натиснути на пусковий важіль, направити газ на вогонь. При цьому розтруб не можна тримати рукою під час його роботи, так як він має дуже низку температуру. Також використовують порошкові вогнегасники ОП-5.

У ДСТУ 3675-98 йдеться про пожежну техніку, вогнегасники переносні, загальні технічні вимоги та методи випробовування. Вогнегасники потрібно грамото розташовувати на підприємстві згідно норм та правил, встановити потрібну кількість та їх положення. Вогнегасники повинні бути на кожному поверсі у кількості не менше ніж 2, у кожного повинен бути сертифікат. Вони повинні бути легкодоступними та розташовуватися у виділених місцях близько до передбачуваного місця пожежі, а також біля евакуаційних шляхів та виходів з приміщення. Вогнегасник повинен бути у робочому стані з запломбованим запірно-пусковим пристроєм. Маса вогнегасника не повинна перевищувати 20 кг. Розташування від підлоги не більше ніж півтора метри до верхньої точки, якщо маса вогнегасника менша ніж 15 кг та один метри, якщо більша. Також можна установити вогнегасник на підставці та на підлогу з надійною фіксацією від падіння. При цьому вогнегасник не повинен заважати пересуванню працівників.

Щоб забезпечити якісний пожежний захист необхідно знати принцип припинення горіння.

Однією з важливих задач пожежної безпеки є забезпечення достатньої міцності будівельної конструкції та захисту приміщень від руйнувань в умовах дії високої температури при пожежі. Приміщення з ПК повинні бути першого та другого ступеня вогнестійкості, через свою велику вартість та категорію пожежної небезпеки.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи було:

– Розглянуто протоколи передачі інформації, датчики вимірювання температури та газу в повітрі. Протоколи передачі інформації існують: ZigBee, KNX, Z-Wave, Wi-Fi та Bluetooth та їх реалізації ESP-01, HM-10 та XBee. Датчики вимірювання температури: DS18B20 та TMP36. Датчики газу використовуються найчастіше серії MQ (від MQ-2 до MQ-8).

– Розроблено систему безпечної передачі інформації від модуля до головного сервера шляхом ідентифікації кожного датчика за його номером і перевірки очних показань на коректність.

ПЕРЕЛІК ПОСИЛАНЬ

1. ZigBee-модулі XBee: питання практичного застосування. URL: https://wireless-e.ru/wpan/zigbee/zigbee-moduli/
2. Специфікація ZigBee. Безпека. URL: https://habr.com/ru/post/158355/
3. Безпечна передача даних у мережі ZigBee на прикладі радіомодулів XBee. URL: https://russianelectronics.ru/bezopasnaya-peredacha-dannyh-v-seti-zigbee-na-primere-radiomodulej-xbee
4. Злам систем розумного будинку від А до Я на прикладі протоколу ZigBee. URL: https://cryptoworld.su/vzlom-sistem-umnogo-doma-ot-a-do-ya-na-primere-protokola-zigbee/#ZigBee3
5. Атака повторного відтворення (Replay Attack). URL: https://encyclopedia.kaspersky.ru/glossary/replay-attack/
6. Розумний будинок, а в ньому – злом. URL: https://www.kaspersky.ru/blog/vulnerable-smart-home/23116/
7. Апокаліпсис у розумному домі. URL: https://www.kaspersky.ru/blog/mwc2018-insecure-iot/19780/
8. Основні небезпеки приладів у складі розумного будинку. Із чим стикаються споживачі? URL: https://www.itsec.ru/articles/osnovnye-opasnosti-ustrojstv-v-sostave-umnogo-doma-s-chem-stalkivayutsya-potrebiteli
9. Ризики інформаційної безпеки систем, побудованих за технологією «Розумний дім». URL: file:///C:/Users/Admin/Downloads/riski-informatsionnoy-bezopasnosti-sistem-postroennyh-po-tehnologii-umnyy-dom.pdf
10. Протоколи зв'язку для "розумного дому". URL: https://www.ferra.ru/review/smarthome/SmartHome-Protocols.htm
11. Складності і ризики розумного будинку. URL: https://tech-house.su/slozhnosti-i-riski-umnogo-doma/
12. Бездротові системи домашньої автоматизації. URL:

https://skomplekt.com/zwave_intro.htm/

13. Чотири типи розумних будинків. URL: https://ittell.ru/stati-signalizatsii/vidy-umnykh-domov-chetyre-tipa
14. Який вибрати розумний будинок, бездротовий чи дротовий? URL: https://smartx.kz/blog/kakoj-vybrat-umnyj-dom-besprovodnoj-ili-provodnoj
15. Розумний будинок - принцип роботи. URL: https://freehomeabb.ru/info/sistema-umnyj-dom/
16. Які бувають "розумні будинки". Огляд. Види розумних будинків. URL: http://www.besmart.su/article/kakie-byvayut-umnye-doma
17. Які бувають розумні будинки. URL: https://www.smarthouse.ua/kakie-byvayut-umnye-doma.html
18. Обладнання для розумного будинку. URL: http://electrica-prom.ru/clauses/umnyy-dom/sistema-umnyy-dom/oborudovanie-dlya-umnogo-doma/
19. «Розумний дім»: порівняння дротової та бездротової технологій. URL: https://umnye-doma.ru/reputatsiya/ob_umnom_dome_stati_/umnyi_dom_sravnenie_provodnoi_i_besprovodnoi_tehnologiy/
20. Протоколи Розумний Дім. URL: https://knx24.com/news/base/smart_home_protocols/
21. Розумний будинок. Протоколи. URL: https://sprut.ai/article/umnyy-dom-protokoly
22. Власний протокол - Proprietary protocol. URL: https://ua.wikibrief.org/wiki/Proprietary_protocol
23. Транспортний протокол Вентурі - Venturi Transport Protocol. URL: https://ua.wikibrief.org/wiki/Venturi_Transport_Protocol
24. Правила розумного будинку. URL: https://habr.com/ru/post/577052/
25. Природне і штучне освітлення. URL: https://www.minregion.gov.ua/wp-content/uploads/2018/09/DBN_Osvitlennya-ostatochna.pdf

26. Ергономіка робочого місця в офісі: організація за всіма правилами. URL: https://vobox.ru/publications/mebelnyy-ekspert/ergonomika-rabochego-mesta-v-ofise-organizatsiya-po-vsem-pravilam
27. Ергономіка та її значення для оптимізації трудової діяльності людини. URL: https://moluch.ru/archive/64/10404/
28. Система стандартів безпеки праці. URL: https://docs.cntd.ru/document/1200003913
29. Мікроклімат приміщення з комп'ютером. URL: https://it.wikireading.ru/60607
30. Освітлення робочого місця. URL: https://interalighting.ru/blog/2518_rabochee-mesto
31. Як правильно зробити освітлення робочої зони біля комп'ютера. URL: https://1posvetu.ru/istochniki-sveta/osveshhenie-rabochego-mesta-za-kompyuterom.html
32. Охорона праці в офісі. Вимоги до робочого місця офісного працівника. URL: https://gc.ua/uk/oxorona-praci-v-ofisi-vimogi-do-robochogo-miscya-ofisnogo-pracivnika/
33. Інструкція щодо заходів пожежної безпеки. URL: https://katalog-ukr.ru/2018/05/01/instrukciya-o-merah-pozharnoj-bezopasnosti-pri-polzovanii-kompyuterom/
34. Характеристика небезпечних для людини факторів пожежі". URL: https://nuczu.edu.ua/images/topmenu/kafedry/kafedra-viiskovoi-pidhotovky/distant-content/Zanytie_2.pdf
35. Основні причини виникнення пожежі в офісі. URL: http://stroyinzproekt.ru/information/info_page/995/
36. Пожежна безпека під час роботи з комп'ютером. URL: https://bstudy.net/989733/bzhd/pozharnaya_bezopasnost_rabote_kompyuterom
37. Основні причини виникнення пожеж на підприємстві. URL: https://ts.kiev.ua/osnovni-prychyny-vynyknennya-pozhezh-na-pidpryemstvi/