

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики

(інститут)

Факультет інформаційних технологій

(факультет)

Кафедра інформаційних технологій та комп'ютерної інженерії

(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента Купця Євгенія Сергійовича

(ПІБ)

академічної групи 123М-22-1

(шифр)

спеціальності 123 Комп'ютерна інженерія

(код і назва спеціальності)

за освітньо-професійною програмою «Комп'ютерна інженерія»

(офіційна назва)

на тему «Обґрунтування структури комплексу IoT для підвищення безпеки корпоративної мережі малого підприємства «Агентства розвитку Дніпра»

(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц.Шедловський І.А.			
розділів:				
теоретичний розділ	доц.Шедловський І.А.			
синтез системи	доц.Бешта Д.О.			
розроблення програмного забезпечення	ас.Панферова Я.В.			
Рецензент				
Нормоконтролер	доц. Шедловська Я.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії

(повна назва)

Гнатушенко В.В.

(підпис)

(прізвище, ініціали)

"06" вересня 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра
(бакалавра, спеціаліста, магістра)

студенту Купця Є.С. академічної групи 123М-22-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)

на тему «Обґрунтування структури комплексу IoT для підвищення безпеки корпоративної мережі малого підприємства «Агентства розвитку Дніпра»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.2023р. №1227-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів практик, інших науково-технічних джерел сформулювати наукове завдання, конкретизувати предмет та мету досліджень	10.10.2023
Теоретичний	Обґрунтувати теоретичну базу розв'язання наукового завдання, якому присвячено роботу	25.10.2023
Синтез системи	Розробка комп'ютерної системи	15.11.2023
Розроблення програмного забезпечення	Розробка програмного забезпечення	29.11.2023
Експериментальний розділ	Проведення і обробка результатів експериментів	06.12.2023

Завдання видано

(підпис керівника)

доц. Шедловський І.А.

(прізвище, ініціали)

Дата видачі

06.09.2023 р.

Дата подання до екзаменаційної комісії 10.12.2023

Прийнято до виконання

(підпис студента)

Купець Є.С.

(прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка 99 с., 56 рис., 5 табл., 1 дод., 32 джерел
КОРПОРАТИВНА МЕРЕЖА, КОМП'ЮТЕРНА МЕРЕЖА, КОМПЛЕКС ІОТ,
СИСТЕМА МОНІТОРІНГУ, БЕЗПЕКА

Об'єкт дослідження: Система моніторингу, у данному випадку комплекс ІоТ, який буде інтегрований у корпоративну мережу малого підприємства «Агентство розвитку Дніпра».

Мета роботи: Обрати для корпоративної мережі систему моніторингу, яка буде задовольняти всі потреби невеликого підприємства.

Виявити всі можливі протиріччя, які можуть виникнути під час запровадження системи моніторингу у комп'ютерну мережу підприємства і запропонувати їх вирішення.

Проаналізувати ефективність кожного обраного девайсу, який буде підключений до системи моніторингу.

Розробити програмне забезпечення, яке буде керувати системою моніторингу.

Оцінити швидкість реагування пристроїв, які входять до системи моніторингу, на виникнення певних загроз, проти яких ці пристрої були запроваджені.

Практичні результати: реалізація комплексу ІоТ у корпоративній мережі малого підприємства з урахуванням всіх можливих протиріч, які можуть виникнути під час інтеграції системи моніторингу.

Правильна оцінка запровадженого комплексу ІоТ. Зробити аналіз, щодо швидкості реагування на певну кількість загроз, протия яких запроваджується система моніторингу ІоТ.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів	7
Вступ	8
1 Стан питання і завдання дослідження	10
1.1 Загальна характеристика об'єкта дослідження	10
1.2 Корпоративна мережа підприємства	11
1.3 Критичний аналіз і класифікація напрямків досліджень у сфері моніторингу інформації	15
1.4 Мета роботи	23
1.5 Визначення можливих ризиків при запровадженні технології Інтернету речей	23
1.6 Ідеї щодо вирішення зазначених ризиків	24
1.7 Висновки	25
2 Теоретична частина	26
2.1 Обґрунтування вибору платформи (хабів) для системи моніторингу ..	26
2.2 Обґрунтування вибору пристроїв у комплекс IoT	27
2.2.1 Обґрунтування вибору зв'язок IoT пристроїв, які будуть знаходитись у кожному відділі підприємства	28
2.2.1.1 Визначення можливих проблем з системою пожежогасіння та ідеї, щодо їх вирішення	31
2.2.2 Обґрунтування вибору пристроїв до відділу по роботі з клієнтом	33
2.2.3 Обґрунтування вибору пристроїв до відділів туризму, індустріального розвитку і грантових програм	34
2.2.4 Обґрунтування вибору пристроїв до відділу технічної підтримки	36
2.2.5 Обґрунтування вибору пристроїв до серверної	37
2.2.6 Обґрунтування вибору пристроїв до юридичного відділу і бухгалтерії	38

2.2.7	Обґрунтування вибору пристроїв до кабінету директора	39
2.2.8	Обґрунтування вибору пристроїв до конференц залу і приміщення для наради	39
2.2.9	Обґрунтування вибору пристроїв до складу	39
2.2.10	Визначення можливих проблем з комплексом IoT та ідеї, щодо їх вирішення	40
2.3	Висновки	40
3	Синтез системи моніторингу підприємства	41
3.1	Функціональна схема системи моніторингу IoT підприємства «Агентство розвитку Дніпра»	41
3.2	Структурна схема системи моніторингу IoT підприємства «Агентство розвитку Дніпра»	42
3.3	Основні вимоги до системи керування комплексу IoT	56
3.4	Опис функцій і кількості IoT пристроїв у відділах підприємства «Агентство розвитку Дніпра»	56
3.5	Характеристика пристроїв і кабелів системи моніторингу IoT	59
3.6	Висновки	61
4	Розроблення програмного забезпечення	62
4.1	Призначення і сфера застосування програмного забезпечення	62
4.2	Обґрунтування технічних характеристик програм	62
4.2.1	Постановка завдання на розробку програми	62
4.2.2	Опис алгоритму функціонування програми	62
4.2.3	Опис і обґрунтування вибору методу організації вхідних та вихідних даних	65
4.2.4	Опис і обґрунтування вибору складу технічних і програмних засобів	65
4.3	Опис розробленої програми	66
4.3.1	Загальні відомості	66
4.3.2	Функціональне призначення	66
4.3.3	Опис логічної структури програми	66

4.3.4	Використовувані технічні засоби	70
4.3.5	Виклик і завантаження	70
4.4	Очікувані техніко-економічні показники	71
4.5	Висновки	71
5	Експериментальний розділ	72
5.1	Мета і умови експерименту	72
5.2	Опис методик експерименту кожних зв'язок IoT пристроїв	73
5.2.1	Система пожежогасіння	73
5.2.2	Датчик руху, камера відеоспостереження і сирена	74
5.2.3	Датчик вуглекислого газу і стельовий вентилятор	74
5.2.4	RFID зчитувач, RFID картка і розумний замок	75
5.2.5	Кондиціонер	76
5.2.6	Датчик температури і стельовий вентилятор	77
5.2.7	Датчик вологості і осушувач повітря	78
5.3	Тестування системи моніторингу IoT	78
5.4	Аналіз експериментальних досліджень у порівнянні з теоретичними цілями	84
5.5	Висновки	87
	Висновки	89
	Перелік посилань	90
	Додаток А	94

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IoT – Internet of Thing (Інтернет речей);

PC – Personal Computer (Персональний Комп'ютер);

IP-адреса – унікальний ідентифікатор комп'ютера або іншого пристрою локальної мережі;

PT – Packet Tracer;

LAN – Local Area Network (Локальна Мережа);

SCADA – Supervisory Control and Data Acquisition (Система моніторинга і управління процесами);

MLA – Machine Learning Algorithms (Алгоритми машинного навчання);

ШІ – Штучний інтелект;

СМ – Система моніторингу;

ПЗ – Програмне забезпечення;

АЗ – Апаратне забезпечення;

PPTP – Point-to-Point Tunneling Protocol (Тунельний Протокол Типу Точка-Точка);

AES – Advanced Encryption Standard (Розширений стандарт шифрування);

Wi-Fi – Wireless Fidelity (Бездротова Мережа);

ТП – Технологічні Процеси;

АСК – Автоматизовані Системи Керування;

НМІ – Human Machine Interface;

БД – База Даних;

NFC – Near Field Communication (Зв'язок Ближнього Радіусу Дії);

АСКОЕ – Автоматизована Система Комерційного Обліку Електроенергії;

WAN – Wide Area Network (глобальна мережа);

RFID – Radio Frequency Identification (радіочастотна ідентифікація);

ВСТУП

Очевидно, що аварійні ситуації на підприємстві можуть виникнути у більшості випадках через порушення робочим персоналом правил безпеки при перебуванні на робочому місці, але, завжди залишається вірогідність того, що в комп'ютерній мережі підприємства може виявитись дефект будь-якого приладу, який може стати причиною виникнення певних труднощів під час одночасного використання декількох електронних пристроїв.

Можна зменшити відсоток виникнення аварійних ситуацій через недбале ставлення до правил безпеки наполегливим нагадуванням про їх повторне прочитання, проте маленьким підприємствам занадто затратно зменшувати відсоток виникнення аварійних ситуацій через помилку в роботі неякісного обладнання. Великі підприємства можуть дозволити собі тримати відсоток виникнення обох видів аварійних ситуацій якомога низьким, а для маленьких підприємств нехтування можливостями швидкого вирішення наслідків, які можуть виникнути під час аварійної ситуації, чи запобігти ситуації, що передуює аварії, може значно збільшити можливість виникнення нещасних випадків на підприємстві.

Під час розробки корпоративної мережі підприємства «Агентство розвитку Дніпра» був сформований розділ «Вимоги до безпеки» у технічних вимогах до комп'ютерної системи в цілому. Дотримучись поставлених вимог можна зменшити відсоток виникнення аварійних ситуацій, але це підприємство достатню кількість грошей, які можна вкласти у новітні комплексні системи моніторингу, що значно б допомогло знизити ризик появи аварійних ситуацій. Тому і виникає потреба у малих підприємств знайти оптимальний варіант, який би влаштовував їх одночасно за витраченими коштами на впровадження певної системи моніторингу та за її ефективністю.

Існує кілька сучасних систем, які допоможуть вирішити поставлені задачі, такі як «Система моніторингу і управління процесами» (SCADA), Інтернет речей (IoT) і використання алгоритмів машинного навчання (MLA).

Щоб мати можливість швидко реагувати на небезпечні ситуації і максимально зменшити ймовірність появи руйнівних наслідків для підприємства від аварійних ситуацій потрібно обрати відповідну систему моніторингу з урахуванням всіх особливостей маленького підприємства «Агентство розвитку Дніпра».

Мета і завдання дослідження

Обрати систему моніторингу для невеликого підприємства «Агентство розвитку Дніпра», яка буде підходити по всім важливим критеріям.

Оцінити всі можливості, які запропонує система моніторингу і обрати найважливіші з них для інтеграції у комп'ютерну мережу підприємства.

Розробити програмне забезпечення, завдяки якому відділ технічної підтримки зможе забезпечити просте керування приладами системи моніторингу.

Протестувати розроблену систему моніторингу.

Об'єкт дослідження

Система моніторингу, яка буде інтегрована у підприємство «Агентство розвитку Дніпра».

Предмети дослідження

Елементи, з яких буде складатись комплексна система моніторингу, апаратне забезпечення, через яке буде можливість керувати окремими елементами системи моніторингу і програмне забезпечення, яке буде забезпечувати правильний набір функцій, які будуть виконувати обрані елементи системи моніторингу.

Методи дослідження

Для проведення дослідження буде використовуватись модель корпоративної мережі підприємства «Агентство розвитку Дніпра» у програмі РТ, де буде перевірено швидкість реагування IoT пристроїв на зовнішні загрози. Під час дослідження будуть виявлені всі недоліки запровадженної системи моніторингу.

1 СТАН ПИТАННЯ І ЗАВДАННЯ ДОСЛІДЖЕННЯ

1.1 Загальна характеристика об'єкта дослідження

Всю історію людство прагнуло автоматизувати важку і репетитивну частину праці. Інженери винаходили нові механізми, які могли замінювати людей на різних виробництвах і паралельно з цим зростав не тільки прибуток, який отримував директор підприємства, з-за того, що ці механізми, зазвичай, замінювали цілу групу працівників, яким більше не потрібно було платити зарплатню, а ще й зазначалось зростання аварійних ситуацій, або нещасних випадків на підприємстві. Безсумнівів, не можна у такій ситуації звинувачувати тільки механічні прилади і забувати про малограмотне населення та непрості умови експлуатації цих механізмів тих часів, у порівнянні з сучасними приладами. Однак, зараз правила безпеки на робочому місці змушують повторювати по декілька разів на місяць, але все одно дуже важко застрахувати робітників різних підприємств від несподіванної несправності якогось приладу, яка може спричинити стрімке збільшення ймовірності виникнення ситуації, що передуює аварію на підприємстві. Допомогти персоналу менше хвилюватись на робочому місці через постійно присутню можливість появи аварійної ситуації може допомогти система моніторингу.

Поява технології «Інтернету речей» популяризувало запровадження систем моніторингу на підприємство, оскільки відбулась технічна революція даної технології, яка полягає у можливості передачі інформації по інтернету від різних сенсорів, які підключені до однієї глобальної мережі. Отримати користь від запровадження такої системи моніторингу для великих підприємств не складе труднощів, оскільки сьогодні така технологія використовується не тільки великими підприємствами, а ще і має попит серед громадян розвинутих країн, яку називають «Розумним будинком».

Але, якщо подивитись на статистику, чомусь більшість (97%) організацій стикаються з труднощами в отриманні цінності з IoT [1]. Безсумнівво, сама по собі система моніторингу після запровадження не може допомогти підприємству, у більшості випадках, згенерувати вагомий прибуток, який повністю б відшкодував

всі витрачені на таку систему кошти. При запровадженні даної технології потрібно грамотно оцінити кожен пристрій, який буде підключений до системи моніторингу, та правильно спрогнозувати користь від місця розташування кожного приладу, який повинен буде при виникненні небезпечної ситуації максимально допомогти в її швидкому вирішенні. Тому, підприємство може отримати у повному обсязі цінність від запровадженої системи моніторингу тільки у тому разі, якщо буде проведена правильна оцінка всіх вразливих елементів самого підприємства. У даному випадку під «вразливими елементами» можна розуміти особливості будівлі, яку арендує підприємство, і в якій знаходиться корпоративна мережа, і саму корпоративну мережу та прилади, які до неї підключені.

1.2 Корпоративна мережа підприємства

Підприємство «Агентство розвитку Дніпра» є посередницькою організацією, яка займається пошуком грантів, розвитком міста, комунікацією з потенційними підрядчиками, підвищує свій прибуток за рахунок посередницької діяльності, а саме з організації процесів будови різних споруд [2].

Підприємство орендує повністю перший поверх у будівлі та дві кімнати другого поверху для корпоративної мережи. Це було зроблено для того, щоб ключові відділи підприємства мали змогу швидко комунікувати один з одним навіть без використання комп'ютерної мережи і, якщо все ж таки потрібно використати комп'ютерну мережу, процес обміну інформації між ключовими відділами проходив також максимально швидко. Підприємству на другому поверсі будівлі необхідно було виділити місце для певного комплексу, з яким би всі інші відділи комунікували менше всього. Оскільки серверну необхідно було розташувати максимально близько до технічного відділу, директор мав бути поруч з конференц залом, а бухгалтерія пов'язана з юридичним відділом, було вирішено розмістити на другому поверсі склад речей та запасних технічних приладів (рисунок 1.1).

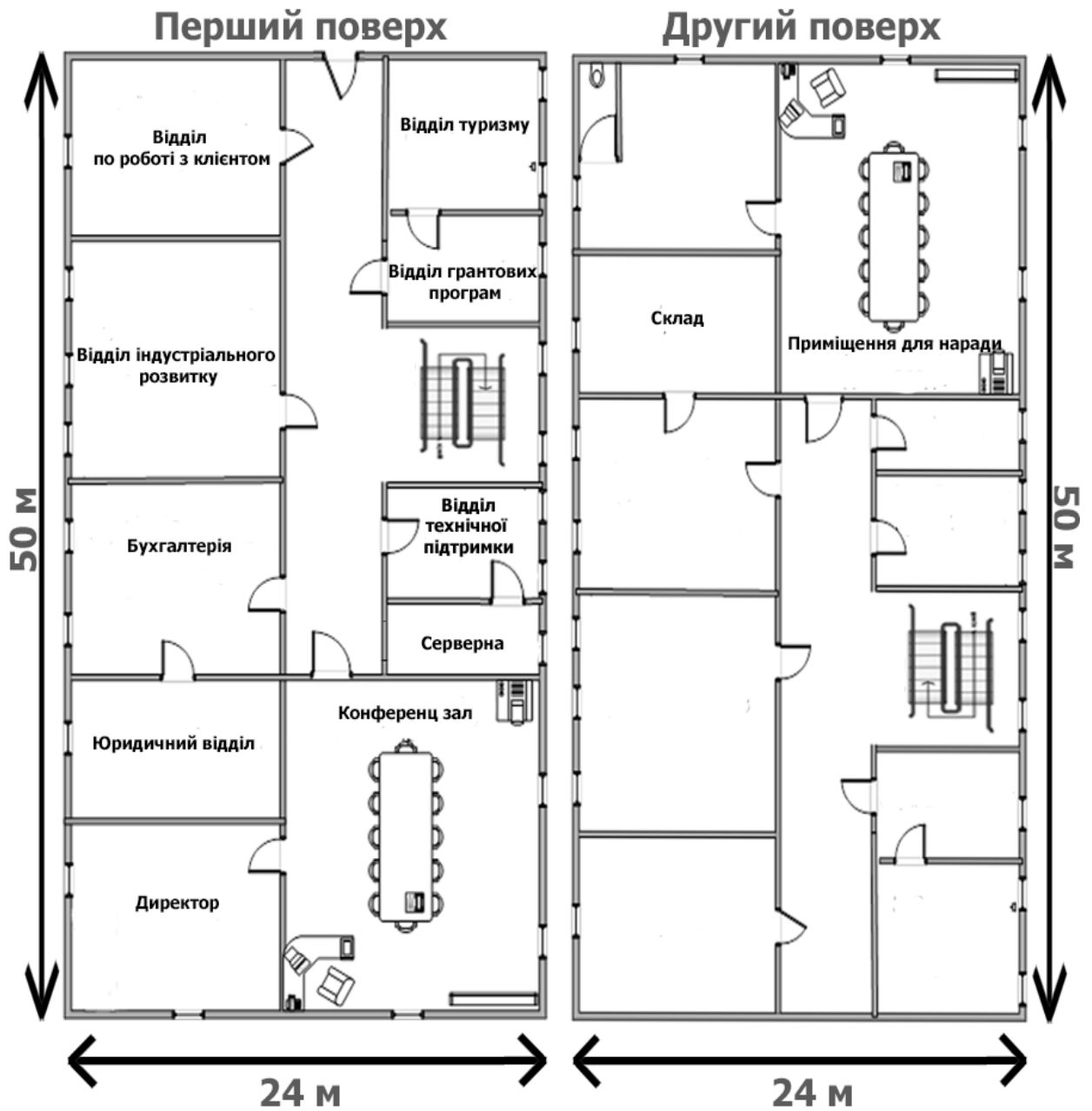
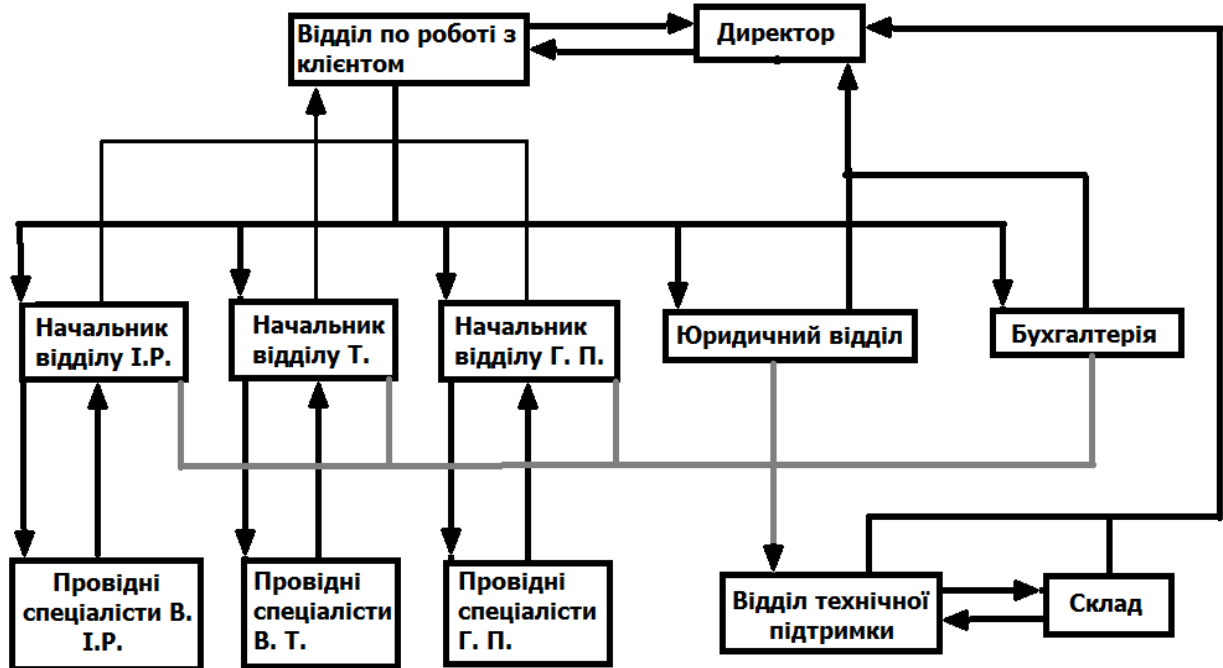


Рисунок 1.1 – План двох поверхів, які використовує підприємство

Функціональна схема допоможе краще зрозуміти всю потребу в комунікації між відділами підприємства, яку задовольняє побудована комп'ютерна мережа (рисунок 1.2).

**Функціональна схема
Комунального підприємства "Агентство розвитку Дніпра" Дніпровської міської ради**



*
В. - Відділ
І.Р. - Індустріального Розвитку
Т. - Туризму
Г. П. - Грантових Програм

Рисунок 1.2 – Функціональна схема

На рисунку 1.3 зображена комп'ютерна мережа підприємства, змодельована у програмі Packet Tracer 8.2.1.

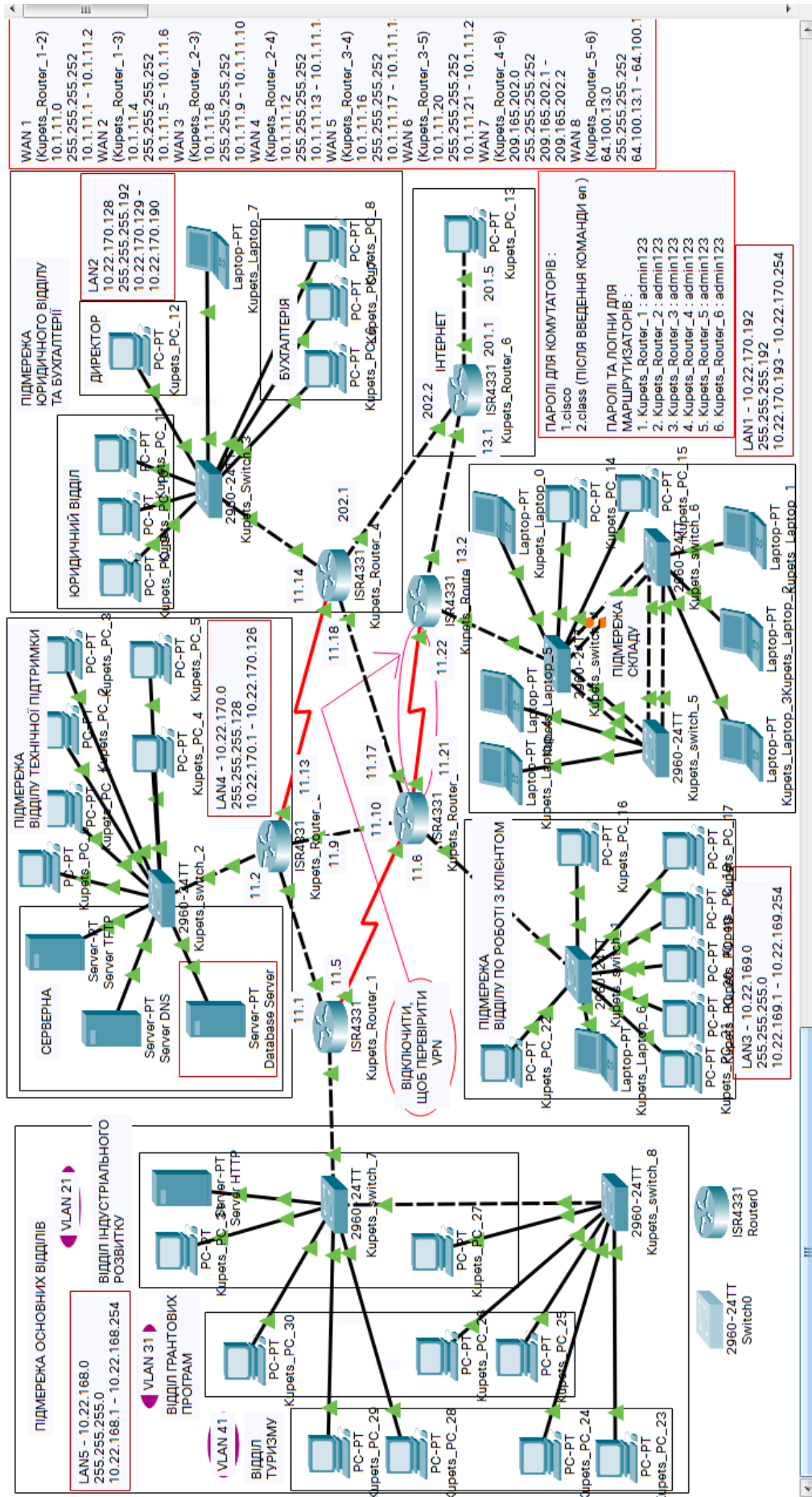


Рисунок 1.3 – Модель комп’ютерної мережі підприємства

Комп'ютерна мережа має 40 підключених до неї РС, чотири сервера, вісім комутаторів і шість маршрутизаторів.

Для інтеграції системи моніторингу у корпоративну мережу не потрібно орендувати більше кімнат другого поверху будівлі. РС, через який можна керувати системою моніторингу буде розміщений у відділі технічної підпримки.

1.3 Критичний аналіз і класифікація напрямків досліджень у сфері моніторингу інформації

Насамперед необхідно звернути увагу на рід діяльності, яка приносить підприємству «Агентство розвитку Дніпра» дохід і зразу стає очевидним той факт, що посередницька діяльність не може забезпечити швидкий розвиток підприємства. Обмеженість коштів, які можна використати на будь-який проект, і є основним фактором, який заважає використати універсальні рішення тих чи інших систем та змусить ретельно визначати тільки корисні елементи певної системи моніторингу для інтеграції їх з комп'ютерною мережею підприємства.

Критичний аналіз почнеться з визначення системи моніторингу враховуючи більшість індивідуальних особливостей малого підприємства «Агентство розвитку Дніпра», а саме:

- дефіцит висококваліфікованого персоналу;
- обмеженість виділених коштів, на впровадження системи моніторингу;
- неможливість масштабного розширення комп'ютерної мережи підприємства;
- сумісність з недуже потужним апаратним забезпеченням певних відділів.

Із сучасних систем моніторингу були обрані три системи, які мають попит на нашому ринку і зарекомендували себе, як якісний варіант для збільшення рівня безпеки на підприємстві:

- система моніторинга і управління процесами (SCADA),
- система Інтернету речей (IoT);
- система алгоритмів машинного навчання (MLA).

Краще всього буде почати опис кожної СМ з тієї, яка менше всього підходить для запровадження у невелике підприємство, тобто почати з системи алгоритмів машинного навчання (MLA).

Машинне навчання (ML) — це галузь штучного інтелекту (ШІ), яка зосереджена на використанні даних і алгоритмів для імітації способу навчання людей, поступово підвищуючи точність з часом. Машинне навчання передбачає передачу великої кількості даних у комп'ютерні алгоритми, щоб вони могли навчитися визначати шаблони та зв'язки в цьому наборі даних. Потім алгоритми починають робити власні прогнози або приймати рішення на основі свого аналізу [3].

Система алгоритмів машинного навчання не підходить для інтеграції у підприємство «Агентство розвитку Дніпра» з трьох причин.

Перш за все, для впровадження цієї системи підприємству необхідно буде залучити кваліфікований персонал, який має досвід у роботі з алгоритмами машинного навчання. Потрібні, як мінімум, декілька провідних спеціалістів і аналітиків для запровадження невеликої системи (MLA).

Наступною причиною є велика сума грошей, яку потрібно буде виділити на інтеграцію системи алгоритмів машинного навчання у підприємство. Кошти будуть витрачатись на:

- аналітиків, з якими можна буде проводити консультацію з приводу масштабності даної системи і її потенційних можливостей;
- провідних спеціалістів, які будуть займатись впровадженням цієї системи і навчати персонал відділу технічної підтримки працювати з нею;
- ліцензійне ПЗ, яке знадобиться для кращої взаємодії алгоритмів машинного навчання з АЗ підприємства;
- фреймворки і різні інструменти для роботи з даними.

Можна було додати до списку ще і оновлення АЗ, яке буде швидше працювати з чималою кількістю даних у комп'ютерній мережі, але через те, що переважна більшість відділів використовує комп'ютери та інше АЗ у «офісних» задачах, для підприємства немає необхідності оновлювати у даному разі АЗ.

І остання причина не запроваджувати систему алгоритмів машинного навчання стосується однієї з основних задач, яка виконуються завдяки АЗ і, при цьому, може виконуватись без участі людини – це збереження і аналіз інформації на серверах підприємства. Сервера, на яких реалізована база даних, використовуються лише для організації таблиць з важливою для підприємства інформацією, яка зберігає лише:

- паролі та логіни користувачів корпоративної мережи;
- грантові програми;
- індустріальні проекти;
- звіти від працівників агентства;
- таблицю маршрутизації;
- плани, щодо розвитку туристичної галузі;
- мережеве обладнання, яке включене у корпоративну мережу підприємства;
- мережеве обладнання, яке зберігається на складі;
- укладені договори;
- інформацію, щодо клієнтів агентства [4].

Однією з основних функцій MLA при інтеграції їх з базами даних є сортування у реальному часі тієї інформації, яка стрімко надходить до серверів підприємства. Навіть якщо взяти до уваги таку ситуацію, що у далекій перспективі розвитку підприємства, коли список завдань, які буде виконувати база даних, розшириться, класифікацією та іншими видами аналізу і групуванню даних все ще буде можливо робити вручну провідному спеціалісту з відділу технічної безпеки, оскільки об'єм інформації, яка буде надходити до серверів, не створить великих черг через повільну, у порівнянні з працюючими алгоритмами, обробку даних людиною. Внаслідок того, що не дозволяється масштабно розширити комп'ютерну мережу, додавши нових відділів, рід діяльності яких унеможливить власноруч провідному спеціалісту з відділу технічної безпеки заповнювати таблиці баз даних і напряду змусить почати використовувати функції системи алгоритмів машинного

навчання для аналізу та групування інформації у базах даних, впровадження великої і складної системи MLA недоцільно.

В цілому, система алгоритмів машинного навчання не підходить для керування системою безпеки невеликого підприємства «Агентство розвитку Дніпра», через ігнорування всіх індивідуальних особливостей даного підприємства, окрім сумісності зі слабким АЗ, але і ця особливість могла бути проігнорована, якщо б базою даних зручніше було керувати через алгоритми.

Наступні дві системи моніторингу вже не можна назвати складними, оскільки для запровадження цих систем не потрібно залучати висококваліфікований персонал та витратити значну суму грошей на обладнання для їх працездатності у порівнянні з системою MLA. Якщо поверхнево прочитати інформацію про системи моніторингу і управління процесами (SCADA) і Інтернету речей (IoT) може скластися враження, що обидві системи ідентичні і відрізняються тільки можливістю другою відправляти дані сенсорів через інтернет мережу, але такий опис невірне відображає процес збору і обробки даних з сенсорів обох систем, і спочатку необхідно розібратися у особливостях, які відрізняють систему моніторингу «SCADA» від IoT та чітко визначитись у тому, який комплекс сенсорів краще підійде для інтеграції у підприємство «Агентство розвитку Дніпра».

SCADA (Supervisory Control and Data Acquisition) є програмним пакетом, призначеним для виконання функцій збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління в реальному часі. ПЗ цього класу може бути частиною АСУ ТП, АСКОЕ, системи екологічного моніторингу, наукового експерименту, автоматизації будівлі тощо. SCADA-системи використовують у всіх галузях діяльності, де потрібно забезпечувати операторський контроль над технологічними процесами. В основному, СКАДА є частиною АСУ, диспетчерської системи, що відповідає за моніторинг технологічних параметрів та віддалене керування обладнанням. Основні функції hmi scada:

- Збір даних від апаратури процесу та дистанційне керування обладнанням. Ведення БД реального часу;

- Створення графічного інтерфейсу для моніторингу та управління процесом оператором. Вилучення інформації з БД та подання оператору у зручному вигляді для аналізу;
- Автоматизація виконання робочих процесів прийняття рішень оператором;
- Розрахунок вторинних показників ефективності виробництва, статистики перебігу процесу, роботи обладнання тощо;
- Виконання деяких функцій управління (блокування, некритичне регулювання тощо);
- Автоматична генерація тривог та повідомлень;
- Підготовка рапортів, зведення, звітів та іншої експлуатаційної документації;
- Архівування історії, тривог та дій оператора;
- Розмежування прав доступу за категоріями користувачів. Забезпечення безпеки та контролю над діями оператора;
- Резервування найважливіших складових системи (серверів, мереж, клієнтів);
- Горизонтальний обмін даними із суміжними системами АСУТП та передача даних на верхні рівні управління [5].

SCADA виглядає привабливіше для запровадження у невеликі підприємства ніж алгоритми машинного навчання. Бабільше, система моніторингу і управління процесами без додавання нових функцій коду може зафіксувати кожну дію провідного спеціаліста, який керує певними сенсорами, що у свою чергу може допомогти визначити точну причину виникнення аварійної ситуації навіть за умови появи різних помилок при корегуванні або тестуванні приладів системи моніторингу. До плюсів цієї системи можна додати ще достатню кількість готових рішень ПЗ, як безкоштовних, так і тих, що можуть запропонувати більше можливостей за свою ціну, враховуючи можливість архіву історії користування приладів, не потребують величезних витрат, в порівнянні з системою MLA, та інші,

проте підприємству «Агентство розвитку Дніпра» ця система моніторингу не підійде.

Головна причина відмови від запровадження SCADA полягає у тому, що вже виходячи з опису даної системи моніторингу стає зрозумілим для яких підприємств переважно розроблялась система моніторингу і управління процесами, а саме для підприємств, які використовують маніпулятори чи інші види контролерів задля автоматизації циклічних процесів, щоб виключити людину з важкої або монотонної діяльності на підприємстві. З опису вище стає очевидним, що цією системою можна користуватись також на підприємствах, в яких не застосовуються різноманітні контролери та всю однотипну роботу виконує персонал, як і зазначалось під час опису SCADA у прикладах різних сфер діяльності, де може бути використано програмне забезпечення системи моніторингу, однак практично усі функції системи моніторингу і управління процесами прямо чи опосередковано зроблені для користування у тій системі, в якій неможливо не користуватись різноманітними контролерами.

Саме це було однією з причин того, чому потрібно відмовитись від запровадження системи MLA на підприємство, але, при цьому, необхідно зауважити суттєвий фактор, який би вплинув на вирішення впровадження SCADA на підприємство «Агентство розвитку Дніпра» – це ситуація, при якій неможливо обрати технологію Інтернету речей, як систему моніторингу. Враховуючи цей фактор, при конкуренції з системою алгоритмів машинного навчання – SCADA без винятку залишається єдиною системою, яку доцільно було б впровадити у маленьке підприємство, як систему безпеки, втім технологія IoT вже зараз має окрему сферу використання під назвою «Розумний будинок», яка своїм стрімким розвитком змусила розробників цієї системи полегшити процес впровадження даної технології для масового споживача і підняти на новий рівень ефективність приладів системи безпеки.

Інтернет речей (Internet of things, або скорочено IoT) — мережа апаратів різного роду та призначення, які для спрощення узагальнюють словом "речі". Інтернет речей працює завдяки датчикам, програмному забезпеченню та іншим

технологіям, що дозволяє пристроям обмінюватися даними з іншими пристроями та системами, подібно до того, як комп'ютери зв'язуються через Всесвітню павутину. В ролі "речей" можуть бути різні об'єкти: від складної промислової техніки до побутових гаджетів розміром із таблетку. Інтернет речей простими словами — це всесвітня мережа для "розумної" електроніки. Об'єднання об'єктів за допомогою датчиків і сенсорів створює для них щось подібне до цифрового інтелекту, здатного передавати різні корисні дані в реальному часі самостійно, не вимагаючи постійного контролю з боку людей. Цьому сприяє поширення бездротових інтернет-мереж та розробка дешевих мікропроцесорів [6].

Різниця між системами моніторингу SCADA та IoT полягає у тому, що друга система моніторингу дає більше можливостей щодо захисту підприємства від виникнення небезпечних ситуацій, охоплюючи при цьому під час моніторингу більше пристроїв, ніж система моніторингу SCADA, яка зосереджена на моніторингу та керуванні контролерами і іншими пристроями, якими користуються на промислових підприємствах, а підприємство «Агентство розвитку Дніпра» без сумніву не можна віднести до «промислових підприємств»

Отже, проаналізувавши всі мінуси і плюси трьох обраних систем моніторингу, було обрано єдиний комплекс, який може враховувати всі індивідуальні особливості обраного невеликого підприємства і, паралельно з цим, бути органічною частиною комп'ютерній мережі – це система IoT.

Ознайомлюючись з різними джерелами, які надають інформацію про перше застосування технології IoT (здебільшого це друга половина двадцятого сторіччя), може скластись помилкове враження щодо актуальності системи Інтернету речей. Проте, наступна статистика «Кількість пристроїв, підключених до Інтернету речей (IoT), у всьому світі з 2019 по 2023 рік, з прогнозами з 2022 по 2030 рік» [7] може повністю розвіяти всі сумніви щодо неактуальності технології IoT. Зробивши аналіз цієї статистики можна сформулювати тільки позитивні висновки по відношенню до системи IoT, а саме:

- з 2023 року по 2030 рік кількість IoT пристроїв збільшиться у два рази (з п'ятнадцяти до тридцяти мільярдів);

- технологія Інтернету речей є актуальною і сучасною системою моніторингу, яка покриває попит у клієнтів на використання системи безпеки у різних цілях;
- у перспективі буде легше розширити список функцій, які може виконувати система моніторингу IoT, завдяки стрімкому розвитку технології Інтернету речей, додавши нові прилади у мережу;
- з часом недешеві і високоякісні на теперішній час комплекси приладів IoT стануть доступнішими для більшості користувачів цієї технології.

У ході дослідження, інтегруючи комплекс IoT до комп'ютерної мережі підприємства «Агентство розвитку Дніпра», чітким результатом виконаної роботи буде правильний підбір пристроїв для підвищення безпеки невеликого підприємства і їх швидке реагування на ті загрози, проти яких вони були запроваджені. Під час вибору пристроїв, які будуть підключені до системи моніторингу підприємства, потрібно буде чітко розділити ефективні пристрої, які будуть приносити максимальну користь підприємству після їх підключення до комп'ютерної системи підприємства і при цьому мати невелику ціну, від неефективних, вигода від підключення яких буде мінімальною, або взагалі від'ємною.

Про інтеграцію комплексу IoT у корпоративну мережу зазвичай замислюються великі підприємства, які мають достатню кількість грошей для виділення їх на такі потреби. Підприємство «Агентство розвитку Дніпра» не має таких можливостей, тому і новизна даного дослідження буде полягати у правильному підборі пристроїв, які будуть підключені до комп'ютерної мережі підприємства та стануть частиною комплексу IoT, щоб при виникненні аварійних ситуацій обрані пристрої змогли допомогти локалізувати негативні наслідки непередбаченої обставини і швидко її зупинити або взагалі запобігти виникненню небезпечних ситуацій.

1.4 Мета роботи

Мета даного дослідження полягає у тому, що необхідно розробити для підприємства «Агентство розвитку Дніпра» систему моніторингу IoT. Пристрої, з яких буде складатись IoT комплекс, необхідно підібрати таким чином, щоб система моніторингу змогла продемонструвати максимальну ефективність, враховуючи обмеженість коштів, які підприємство може виділити на запровадження системи моніторингу. Важливо обґрунтовувати користь кожного IoT пристрою, який буде вважатись частиною IoT комплексу, щоб уникнути можливості купівлі неефективних пристроїв для системи моніторингу.

Провідним спеціалістам відділу технічної безпеки необхідно буде розробити програмне забезпечення до системи моніторингу IoT, задля забезпечення простого керування IoT пристроями.

Після запровадження комплексу IoT важливо дуже уважно протестувати роботу кожного пристрою системи моніторингу, задля виявлення можливих несправностей.

1.5 Визначення можливих ризиків при запровадженні технології Інтернету речей

Визначаючись з можливими проблемами при запровадженні технології Інтернету речей, потрібно у першу чергу зосередити увагу на тих проблемах, при ігноруванні котрих, підприємство зазнає значних збитків. Аналітики з компанії Argiorit дійшли висновку: IoT схильний приблизно до тих самих ризиків, що і звичайний інтернет:

- вразливість програмного забезпечення;
- незахищені канали зв'язку;
- витік з інформаційних систем;
- шкідливі програми;
- кібератаки [6].

Необхідно правильно зрозуміти кожен ризик, відштовхуючись від особливостей підприємства «Агентство розвитку Дніпра», оскільки тлумачення

загрози, яка надходить від вказаних ризиків, на пряму залежить від типу підприємства, яке хоче запровадити у власну комп'ютерну мережу комплекс IoT.

Правильним рішенням буде почати з 2, 3 і 5 ризиків, через те, що вони пов'язані з недостатнім захистом комп'ютерної мережі підприємства. Загрози для корпоративної мережі переважно будуть надходити з підмережи «Інтернет», яка має вихід до мережі Інтернету.

1 і 4 загроза залежить від зовнішнього впливу на АЗ комп'ютерної мережі з урахуванням того, що підприємству для захисту від хакерських атак буде достатньо вже налаштованого VPN. Тому, у даному разі необхідно обмежити фізичну доступність апаратного забезпечення, від якого залежить працездатність усього комплексу IoT.

1.6 Ідеї щодо вирішення зазначених ризиків

Для того, щоб вирішити 2, 3 і 5 ризики одночасно необхідно проаналізувати інформаційні потоки, логістику яких забезпечують канали зв'язку у корпоративній мережі підприємства і вимкнути той канал зв'язку, з-за якого завжди буде існувати ризик хакерських атак, які надходять з підмережи Інтернет, при тому маючи працюючий VPN канал, між маршрутизаторами Kupets_Router_5 і Kupets_Router_6, який був зроблений у WAN 8 для регулювання трафіка з Інтернет мережі. Тому, канал зв'язку WAN 7 потрібно вимкнути і після цього комп'ютерна мережа підприємства буде захищена від переважної більшості хакерських атак (рисунок 1.4).

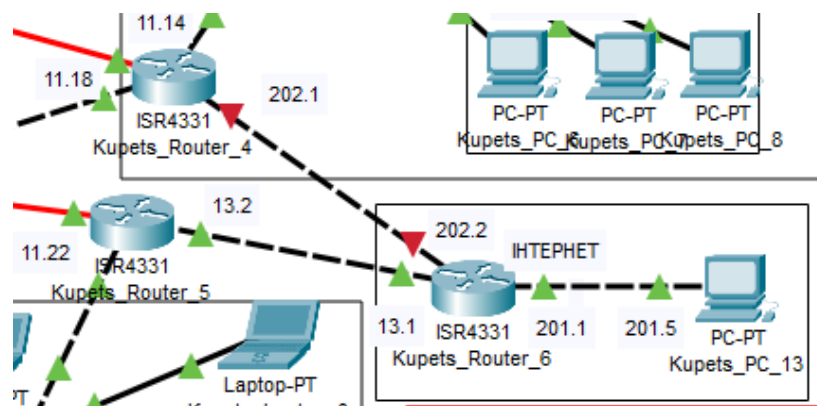


Рисунок 1.4 – Вимкнений канал

Перевірка надійності зв'язку з маршрутизатором Kupets_Router_6 наведена на рисунку 1.5.





Fire	Last Status	Source	Destination	Type	Color	Time
	Successful	Kupets_Router_6	Kupets_Router_4	ICMP		0
	Successful	Kupets_Router_4	Kupets_Router_6	ICMP		0

Рисунок 1.5 – Успішний зв'язок з маршрутизатором Kupets_Router_6 в в обидві сторони

1 і 4 загроза вирішується відключенням всіх USB портів на РС персоналу. Винятком є лише РС персоналу відділу технічної безпеки, оскільки вони проводять моніторинг пристроїв IoT комплексу. Потрібно буде розташувати одноплатний РС, на якому буде працювати ПЗ комплексу IoT, у безпечному місці, щоб виключити можливість навмисного чи випадкового пошкодження маленької плати.

1.7 Висновки

Система моніторингу Інтернету речей допоможе невеликому підприємству «Агентство розвитку Дніпра» швидко реагувати на виникнення аварійних ситуацій у різних відділах підприємства. При запровадженні системи Інтернету речей необхідно відразу вирішити усі можливі ризики, які можуть завадити безперервній роботі IoT комплексу. Обґрунтування вибору певних IoT приладів, які будуть входити до комплексу IoT і водночас приносити користь даному підприємству, та їх правильна організація у різних відділах буде наведена у теоретичному розділі.

2 ТЕОРЕТИЧНА ЧАТСИНА

2.1 Обґрунтування вибору платформи (хабів) для системи моніторингу

Користуючись вже розробленою комп'ютерною мережею можна використати сервер TFTP у якості хабу, який знаходиться у серверній і не виконує важливу роботу у корпоративній мережі підприємства.

Важливо зазначити, що IoT пристрої у системі моніторингу будуть використовувати технологію Wi-Fi для передачі даних, оскільки провідним спеціалістам відділу технічної безпеки буде легше працювати корпоративній мережі, коли всі пристрої між собою сумісні.

До нового серверу IoT (колишній TFTP сервер) можна приєднати всі IoT пристрої, які будуть обрані для системи моніторингу, але, враховуючи статистику, яка приведена у першому розділі, щодо актуальності технології IoT, не можна розглянути і інші варіанти хабів для пристроїв системи моніторингу. Можна згадати дешеві одноплатні ПК, які вже давно представлені на ринку. З популярних рішень можна виділити 2 моделі одноплатних комп'ютерів: Arduino та Raspberry Pi.

Оскільки зазначені два одноплатних комп'ютера мають незначні відмінності (Arduino має програмне забезпечення, яке практично повністю схоже на мову C++, коли Raspberry Pi використовує мову Python) провідним спеціалістам з відділу технічної підтримки, які відповідальні за систему моніторингу, необхідно обрати для себе таку платформу, про яку легше знайти потрібну інформацію, під час удосконалювання системи моніторингу.

Важко об'єктивно оцінити кількість інформації в інтернеті про використання Arduino чи Raspberry Pi в якості платформи для комплексу IoT, в результаті чого було вирішено звернутись до популярної цифрової бібліотеки ACM. Цифрова бібліотека ACM – це платформа для досліджень, відкриттів і мереж [8]. На сайті ACM у пошуковий рядок можна ввести теги, по яким буде знайдено величезну кількість наукових робіт. Саме за цією кількістю буде порівнюватись корисність обраних платформ для підприємства (рисунок 2.1 – 2.2).

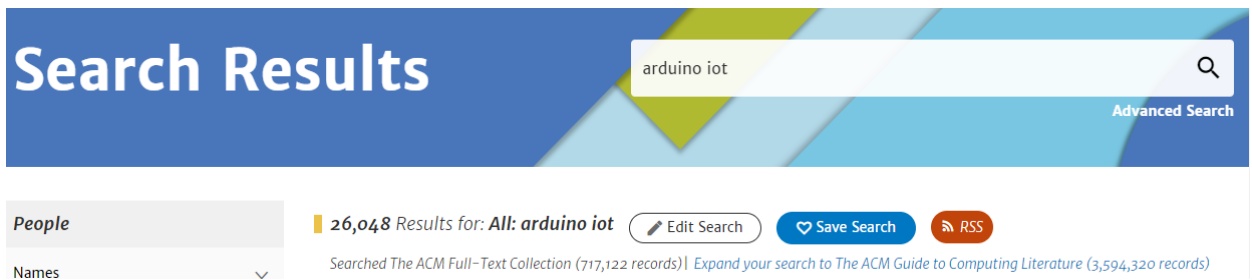


Рисунок 2.1 – Результат пошуку наукових робіт за словами «arduino» та «IoT»

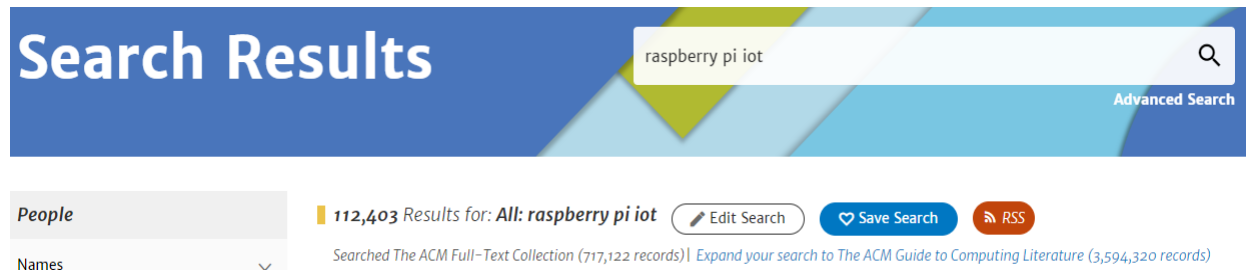


Рисунок 2.2 – Результат пошуку наукових робіт за словами «Raspberry Pi» та «IoT»

Порівнюючи результати пошуків стає очевидним, що Raspberry Pi буде більш актуальною платформою ніж Arduino для використання її в якості хабу для системи моніторингу.

2.2 Обґрунтування вибору пристроїв у комплекс IoT

До кожного відділу необхідно підібрати декілька IoT пристроїв, які будуть залежати один від одного і бути частиною системи моніторингу IoT. Такі зв'язки IoT пристроїв будуть захищати підприємство від різних зовнішніх загроз. Тому, спочатку необхідно обрати ті зв'язки IoT пристроїв, які будуть присутні у кожному відділі підприємства, а потім обґрунтувати вибір пристроїв окремо для кожного відділу.

Від кожної зв'язки IoT пристроїв очікується, що при виникненні певної зовнішньої загрози, відповідна зв'язка IoT пристроїв повинна якомога швидше спрацювати і запобігти руйнівним наслідкам від цієї загрози, задля протидії якій вона запроваджувалась.

2.2.1 Обґрунтування вибору зв'язок IoT пристроїв, які будуть знаходитись у кожному відділі підприємства

У кожному відділі підприємства доцільно буде запровадити лише систему пожежогасіння, оскільки пожежа на підприємстві:

- це найнебезпечніший вид аварійних ситуацій, який за короткий проміжок часу може нанести масштабні збитки для підприємства;
- створює загрозу водночас для життя персоналу та технічному обладнанню;
- при довгому розгоранні пожежа переходить у такий тип аварійних ситуацій, який неможливо вирішити без сторонньої допомоги.

Крім того, дві статистики, які приведені інститутом державного управління та наукових досліджень з цивільного захисту, змушують поставити питання захисту від пожеж на перше місце серед інших можливих загроз (рисунок 2.3 – 2.4).

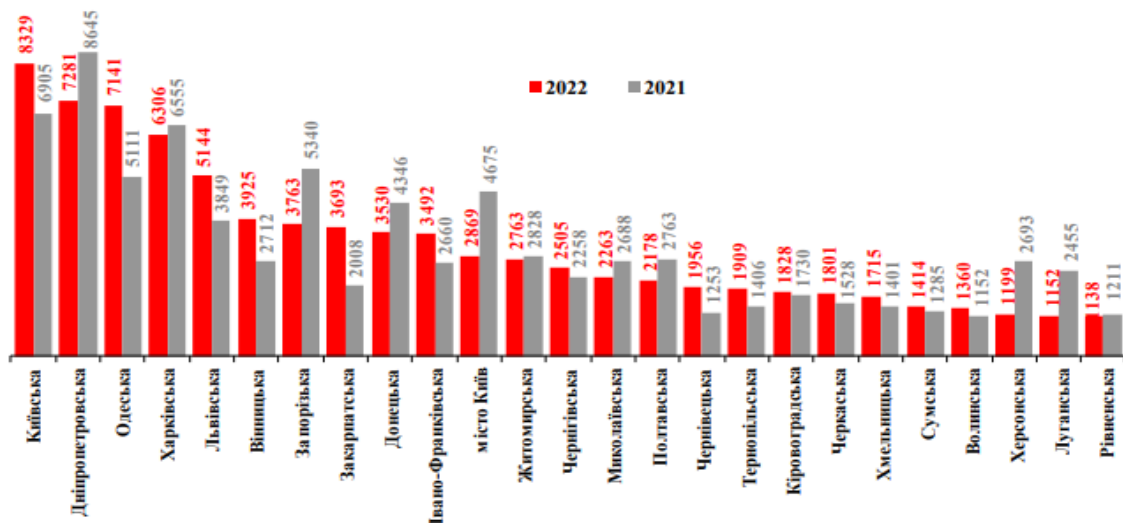


Рисунок 2.3 – Ранжування регіонів України за кількістю пожеж у 2022 році порівняно з 2021 роком [9]

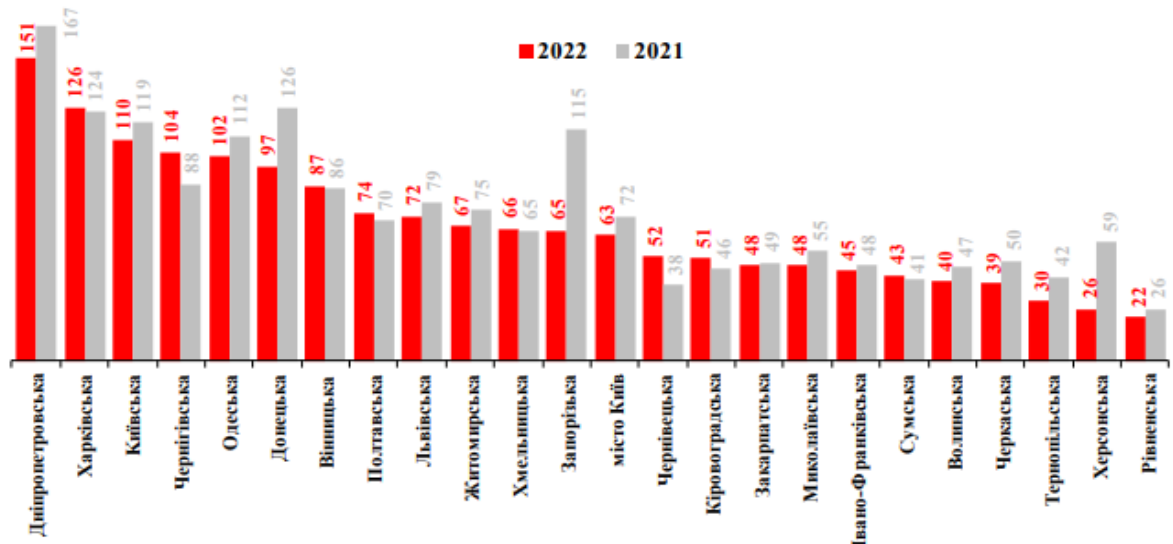


Рисунок 2.4 – Ранжування регіонів України за кількістю загиблих унаслідок пожеж у 2022 році порівняно з 2021 роком [9]

Враховуючи інформацію, яка приведена вище, стає неможливо відвернутись від проблеми виникнення пожежі на підприємстві, тому було прийняте рішення додати до системи моніторингу IoT систему пожежогасіння.

При виборі системи пожежогасіння необхідно опиратися на наступні вимоги до цієї системи:

- працююча система пожежної безпеки мусить завдати якомога менше шкоди працюючій техніці і людям, які знаходяться на перших двох поверхах будівлі підприємства;
- на впровадження даної системи не повинно витратись багато коштів.

На вибір представлені чотири системи пожежогасіння, які можуть бути додані до комплексу IoT:

- система порошкового пожежогасіння;
- система CO₂;
- система пінного пожежогасіння;
- система інергійного газу.

Відразу можна забути про впровадження системи CO₂, оскільки вона становить небезпеку для людей, які можуть не встигнути залишити будівлю, у разі виникнення пожежі.

Головна проблема запровадження системи інергійного газу полягає у тому, що така система є найдорожчою з усіх запропонованих. Великі підприємства можуть дозволити витратити велику кількість грошей на систему пожежогасіння інергійного газу, тому маленьким підприємствам, потрібно буде обирати якусь іншу систему пожежогасіння.

Останні дві запропоновані системи пожежогасіння не можна назвати дорогими, у порівнянні з системами інергійного газу. Пінна система пожежної безпеки може мати у своєму складі воду, що неприпустимо для використання у будівлях з електронними пристроями, і «сухою», яка складається виключно з хімічних речовин, які не мають у своєму складі води та не викликають у більшості випадках загрозу для життя людини, якщо контакт речовиною був нетривалим. Порошкові системи пожежогасіння також можуть нашкодити здоров'ю людини при тривалому контакті, через можливість викликати подразнення легень.

Запропоновані чотири системи пожежогасіння не підходять по різних причинах підприємству «Агентство розвитку Дніпра», тому необхідно знайти якусь іншу речовину, яка б задовольняла всі зазначені умови, на які потрібно звернути увагу при виборі системи пожежної безпеки. Цією речовиною є «суха вода» FK-5-1-12.

FK-5-1-12 була обрана в якості речовини для пожежогасіння через наступні властивості:

- не впливає на працюючу електроніку, не руйнує паперові документи та мистецькі твори. Ці властивості забезпечили застосування FK-5-1-12 в системах пожежної безпеки для серверних приміщень та іншої електроніки, бібліотек, музеїв, архівів [10];

- не застосовується в медицині, ветеринарії, не є товаром подвійного призначення та застосування, не містить токсичні та отруйні речовини та компоненти [10].

Необхідно проконсультуватись з певними спеціалістами перед придбанням FK-5-1-12, які займаються впровадженням систем пожежної безпеки на підприємства. Вони допоможуть у вирішенні наступних питань:

- підібрати оптимальну кількість речовини FK-5-1-12 для майбутньої системи пожежогасіння;
- допомогти побудувати систему зливу і обрати якісне обладнання для майбутньої системи пожежогасіння;
- проконсультуватися про те, як необхідно обслуговувати майбутню запроваджену систему пожежної безпеки.

Якщо ціна за консультацію у міжнародних організацій вийде занадто великою, можна спробувати знайти подібні організації в Україні.

2.2.1.1 Визначення можливих проблем з системою пожежогасіння та ідеї, щодо їх вирішення

Проблема, яка може виникнути ще до запровадження системи пожежогасіння – це достатньо велика сума грошей, яку треба витратити на:

- достатню кількість речовини FK-5-1-12 для системи пожежної безпеки;
- консультацію зі спеціалістами, які допоможуть організувати на підприємстві систему пожежогасіння;
- елементи системи пожежної безпеки (труби, по яким буде текти суха вода, розпилювачі та інше);
- встановлення системи пожежогасіння.

Ціна за систему пожежної безпеки може бути непомірною для невеликих підприємств, внаслідок чого було знайдено дві ідеї, щодо вирішення цієї проблеми.

Оскільки підприємство «Агентство розвитку Дніпра» орендує тільки два поверхи будівлі, можна домовитись з орендодавцем на вигідних для обох сторін умовах про те, що запроваджена система пожежогасіння після закінчення строку оренди двох поверхів будівлі залишається у володіннях орендодавця. Орендодавець, у свою чергу, зобов'язується вкласти певну кількість власних грошей на встановлення системи пожежної безпеки і купівлю всіх важливих елементів цієї системи. Якщо орендодавець відмовиться від запропонованої пропозиції – є можливість домовитись на інших умовах, що під час запровадження системи пожежогасіння, вона може охоплювати не тільки перші два поверхи, а і

іншу частину будівлі, яка не орендується підприємством «Агентство розвитку Дніпра».

Друга ідея полягає у тому, що запроваджувати систему пожежної безпеки потрібно поступово, інтегруючи у систему спочатку ті відділи, які принесуть колосальні для підприємства збитки, у разі виникнення в них пожежі. Оскільки тільки найдешевші датчики вогню коштують від двох тисяч гривень, які потрібно буде встановити у кожному відділі, реалізація такої ідеї, як запровадження системи пожежогасіння поступово, здатна заощадити достатню за розміром суму грошей для підприємства.

Необхідно докласти максимум зусиль, щоб домовитися з орендодавцем на вигідних для обох сторін умовах про запровадження системи пожежної безпеки, тому що така ідея набагато вигідніша для підприємства «Агентство розвитку Дніпра» ніж поступове запровадження системи пожежогасіння, при якому потрібно оперувати тільки власними коштами. У тому випадку, якщо друга ідея буде єдиним можливим рішенням проблеми заощадження грошей, необхідно визначитись з яких відділів потрібно починати запроваджувати систему пожежної безпеки. Підприємство «Агентство розвитку Дніпра» орендує дванадцять кімнат для різних відділів і кабінетів (рисунок 1.1).

Перш за все важливо запровадити систему пожежогасіння до відділу по роботі з клієнтом, тому що для деяких домовленостей з клієнтами, які зберігає персонал даного відділу на власних комп'ютерах, потребується більше часу, щоб обговорити усі нюанси договору. У цей час, вказаний договір не може бути відправлений до бази даних підприємства, оскільки він ще вважається неукладеним. Тому, щоб захистити ті єдині екземпляри договорів, важливо не оминати відділ по роботі з клієнтами у той час при визначенні тих відділів, до яких буде запроваджена система пожежної безпеки у першу чергу.

Наступний відділ, в якому передусім важливо запровадити систему пожежної безпеки – це відділ технічної підтримки і серверна кімната. Відділ технічної підтримки займається переважно технічними приладами, які вийшли з ладу і які треба відремонтувати, отже у разі виникнення пожежі потрібно максимально

знизити ймовірність того, що ця пожежа стане затяжною. Це також стосується серверної кімнати, оскільки інформацію, яка знаходиться на серверах бази даних є можливість відновити практично після будь-якої аварійної ситуації, окрім пожежі.

Остання кімната, яку без винятку слід забезпечити захистом від затяжної пожежі є склад. У зв'язку з тим, що на складі зберігається чимала кількість запасного технічного обладнання спеціально для того, щоб за короткий проміжок часу була можливість у провідних спеціалістів відділу технічної безпеки зайти заміну для пристрою, який вийшов з ладу, необхідно належним чином захистити запасне технічне обладнання.

Продовжити запроваджувати систему пожежогасіння можна лише після того, як підприємство отримає достатній прибуток, який дозволено буде витратити на посилення безпеки від затяжної пожежі.

2.2.2 Обґрунтування вибору пристроїв до відділу по роботі з клієнтом

Очевидно, що при роботі з клієнтами, і укладанням з ними певних договорів, навіть незначні нюанси під час обговорення контроверсійних умов, які зобов'язується виконувати кожна зі сторін підписантів, можуть впливати на результат спілкування з клієнтами, який може бути успішним для різних учасників договору та в небагатьох випадках для обох сторін. Тому, маючи нагоду суттєво підвищити рівень комфорту у відділі по роботі з клієнтами задля зменшення ймовірності появи умов, при яких персоналу відділу буде важче домовитись з клієнтом, можна встановити IoT кондиціонер.

Зрозуміло, що такий пристрій суттєво не впливає на підвищення безпеки підприємства «Агентство розвитку Дніпра», а в деяких випадках можна вважати, що кондиціонер більше зашкодить підприємству, ніж допоможе збільшити рівень безпеки. І все ж таки, після встановлення цього пристрою відділ по роботі з клієнтом отримає не тільки значуще підвищення рівня комфорту для клієнтів і персоналу цього відділу, а ще і зниження вірогідності виходу з ладу технічного обладнання. Постійна висока температура може призвести до незворотного пошкодження вашого пристрою [11]. Враховуючи той факт, що у відділі по роботі

з клієнтом знаходиться найбільша кількість ПК, які у увімкненому стані також будуть впливати на підйом температури у відділі, що в свою чергу тільки прискорить процес деградації електронних приладів, не можна стверджувати, що підприємство отримає тільки негативні наслідки від встановлення IoT кондиціонеру. Тому встановлення IoT кондиціонеру у відділ по роботі з клієнтом більшою мірою допоможе підприємству у тривалій перспективі. Основна характеристика, на яку треба звернути увагу під час вибору кондиціонеру – це підключення до мережі Wi-Fi. Для відділу по роботі з клієнтом потрібно обрати недорогу модель IoT кондиціонеру.

У відділ по роботі з клієнтом буде встановлені чотири IoT пристрою, які необхідно запровадити у систему пожежогасіння:

- датчик вогню;
- спринклер;
- трап для зливу води;
- сигналізація.

Останнє, що необхідно встановити до відділу по роботі з клієнтом з IoT пристроїв для підвищення безпеки – це камеру відеоспостереження, датчик руху і сирену. Враховуючи той фактор, що на комп'ютерах персоналу цього відділу зберігаються договори, які ще не можна відправити до бази даних, важливо захистити ще непідписані договори від спроб заволодіння ними третіми особами. Оскільки корпоративна мережа підприємства «Агентство розвитку Дніпра» захищена від хакерських атак, камери відеоспостереження допоможе ідентифікувати всіх осіб, які знаходились у відділі по роботі з клієнтом після закінчення робочого дня.

2.2.3 Обґрунтування вибору пристроїв до відділів туризму, індустріального розвитку і грантових програм

У зв'язку з тим фактом, що персонал наведених трьох відділів займається однаковою роботою (опрацюванням укладених відділом по роботі з клієнтом

договорів), наступні зазначені IoT пристрої будуть запроваджені до кожного з цих трьох відділів:

- комплекс IoT пристроїв для системи пожежогасіння (датчик вогню, спринклер, трап для зливу води);
- камера відеоспостереження;
- сигналізація;
- датчик руху;
- датчик температури;
- стельовий вентилятор.

Персонал відділів туризму, індустріального розвитку і грантових програм займається реалізацією умов, які були зазначені у підписаних договорах між клієнтом і відділом по роботі з клієнтом, тому камери відеоспостереження допоможуть забезпечити належний рівень захисту від несанкціонованого зовнішнього впливу третіх осіб на процес роботи, оскільки запис з камер залишається у базі даних підприємства довгий проміжок часу, що дає можливість встановити всіх осіб, які знаходились у цих відділах під час робочого дня. Також, сигналізація запрограмована на спрацювання під час виникнення пожежі навіть, якщо пожежа знаходиться не в цих відділах.

Проблема погано провітрюваних робочих місць може зашкодити як працівникам так і технічному обладнанню. У персоналу підприємства, який працює у відділі з поганою вентиляцією повітря може з'явитись запаморочення і знизитись продуктивність на робочому місці. Оскільки у погано провітрюваних робочих місцях завжди вища температура повітря, ніж у приміщеннях з нормальною вентиляцією повітря, технічне обладнання буде працювати з підвищеним ризиком перегріву, що, у свою чергу, підійме ризик виникнення аварійних ситуацій. Тому, щоб прискорити процес вентиляції повітря у відділах необхідно запровадити IoT стельовий вентилятор, який буде спрацьовувати при підвищенні температури у відділі.

Потрібно зазначити, що підприємство «Агентство розвитку Дніпра» не має можливості запровадити у кожний відділ власний кондиціонер для регулювання

температури, оскільки тільки для відділу по роботі з клієнтом кондиціонер був необхідним не тільки для вирішення задач, які пов'язані з проблемою захисту комплектуючих ПК від високих температур, внаслідок цього для підприємства не вигідно вирішувати лише одну проблему підйому температури у інших відділах за рахунок купівлі кондиціонеру і необхідно знайти дешевший спосіб вирішити зазначену проблему. Альтернатива встановлення кондиціонеру у кожний відділ підприємства, окрім відділу по роботі з клієнтом, буде купівля датчику температури і встановлення IoT стельового вентилятору.

Може виникнути питання, щодо ефективності такої дешевшої альтернативи для підприємства, тому що очевидно, що працюючий вентилятор не зможе так швидко знижувати температуру у відділі, як це робить кондиціонер. Це дійсно так, але стельовий вентилятор, при високій температурі повітря, допоможе швидше вивести гаряче повітря з кімнати відділу, оскільки затхле повітря завжди підіймається наверх.

Існує можливість запровадити ще IoT вікна для того, щоб при наявності критичної температури у певному відділі, разом з початком роботи стельового вентилятору, для скорішого виведення гарячого повітря, автоматично відкривалось IoT вікно. Але, заміна звичайних вікон на IoT вікна створить для підприємства дві проблеми, які змусять відмовитись від цієї ідеї:

- взимку, коли температура на вулиці буде дуже низькою, або коли іде дощ, автоматичне відкривання IoT вікон буде зайвим;
- для підприємства «Агентство розвитку Дніпра» сума грошей, яку необхідно витратити на заміну звичайних вікон, та на купівлю IoT вікон у кількості більше десяти штук, достатньо велика (рисунок 1.1), щоб витратити її на вирішення такої проблеми, як автоматизація процесу відкриття вікон.

2.2.4 Обґрунтування вибору пристроїв до відділу технічної підтримки

Відділ технічної підтримки не тільки час від часу перевіряє працюючі пристрої, які відносяться до комп'ютерної мережі на несправність, а ще і допомагає

іншим відділам з ремонтом пристроїв, які вийшли з ладу, тому необхідно в достатній мірі захистити відремонтовані пристрої.

Окрім запровадження чотирьох основних IoT пристроїв для системи пожежогасіння, а саме датчик вогню, спринклер, трап для зливу води і сигналізацію, необхідно запровадити IoT стельовий вентилятор і датчик температури, оскільки висока температура повітря негативно впливає на процес ремонту пошкоджених пристроїв. Провідні спеціалісти будуть швидше втомлюватись і менш зосереджено ремонтувати пристрої.

Крім того, потрібно зауважити, що підвищена вологість у приміщенні також може негативно вплинути, як на процес ремонту електронних пристроїв, так і на звичайні електронні прилади, тому додатково буде запроваджений датчик, який вимірює вологість у приміщенні і IoT осушувач повітря, який унеможливить появи вогкості.

2.2.5 Обґрунтування вибору пристроїв до серверної

На серверах бази даних зберігається практично вся інформація про підприємство «Агентство розвитку Дніпра» і про діяльність всіх відділів, тому необхідно приділити увагу захисту серверної від можливих зовнішніх загроз.

Так як, на серверах агентства встановлені пристрої для збереження інформації типу «HDD», необхідно забезпечити сприятливі умови для працездатності таких серверів. Одні із основних правил приведені нижче :

- задля уникнення проблеми порушення роботи пристрою або ураження електричним струмом, не можна розташовувати сервера у місцях з підвищеною вологістю;
- робоча температура серверної повинна бути від $+5^{\circ}\text{C}$ і до $+55^{\circ}\text{C}$;
- розташовувати сервера не ближче ніж два метри к джерелу тепла, сонячного світла та сильного магнітного поля [12].

Рівень вогкості у серверній буде вимірювати спеціальний датчик, а IoT осушувач повітря допоможе зменшити вологість у приміщенні.

Необхідно запровадити IoT вентилятор і датчик температури, щоб температура у приміщенні була у допустимому діапазоні.

Чотири основні IoT пристрої системи пожежної безпеки допоможуть захистити серверну від спалаху пожежі, а IoT камера відеоспостереження, яка увімкнеться після спрацювання IoT датчика руху, допоможе ідентифікувати зловмисників при спробі вторгнення до серверної.

Для забезпечення достатнього рівня захисту серверної не вистачає тільки додання RFID зчитувача, RFID картки і розумного замка. RFID зчитувач дозволить зайти до серверної тільки директору та провідним спеціалістам відділу технічної підтримки, що виключить можливість для зловмисників легко потрапити до серверної під час робочого дня.

Існує багато дискусій щодо найдійності розумного (електронного) замка, порівнюючи його зі звичайним замком. Електронні замки не усувають ризик того, що хтось вимахне ключ з-під вашого килимка, виламає ваш замок або проникне у ваші двері – але, якщо і коли це станеться, ваш розумний замок зможе негайно оповістити вас про це, незалежно від того де ви знаходитесь [13].

2.2.6 Обґрунтування вибору пристроїв до юридичного відділу і бухгалтерії

Основна робота юридичного відділу і бухгалтерії пов'язана з перевіркою та оформленням певних документів, тому ті IoT пристрої, які необхідно підібрати до системи захисту, будуть запроваджені до кожного з цих двох відділів.

Найважливіші IoT пристрої, які в першу чергу потрібно запровадити до юридичного відділу і бухгалтерії є чотири основні IoT пристрої системи пожежної безпеки, для захисту персоналу і документів.

IoT камера відеоспостереження і датчик руху також допоможуть захистити документи, які залишаються у відділах після закінчення робочого дня.

2.2.7 Обґрунтування вибору пристроїв до кабінету директора

У кабінеті директора буде зберігатись уся необхідна інформація, яка стосується договорів і пропозицій клієнтів. Через це важливо обирати IoT пристрої, які допоможуть максимально захистити конфіденційну інформацію, яка буде знаходитись у кабінеті директора підприємства.

Чотири основні IoT пристрої системи пожежогасіння та RFID зчитувач, RFID картка і розумний замок забезпечать ефективний захист конфіденційної інформації від пожеж та зловмисників під час робочого дня відповідно.

IoT камера відеоспостереження та датчик руху вже після закінчення робочого дня не дозволять зловмисникам отримати доступ до документів і ПК, які знаходяться у кабінеті директора.

2.2.8 Обґрунтування вибору пристроїв до конференц залу і приміщення для наради

Конференц зал і приміщення для наради – це окремі кімнати, які будуть використовуватись персоналом виключно для обговорення важливих питань.

Під час проведення нарад у конференц залі або у приміщенні для наради чотири основні IoT пристрої системи пожежної безпеки зможуть знизити вирогідність для персоналу постраждати від пожеж.

Оскільки приймати участь у нараді може весь персонал підприємства, IoT сенсор вуглекислого газу і стельовий вентилятор допоможуть тримати відсоток вуглекислого газу у повітрі у нормі.

IoT камеру відеоспостереження і датчик руху на відміну від всіх інших відділів не потрібно запроваджувати до конференц залу і приміщенні для наради, тому що у цих приміщеннях не зберігаються важливі речі або інформація, які необхідно захистити після закінчення робочого дня.

2.2.9 Обґрунтування вибору пристроїв до складу

На складі підприємство зберігає резервні пристрої у вимкненому стані для корпоративної мережі, тому немає сенсу запроваджувати IoT стельовий вентилятор

і датчик температури, які допоможуть залишати температуру повітря у безпечному діапазоні для працюючих пристроїв.

IoT камера відеоспостереження, датчик руху необхідні складу для того, щоб мати можливість ідентифікувати усіх зловмисників, які можуть потрапити до цієї кімнати після закінчення робочого дня.

IoT осушувач повітря, датчик для вимірювання рівня вогкості у приміщенні і чотири основні IoT пристрої системи пожежної безпеки будуть встановлені на складі і унеможливлуватимуть виникнення вологого повітря і пожежі відповідно.

RFID зчитувач, RFID картка і розумний замок останнє, що буде запроваджено до IoT комплексу системи моніторингу підприємства.

2.2.10 Визначення можливих проблем з комплексом IoT та ідеї, щодо їх вирішення

Необхідно проінформувати персонал підприємства, щодо правил експлуатації IoT пристроями через те, що при не проведенні інструктажу існує ризик випадкового пошкодження IoT пристроїв персоналом підприємства.

Продовжуючи тему, щодо випадкового пошкодження IoT пристроїв неможливо не зазначити, що деякі IoT пристрої мають невеликий розмір і крихку конструкцію. Тому, щоб випадково не зламати певні пристрої перед встановленням і інтегруванням з комп'ютерною мережею провідним спеціалістів відділу технічної підтримки необхідно досконально прочитати інструкцію, яка додається у комплект до IoT пристроїв після придбання.

2.3 Висновки

Здійснивши і обгрунтувавши підбір IoT пристроїв до кожного відділу підприємства, які будуть складати систему моніторингу IoT та платформи, завдяки якій обраним IoT пристроям можна зазначити виконувані функції, необхідно зазначити, що до комплексу IoT були додані лише тільки ті IoT пристрої, які зможуть знизити ризик аварійних ситуацій у різних відділах підприємства.

3 СИНТЕЗ СИСТЕМИ МОНІТОРІНГУ ПІДПРИЄМСТВА

3.1 Функціональна схема системи моніторингу IoT підприємства «Агентство розвитку Дніпра»

При розробці комплексу IoT важливо правильно організувати функціональну схему, за допомогою якої можна побачити процес передачі інформації у системі моніторингу IoT.

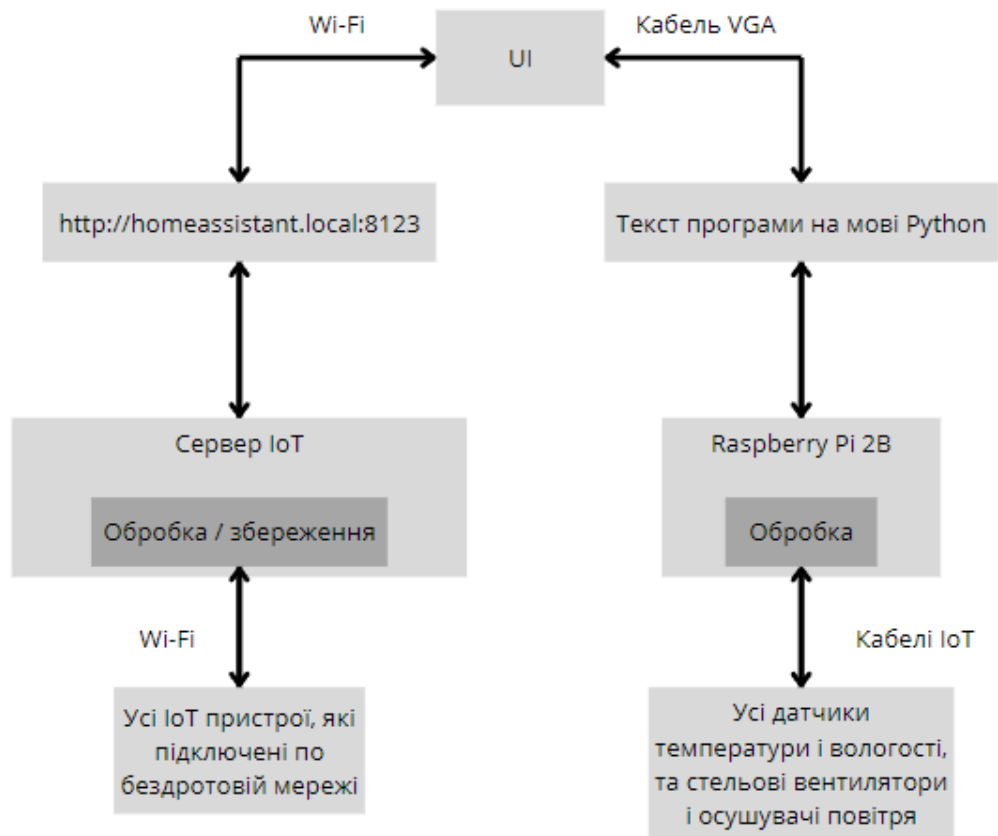
На найнижчому рівні повинні розташовуватись усі пристрої, які будуть створювати систему моніторингу IoT.

На нижчому рівні повинні розташовуватись хаби, до яких буде підключено пристрої системи моніторингу IoT. Також потрібно вказати які операції виконують хаби, отримуючи дані від пристроїв системи моніторингу IoT.

На середньому рівні потрібно вказати файл або інше місце, де знаходяться функції, які керують робочим процесом пристроїв системи моніторингу IoT. Буде розроблений текст програми на мові Python, у якому будуть використані дані від датчиків температури і датчиків вологості задля регулювання роботи стельових вентиляторів і осушувачів повітря відповідно. Функції для усіх інших IoT пристроїв будуть розташовані у хмарі Home Assistant, до якої буде підключено IoT сервер.

На вищому рівні потрібно вказати, що буде використовувати провідний спеціаліст відділу технічної підтримки, щоб мати можливість керувати робочим процесом пристроїв системи моніторингу IoT і бачити статус IoT пристроїв, або дані від датчиків. Також необхідно вказати тип підключення до хабів. Щоб змінити дані у функціях стельових вентиляторів і осушувачів повітря необхідно підключити до Raspberry Pi монітор за допомогою VGA кабелю і через клавіатуру змінити потрібні рядки тексту. Для усіх інших IoT пристроїв буде виділено окремий ПК у відділі технічної підтримки, який буде мати можливість редагувати сценарії спрацювання IoT пристроїв, які підключені до нового маршрутизатору з Wi-Fi підключенням і передивляться їх статуси.

Функціональну схему можна побачити на рисунку 3.1.



*
UI - User Interface

Рисунок 3.1 – Функціональна схема системи моніторингу IoT

3.2 Структурна схема системи моніторингу IoT підприємства «Агентство розвитку Дніпра»

Підприємство «Агентство розвитку Дніпра» орендує перші два поверхи будівлі в центрі міста, де і розташована комп'ютерна мережа підприємства. Усі відділи, окрім складу і приміщення для наради, знаходяться на першому поверсі.

Оскільки, для одного Raspberry Pi у системі моніторингу IoT знаходиться багато пристроїв, які необхідно підключити до хабу, було прийняте рішення придбати 4 плати Raspberry Pi, до яких будуть підключені усі стельові вентилятори, осушувачі повітря і датчики температури та вологості повітря.

Щоб не перенавантажувати структурну схему системи моніторингу IoT було прийняте рішення розділити її на загальну структурну схема, та структурну схему усіх відділів підприємства. Структурна схема зроблена у програмі Packet Tracer

зادля того, щоб детальніше показати розроблену систему моніторингу IoT (рисунок 3.2 – 3.12).

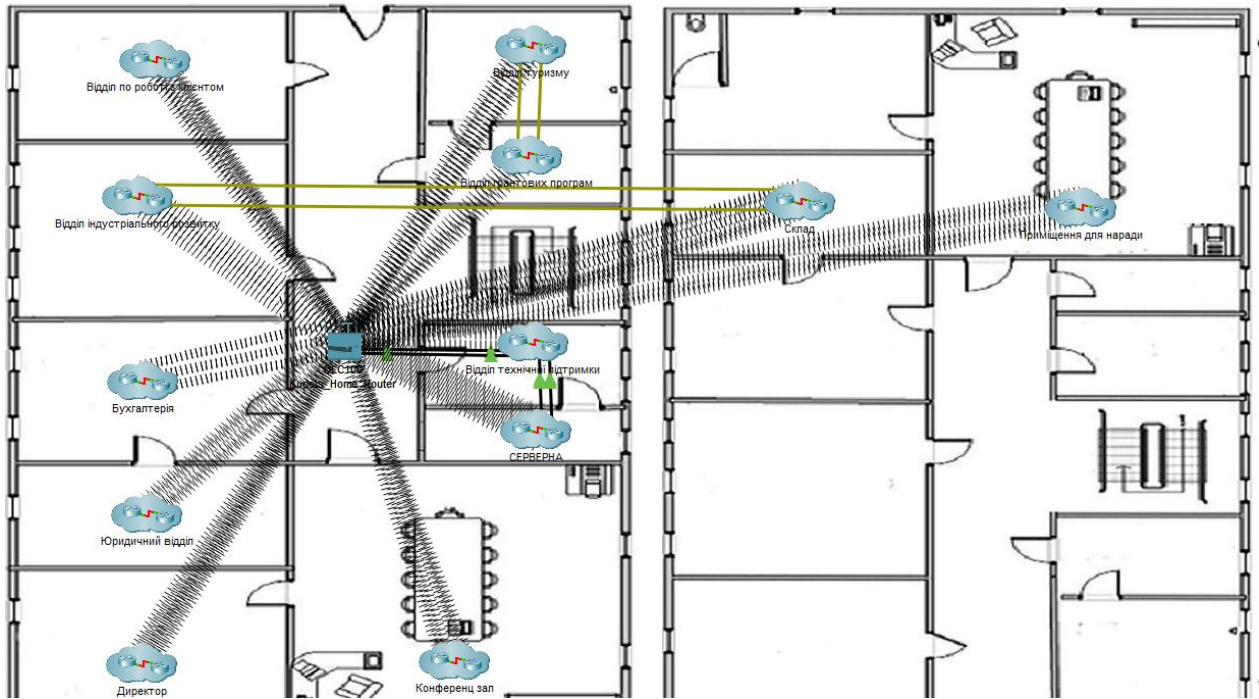


Рисунок 3.2 – Загальна структурна схема системи моніторингу IoT

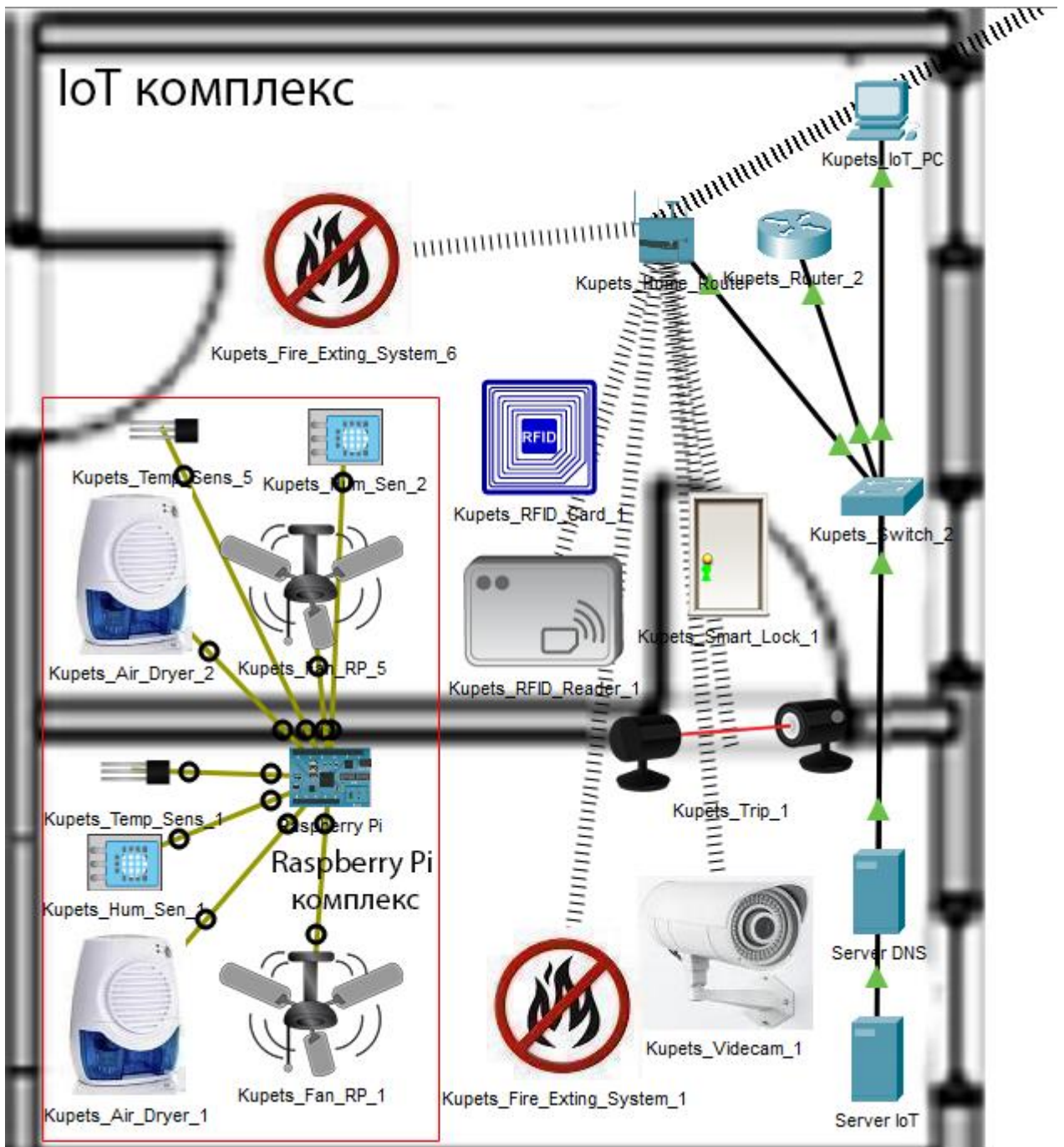


Рисунок 3.3 – Структурна схема відділу технічної підтримки і серверної

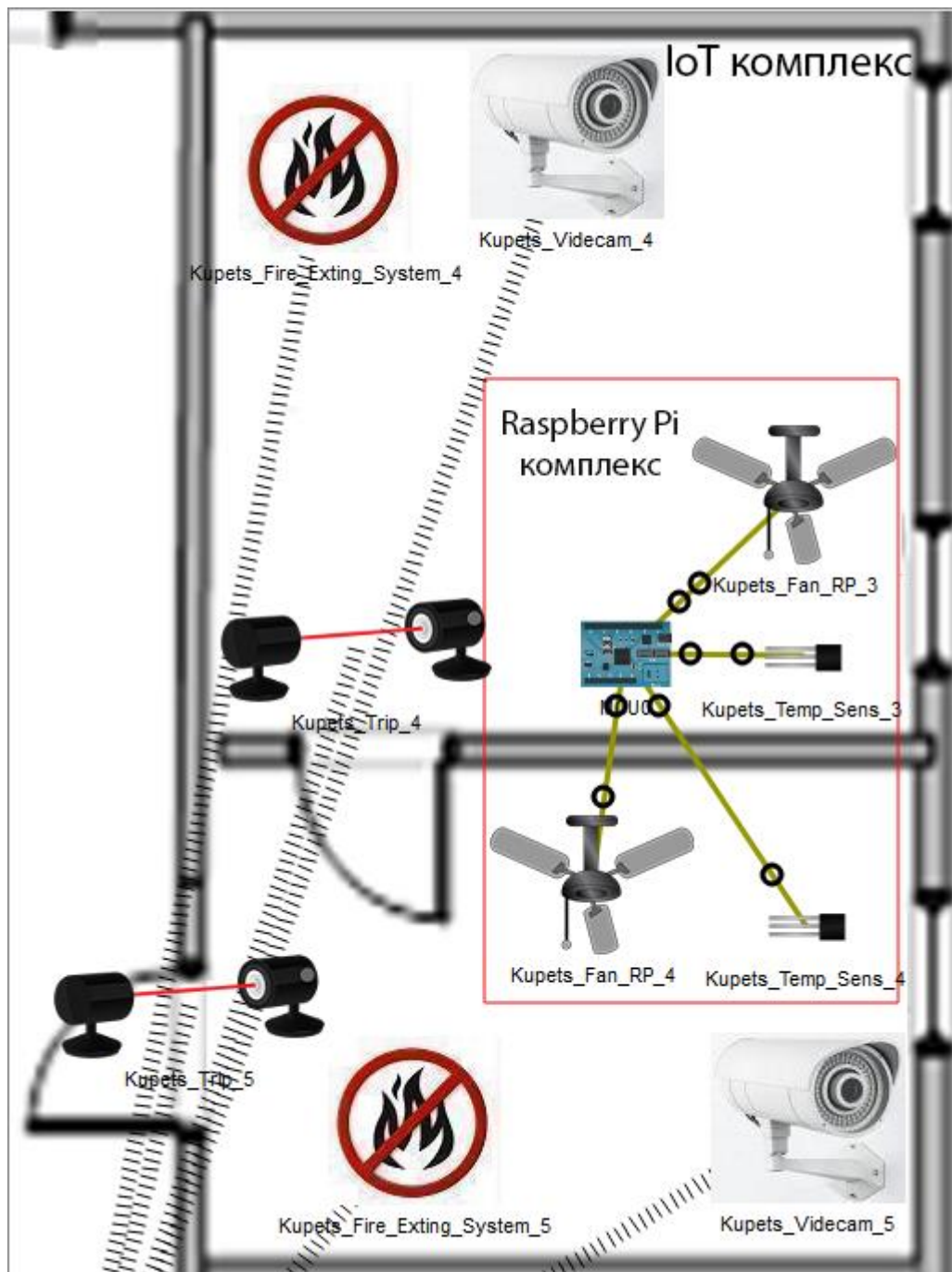


Рисунок 3.4 – Структурна схема відділу грантових програм і відділу туризму

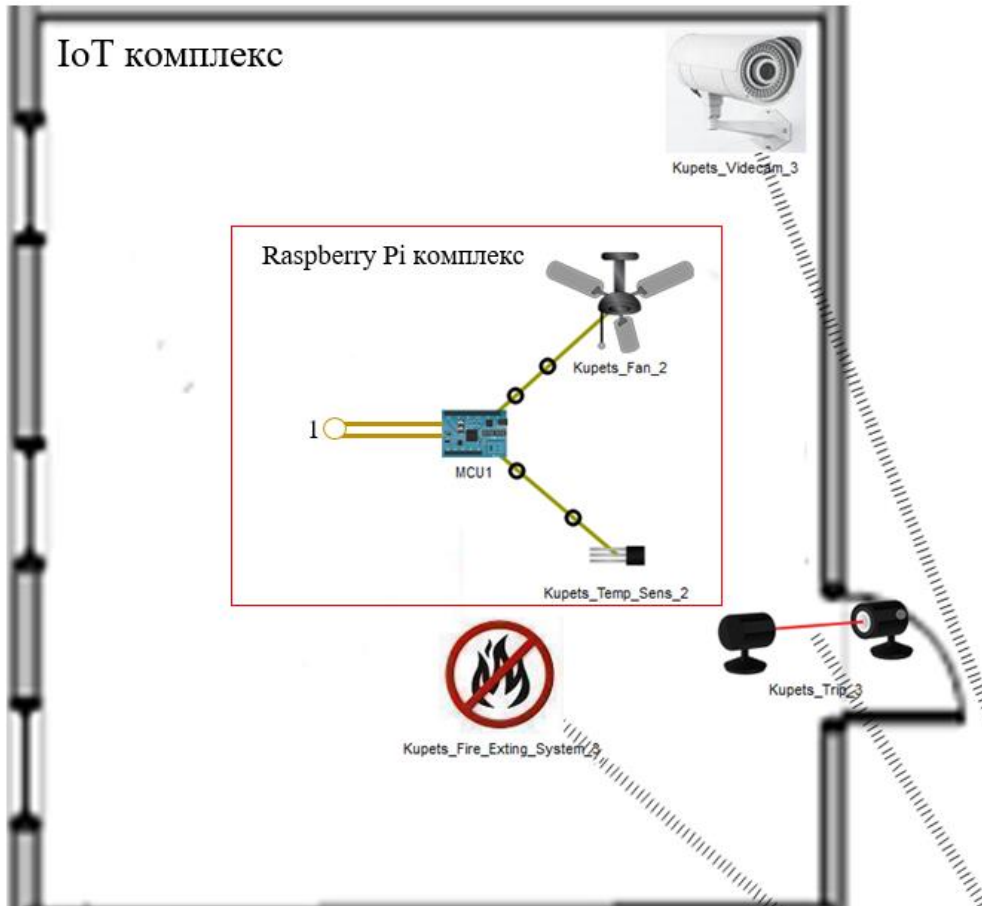


Рисунок 3.5 – Структурна схема відділу індустріального розвитку

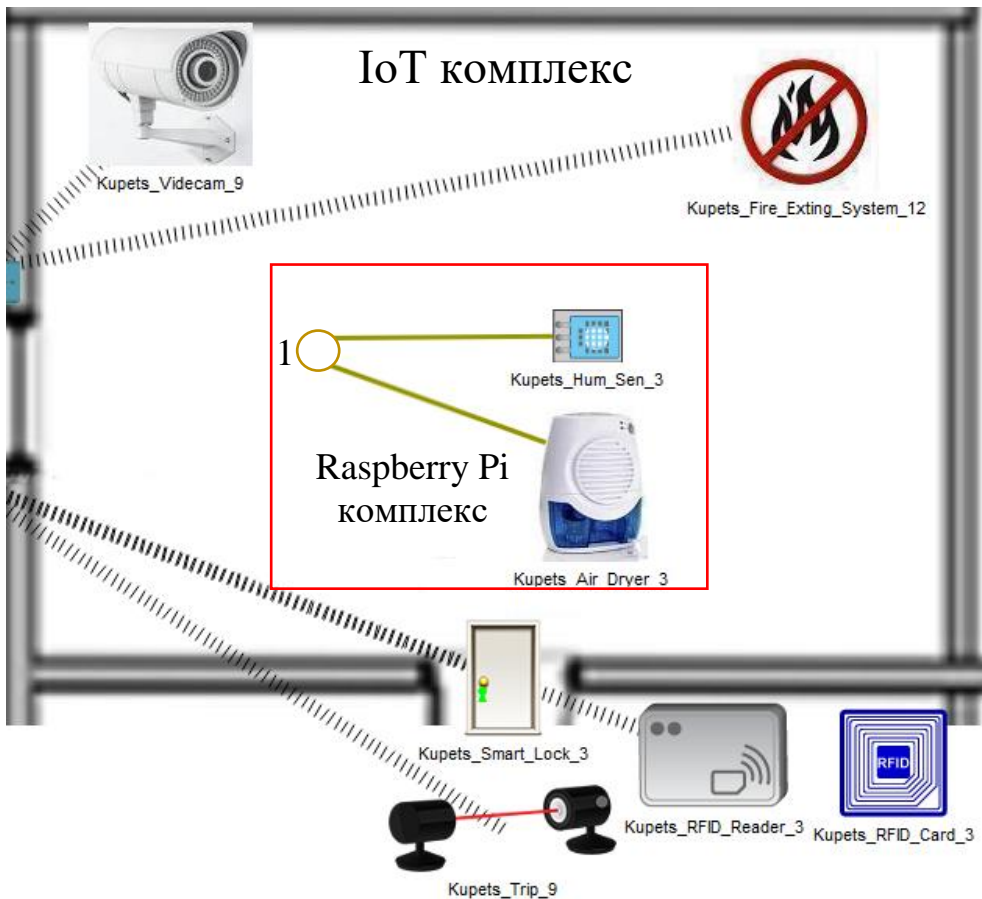


Рисунок 3.6 – Структурна схема складу

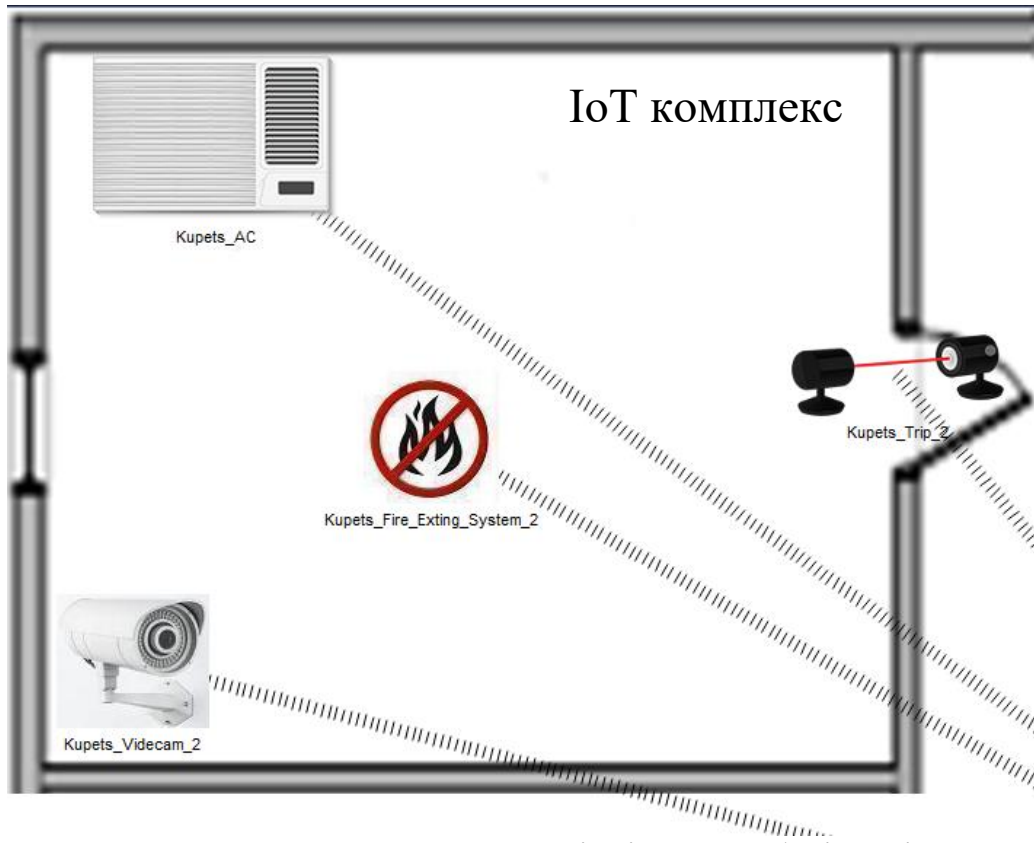


Рисунок 3.7 – Структурна схема відділу по роботі з клієнтом

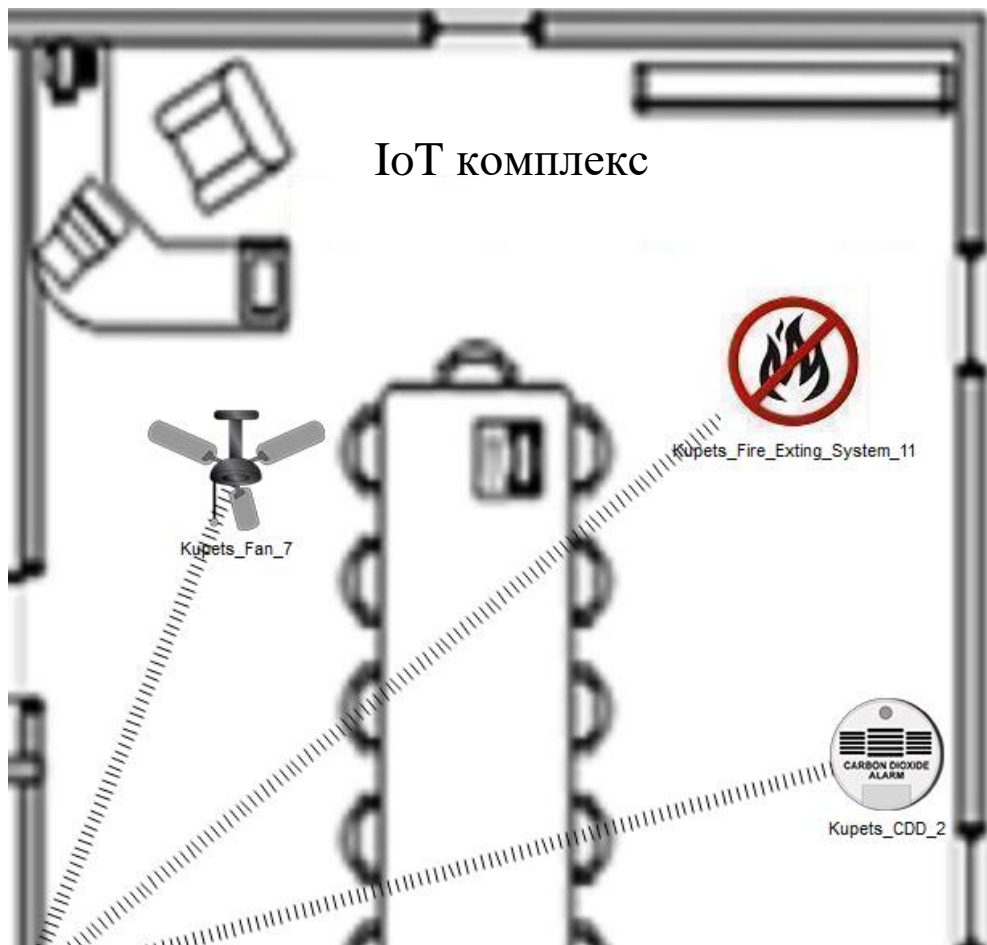


Рисунок 3.8 – Структурна схема приміщення для наради

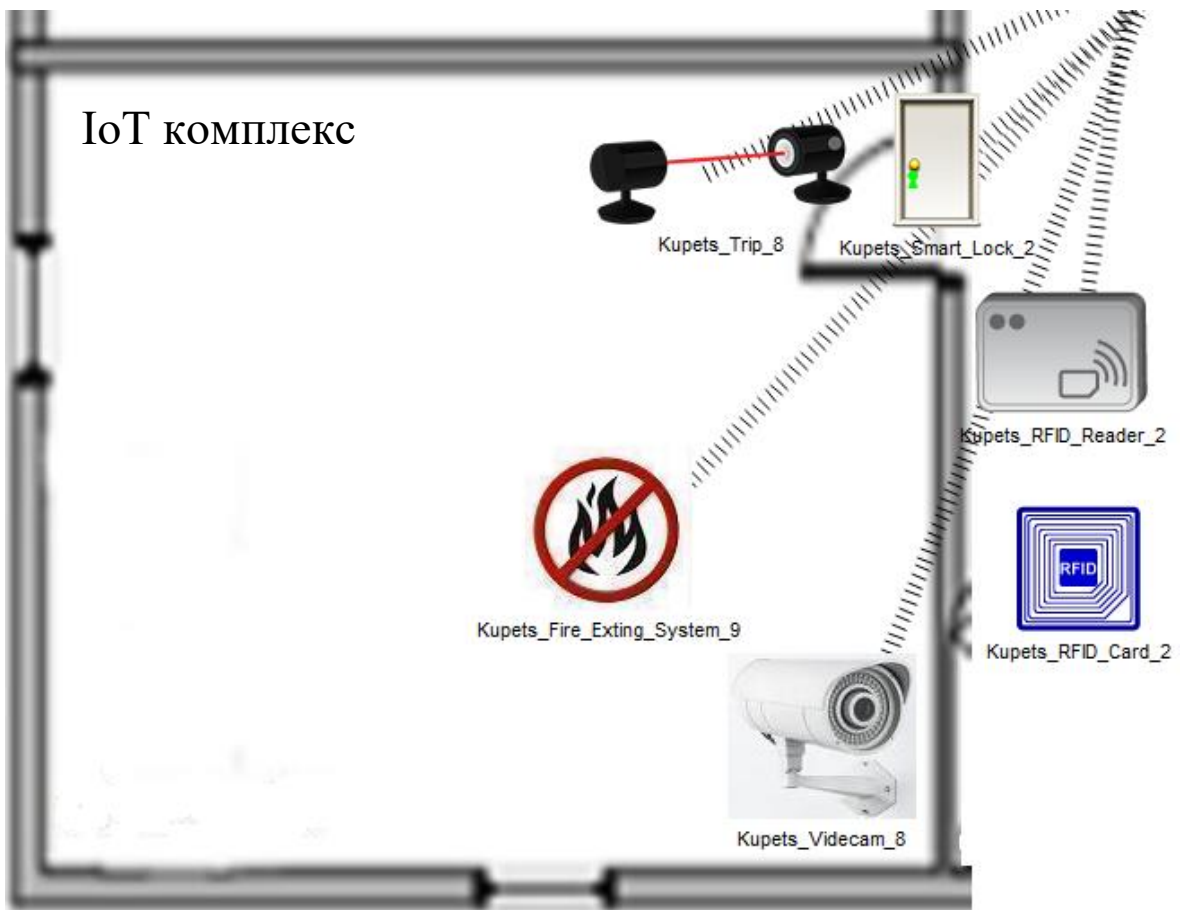


Рисунок 3.9 – Структурна схема відділу директора

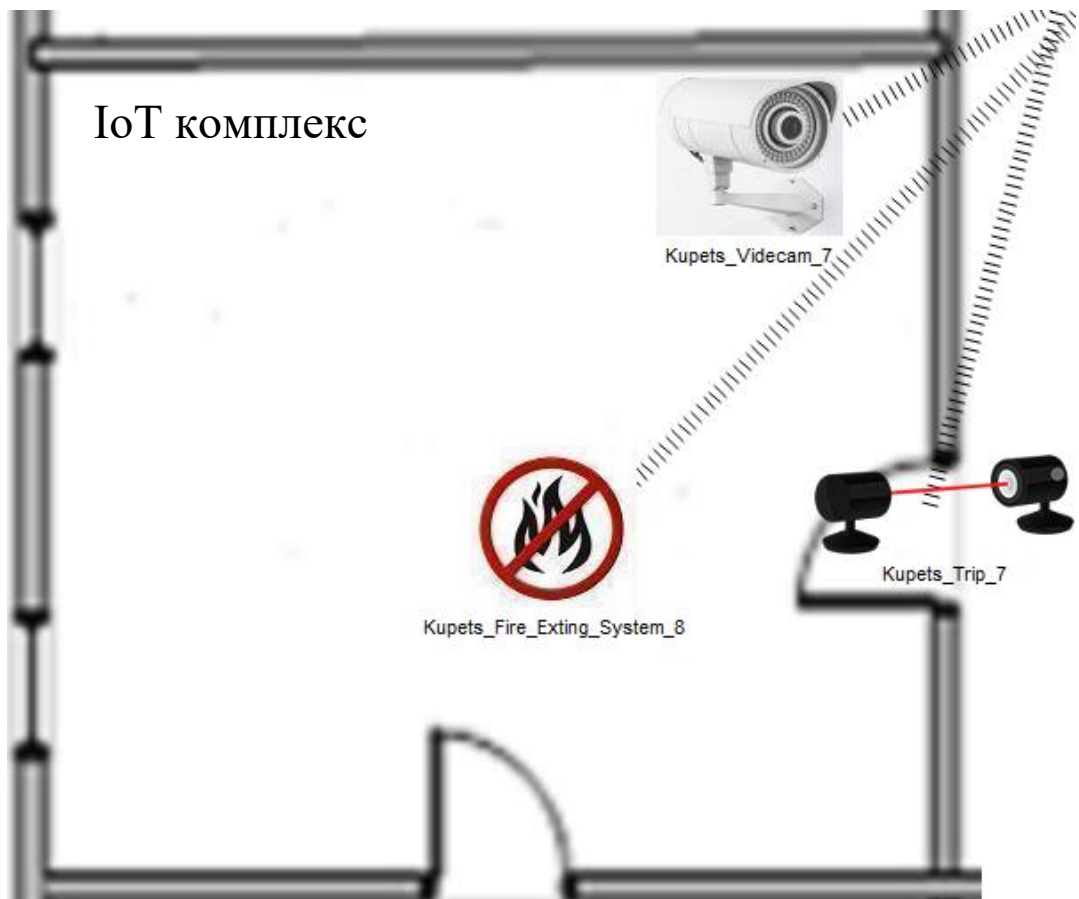


Рисунок 3.10 – Структурна схема бухгалтерії

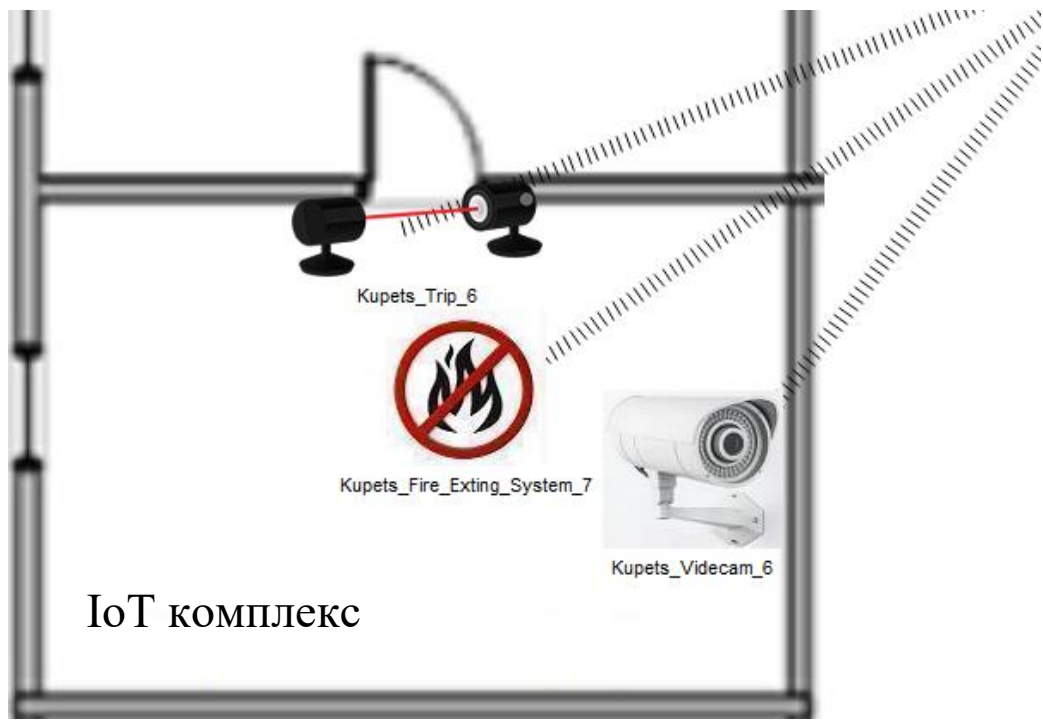


Рисунок 3.11 – Структурна схема юридичного відділу

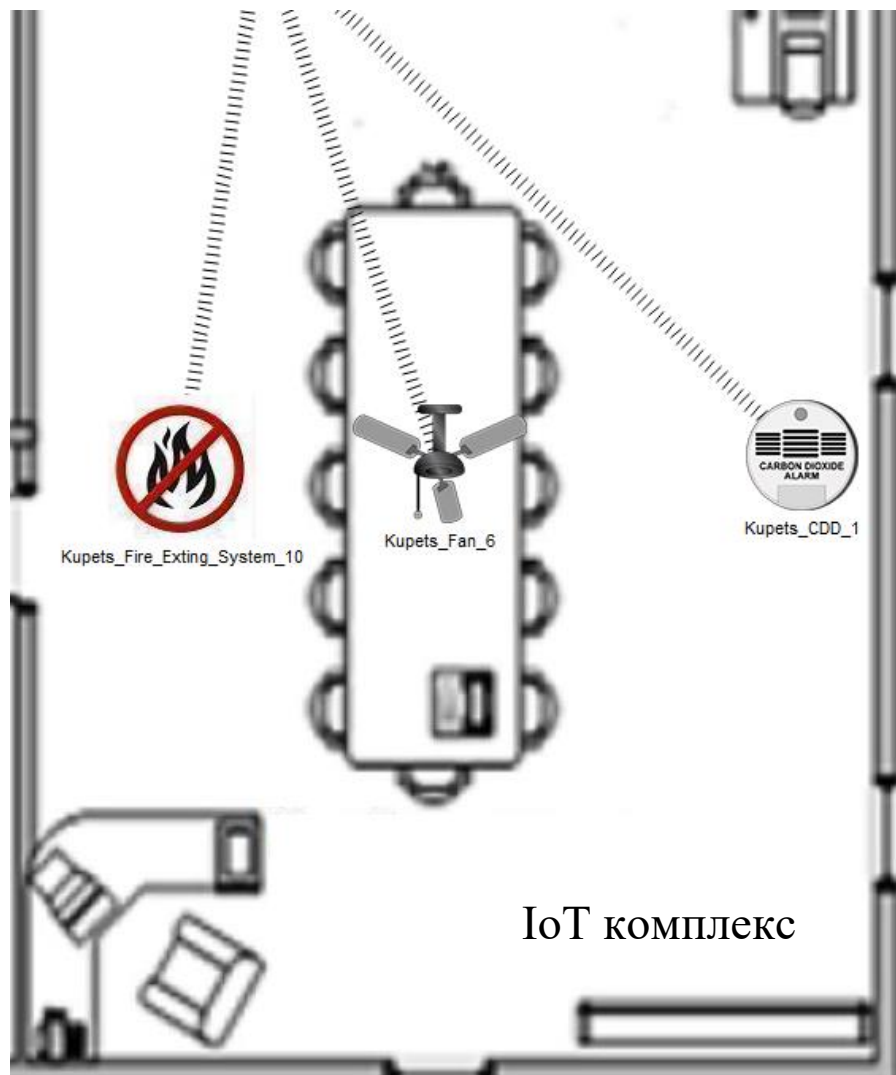


Рисунок 3.12 – Структурна схема конференц залу

На рисунку 3.2 можна побачити процес передачі інформації у системі моніторингу IoT. Усі IoT пристрої, окрім стельових вентиляторів і осушувачів повітря, підключені до маршрутизатору Kupets_Home_Router за допомогою бездротового підключення Wi-Fi (рисунок 3.2). До цього маршрутизатора також підключений IoT сервер, який є хабом для збереження і обробки даних, які поступають від IoT пристроїв і ПК Kupets_IoT_PC, через який можна редагувати функції кожного IoT пристрою, який підключений до IoT серверу, та побачити статус цих пристроїв (рисунок 3.3).

Усі стельові вентилятори і осушувачі повітря не можуть бути підключеними на пряму до Raspberry Pi тому було прийняте рішення підключити їх до розумної розетки, яка буде підключена по Wi-Fi сигналу до Raspberry Pi. На структурній схемі стельові вентилятори і осушувачі повітря на пряму підключені до Raspberry Pi через те, що програма RT не підтримує можливість під'єднання до плати Raspberry Pi інших пристроїв за допомогою мережи Wi-Fi.

На рисунках 3.3 – 3.4 можна побачити що до Raspberry Pi комплексу під'єднанні пристрої, які знаходяться у іншому відділу, який знаходиться поруч. Оскільки до Raspberry Pi буде придбано Wi-Fi модуль, який не зможе передавати сигнал на велику відстань – усі пристрої Raspberry Pi комплексу знаходяться якомога ближче до Wi-Fi модулю Raspberry Pi. Передача Wi-Fi сигналу до іншого відділу можливо тільки через те, що стіни між відділами складаються з гіпсокартону. На рисунку 3.6 можна побачити, що пристрої, які відносяться до Raspberry Pi комплексу складу підключені до Raspberry Pi, яке знаходиться у відділі індустріального розвитку (рисунок 3.5).

Через те, що програма RT некоректно відображає підключення пристроїв до Raspberry Pi, які знаходяться у різних кластерах, було прийняте рішення зробити схему підключення стельових вентиляторів, осушувачів повітря і датчиків температури та вологості до усіх плат Raspberry Pi (рисунок 3.13 – 3.16).

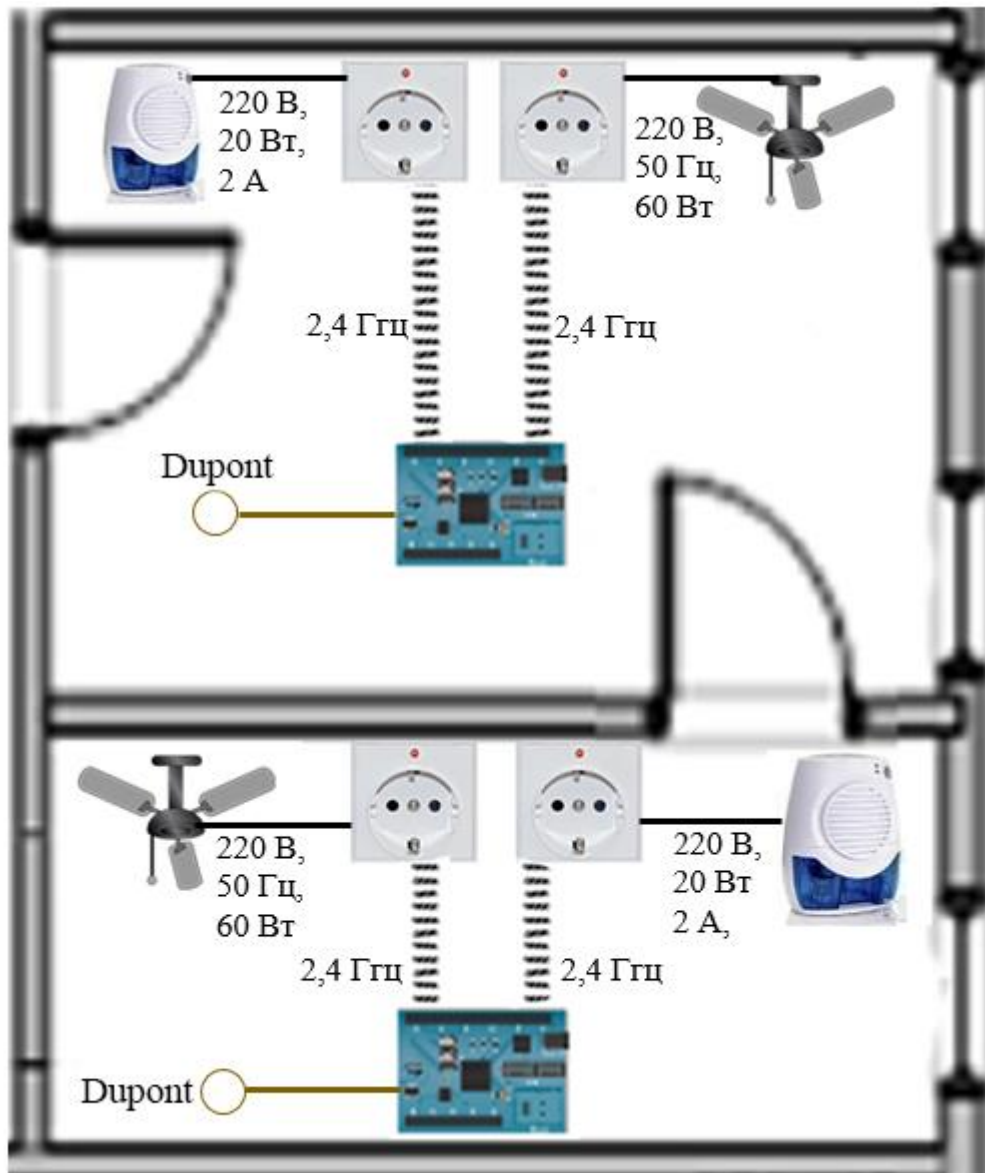


Рисунок 3.13 – Схема з'єднань відділу технічної підтримки і серверної

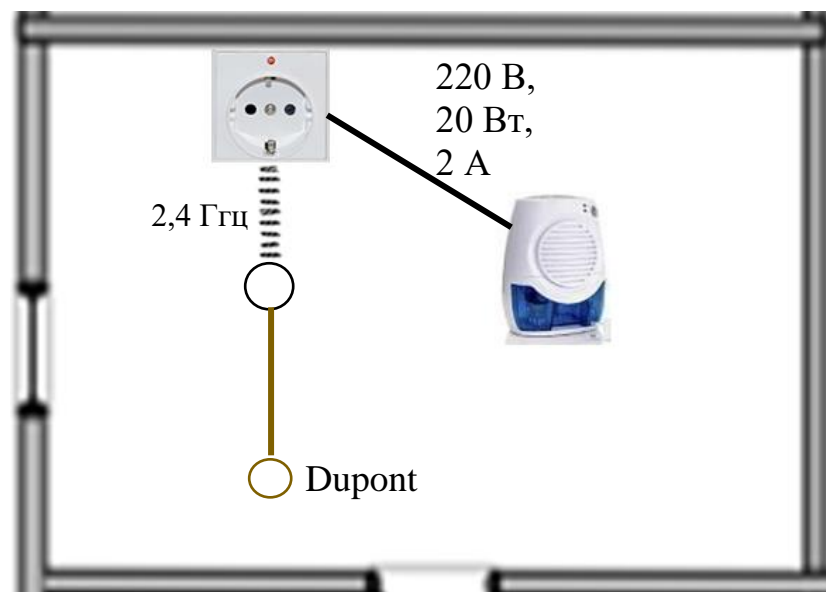


Рисунок 3.14 – Схема з'єднань другого поверху будівлі

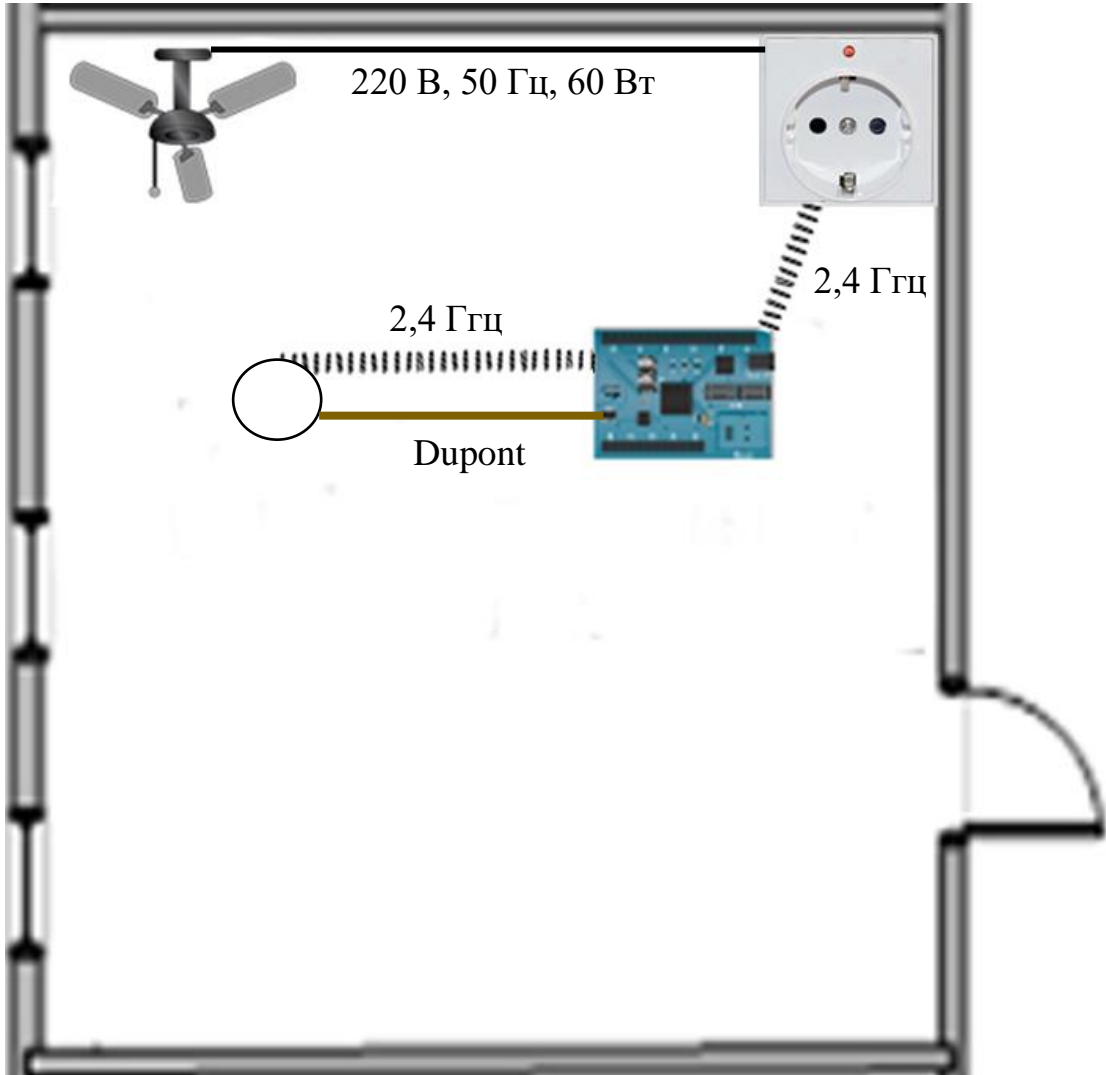


Рисунок 3.15 – Схема з'єднань відділу індустріального розвитку

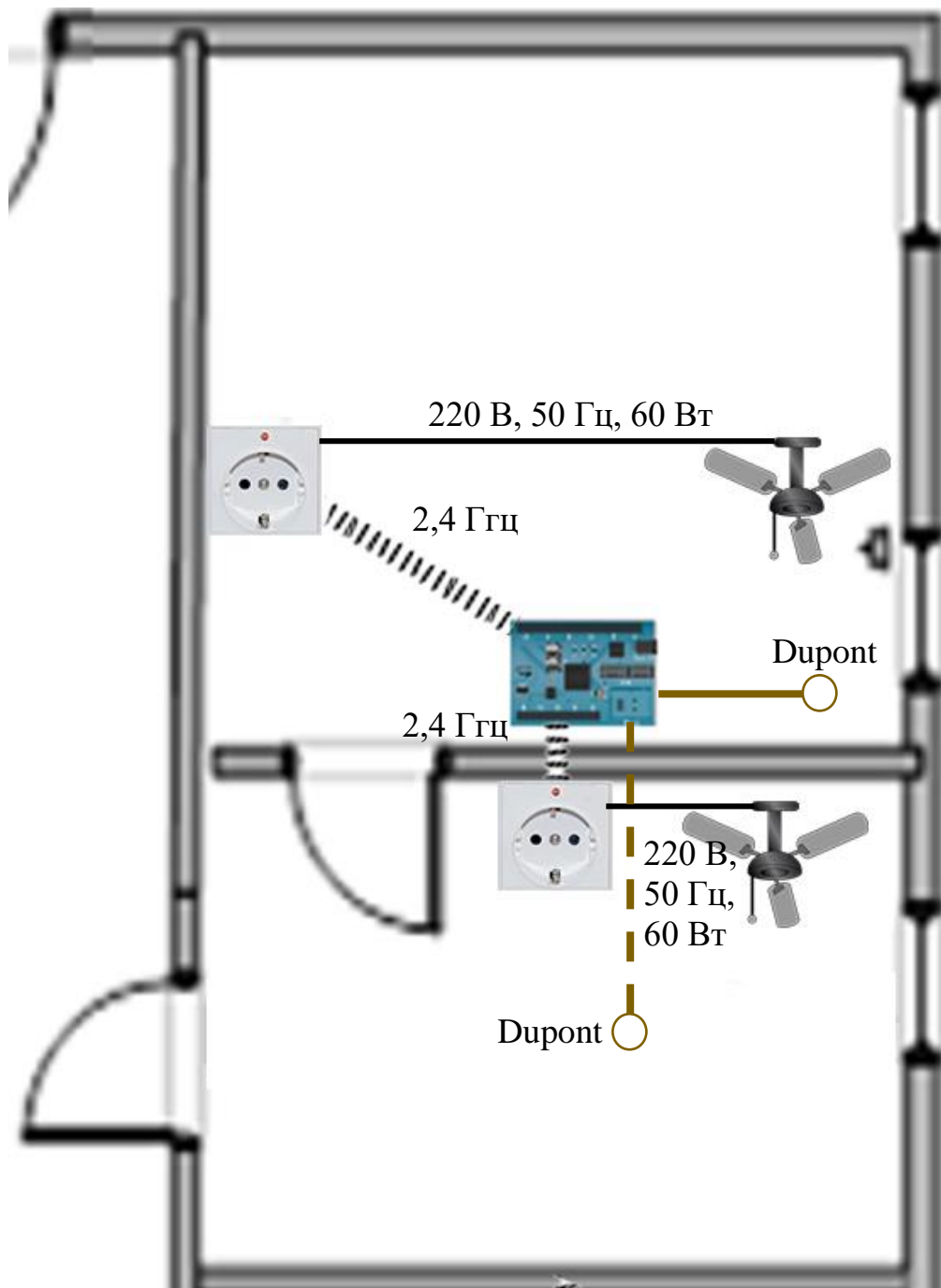


Рисунок 3.16 – Схема з'єднань відділу туризму і відділу грантових програм

На рисунках 3.13 – 3.16 можна побачити, що всі стельові вентилятори і осушувачі повітря підключені темним дротом до розумної розетки (синій прямокутник), який підключений по бездротовій мережі до Raspberry Pi (пунктирні лінії). Також до Raspberry Pi підключені датчики вологості і температури повітря за допомогою кабелів Dupont. На рисунку 3.15 можна побачити, що Dupont кабель від датчика температури та вологості повітря, який знаходяться на складі,

прокладений до відділу індустріального розвитку, який знаходиться на першому поверху відразу під складом. Довжина передачі даних буде достатньою, щоб використовувати кабель канали у відділах туризму і індустріального розвитку, які розроблялись під час запровадження комп'ютерної мережі підприємства, що значно полегшило прокладання кабелів через стіну. При запровадженні Raspberry Pi комплексу необхідно перевірити, чи не будуть втрачатись сигнали від датчиків температури і вологості. Якщо, під час тестування, сигнали від датчиків будуть не доходити до Raspberry Pi, можна буде обрати спеціальний підсилювач сигналу для датчиків від компанії Adafruit. Принципова схема з'єднань датчиків температури і вологості повітря до Raspberry Pi В наведена на рисунку 3.17.

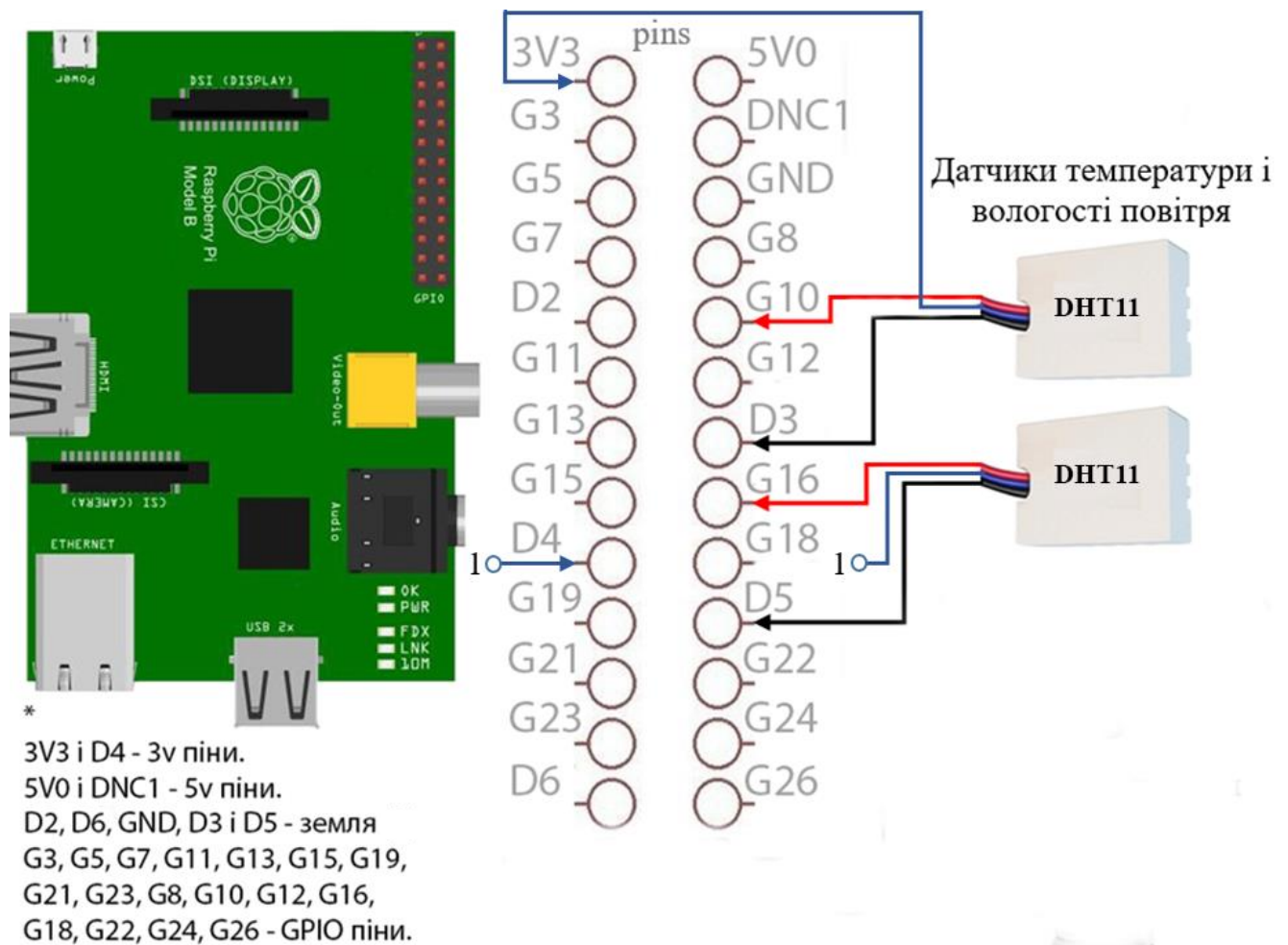


Рисунок 3.17 – Принципова схема підключення до Raspberry Pi В датчиків температури і вологості повітря

На рисунку 3.17 можна побачити у якій пини Raspberry Pi B підключаються датчики температури і вологості повітря. Датчик температури і вологості повітря має роз'єм, який складається з трьох пинів, у якому червоний пін передає сигнал (дані з датчика), синій – це плюс, а чорний – мінус (земля). Орієнтуючись за розшифровкою пинів плати Raspberry Pi B, яка приведена на рисунку 3.17, стає зрозумілим, що підключати червоний пін можна у будь-який GPIO пін, синій тільки у 3V3 або D4, а чорний тільки у GND або D2, D3, D5, D6. Стельові вентилятори і осушувачі повітря живляться підключені до розумних розеток, щоб мати можливість змінювати режим роботи цих пристроїв за допомогою Raspberry Pi, до якого розумні розетки підключені по Wi-Fi. Якщо з'явиться потреба змінити режим роботи стельового вентилятора або осушувача повітря необхідно звернутись до спеціалісту з відділу технічної підтримки, який підключить до Raspberry Pi B монітор і клавіатуру, і змінить у тексті програми дані температур або відсоток вологості повітря, при яких стельовий вентилятор або осушувач повітря змінє режим роботи і буде працювати від мережи живлення.

Через те, що система пожежогасіння запроваджена у кожній відділ підприємства «Агентство розвитку Дніпра» і складається з чотирьох основних пристроїв, розмір іконок яких у програмі РТ не дозволяє додати їх до невеликих моделей структурних схем відділу технічної підтримки, відділу грантових програм і серверної, було прийняте рішення на структурних схемах усіх відділів замінити чотири іконки IoT пристроїв системи пожежогасіння на одну (рисунок 3.18 – 3.19), враховуючи те, що під час тестування комплексу IoT у програмі РТ, система пожежогасіння буде позначатись чотирма IoT пристроями, які зазначені на рисунку 3.18.



Рисунок 3.18 – Чотири IoT пристрої, які входять до системи пожежогасіння



Рисунок 3.19 – Позначення системи пожежогасіння на структурних схемах відділів підприємства

3.3 Основні вимоги до системи керування комплексу IoT

Для того, щоб підібрати потрібне технічне обладнання до системи моніторингу IoT необхідно враховувати основні вимоги до пристроїв комплексу IoT:

- модель Raspberry Pi повинна мати достатню кількість портів для датчиків вологості повітря, температури, стельових вентиляторів і осушувачів повітря, які необхідно підключити до системи моніторингу IoT;
- маршрутизатор, до якого будуть підключені всі пристрої комплексу IoT, повинен бути від компанії Cisco, оскільки від бренду Cisco були придбані всі інші маршрутизатори, які запроваджені у комп'ютерну мережу;
- IoT пристрої не повинні конфліктувати один з одним, через те, що технічне обладнання придбано у різних виробників;
- всі IoT пристрої повинні підтримувати бездротовий зв'язок;
- камери відеоспостереження повинні мати високу роздільну здатність і широке поле зору.

3.4 Опис функцій і кількості IoT пристроїв у відділах підприємства «Агентство розвитку Дніпра»

Перед тим, як обрати обладнання для системи моніторингу IoT слід визначитись з кількістю IoT пристроїв, які будуть запроваджені до IoT комплексу і надати короткий опис функцій, які ці пристрої будуть виконувати (таблиця 3.1).

Таблиця 3.1 – Функції і кількість IoT пристроїв у відділах підприємства

№	Назва IoT пристрою	Короткий опис функцій	Вимоги до вибору пристрою	Необхідна кількість IoT пристроїв / в які відділи будуть запроваджені
1	Датчик вогню	Спрацьовує, при наявності поруч з ним вогню	Тип сигналу: цифровий. Гучність: 50 дб+	12 / в усі відділи
2	Спринклер	Зрошує рідину або порошок, яка гасить пожежі у приміщеннях	Тип задіяної речовини: вода	12 / в усі відділи
3	Сигналізація	При спрацюванні сповіщає людей про небезпеку	Радіус дії: більше 20 метрів Гучність: 80 дб+	12 / в усі відділи
4	Трап для зливу води	Забезпечує відтік рідини, яка гасить пожежі у приміщенні	Час, який відводиться для активації: не більше 10 секунд	12 / в усі відділи
5	Камера відеоспостереження	Пристрій, який записує на відео всі події, які відбуваються у приміщенні	Роздільна здатність: 4К. Тип живлення: за допомогою блоку живлення.	9 / в усі відділи, окрім конференц залу, приміщення для наради і відділу технічної підтримки
6	Датчик руху	Спрацьовує, при перетненні невидимого лазера	Дальність виявлення: більше 4 метрів	9 / в усі відділи, окрім конференц залу, приміщення для наради і відділу технічної підтримки
7	Стельові вентилятори	Пристрій, який розганяє повітря	USB порт: 1 шт, лопаті: три або більше	7 / в усі відділи, окрім складу, директору, юридичного відділу, бухгалтерії і відділу по роботі з клієнтами

8	Розумна розетка	Пристрій, який дозволить змінювати режим роботи стельових вентиляторів і осушувачів повітря	Напруга: до 240 В Wi-Fi: 2.4 ГГц	6 / відділ туризму, відділ грантових програм, відділ технічної підтримки, серверна, відділ індустріального розвитку і склад
8	Температурний датчик	Пристрій, який вимірює температуру	Порт для виводу даних: 1 шт	5 / відділ туризму, відділ грантових програм, відділ технічної підтримки, серверна і відділ індустріального розвитку
9	Датчик вологості	Пристрій, який вимірює вологість у повітрі	Порт для виводу даних: 1 шт	3 / склад, серверна і відділ технічної підтримки
10	Осушувач повітря	Пристрій, який зменшує вологість повітря	Ефективна площа осушення: більше десяти метрів	3 / склад, серверна і відділ технічної підтримки
11	RFID зчитувач і RFID картки	RFID зчитувач зчитує ідентифікатори RFID карток	Дальність зчитування: 3 см+, Картки: NFC, Bluetooth	3 / склад, серверна і директору
12	Розумний замок	Спеціальний замок, який при спробі злому сповіщає про це власника пристрою	Тип живлення: за допомогою батарейок	3 / склад, серверна і директору
13	Датчик вуглекислого газу	Пристрій, який вимірює рівень вуглекислого газу у повітрі	Тип живлення: акумулятор	2 / приміщення для наради і конференц зал
14	Кондиціонер	Пристрій, для зменшення температури у приміщенні	Потужність: менше 900 Вт, площа покриття: більше п'ятнадцяти метрів	1 / відділ по роботі з класентом

3.5 Характеристика пристроїв і кабелів системи моніторингу IoT

При виборі пристроїв до системи моніторингу IoT підприємства «Агентство розвитку Дніпра», які будуть підключені до хмари Home Assistant, необхідно звернути увагу на наявність бездротового зв'язку з маршрутизатором Kurpets_Home_Router. Кількість підібраних пристроїв, їх моделі і характеристики наведені у таблиці 3.2.

Таблиця 3.2 – Бездротові пристрої

№	Кіл.	Назва	Модель	Характеристика
1	12	Бездротовий датчик вогню	Ajax FireProtect 2 RB (Heat/Smoke) Jeweller [14]	Гучність сирени – 85 дБ
				Діапазони частот – 866 - 922 МГц
				Дальність зв'язку – до 1700 м (без перешкод)
				Відповідність спеціалізованим пожежним стандартам – EN 14604:2005/AC:2008 EN 50291-1:2018, Qmark
2	12	Бездротові спринклери	ZSTX-15 [15]	Діаметр різьблення – 1/2"
				Робочий тиск у трубопроводі – 0.5 – 12 бар
				Температура спрацювання – 68 °С
				Тип системи пожежогасіння – Водяна
3	12	Бездротові трапи для зливу води	Tuya Smart Water [16]	Час спрацювання – 7 с
				Крутячий момент – 40 кг/см
4	12	Бездротові сигналізації	IoT-HUB10WG [17]	Радіус дії – до 100 метрів
				Кількість номерів сповіщення – 6
				Діапазони частот – 868 МГц
				Робоча напруга – 5 В
5	9	Бездротові датчики руху	Ajax MotionProtect White [18]	Дальність детектування – До 12 метрів
				Захист від злому тампером – Є
				Частота передавання – 868 МГц
				Розміри – 110 x 65 x 50 мм

6	9	Бездротові камери відеоспостереження	QeaRim P6 IPC360 Home live [19]	Роздільна здатність – 4К 8MP
				Нічне бачення – 25 м (82 фути)
				Відстань
				Фокусна відстань – 3,6 мм
				Поле зору – 93°(Г), 48°(В), 115°(Г)
				Частота кадрів – 25 кадрів за секунду
7	3	Бездротові розумні замки	TTLOCK BOSS [20]	Елементи живлення – AAA – 4 шт
				WiFi – шлюз – Є
				Кріпильні аксесуари – Є
8	3	Бездротовий RFID зчитувачі разом з RFID картками	Wi-Fi Wiegand 1D 2D IC [21]	Інтерфейси зв'язку – Wiegand
				Відстань зчитування – 3-10 см
				Тип читання карток – Карта IC/NFC/Blue-tooth
				Розміри, мм – 114*74*21 мм
9	2	Бездротові датчик вуглекислого газу	CO2 PTH-5 (PTH5-12) [22]	Вага – 0.15 кг
				Тип живлення – Акумулятор
				Розміри – 83 × 83 × 32 мм
10	2	Бездротові стельові вентилятори	Nickel LED Indoor Smart WI-FI Ceiling Fan [23]	Кількість швидкостей – 3
				Кількість лопатів – 3
11	1	Бездротовий Кондиціонер	TCL TAC-09CHSA/XAB1 [24]	Споживання потужність – 640 Вт
				Площа – до 30м ²
				Розміри (Ш x В x Г) – 700 × 256 × 190 мм
12	4	Плата	Raspberry Pi Model B [25]	SDRAM – 512 Mb
				USB – 2
				GPIO – 26-pin
				Розмір – 86 x 56 x 20 мм
13	1	Wi-Fi Маршрутизатор	Cisco SB RV110W Wireless N VPN Firewall [26]	Частота роботи Wi-Fi – 2.4 ГГц
				Швидкість LAN портів – 100 Мбіт/с

У таблиці 3.3 зазначені IoT пристрої з дротовим підключенням до Raspberry Pi B.

Таблиця 3.3 – Пристрої з дротовим підключенням до Raspberry Pi B

№	Кіл.	Назва	Модель	Характеристика
1	6	Датчик вологості і температури	DHT11 [27]	Діапазон вимірювання температури – від 0°C до 50°C
				Діапазон вимірювання вологості – від 20% до 95%
				Точність вимірювання температури – 2°C
				Точність вимірювання вологості – 5%
2	5	Стельові вентилятори	Westinghouse Lighting 7217000 [28]	Кількість швидкостей – 1
				Кількість лопатів – 5
				Функція реверсу – Є
				Потужність – 56 Вт
3	3	Осушувачі повітря	Bautech USB [29]	Ефективна S осушення – До 20 м
				Об'єм резервуару для води – 500 мл
				Розміри – 21,5 x 15 x 12 см
				Споживання – 2 - 20Вт
4	6	Розумна розетка	TuYa Wi-Fi [30]	Тип підключення – Wi-Fi
				Частота бездрот. датчиків – 2.4 ГГц
				Напруга – до 240 В
				Максимальна сила струму – 16 А
5	4	USB Wi-Fi модуль з антеною для RP	Lb – Link [31]	Частота сигналу – 2.4 ГГц

3.6 Висновки

Після розробки структурної схеми кожного відділу підприємства, з вже запровадженим комплексом IoT та також основних вимоги до пристроїв, які будуть запроваджені, кількості запроваджених пристроїв і їх технічних характеристик, можна отримати точний вигляд майбутньої системи моніторингу IoT.

Залишається тільки задати умови для активації певних датчиків і розробити текст програми для початку тестування пристроїв комплексу IoT.

4 РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1 Призначення і сфера застосування програмного забезпечення

Програмне забезпечення для системи моніторингу IoT буде розділено на дві частини.

Перше програмне забезпечення буде знаходитись на Raspberry Pi B, в якому будуть зазначені умови для спрацювання датчиків температури і вологості та стельвих вентиляторів і осушувачів повітря. Ці пристрої будуть застосовуватись у відділах індустріального розвитку, туризму, грантових програм, технічної підтримки, серверної і складі.

Друге програмне забезпечення буде знаходитись на IoT сервері, в якому будуть створені сценарії для спрацювання всіх IoT пристроїв. IoT пристрої знаходяться у кожному відділі підприємства і усім IoT пристроям надані унікальні адреси і унікальні назви.

4.2 Обґрунтування технічних характеристик програм

4.2.1 Постановка завдання на розробку програми

Необхідно створити для Raspberry Pi текст програми на мові Python, який міг би контролювати стельовий вентилятор і осушувач повітря. Стельовий вентилятор буде забезпечувати комфортну температуру у відділах, а осушувач повітря повинен тримати рівень вологості повітря у нормі.

Сценарії, які потрібно зробити на ПК у відділі технічної підтримки, будуть контролювати всі IoT пристрої системи моніторингу, для забезпечення достатнього рівня безпеки у всіх відділах підприємства «Агентство розвитку Дніпра».

4.2.2 Опис алгоритму функціонування програми

Схема алгоритму текста програми на мові Python, який буде працювати на Raspberry Pi B зазначена на рисунку 4.1 – 4.3.

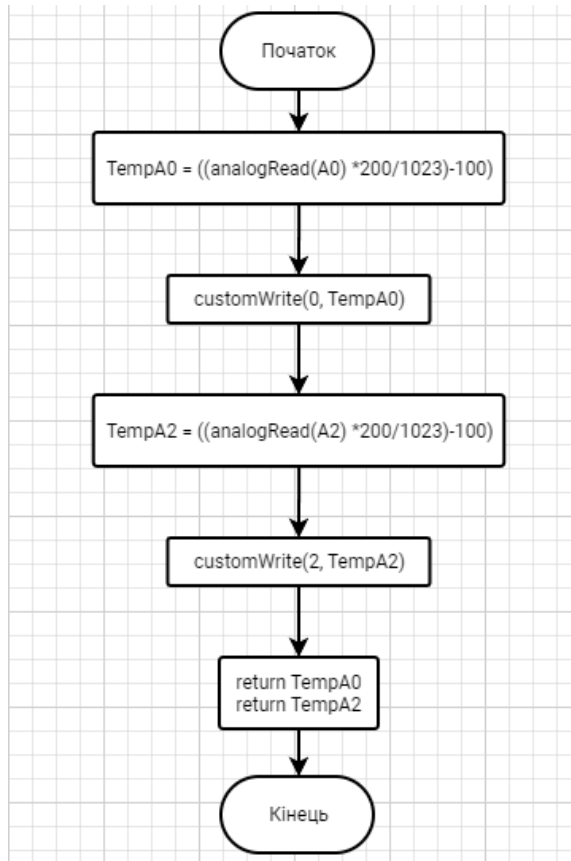


Рисунок 4.1 – Схема алгоритму функції Temp()

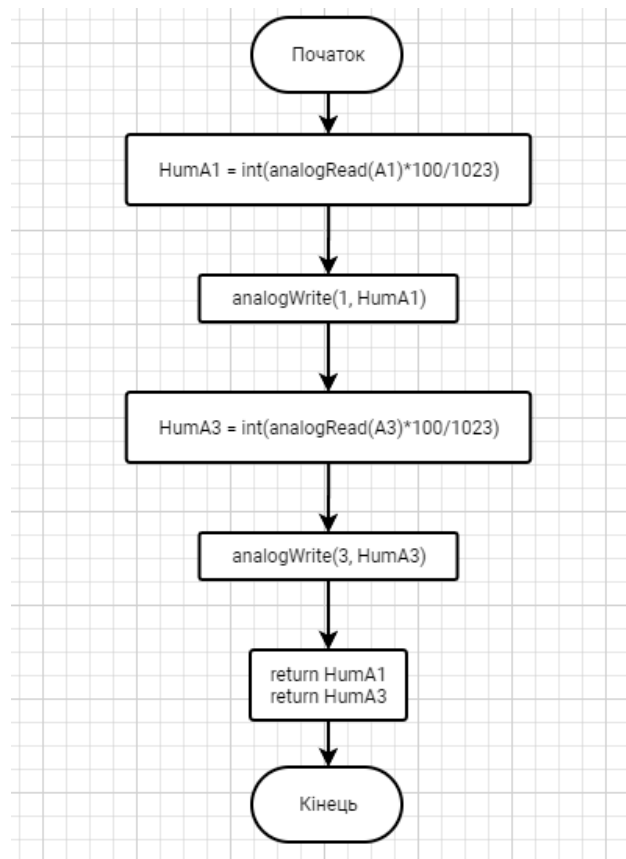


Рисунок 4.2 – Схема алгоритму функції Hum()

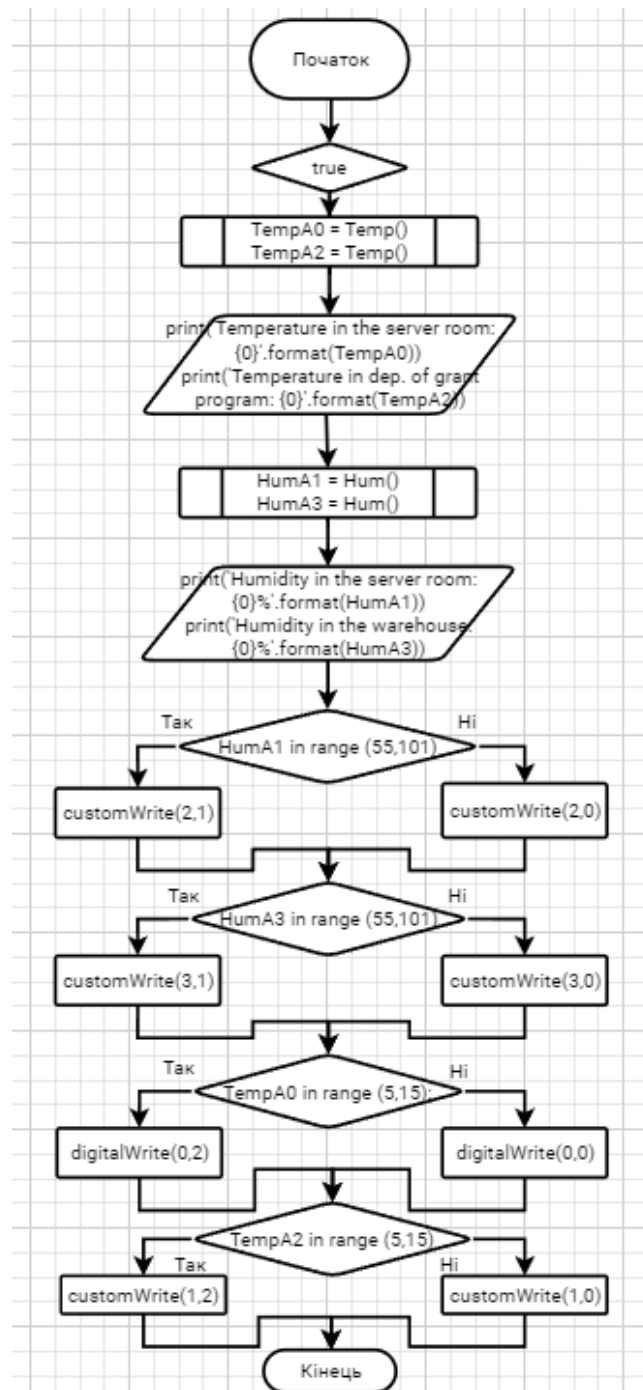


Рисунок 4.3 – Схема алгоритму функції main()

Програмі, яка зроблена на мові Python і буде працювати на Raspberry Pi, спочатку необхідно перевести отримані дані з датчиків температури і вологості повітря у градуси Цельсія і відсотки вологості відповідно, потім потрібно вивести ці дані використовуючи функцію `printf` і в кінці при певних значеннях температури та вологості слід увімкнути стельовий вентилятор і осушувач повітря.

Принцип роботи сценаріїв другого програмного забезпечення буде полягати у виконанні наступних вимог:

- після спрацювання датчика вогню необхідно увімкнути спринклер і трап для зливу води. Сирена повинна бути увімкнена у всіх відділах підприємства;
- після спрацювання датчика руху необхідно увімкнути камеру відеоспостереження і сирену;
- після спрацювання датчика вуглекислого газу необхідно увімкнути стельовий вентилятор;
- якщо температура у відділі по роботі з клієнтом буде занадто висока потрібно увімкнути кондиціонер;
- якщо до RFID зчитувача піднесена RFID картка з правильним ідентифікатором необхідно відчинити розумний замок;
- якщо будь-який датчик перестав працювати необхідно вимкнути пристрої, які були увімкнені після його спрацювання.

4.2.3 Опис і обґрунтування вибору методу організації вхідних та вихідних даних

Вхідні дані Raspberry Pi отримує від датчиків температури і вологості повітря. У функціях Temp() і Hum() зазначені змінні TempAN і HumAN відповідно, де замість літери N пишеться номер аналогового порту плати, до якого підключений датчик. Вихідні дані переводяться у градуси Цельсія і відсотки вологості для змінних TempAN і HumAN у функції main() відповідно.

Друге програмне забезпечення також отримує вхідні дані з датчиків системи моніторингу IoT. При спрацюванні датчиків за сценарієм, який знаходиться на IoT сервері, будуть увімкнені певні IoT пристрої, які пов'язані з цими датчиками.

4.2.4 Опис і обґрунтування вибору складу технічних і програмних засобів

Для запуску та безперервної роботи першого програмного забезпечення буде достатньо тих технічних характеристик, які має Raspberry Pi B. Текст програми буде написаний на мові Python з використанням модулів gpio та time.

Друге програмне забезпечення буде знаходитись на сервері HP ProLiant DL380 Gen9 (4 LFF) [32], технічні характеристики якого дозволяють зберігати на ньому сценарії для спрацювання всіх IoT пристроїв. Редагувати створені сценарії зможуть провідні спеціалісти відділу технічної підтримки, користуючись офісними комп'ютерами від ZEVS PC 108 [33].

4.3 Опис розробленої програми

4.3.1 Загальні відомості

Задля того, щоб керувати IoT пристроями у системі моніторингу були розроблені два програмних забезпечення, які отримують інформацію ззовні від датчиків і вмикають або вимикають певні IoT пристрої.

4.3.2 Функціональне призначення

Перше ПЗ буде керувати лише осушувачами повітря і стельовими вентиляторами, а друге ПЗ буде працювати зі створеними сценаріями, які зберігаються на IoT сервері та керувати усіма іншими пристроями, які підключені до маршрутизатора. Перше ПЗ буде обмежено кількістю портів у Raspberry Pi B, через які до плати будуть підключатись стельові вентилятори, осушувачі повітря і датчики, а друге ПЗ буде обмежено кількістю IP, які маршрутизатор може виділити до підключених пристроїв.

4.3.3 Опис логічної структури програми

Перше ПЗ написано на мові Python, буде реалізоване у одному файлі main.py і складатиметься з 3 функцій (Temp(), Hum() і main()). Перші дві функції будуть отримувати дані з датчиків температури і вологості та переводити дані у градуси Цельсія і відсотки вологості повітря відповідно. У функції main() виводяться дані з датчиків на екран та будуть перевірятись наступні умови спрацювання стельових вентиляторів, якщо температура буде від 5 до 15 градусів Цельсія, і осушувачів повітря, якщо відсоток вологості повітря буде більший за 55%. Були імпортовані два необхідних модуля gpio та time, задля ідентифікації підключених пристроїв та

налаштування затримки на продовження роботи (додаток А). Працювати створене ПЗ буде на Raspberry Pi 4B під час робочого дня. Текст програми персонал відділу технічної підтримки буде викликати кожен день на початку робочого дня і вимикати його вже після закінчення робочого дня.

Друге ПЗ буде реалізоване через сценарії, які будуть зберігатись на сервері IoT. Кожен сценарій буде складатись з певних умов, при виконанні яких певні IoT пристрої, які підключені по мережі Wi-Fi до маршрутизатору Kupets_Home_Router, будуть змінювати свій стан. Доступ до створених сценаріїв буде мати персонал відділу технічної підтримки, підключившись до IoT серверу через працюючі ПК у відділі (рисунок 4.4).

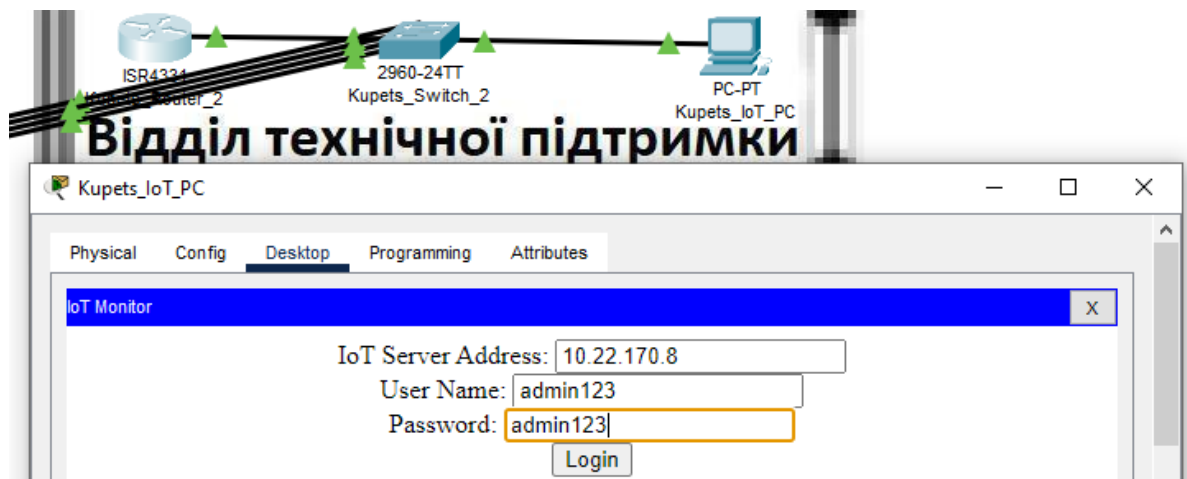


Рисунок 4.4 – Підключення до IoT серверу

За першим сценарієм при появі вогню у відділі повинен спрацювати датчик вогню, після чого увімкнуться спринклер, трап для зливу води і всі сирени підприємства (рисунок 4.5).

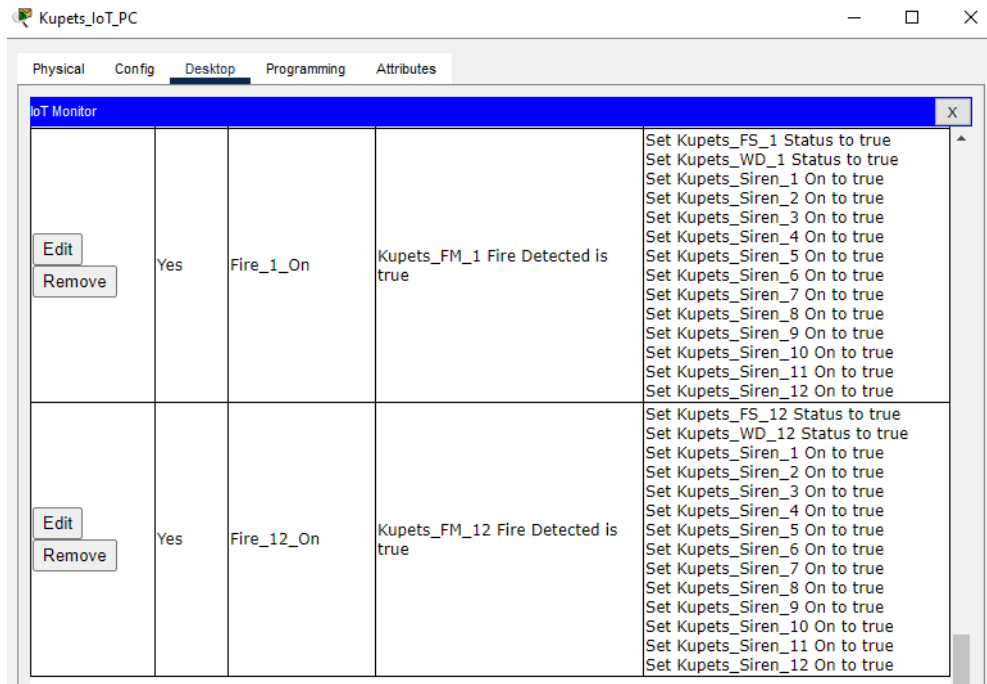


Рисунок 4.5 – Сценарії до всіх 12 відділів, у яких датчик вогню спрацьовує при наявності пожежі

Після усунення пожежі треба вимкнути всі IoT пристрої системи пожежогасіння, для цього був створений сценарій для кожного відділу (рисунок 4.6).

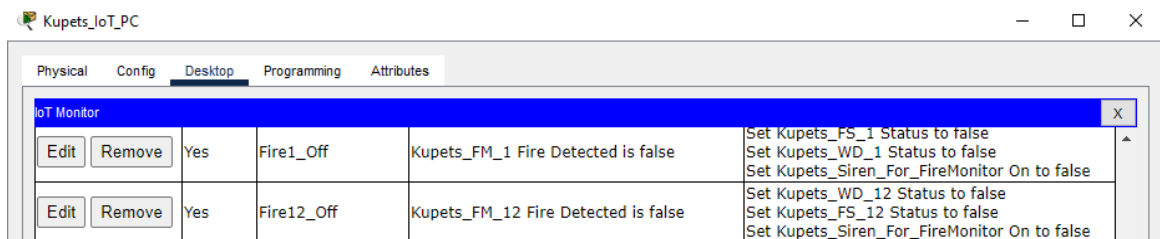


Рисунок 4.6 – Сценарії до всіх 12 відділів, у яких пристрої системи пожежогасіння перестають працювати після усунення пожежі

Сценарій для спрацювання кондиціонера у відділу по роботі з клієнтом при температурі більше ніж 15 градусів Цельсія зазначений на рисунку 4.7.

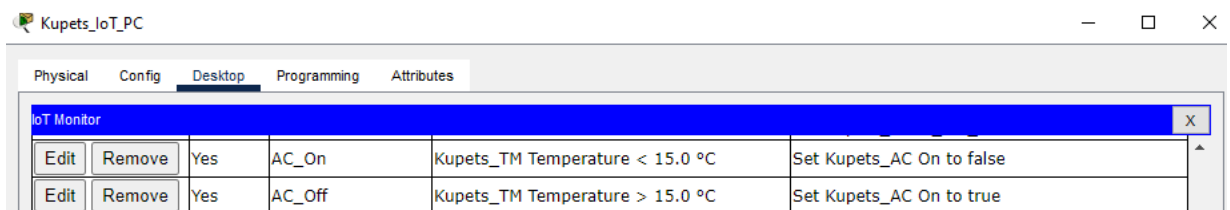
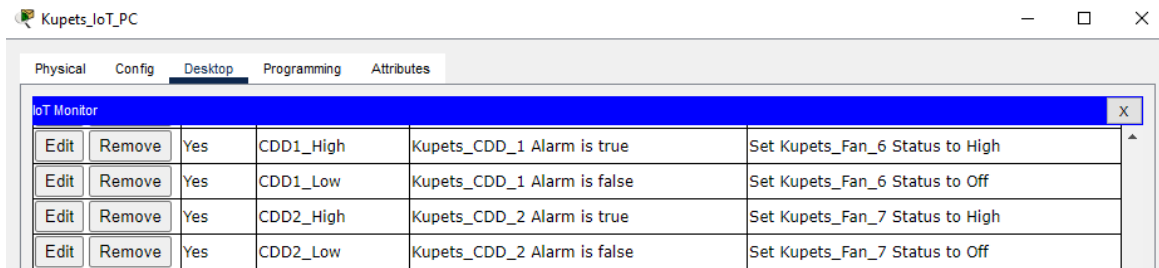


Рисунок 4.7 – Сценарій для спрацювання кондиціонера

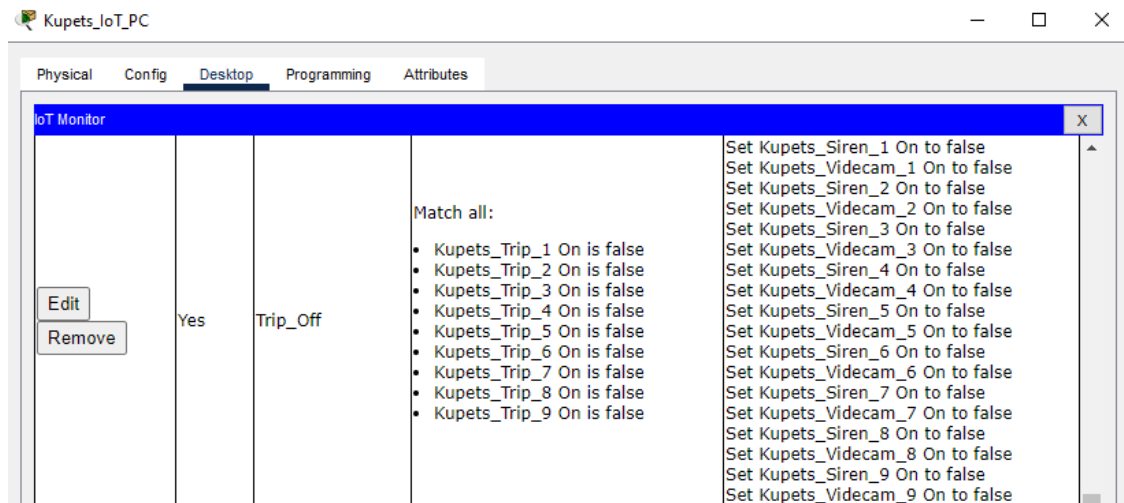
При спрацюванні датчика CO₂, у конференц залі або у приміщенні для наради, необхідно увімкнути стельові вентилятори (рисунок 4.8).



IoT Monitor					
Edit	Remove	Yes	CDD1_High	Kupets_CDD_1 Alarm is true	Set Kupets_Fan_6 Status to High
Edit	Remove	Yes	CDD1_Low	Kupets_CDD_1 Alarm is false	Set Kupets_Fan_6 Status to Off
Edit	Remove	Yes	CDD2_High	Kupets_CDD_2 Alarm is true	Set Kupets_Fan_7 Status to High
Edit	Remove	Yes	CDD2_Low	Kupets_CDD_2 Alarm is false	Set Kupets_Fan_7 Status to Off

Рисунок 4.8 – Сценарій, за яким при спрацюванні датчика вуглекислого газу стельові вентилятори починають працювати

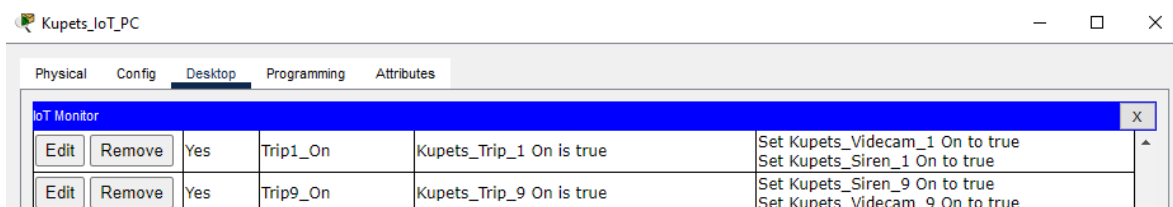
Зроблений сценарій на рисунку 4.9, за яким якщо датчики руху не працюють – камери відеоспостереження і сирени також вимкнені.



IoT Monitor					
Edit	Remove	Yes	Trip_Off	Match all: <ul style="list-style-type: none"> • Kupets_Trip_1 On is false • Kupets_Trip_2 On is false • Kupets_Trip_3 On is false • Kupets_Trip_4 On is false • Kupets_Trip_5 On is false • Kupets_Trip_6 On is false • Kupets_Trip_7 On is false • Kupets_Trip_8 On is false • Kupets_Trip_9 On is false 	Set Kupets_Siren_1 On to false Set Kupets_Videcam_1 On to false Set Kupets_Siren_2 On to false Set Kupets_Videcam_2 On to false Set Kupets_Siren_3 On to false Set Kupets_Videcam_3 On to false Set Kupets_Siren_4 On to false Set Kupets_Videcam_4 On to false Set Kupets_Siren_5 On to false Set Kupets_Videcam_5 On to false Set Kupets_Siren_6 On to false Set Kupets_Videcam_6 On to false Set Kupets_Siren_7 On to false Set Kupets_Videcam_7 On to false Set Kupets_Siren_8 On to false Set Kupets_Videcam_8 On to false Set Kupets_Siren_9 On to false Set Kupets_Videcam_9 On to false

Рисунок 4.9 – Сценарій, за яким камери і сирени не працюють, якщо датчик руху теж не працює

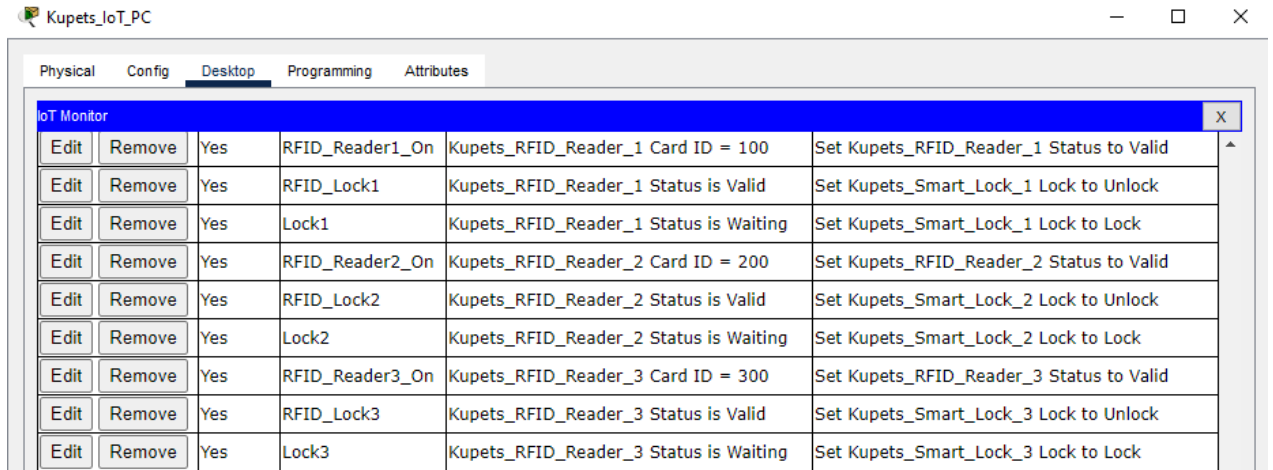
Для 9 датчиків руху необхідно розробити сценарії, згідно з якими камери відеоспостереження і сирени повинні увімкнутись (рисунок 4.10).



IoT Monitor					
Edit	Remove	Yes	Trip1_On	Kupets_Trip_1 On is true	Set Kupets_Videcam_1 On to true Set Kupets_Siren_1 On to true
Edit	Remove	Yes	Trip9_On	Kupets_Trip_9 On is true	Set Kupets_Siren_9 On to true Set Kupets_Videcam_9 On to true

Рисунок 4.10 – Сценарії, за якими при спрацюванні датчиків руху вмикаються камери відеоспостереження і сирени

Для 3 RFID зчитувачів і розумних замків необхідно зробити сценарії, у яких буде зазначено, що RFID картка з певним ідентифікатором повинна переводити RFID зчитувач у стан «Valid», чим змусить розумний замок відчинитись (рисунк 4.11).



Physical	Config	Desktop	Programming	Attributes	
IoT Monitor					
Edit	Remove	Yes	RFID_Reader1_On	Kupets_RFID_Reader_1 Card ID = 100	Set Kupets_RFID_Reader_1 Status to Valid
Edit	Remove	Yes	RFID_Lock1	Kupets_RFID_Reader_1 Status is Valid	Set Kupets_Smart_Lock_1 Lock to Unlock
Edit	Remove	Yes	Lock1	Kupets_RFID_Reader_1 Status is Waiting	Set Kupets_Smart_Lock_1 Lock to Lock
Edit	Remove	Yes	RFID_Reader2_On	Kupets_RFID_Reader_2 Card ID = 200	Set Kupets_RFID_Reader_2 Status to Valid
Edit	Remove	Yes	RFID_Lock2	Kupets_RFID_Reader_2 Status is Valid	Set Kupets_Smart_Lock_2 Lock to Unlock
Edit	Remove	Yes	Lock2	Kupets_RFID_Reader_2 Status is Waiting	Set Kupets_Smart_Lock_2 Lock to Lock
Edit	Remove	Yes	RFID_Reader3_On	Kupets_RFID_Reader_3 Card ID = 300	Set Kupets_RFID_Reader_3 Status to Valid
Edit	Remove	Yes	RFID_Lock3	Kupets_RFID_Reader_3 Status is Valid	Set Kupets_Smart_Lock_3 Lock to Unlock
Edit	Remove	Yes	Lock3	Kupets_RFID_Reader_3 Status is Waiting	Set Kupets_Smart_Lock_3 Lock to Lock

Рисунок 4.11 – Сценарії спрацювання 3 RFID зчитувачів і розумних замків

4.3.4 Використовувані технічні засоби

Для працездатності пешого програмного забезпечення необхідно купити Raspberry Pi B, оскільки ця модель Raspberry Pi має дешеву ціну і потрібну кількість пінів. Якщо персоналу певних відділів, де буде встановлено стельовий вентилятор або осушувач повітря, з'явиться потреба змінити умови увімкнення притроїв, необхідно буде підключити до певного Raspberry Pi у вільні HDMI і USB порти монітор і клавіатуру відповідно. Налаштування відбувається тільки у присутності спеціалісту з відділа технічної підтримки. Друге програмне забезпечення знаходиться на виділеному офісному ПК, на якому можна змінювати сценарії, які зберігаються на сервері TFTP, для спрацювання IoT пристроїв.

4.3.5 Виклик і завантаження

Щоб здійснити запуск першого програмного забезпечення необхідно під'єднати до Raspberry Pi будь-який монітор до HDMI порту і будь-яку клавіатуру до USB порту. Пінів у даної плати вистачає, для того, щоб додати нові прилади у майбутньому.

Сценарії другого програмного забезпечення можна запуснути і редагувати через ПК у відділі технічної підтримки. IP-адрес також буде достатньо для підключення нових IoT пристроїв у майбутньому.

4.4 Очікувані техніко-економічні показники

Запроваджений IoT комплекс допоможе підприємству заощадити кошти при виникненні аварійних ситуацій, негативні наслідки від яких можуть пошкодити технічне обладнання або збільшити можливість виникнення нещасних випадків на підприємстві. Однозначно дешевшим варіантом для підприємства буде заздалегідь приготуватись до можливих ситуації, що передують аварії, щоб швидко їх вирішити, чи навіть запобігти виникненню таких ситуацій.

4.5 Висновки

Для того, щоб правильно організувати тестування апаратного забезпечення системи моніторингу IoT, було розроблено сценарії для IoT приладів і текст програми для датчиків температури та вологості.

Створена модель системи моніторингу IoT у програмі RT допоможе знайти слабкі сторони комплексу IoT перед закупівлею технічного обладнання. Оскільки у теоретичних розділах було зазначено, що створена система моніторингу повинна швидко розпізнавати і реагувати на зовнішні загрози – будь-який повільний результат тестування IoT пристроїв буде не відповідати заданим очікуванням.

5 ЕКСПЕРИМЕНТАЛЬНИЙ РОЗДІЛ

5.1 Мета і умови експерименту

Перед тим, як запроваджувати систему моніторингу IoT слід протестувати її налаштовану модель у програмі RT. Під час тестування комплексу IoT можна буде побачити усі слабкі сторони побудованої моделі і виправити їх ще до початку купівлі IoT пристроїв. Тому, метою експериментів можна назвати пошук у моделі системи моніторингу IoT усіх можливих недоліків і їх усунення.

Перевірку і пошук недоліків необхідно провести у всіх зв'язках IoT пристроїв, а саме:

- комплекс IoT пристроїв системи пожежогасіння (датчик вогню, спринклер, трап для зливу води і сигналізацію);
- датчик руху, камеру відеоспостереження і сирену;
- датчик вуглекислого газу і стельовий вентилятор;
- RFID зчитувач і картку та розумний замок;
- кондиціонер;
- датчик температури і стельовий вентилятор;
- датчик вологості і осушувач повітря.

Буде перевірятись швидкість реагування IoT пристроїв на зовнішні загрози. Кожні зв'язки IoT пристроїв будуть тестуватись п'ять разів, задля зменшення ймовірності отримання неточного результату. Дані про тестування можна буде побачити у відповідних таблицях. Швидкість отримання сигналу буде вимірюватись у секундах. Якщо результат буде менше секунди – у таблицю буде записано «<1 секунди». Через те, що програма RT не може надати точний час зміни статусу IoT пристрої, було прийняте рішення для вимірювання швидкості спрацювання IoT пристроїв використовувати секундомір. Користуючись секундоміром важливо враховувати виникнення можливих похибок у вимірюванні швидкості 0,3 – 0,5 секунди. Задовільним результатом при тестуванні IoT приладів буде вважатись результат «<1 секунди» зміна стану IoT пристроїв. При незадовільному результаті тестування буде запропоновано два шляхи вирішення

проблеми: змінення умов спрацювання IoT пристроїв або корегування зв'язків IoT пристроїв з датчиками, які надають вхідні дані. У експерименті не приймали участь інші особи.

5.2 Опис методик експерименту кожних зв'язок IoT пристроїв

5.2.1 Система пожежогасіння

Комплекс IoT пристроїв системи пожежогасіння буде тестуватись за допомогою Kupets_Heating_Element. Щоб протестувати у моделі RT датчик вогню необхідно додати Heating Element і змінити його текст програми, з метою створення «пожежі», яку датчику вогню необхідно помітити (рисунок 5.1 – 5.2).



Рисунок 5.1 – Kupets_Heating_Element



Рисунок 5.2 – Змінений код Kupets_Heating_Element

Тестування буде проходити у кожному відділі підприємства. Буде зроблено п'ять спроб тестування у кожному відділі, де Heating Element буде знаходитись поруч з датчиком вогню, чим буде викликати спрацювання датчика і всіх IoT пристроїв системи пожежогасіння (рисунок 5.3 – 5.4).



Рисунок 5.3 – Підготовка до тестування системи пожежогасіння



Рисунок 5.4 – Момент спрацювання системи пожежогасіння

5.2.2 Датчик руху, камера відеоспостереження і сирена

За допомогою розроблених сценаріїв тестування датчика руху, при спрацюванні якого повині увімкнутись камера відеоспостереження і сирена, перевірка його працездатності буде проходити у кожному відділі підприємства. Щоб імітувати спрацювання датчика руху потрібно натиснути на нього у моделі, яка зроблена у програмі RT (рисунок 5.5 – 5.6).

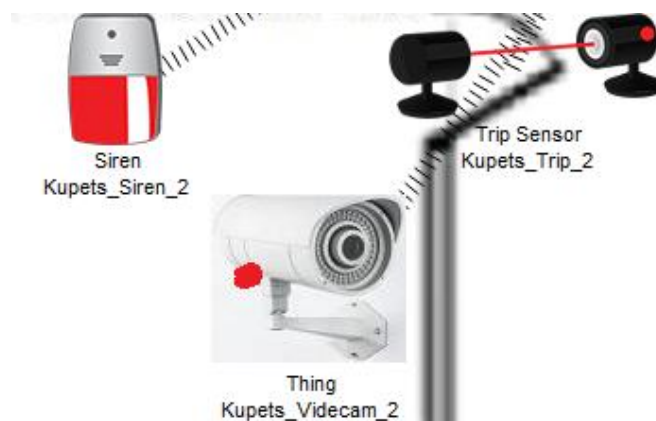


Рисунок 5.5 – Момент спрацювання двох IoT пристроїв після натискання на датчик руху

5.2.3 Датчик вуглекислого газу і стельовий вентилятор

Для того, щоб перевірити сценарій спрацювання датчика вуглекислого газу і стельового вентилятору потрібно буде додати до моделі «Old Car», оскільки тільки воно у програмі RT може підіймати рівень вуглекислого газу у повітрі (рисунок 5.6 – 5.7).

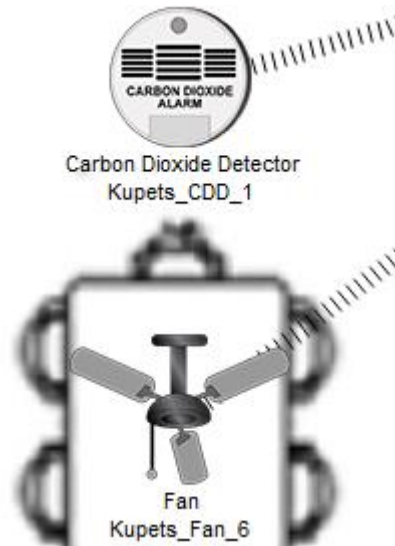


Рисунок 5.6 – Датчик вуглекислого газу і стельовий вентилятор у непрацюючому стані

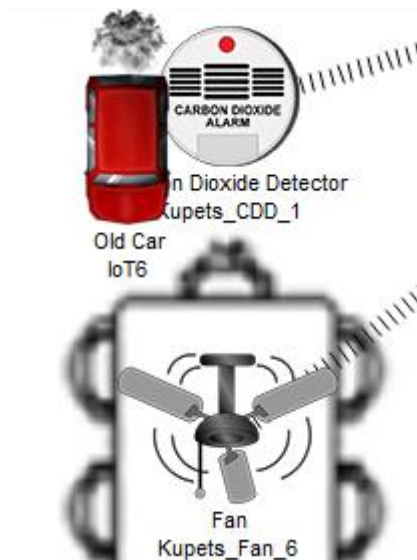


Рисунок 5.7 – Момент спрацювання датчика вуглекислого газу і стельового вентилятору

5.2.4 RFID зчитувач, RFID картка і розумний замок

За розробленими сценаріями, коли поруч з RFID зчитувачем знаходиться RFID картка з правильним ідентифікаційним номером – це змушує RFID зчитувач перейти у стан «Valid», після чого розумний замок відчиниться (рисунок 5.8 – 5.9).

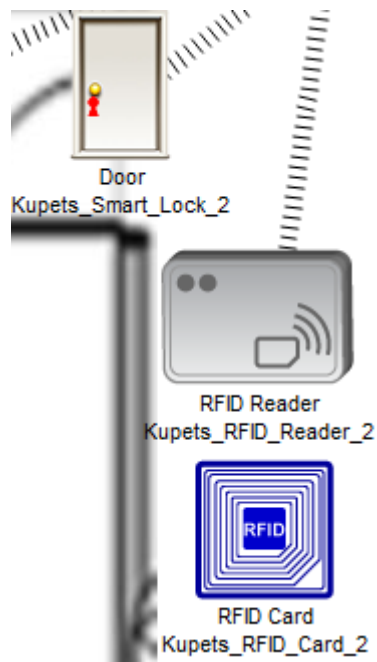


Рисунок 5.8 – RFID картка знаходиться далеко від RFID зчитувача

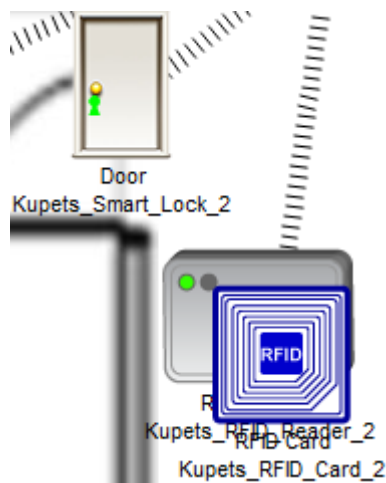


Рисунок 5.9 – Момент спрацювання RFID зчитувача

5.2.5 Кондиціонер

Якщо у відділі по роботі з клієнтом температура повітря підійметься вище норми (у даному випадку вище 15 градусів Цельсія) кондиціонер автоматично увімкнеться (рисунок 5.10 – 5.11).



Рисунок 5.10 – Кондиціонер вимкнений



Рисунок 5.11 – Кондиціонер працює

5.2.6 Датчик температури і стельовий вентилятор

Датчик температури щосекундно надає температуру у градусах Цельсія і якщо значення температури буде знаходитись між п'яти і п'ятнадцяти градусів – стельовий вентилятор почне працювати (рисунок 5.12 – 5.13).

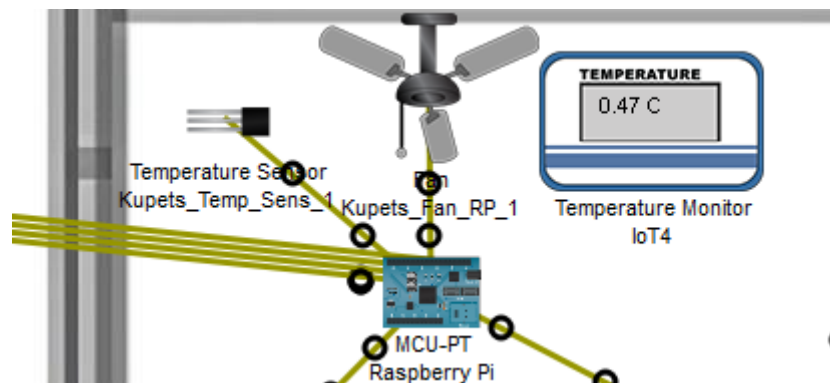


Рисунок 5.12 – Стельовий вентилятор вимкнений

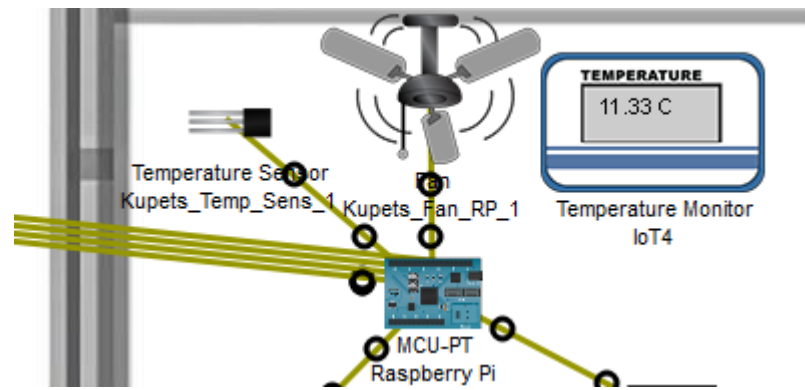


Рисунок 5.13 – Стельовий вентилятор працює

5.2.7 Датчик вологості і осушувач повітря

При відсотку вологості повітря нижче ніж 55 – осушувач повітря не повинен бути увімкнений. Якщо значення, яке передає датчик вологості, вище ніж 55 – осушувач повітря буде увімкнений (рисунок 5.14 – 5.15).

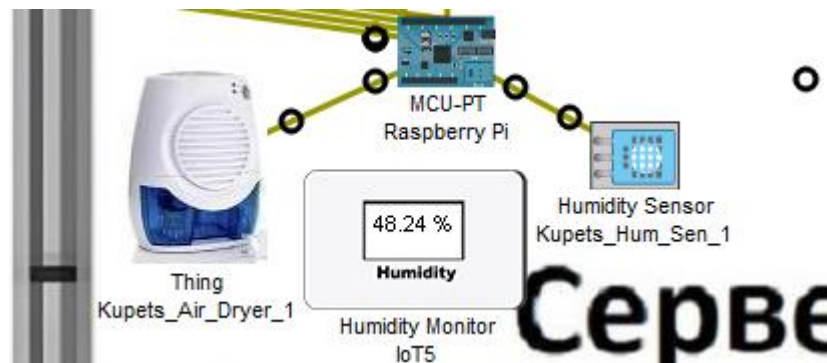


Рисунок 5.14 – Осушувач повітря вимкнений

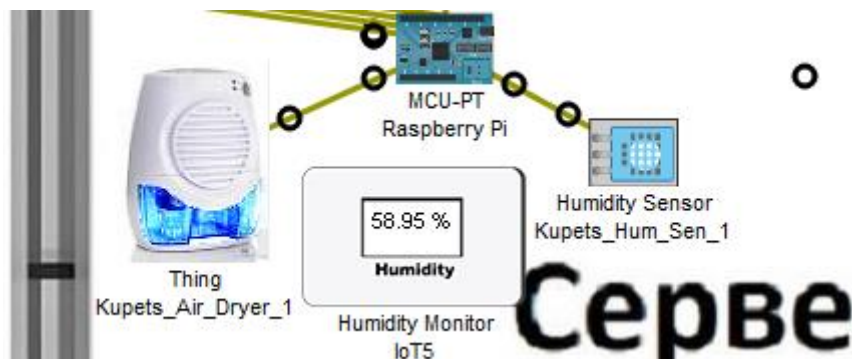


Рисунок 5.15 – Осушувач повітря увімкнений

5.3 Тестування системи моніторингу IoT

У таблиці 5.1 можна побачити тестування всіх IoT пристроїв.

Таблиця 5.1 – Тестування системи моніторингу IoT

№	Назва відділу	Зв'язка IoT пристроїв	Результат тестування зв'язки
1	Відділ по роботі з клієнтом	Система пожежігасіння	1 спроба – 1.9 секунди
			2 спроба – 1.5 секунди
			3 спроба – 1.7 секунди
			4 спроба – 1.6 секунди
			5 спроба – 1.5 секунди
		Датчик руху, камера відеоспостереження і сирена	1 спроба – 0.9 секунди
			2 спроба – 0.7 секунди
			3 спроба – 0.8 секунди
			4 спроба – 0.8 секунди
			5 спроба – 0.7 секунди
		Кондиціонер	1 спроба – 0.9 секунду
			2 спроба – 0.7 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.6 секунди
			5 спроба – 0.6 секунди
2	Відділ туризму	Система пожежігасіння	1 спроба – 1.8 секунди
			2 спроба – 1.5 секунди
			3 спроба – 1.6 секунди
			4 спроба – 1.6 секунди
			5 спроба – 1.6 секунди
		Датчик руху, камера відеоспостереження і сирена	1 спроба – 0.8 секунди
			2 спроба – 0.6 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.6 секунди
		Датчик температури і стельовий вентилятор	1 спроба – 0.9 секунди
			2 спроба – 0.7 секунди
			3 спроба – 0.7 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.6 секунди
3	Відділ грантових програм	Система пожежігасіння	1 спроба – 1.8 секунди
			2 спроба – 1.8 секунди

			3 спроба – 1.7 секунди		
			4 спроба – 1.5 секунди		
			5 спроба – 1.5 секунди		
		Датчик руху, камера відеоспостереження і сирена	1 спроба – 0.8 секунди		
			2 спроба – 0.7 секунди		
			3 спроба – 0.6 секунди		
			4 спроба – 0.5 секунди		
			5 спроба – 0.7 секунди		
		Датчик температури і стельовий вентилятор	1 спроба – 0.9 секунди		
			2 спроба – 0.6 секунди		
			3 спроба – 0.7 секунди		
			4 спроба – 0.7 секунди		
			5 спроба – 0.6 секунди		
		4	Відділ індустріального розвитку	Система пожежігасіння	1 спроба – 1.9 секунди
					2 спроба – 1.8 секунди
3 спроба – 1.8 секунди					
4 спроба – 1.5 секунди					
5 спроба – 1.5 секунди					
Датчик руху, камера відеоспостереження і сирена	1 спроба – 0.8 секунди				
	2 спроба – 0.8 секунди				
	3 спроба – 0.7 секунди				
	4 спроба – 0.5 секунди				
	5 спроба – 0.7 секунди				
Датчик температури і стельовий вентилятор	1 спроба – 0.6 секунди				
	2 спроба – 0.7 секунди				
	3 спроба – 0.5 секунди				
	4 спроба – 0.6 секунди				
	5 спроба – 0.7 секунди				
5	Бухгалтерія	Система пожежігасіння	1 спроба – 1.8 секунди		
			2 спроба – 1.6 секунди		
			3 спроба – 1.3 секунди		
			4 спроба – 1.4 секунди		
			5 спроба – 1.3 секунди		
		Датчик руху, камера	1 спроба – 0.7 секунди		

		відеоспостереження і сирена	2 спроба – 0.6 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.5 секунди
6	Відділ технічної підтримки	Система пожежігасіння	1 спроба – 1.8 секунди
			2 спроба – 1.5 секунди
			3 спроба – 1.5 секунди
			4 спроба – 1.6 секунди
			5 спроба – 1.5 секунди
		Датчик температури і стельовий вентилятор	1 спроба – 0.6 секунди
			2 спроба – 0.7 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.5 секунди
			5 спроба – 0.7 секунди
		Датчик вологості і осушувач повітря	1 спроба – 0.7 секунди
			2 спроба – 0.6 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.5 секунди
			5 спроба – 0.6 секунди
7	Серверна	Система пожежігасіння	1 спроба – 2 секунди
			2 спроба – 1.9 секунди
			3 спроба – 1.8 секунди
			4 спроба – 1.8 секунди
			5 спроба – 1.8 секунди
		Датчик руху, камера відеоспостереження і сирена	1 спроба – 0.8 секунди
			2 спроба – 0.5 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.6 секунди
		Датчик температури і стельовий вентилятор	1 спроба – 0.7 секунди
			2 спроба – 0.5 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.6 секунди

		Датчик вологості і осушувач повітря	1 спроба – 0.7 секунди
			2 спроба – 0.5 секунди
			3 спроба – 0.8 секунди
			4 спроба – 0.6 секунди
			5 спроба – 0.5 секунди
		RFID зчитувач, RFID картка і розумний замок	1 спроба – 0.5 секунди
			2 спроба – 0.7 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.5 секунди
			5 спроба – 0.6 секунди
8	Юридичний відділ	Система пожежігасіння	1 спроба – 1.7 секунди
			2 спроба – 1.4 секунди
			3 спроба – 1.4 секунди
			4 спроба – 1.5 секунди
			5 спроба – 1.6 секунди
		Датчик температури і стельовий вентилятор	1 спроба – 0.7 секунди
			2 спроба – 0.6 секунди
			3 спроба – 0.5 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.5 секунди
9	Директор	Система пожежігасіння	1 спроба – 2 секунди
			2 спроба – 1.8 секунди
			3 спроба – 1.7 секунди
			4 спроба – 1.8 секунди
			5 спроба – 1.8 секунди
		Датчик руху, камера відеоспостереження і сирена	1 спроба – 0.9 секунди
			2 спроба – 0.5 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.6 секунди
		RFID зчитувач, RFID картка і розумний замок	1 спроба – 0.7 секунди
			2 спроба – 0.5 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.5 секунди

			5 спроба – 0.8 секунди
10	Конференц зал	Система пожежігасіння	1 спроба – 1.5 секунди
			2 спроба – 1.4 секунди
			3 спроба – 1.3 секунди
			4 спроба – 1.1 секунди
			5 спроба – 1.2 секунди
		Датчик вуглекислого газу і стельовий вентилятор	1 спроба – 0.8 секунди
			2 спроба – 0.7 секунди
			3 спроба – 0.8 секунди
			4 спроба – 0.5 секунди
			5 спроба – 0.6 секунди
11	Склад	Система пожежігасіння	1 спроба – 2.1 секунди
			2 спроба – 1.8 секунди
			3 спроба – 1.9 секунди
			4 спроба – 1.8 секунди
			5 спроба – 1.7 секунди
		Датчик руху, камера відеоспостереження і сирена	1 спроба – 0.9 секунди
			2 спроба – 0.8 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.5 секунди
		Датчик вологості і осушувач повітря	1 спроба – 0.7 секунди
			2 спроба – 0.5 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.5 секунди
		RFID зчитувач, RFID картка і розумний замок	1 спроба – 0.8 секунди
			2 спроба – 0.6 секунди
			3 спроба – 0.6 секунди
			4 спроба – 0.7 секунди
			5 спроба – 0.5 секунди
12	Приміщення для наради	Система пожежігасіння	1 спроба – 1.5 секунди
			2 спроба – 1.3 секунди
			3 спроба – 1.3 секунди

			4 спроба – 1.2 секунди
			5 спроба – 1.4 секунди
		Датчик вуглекислого газу і стельовий вентилятор	1 спроба – 0.8 секунди
			2 спроба – 0.7 секунди
			3 спроба – 0.7 секунди
			4 спроба – 0.5 секунди
			5 спроба – 0.6 секунди

5.4 Аналіз експериментальних досліджень у порівнянні з теоретичними цілями

Результати тестувань системи моніторингу IoT показали, що практично всі зв'язки IoT пристроїв у кожному відділі реагують на зовнішні загрози дуже швидко, окрім системи пожежогасіння. Така затримка у активації IoT пристроїв системи пожежогасіння може створюватись через дві можливі причини:

- симуляція РТ не може миттєво обробити запит на увімкнення дванадцяти сирен при спрацюванні датчика вогню;
- сценарії спрацювання датчика руху також задіюють ті самі сирени, які пов'язані зі сценаріями спрацювання датчика вогню.

Пропонується наступний варіант оптимізації системи пожежогасіння – залишити у системі моніторингу IoT дев'ять сирен, які використовуються у сценаріях спрацювання датчика руху і замінити решту сирен, на дві гучні сирени (одна буде знаходитись на першому поверсі будівлі, інша – на другому), які увімкнуться при спрацюванні датчика вогню. При цьому варіанті вмикатись будуть лише дві сирени одночасно, замість дванадцяти.

На рисунку 5.16 можна побачити дві сирени, які будуть працювати при увімкненні датчика вогню.

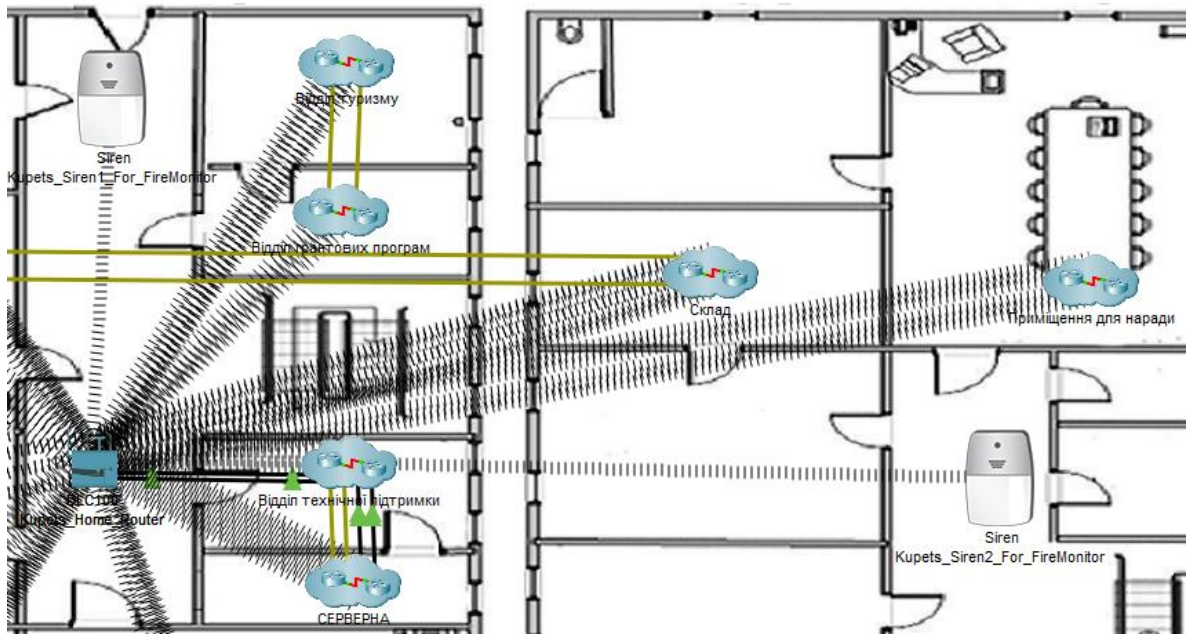


Рисунок 5.16 – Дві сирени системи пожежогасіння

Сценарії, які стосуються системи пожежогасіння будуть змінені (рисунок 5.17).

Actions	Enabled	Name	Condition	Actions
<input type="button" value="Edit"/> <input type="button" value="Remove"/>	Yes	Fire1_On	Kupets_FM_1 Fire Detected is true	Set Kupets_FS_1 Status to true Set Kupets_WD_1 Status to true Set Kupets_Siren1_For_FireMonitor On to true Set Kupets_Siren2_For_FireMonitor On to true
<input type="button" value="Edit"/> <input type="button" value="Remove"/>	Yes	Fire12_On	Kupets_FM_12 Fire Detected is true	Set Kupets_WD_12 Status to true Set Kupets_FS_12 Status to true Set Kupets_Siren1_For_FireMonitor On to true Set Kupets_Siren2_For_FireMonitor On to true

Рисунок 5.17 – Змінені сценарії для всіх двадцяти датчиків вогню

Тепер необхідно знову протестувати п'ять разів систему пожежогасіння у кожному відділі. Результати тестування можна побачити у таблиці 5.2.

Таблиця 5.2 – Повторне тестування системи пожежогасіння

№	Назва відділу	Результат тестування системи пожежогасіння
1	Відділ по роботі з клієнтом	1 спроба – 1 секунда
		2 спроба – 0.8 секунди
		3 спроба – 0.7 секунди
		4 спроба – 0.8 секунди
		5 спроба – 0.6 секунди

2	Відділ туризму	1 спроба – 0.8 секунди
		2 спроба – 0.5 секунди
		3 спроба – 0.7 секунди
		4 спроба – 0.8 секунди
		5 спроба – 0.7 секунди
3	Відділ грантових програм	1 спроба – 0.8 секунди
		2 спроба – 0.6 секунди
		3 спроба – 0.7 секунди
		4 спроба – 0.7 секунди
		5 спроба – 0.7 секунди
4	Відділ індустріального розвитку	1 спроба – 0.9 секунди
		2 спроба – 0.7 секунди
		3 спроба – 0.6 секунди
		4 спроба – 0.5 секунди
		5 спроба – 0.7 секунди
5	Бухгалтерія	1 спроба – 0.8 секунди
		2 спроба – 0.7 секунди
		3 спроба – 0.7 секунди
		4 спроба – 0.7 секунди
		5 спроба – 0.6 секунди
6	Відділ технічної підтримки	1 спроба – 0.6 секунди
		2 спроба – 0.8 секунди
		3 спроба – 0.7 секунди
		4 спроба – 0.5 секунди
		5 спроба – 0.7 секунди
7	Серверна	1 спроба – 0.9 секунди
		2 спроба – 0.7 секунди
		3 спроба – 0.5 секунди
		4 спроба – 0.6 секунди
		5 спроба – 0.8 секунди
8	Юридичний відділ	1 спроба – 0.8 секунди
		2 спроба – 0.7 секунди
		3 спроба – 0.5 секунди
		4 спроба – 0.5 секунди

		5 спроба – 0.6 секунди
9	Директор	1 спроба – 0.8 секунди
		2 спроба – 0.5 секунда
		3 спроба – 0.6 секунди
		4 спроба – 0.5 секунди
		5 спроба – 0.7 секунди
10	Конференц зал	1 спроба – 0.9 секунди
		2 спроба – 0.7 секунди
		3 спроба – 0.5 секунди
		4 спроба – 0.6 секунди
		5 спроба – 0.7 секунди
11	Склад	1 спроба – 0.9 секунди
		2 спроба – 0.7 секунди
		3 спроба – 0.8 секунди
		4 спроба – 0.7 секунди
		5 спроба – 0.6 секунди
12	Приміщення для наради	1 спроба – 0.7 секунди
		2 спроба – 0.8 секунди
		3 спроба – 0.7 секунди
		4 спроба – 0.5 секунди
		5 спроба – 0.6 секунди

Досліджено реагування системи пожежогасіння на пожежу після заміни сценарію спрацювання, що показало відсутність затримки, яка виникала до зміни сценарію під час перевірки працездатності датчика вогню.

Тепер система моніторингу IoT працює згідно тих очікувань, які зазначались у теоретичному розділі, з-за того, що усі зв'язки IoT пристроїв можуть швидко реагувати на зовнішні загрози.

5.5 Висновки

Розроблена система моніторингу IoT повністю задовільняє усі вимоги, які були зазначені у теоретичному розділі, а саме швидке спрацювання і запобігання

руйнівним наслідкам від загрози, задля протидії якої вона запроваджувалась. Під час тестування системи моніторингу IoT було виявлено, що система пожежогасіння реагує на зовнішню загрозу повільніше будь-якої іншої запровадженої зв'язки IoT пристроїв. Тому, було прийняте рішення змінити сценарій спрацювання системи пожежогасіння, видалив з нього одночасну активацію сирен з усіх відділів. Встановлені дві сирени у холі першого і другого поверхів можуть стати альтернативою для сповіщення людей, які знаходяться у будівлі підприємства, про спрацювання системи пожежогасіння.

ВИСНОВКИ

У кваліфікаційній роботі було вирішено наукове завдання – створення IoT комплексу для підприємства «Агентства розвитку Дніпра» і тестування швидкості реагування на зовнішні загрози IoT пристроїв, які входять до системи моніторингу.

Під час розробки теоретичного розділу, було обґрунтоване додання у систему моніторингу наступних зв'язків IoT пристроїв:

- система пожежогасіння (датчик вогню, спринклер, сирена і трап для зливу води);
- датчик руху і камера відеоспостереження;
- датчик вуглекислого газу і стельовий вентилятор;
- RFID зчитувач, RFID картка і розумний замок;
- кондиціонер, який реагує на підвищення температури повітря;
- датчик температури і стельовий вентилятор;
- датчик вологості і осушувач повітря.

Були обрані дешеві пристрої для системи моніторингу, які повністю відповідають вимогам, які були зазначені у розділі синтезу системи моніторингу.

Для кожної зв'язки IoT пристроїв системи моніторингу було розроблено ПЗ, яке було розділено на дві частини. Перше ПЗ написано на мові Python для «Raspberry Pi комплексу». Друге ПЗ реалізоване через сценарії, які будуть зберігатись на сервері IoT.

Під час тестування системи моніторингу IoT було помічено затримку у спрацюванні системи пожежогасіння. Під час повторного тестування системи пожежогасіння було досліджено, що у момент спрацювання сценарію, у якому зазначена велика кількість IoT пристроїв, які також використовуються і у інших сценаріях, може з'явитись певна затримка, яка не дозволить IoT пристроям швидко переходити у увімкнений стан після спрацювання датчика, з яким вони пов'язані. Після зміни сценарію спрацювання системи пожежогасіння IoT і Raspberry Pi комплекси працювали без помітних затримок, що відповідає очікуванням, які були зазначені у теоретичному розділі.

ПЕРЕЛІК ПОСИЛАНЬ

1. 70 IoT Statistics to Unveil the Past, Present, and Future of IoT [Електронний ресурс]: <https://learn.g2.com/iot-statistics>
2. Купець, Є.С. Комп'ютерна система «Агентства розвитку Дніпра» з опрацюванням побудови та налаштування корпоративної мережі / Є.С. Купець ; Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2022. – 9 с.
3. ML Model Monitoring: Practical guide to boosting model performance [Електронний ресурс]: <https://www.aporia.com/learn/machine-learning-model/model-monitoring-101/#:~:text=What%20is%20ML%20Model%20Monitoring,and%20in%20real%2Dtime%20deployment.>
4. Купець, Є.С. Комп'ютерна система «Агентства розвитку Дніпра» з опрацюванням побудови та налаштування корпоративної мережі / Є.С. Купець ; Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2022. – 61 с.
5. SCADA система, що це таке [Електронний ресурс]: <https://indusoft.com.ua/blog/2019/10/29/scada-systema-cho-to-jeto-takoe/>
6. Як працює Інтернет речей: суть технології та її застосування в сучасному світі [Електронний ресурс]: <https://focus.ua/uk/digital/521863-kak-rabotaet-internet-veshchey-sut-tehnologii-i-ee-primenenie-v-sovremennom-mire>
7. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 [Електронний ресурс]: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>
8. About the ACM Digital Library [Електронний ресурс]: <https://dl.acm.org/about#:~:text=The%20ACM%20Digital%20Library%20is,technical%20magazines%2C%20newsletters%20and%20books.>
9. АНАЛІТИЧНА ДОВІДКА про пожежі та їх наслідки в Україні за 12 місяців 2022 року [Електронний ресурс]: <https://idundcz.dsns.gov.ua/upload/1/6/0/8/6/7/7/analychna-dovidka-pro-pojeji-122022.pdf>

10. Вогнегасна речовина FK-5-1-12 [Електронний ресурс]: <https://universalexport.com.ua/products/vognegasna-rechovina-fk-5-1-12>

11. Electrical and Computer Engineering [Електронний ресурс]: <https://www.ece.cmu.edu/news-and-events/story/2021/06/hot-electronics.html#:~:text=While%20many%20electronics%20are%20designed,down%20to%20avoid%20this%20risk>

12. Купець, Є.С. Комп'ютерна система «Агентства розвитку Дніпра» з опрацюванням побудови та налаштування корпоративної мережі / Є.С. Купець ; Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2022. – 29 с.

13. Why are smart locks actually safer than traditional locks? [Електронний ресурс]: <https://keymitt.com/blogs/keymitt-blog/why-are-smart-locks-actually-safer-than-traditional-locks>

14. Бездротовий Ajax датчик вогню та диму з сиреною FireProtect 2 RB (Heat/Smoke) Jeweller [Електронний ресурс]: https://arduino.ua/prod5873-bezdrotovii-ajax-datchik-vognu-ta-dimy-z-sirenou-fireprotect-2-rb-heatsmoke-jeweller?utm_source=GoogleMerchant&utm_medium=Merchant&utm_campaign=Google&utm_content=AJA114

15. Спринклер ZSTX-15 [Електронний ресурс]: <https://shop-security.com.ua/sprinkler-zstx-15/>

16. Wi-fi електропривод керування краном TuYa Smart Water/Gas [Електронний ресурс]: <https://rozetka.com.ua/259596126/p259596126/characteristics/>

17. КОМПЛЕКТ СИГНАЛІЗАЦІИ ІОТ-HUB10WG [Електронний ресурс]: <https://ccd.dn.ua/komplekt-signalizacii-iot-hub10wg.html>

18. Характеристики Бездротовий датчик руху Ajax MotionProtect White (000001149) [Електронний ресурс]: https://rozetka.com.ua/ua/ajax_motionprotect_white_000005328/p7320826/characteristics/

19. Вулична IP камера 8МП WiFi QeaRim P6 IPC360 Home live Outdoor WiFi PTZ 3840x2160 [Електронний ресурс]: <https://shok.com.ua/product/ulychnaya-ip-kamera-8mp-wifi-qearim-p6-ipc360-home-live-outdoor-wifi-ptz-3840h2160-ulychnaya>

povorotnaya/?utm_source=Google%20Shopping&utm_campaign=Huntsman%20Feed&utm_medium=cpc&utm_term=6238&gad_source=1&gclid=Cj0KCQiA3uGqBhDdARIsAFeJ5r1c0kQezAcLBT5H18CX3Vm06LIKiQxou2rd9Z0OJqN_6iot65MzDcIaAvseEALw_wcB

20. Смарт замок TTLOCK BOSS [Електронний ресурс]:
https://locksmith.com.ua/product/ttlock-boss/?utm_source=google_shopping&utm_medium=cpc&utm_campaign=lock_ru&utm_source=google&utm_medium=cpc&utm_campaign=locksmith_torg&utm_term=&gad_source=1&gclid=Cj0KCQiA3uGqBhDdARIsAFeJ5r1WA-Bru0c9jVne1d06W56fMsPGOVyUc8M0Yg_nEhZNd-meuYpeNGwaAsAaEALw_wcB

21. Интеллектуальный контролер доступа Wi-Fi Wiegand 1D 2D IC/зчитувач NFC Контролер доступа до QR-коду [Електронний ресурс]:
https://prom.ua/p1855356383-intellektualnyj-kontroller-dostupa.html?srsltid=AfmBOops-_5XqTv4hliYDFPiA5ShfKAjD5hccFRWMWugJ8jdvht8FjZNVrI

22. Термогігрометр з датчиком вимірювання CO2 PTH-5 (PTH5-12) [Електронний ресурс]: https://sbtr.com.ua/ua/p1344762619-termogigrometr-datchikom-izmereniya.html?gad_source=1&gclid=CjwKCAiAjfyqBhAsEiwA-UdzJBTjQli8Sfx6seGwm4--ZiK0Xtti9sWpRDIYt6LTFvPszrsiosz5NBoCk_4QAvD_BwE

23. Hunter 54" Nickel LED Indoor Smart WI-FI Ceiling Fan [Електронний ресурс]:
https://www.ebay.com/itm/155672750021?_trkparms=amclksrc%3DITM%26aid%3D1110025%26algo%3DHOMESPLICE.COMPOSITELISTINGS%26ao%3D1%26asc%3D20220405142716%26meid%3Dcf8d1a77b4564e4d84aa6611843b7cd8%26pid%3D101506%26rk%3D3%26rkt%3D25%26sd%3D225760519075%26itm%3D155672750021%26pmt%3D0%26noa%3D1%26pg%3D3458402%26algv%3DAIgoIndex5SimRanker%26brand%3DHunter&_trksid=p3458402.c101506.m1851

24. Кондиціонер TCL TAC-09CHSA/XAB1 On-Off WI-FI Ready [Електронний ресурс]: <https://tcl-aircon.ua/catalog/pobutovi-konditsioneri/konditsioner-tcl-tac-09chsa-xab1-on-off-wi-fi-ready/>
25. RASPBERRY PI MODEL B [Електронний ресурс]: <https://docs.rs-online.com/6403/0900766b8127da4b.pdf>
26. Характеристики Міжмережевий екран Cisco SB RV110W Wireless N VPN Firewall (RV110W-E-G5-K9) [Електронний ресурс]: <https://rozetka.com.ua/ua/256467881/p256467881/characteristics/>
27. Модуль температури та вологості DHT11 зі світлодіодом [Електронний ресурс]: <https://prom.ua/ua/p2030660536-modul-temperature-vlazhnosti.html>
28. Стельовий вентилятор Westinghouse Lighting 7217000 [Електронний ресурс]: <https://izi.ua/uk/p-85498767-steloviy-ventilyator-westinghouse-lighting-7217000>
29. Осушувач повітря USB [Електронний ресурс]: <https://izi.ua/p-75976992-osushitel-vozdukha-usb>
30. Характеристики Умная розетка Tuuya Wi-Fi, EU (HS080419) [Електронний ресурс]: https://rozetka.com.ua/tuuya_hs080419/p320553907/characteristics/
31. USB WiFi (802.11b/g/n) модуль з антеною для Raspberry Pi [Електронний ресурс]: <https://raspberrypi.com/p/usb-wifi-802-11bgn-module-with-antenna-for-raspberry-pi/#!prettyPhoto>
32. Сервер HP ProLiant DL380 [Електронний ресурс] : <https://servak.com.ua/servers/servera-hp-gen9/server-hp-proliant-dl380-gen9-4-lff.html>
33. ZEVS PC 108 [Електронний ресурс] : https://uastore.com.ua/products/nedorogoj-covremennyj-ofisnyj-pk-zevs-pc108-2-yadra-500gb--4gb-ram?gclid=CjwKCAjwTlaVBhBkEiwAsr7-c8APNU4M4nFjJEsaHeN_k0cwl6K0AsnVCUbQtMAYqiJZekdqjUKnaRoCmSQQAvD_BwE

Додаток А

Текст програми для керування стельовими вентиляторами і осушувачами повітря

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ТЕКСТ ПРОГРАМИ ДЛЯ КЕРУВАННЯ СТЕЛЬОВИМИ
ВЕНТИЛЯТОРАМИ І ОСУШУВАЧАМИ ПОВІТРЯ

Текст програми

804.02070743.23012-01 12 01

Листів 7

АНОТАЦІЯ

Даний документ містить текст програми, який написан на мові Python для Raspberry Pi, завдяки якому забезпечується робота усіх стельових вентиляторів і осушувачів повітря у системі моніторингу IoT. У тексті програми наведено дві функції: Temp() і Hum(), які викликаються у main().

ЗМІСТ

1. Текст програми

98

1 ТЕКСТ ПРОГРАМИ

```
from gpio import *
from time import *
import time
#Імпорт важливих функцій з двох модулів
def Temp():
#Функція, яка переводить дані з датчиків температури у градуси Цельсія
    TempA0 = ((analogRead(A0) *200/1023)-100)#Змінна першого датчику температури
    customWrite(0, TempA0)
    TempA2 = ((analogRead(A2) *200/1023)-100)#Змінна другого датчику температури
    customWrite(2, TempA2)
    return TempA0
    return TempA2
#Повернення даних з датчиків температури у градусах Цельсія
def Hum():
#Функція, яка переводить дані з датчиків вологості у відсотки вологості у повітрі
    HumA1 = int(analogRead(A1)*100/1023)#Змінна першого датчику вологості
    analogWrite(1, HumA1)
    HumA3 = int(analogRead(A3)*100/1023)#Змінна другого датчику вологості
    analogWrite(3, HumA3)
    return HumA1
    return HumA3
#Повернення даних з датчиків вологості у відсотках вологості у повітрі
def main():
#Функція main, у якій виводиться на екран дані з усіх датчиків і прописується умови, для
спрацювання вентиляторів і осушувачів повітря
    while True:
        #Початок циклу, який після закінчення роботи повернеться до початку
        TempA0 = Temp()#Отримання даних з датчиків температури
        TempA2 = Temp()
        print('Temperature in the server room: {}'.format(TempA0))#Виведення на екран
температури
        print('Temperature in dep. of grant program: {}'.format(TempA2))
        HumA1 = Hum()#Отримання даних з датчиків вологості
```

```

HumA3 = Hum()
print('Humidity in the server room: {0}%'.format(HumA1))#Виведення на екран
відсотка вологості
print('Humidity in the warehouse: {0}%'.format(HumA3))
if HumA1 in range (55,101):
    customWrite(2,1)
else:
    customWrite(2,0)
if HumA3 in range (55,101):
    customWrite(3,1)
else:
    customWrite(3,0)
#Якщо відсоток вологості у повітрі більше ніж 55 - вмикається осушувач повітря
if TempA0 in range (5,15):
    digitalWrite(0,2)
else:
    digitalWrite(0,0)
if TempA2 in range (5,15):
    customWrite(1,2)
else:
    customWrite(1,0)
#Якщо значення температури знаходиться між 5 і 15 - вмикається вентилятор
delay(1000)
#Перед поверненням до початку цикла while - відбудеться затримка у одну
секунду

if __name__ == "__main__":
    main()
#Запуск функції main

```