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 бакалавра

**студента** Грачова Дмитра Сергійовича
(ПІБ)
**академічної групи** 123-20-2
(шифр)
**спеціальності** 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

**на тему** "IoT система складського приміщення підприємства LANDLORD "
(назва за наказом ректора)

| **Керівники** | **Прізвище, ініціали** | **Оцінка за шкалою** | | **Підпис** |
|---|---|---|---|---|
| | | **рейтинговою** | **інституційною** | |
| кваліфікаційної роботи | проф. Олевський В.І. | | | |
| спеціальної частини | проф. Олевський В.І. | | | |
| розділів: | | | | |
| розробка апаратної частини | доц. Ткаченко С.М. | | | |
| розробка корпоративної мережі | ас. Бешта Л.В. | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент** | | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | проф. Цвіркун Л.І. | | | |

**Дніпро**
**2024**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

*"25" січня 2024 року*

# ЗАВДАННЯ
## на кваліфікаційну роботу
## ступеня бакалавр

**студента** Грачова Д.С. **академічної групи** 123-20-2
(прізвище та ініціали) (шифр)

**спеціальності** 123 «Комп'ютерна інженерія»

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

**на тему** " IoT система складського приміщення підприємства LANDLORD "

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Стан питання та постановка завдання | На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання | 10.05.2024 |
| Розробка апаратної частини | На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи | 17.05.2024 |
| Розробка корпоративної мережі | Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі | 24.05.2024 |
| Розробка компонента системи | Виконується детальна розробка компонента системи | 31.05.2024 |

**Завдання видано** _____ проф. Олевський В.І.
(підпис керівника) (прізвище, ініціали)

**Дата видачі** 25.01.2024

**Дата подання до екзаменаційної комісії** 02.07.2024

**Прийнято до виконання** _____ Грачов Д.С.

# РЕФЕРАТ

Пояснювальна записка : 86 с., 52 рис., 8 табл., 6 дод., 27 джерел.

КОРПОРАТИВНА МЕРЕЖА, IOT, СКЛАД, LANDLORD, МОНІТОРИНГ, БЕЗПЕКА, ДОСТУП.

Об'єкт розробки – IoT система складського приміщення підприємства Landlord з опрацюванням побудови, налаштуваннями безпеки приміщення, контролю доступу та моніторингу середовища.

Мета роботи – створення IoT системи для складського приміщення підприємства Landlord.

Здійснено розробку IoT системи з можливістю зміни і набору виконуваних функцій за допомогою перепрограмування контролерів та зміни сценаріїв на хмарі.

IoT система дозволяє здійснювати масштабування і програмну модернізацію системи, а також забезпечує такі функції:

– контроль вологості у приміщенні;

– моніторинг стану середовища складського приміщення;

– постійний моніторинг системи пожежогасіння;

– безпеку приміщення від неавторизованих користувачів.

Розроблена IoT система виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Робота системи перевірена за допомогою комп’ютерної системи із застосуванням програми Cisco Packet Tracer.

Результати перевірки роботи системи наведені у вигляді рисунків виконаних із застосуванням обчислювальної техніки.

ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ. СКОРОЧЕНЬ І ТЕРМІНІВ

A – Ампер

AES – Розширений стандарт шифрування

DHCP – протокол днамічної маршрутизації вузла

DNS – система доменних імен

CCNA – Сертифікований мережевий фахівець Cisco

GHz – Гігагерц

HTTP – Протокол передачі гіпертексту

HTTP – Протокол передачі гіпертексту з шифруванням

IEEE – Інститут інженерів електротехніки та електроніки

IoT – Інтернет речей

ISO – Міжнародна організація зі стандартизації

IP – інтернет-протокол

PC – Персональний Комп’ютер

LAN – Локальна мережа

LCD – Рідкокристальний дисплей

RFID – Радіочастотна ідентифікація

SWMS – Розумна система управління складськими приміщеннями

V – Вольт

VPN – віртуальна приватна мережа

WAN – Глобальна комп’ютерна мережа

WiFi – Бездротова технологія передачі даних

# ВСТУП

Управління складом – одне з найважливіших завдань у сфері логістики та управління ланцюгами поставок. Провідні установи та організації, науковці та експерти активно працюють над створенням інноваційних систем для підвищення ефективності цих процесів. Серед актуальних розробок – технологія Інтернету речей, автоматизація процесів, технологія RFID та сучасні системи управління запасами.

На глобальному рівні тенденції в управлінні складами зосереджені на автоматизації, використанні хмарних сервісів для моніторингу та управління, а також застосуванні штучного інтелекту для аналізу великих обсягів даних і прийняття рішень у режимі реального часу. Ще одним важливим напрямком розвитку є впровадження роботизованих систем та автономних транспортних засобів. Ця якість є важливою у зв'язку з необхідністю підвищення ефективності управління складом, зниженням витрат і забезпеченням надійності та безпеки зберігання товарів.

Розробка та впровадження систем управління складом IoT відповідає сучасним потребам компаній, які прагнуть оптимізувати свої логістичні процеси.

Метою даної роботи є розробка системи управління складом IoT SWMS, що забезпечує надійний моніторинг стану пристроїв, контроль доступу та аварійну безпеку. Потенційні сфери застосування включають великі підприємства, розподільчі центри та інші промислові комплекси.

Це дослідження є частиною більш широкої дослідницької теми в галузі автоматизації та управління промисловими процесами, а також має відношення до інших досліджень, спрямованих на створення інноваційних систем моніторингу та управління, таких як інтеграція технологій IoT, підвищення ефективності виробничих процесів.

# 1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

## 1.1 Загальна характеристика об’єкта дослідження

LANDLORD спеціалізується на управлінні складським приміщеннями, які ефективно зберігають різні типи меблів та активно використовує у своїй діяльності новітні технології, зокрема Інтернет речей (IoT). IoT визначається як мережа фізичних пристроїв, які з’єднані між собою без прямої взаємодії людини або обміну даними через Інтернет. Вона охоплює низку пристроїв, таких як датчики, зчитувачі RFID, камери відеоспостереження, маршрутизатори, мережеві комутатори, контролери та інші пристрої, які дозволяють аналізувати дані про стан складу та продукту в реальному часі.

Основна цінність Internet of Things у складських приміщеннях полягає в тому, що він дозволяє компаніям отримувати детальну та точну інформацію про всі аспекти їх діяльності, пов’язані зі зберіганням і переміщенням товарів.

Датчики та інші пристрої IoT можна використовувати для вимірювання температури, вологості, та відстеження розташування продуктів у режимі реального часу – це дозволяє підприємствам оптимізувати управління запасами, швидко реагувати на проблеми та збої та підвищити ефективність складу.

Використання IoT також дозволяє побудувати ефективну систему безпеки підприємства, яка може включати в себе систему контролю доступу, систему пожежогасіння та контроль умов зберігання товарів.

Загальна ідея використання IoT на складах полягає у створенні інтелектуальної інфраструктури, яка може адаптуватися до мінливих умов ринку та потреб клієнтів, забезпечуючи максимальну ефективність і конкурентоспроможність компаній.

Рішення Інтернету речей для складів швидко набирають популярності, оскільки пропонують багато переваг для бізнесу.

Від першої ідеї створення «розумного складу» до фактичної реалізації цієї концепції IoT перетворився на центральний інструмент для оптимізації управління запасами та процесів виробничої логістики.

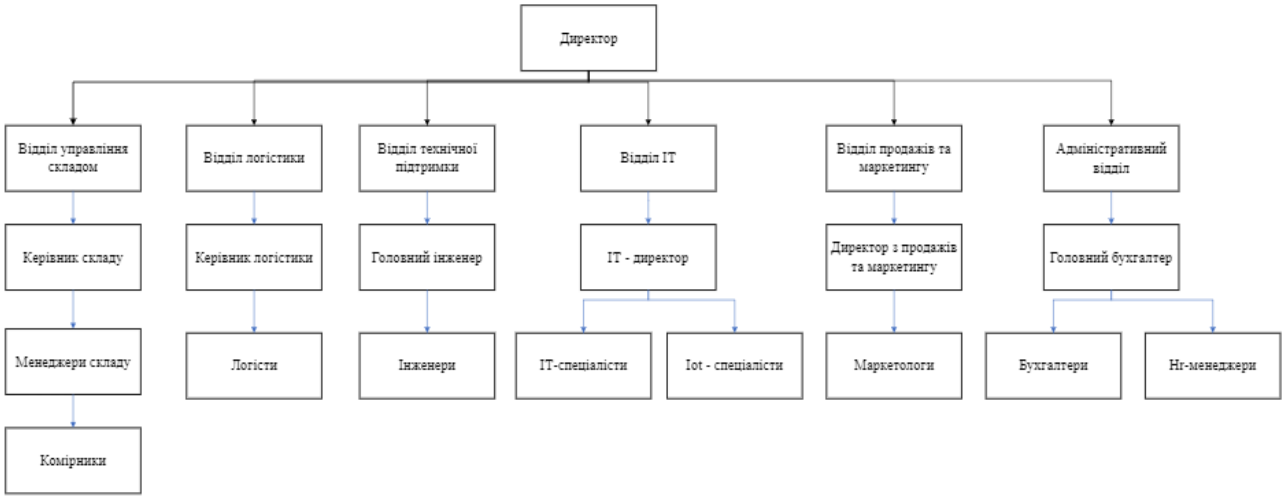



Рисунок 1.1 – Організаційна структура підприємства Landlord

## 1.2 Храктеристика системи підприємства

Система підприємства LANDLORD спеціалізується на управлінні складським господарством і пропонує різноманітні послуги, спрямовані на оптимізацію логістичних та складських операцій для своїх клієнтів. Послуги які надає підприємство:

– надання місця для зберігання різних типів меблів на різні терміни, залежно від потреб клієнтів. Зберігання товарів у спеціальних умовах із контрольованою температурою та вологістю, що особливо важливо для продуктів харчування, медикаментів та інших чутливих до умов зберігання товарів;

– використання IoT технологій для ефективного зберігання різних видів меблів, що включає RFID зчитувачі, датчики та інші автоматизовані системи. Аналіз даних про запаси для визначення оптимального рівня зберігання товарів та мінімізації витрат;

– віддалене управління складськими приміщеннями за допомогою IoT технологій, що дозволяє моніторити стан складу, відстежувати запаси та контролювати умови зберігання товарів у режимі реального часу.

Забезпечення безпеки складських приміщень завдяки системам відеоспостереження.

Підприємство знаходиться на вулиці автопарковая та орендує 3 поверхи будівлі для ефективного впровадження разрахованої корпоратиної мережі та володіє одним складським приміщенням який знаходиться на відстані 1500 метрів офісної будівлі як зображено на рисунку 1.2. Це було зроблено для швидкої комунікації між працівниками підприємства без використання корпоратиної мережі. Якщо ж потрібно використати мережу то процес обміну інформацією між відділами підприємства відбудеться максимально швидко. У будівлі є серверна яка для більш зручного користування була розташована поряд з IT-відділом , кабінет директора розмістили на другому поверсі біля конференц залу , а відділ логістики було вирішено розмістити на першому поверсі біля відділу керування складом бо вони невід’ємно пов’язані.

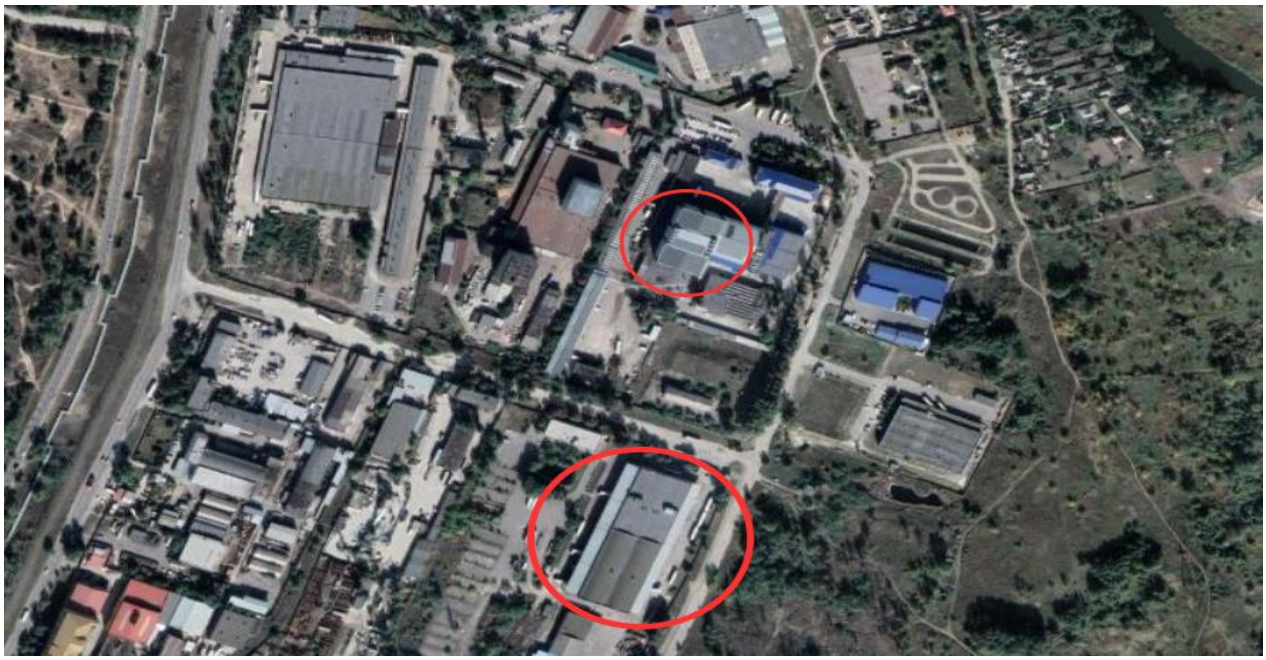


Рисунок 1.2 – Фізичне розташування підприємства

Максимальна кількість зберігання товару у складському приміщенні підприємства Landlord – 900 палет , загальна площа складу – 2000м² , зона прийому та відправлення товару дорівнює 200м² , та зона паркування становить 200м². Навколо підприємства знаходяться часні будинки та такі види комунікацій :

– центральне водопостачання вздовж вулиці Автопарковая;

– центральне електропостачання вздовж дороги;

– центральне газопостачання;

– центральна каналізація;

– оптоволоконні лінії вздовж вулиці для забезпечення високошвидкісного інтернету;

– основні дороги для легкого доступу вантажівок та громадського транспорту;

– спеціально відведені місця для паркування вантажівок та легкових автомобілів, а також зона для відстою вантажівок;

– системи відеоспостереження та охоронні системи для забезпечення безпеки підприємства та складського приміщення.

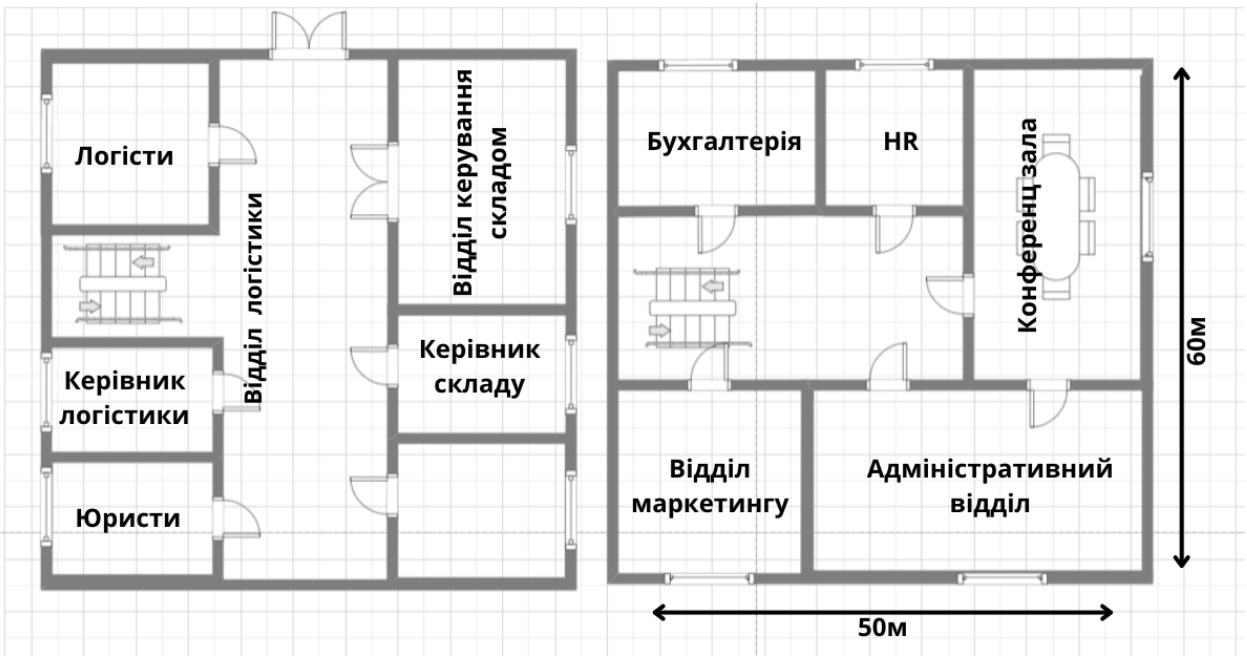



Рисунок 1.3 – План першого та другого поверхів офісної будівлі


Рисунок 1.4 – План третього поверху офісної будівлі

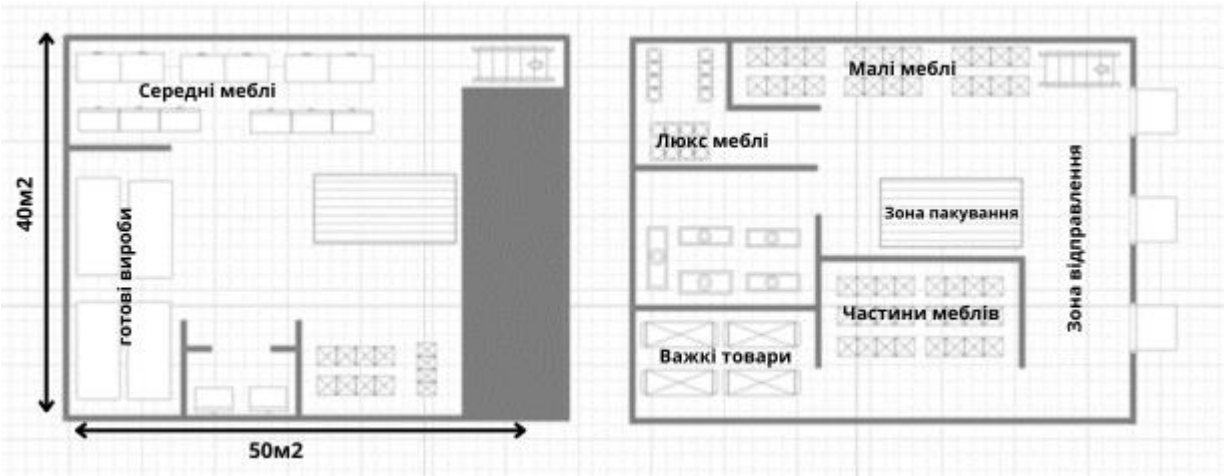



Рисунок 1.5 – План складського приміщення

## 1.3 Відомості про технології збору та передачі інформації

Система SWMS використовує різні технології збору та передачі інформації. Датчики є важливим компонентом системи збору даних.

Інфоречрвоні датчики для забезпечення функцій системи пожежогасіння, щоб забезпечити оптимальні умови зберігання використовуються датчики вологості та датчики температури

Зчитувачі та мітки RFID використовуються для автоматичного відстеження товарів після прибуття, зберігання та відвантаження, щоб вони могли оптимізувати процес інвентаризації та транспортування товарів. Вони також використовуються у системі контролю доступу до складського підприємства.

Камери відеоспостереження забезпечують моніторинг безпеки і моніторинг поведінки персоналу в режимі реального часу, інформація яка було отримана з камер відеоспостереження передається та обробляється на хмарі, що забезпечує зручне та швидке використання системою.

Для передачі інформації використовуються різні мережеві технології. Маршрутизатори забезпечують зв'язок між різними сегментами мережі та забезпечують передачу даних з пристроїв IoT на центральний сервер, а комутатори дозволяють підключати до мережі кілька пристроїв для ефективної передачі даних.

Бездротові мережі, особливо точки доступу Wi-Fi, можуть забезпечувати бездротове підключення до датчиків, камер та інших пристроїв IoT та передавати дані на центральний сервер. Дротові мережі, такі як Ethernet, використовуються для надійного підключення стаціонарних пристроїв до мережі.

Хмарні сервіси використовуються для зберігання, обробки та аналізу даних, отриманих з пристроїв Інтернету речей, що дозволяє підприємствам швидко реагувати на зміни та оптимізувати свої робочі процеси.

## 1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об’єкта впровадження

### 1.4.1 Принципи інформаційного забезпечення

У системі SWMS складського підприємства Landlord використовується низка засобів для забезпечення цілісності інформації, одним із яких є популярний алгоритм шифрування RSA, що забезпечить інформаційну безпеку між пристроями мережі. Використання технології RFID забезпечує безпеку у складському приміщенні.

Доступність даних має вирішальне значення для забезпечення безперебійної роботи системи тому, що система повинна надавати доступ до стану та моніторингу пристроїв у будь-який час. Хмарні сервіси, які налаштовані на центральному маршрутизаторі забезпечують систему резервним копіюванням даних та моніторингом.

Потрібно також не забувати про конфідеційності даних, яку система SWMS підтримує за допомогою авторизації на основі імен користувачів та паролів. Та за допомогою протоколу HTTPS який захищає данні при передачі наприклад з датчиків системи до центрального сервера.

Для забезпечення релевантності даних система SWMS, налаштована так, щоб наприклад камери-відеоспостереження або освітлювання спрацьовувало лише при перетині датчику руху, це зменшить обсяг непотрібної інформації.

### 1.4.2 Технічні способи інформаційного забезпечення

Датчики використовуються для збору даних про температуру, вологість та інші параметри в режимі реального часу. Ці дані передаються в центральну систему по бездротовій мережі за допомогою контролера з встановленим мережевим адптером.

Система використовує бездротову мережу WiFi – вона забезпечую швидку передачу інформацію на відносно невеликі відстані. Такі аналоги, як Zigbee або Bluetooth не підходять для SWMS системи через нижчу порівняно з WiFi швидкість передачі даних.

Також використовується центральний шлюз, який є “мозком” системи, він забезпечує підключення до безпровідної мережі, моніторинг системи та налаштування поведінки приладів.

Також система використовує контролери esp8266 з мережевим адаптером для збору інформації з датчиків та передачі її на центральний сервер.

### 1.5 Огляд відомих рішень для IoT системи складського приміщення

Відомим рішенням в сфері IoT систем для складських підприємств є система компанії Lumive, яка створює готові рішення для складських приміщень на основі Zigbee комунікації. Великим недоліком систем побудованих на Zigbee є їх невеликий розмір, зазвичай продукт компанії Lumive використовують у невеликих приміщеннях, це пов’язано с тим що частота роботи 2.4Ghz через це зона покриття мережі набагато менша ніж порівняно з Wifi. Також важливо згадати про швидкість – Zibee хоч і використовує менше енергії , але швидкість передачі даних на порядок менша ніж у WiFi. На відміну від WiFi не всі пристрої підтримують протокол Zigbee.

Також варто згадати про автоматизовані IoT системи компанії Amazon, які активно використовують RFID технологію для забезпечення точного моніторингу та безпеки системи складського приміщення. Системи складських приміщень майже повність автоматизовані, реалізували вони це за допомогою WiFi піключення та хоч і дорогих але потужних хмарних технологій AmazonAWS.

Враховуючи досвід двох вище згаданих рішень було обрано використання в IoT системі SWMS протоколу WiFi та використання RFID технології.

### 1.6 Мета і завдання робити

Мета роботи полягає у розробці та впровадженні IoT системи SWMS для управління складським приміщенням підприємства LANDLORD. Це дозволить забезпечити надійний моніторинг стану пристроїв системи, впровадити системи контролю доступу та безпеки при аварійних ситуаціях.

Після огляду вже відомих рішень в галузі IoT систем в складських підприємствах потрібно :

– на базі зробленого обстеження об’єкту виконати вибір обладнення для реалізації системи;

– врахувати розмір приміщення, ширину стін та вимоги до функцій системи;

– розробити специфікацію обраних компонентів;

– змоделювати комп’ютерну систему у середовищі Packet Tracer;

– виконати налаштування системи;

– розробити IoT-систему пожежогасіння;

– розробити IoT-систему доступу за допомогою технології Rfid;

– розробити IoT-систему сигналізації;

– розробити IoT-систему стану середовища.

По закінченню виконання побудови та налаштування системи SWMS у програмі Cisco Packet Tracer необхідно провести тестування системи та підвести висновок виконаної роботи.

### 1.7 Визначення можливих напрямків рішення поставлених завдань

По-перше при побудові систему SWMS потрібно проаналізувати план складського приміщення наведеного на рисунку 1.5 та обрати розташування за технічними вимогами датчиків, контролерів та інших виконавчих пристроїв враховуючи:

– розмір приміщення в якому розташовується SWMS;

– товщина та матеріал стін;

– тип підключення пристроїв.

По-друге необхідно забезпечити умови зберігання товарів згідно технічних вимог, це буде реалізовано на стороні контролеру, який буде зчитувати інформацію з датчиків та виконувати відповідні дії по усуненню відхилень умов зберігання.

Також потрібно налаштувати доступ до приміщення підприємства за допомогою технології RFID, кожен працівник повинен отримати картку доступу, яка буде налаштована під відповідні двері з зчитувачем.

### 1.8 Обґрунтування вибраного напрямку інженерного рішення

Складське підприємство компанії Landlord має середній розмір, та нешироκі стіни, що забезпечує оптимальну роботу системи SWMS з використанням безпровідної технології WiFi.

Підприємства виконує зберігання різних видів товарів тому необхідно встановити датчики для моніторингу стану приміщення, щоб позбавитись можливості псування товарів та зменшення доходу підприємства. Висока вологість є дуже небезпечною не тільки для цілісності зберегіння товарів, а й для пристроїв та палетів, які використовуються у підприємстві, тому необхідно встановити систему контролю вологості, яка буде складатись датчиків та венетиляції.

Система пожежогасіння є необхідною топ будуть використовуватись виконавчі пристрої з широким діапазоном дії та датчики з режимом моніторингу середовища 24/7.

Виробники та моделі пристроїв, які обирались в системі SWMS підтримують WiFi та повинні коштувати в маленькому-середньому ціновому діапазоні.

# 2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

## 2.1 Технічні вимоги до системи

### 2.1.1 Вимоги до системи в цілому

IoT система Smart Warehouse Management System складського підприємства Landlord (SWMS). Система забезпечую моніторинг середовища приміщення, безпеку від неавторизованих користувачів та при аварійних ситуаціях.

#### 2.1.1.1 Вимоги до структури і функціонування системи

Система SWMS побудована за допомогою деревовидної топології, що забезпечує легкість в розширені мережі та її частково децентралізована структура забезпечує високу надійність.

Підсистема пожежогасіння відстежує інфрочервоний діапазон за допомогою монітору та забезпечує усунення аварійної ситуації за допомогою спринклерів. Реалізована така підсистема за допомогою контролеру з мережевим адаптером та за допомогою спеціальних вогнестійких кабелів.

Підсистема контролю доступу до приміщення використовує технологію RFID. На кожних дверях складського приміщення встановлено зчитувачі, які налаштовані на певну частоту та відповідають частоті картки доступу виданої персоналу.

Підсистема контролю вологості забезпечує оптимальне використання встановленої вентиляції та підтримку допустимого рівня вологості. Вентиляція підключена за допомогою мережевого адаптера до центрального вузла.

Система має три рівні ієрархії:

- рівень сенсорів;
- рівень контролерів;
- рівень управління.

Система частково централізована, бо підтримує локальну обробку даних на контролерах, що зменшує час затримки та більшу точність обробки інформації.

Зв’язок між IoT пристроїв виконано за допомогою безпровідної технологіх WiFi та спеціальних проводів на рівні підсистем.

Система повинна бути доступною для моніторингу чи діагностування 24/7.

#### 2.1.1.2 Показники призначення

– середній час безвідмовної роботи системи повинен становити не менше 1000 годин;

– середній час для відновлення роботи системи повинен становити не більше 3 годин;

– 100% аутентифікація та авторизація користувачів, що мають доступ до системи;

– 100% шифрування даних під час передачі та зберігання;

– підтримка не менше 20 IoT пристроїв одночасно;

– час на навчання персоналу не більше 10 годин;

– 100% результативність системи пожежогасіння;

– зчитування RFID карток з 5% помилки.

#### 2.1.1.3 Вимоги до патентної чистоти

Система LANDLORD та її компоненти вільні від патентних претензій у відповідності до законодавства наступних країн:

Система не порушує жодних патентів, зареєстрованих в USPTO (Відомстві патентів і товарних знаків США).

Система відповідає патентним законам ЄС, включаючи патенти, зареєстровані в Європейському патентному відомстві (ЄПВ).

Система не порушує патенти, зареєстровані в CIPO (Канадському відомстві інтелектуальної власності).

SWMS дотримується законів та патентних вимог JPO (Японського патентного відомства).

Система відповідає патентним законам, зареєстрованим в CNIPA (Національному управлінні інтелектуальною власністю Китаю).

Дотримується патентних вимог та законів IP Australia.

Система не порушує патенти, зареєстровані в IPO (Індійському патентному відомстві).

**2.1.1.4 Вимоги до експлуатації системи**

Відносна вологість не повинна становити більше 70%.

Система має безперервне підключення до моніторингу та управління системи.

Мережа енергопостачання містить такі параметри:

– напруга живлення 220V;

– частота 50 Hz;

– опір заземлення становить не більше 4Ом.

Персонал, який працює з системою має таку освіту:

– середня технічна освіта;

– вища технічна освіта;

– курси CCNA.

Комплект запасних частин включає по два екземпляри датчиків кожного типу, контролери, кабелі живлення. Вони зберігаються у спеціальному приміщенні на першому поверсі складського приміщення.

Умови збереження:

– температура зберігання від +5°C до +35 °C;

– відносна вологість не більше 70%;

– зона зберігання захищена від пилу, прямих сонячних променів та вібрацій.

Щоденно систему перевіряють на працездатність основних компонентів SWMS. Щотижня проводиться тестування системи на наявність збоїв у роботи

датчиків та інших IoT пристроїв. Щомісяця за необхідності проводиться оновлення програмного забезпечення.

### 2.1.2 Вимоги до задач виконуваним Системою

Підсистема пожежогасіння розташована на контролері esp8266 та складається з датчиків полум’я та спринклерів. При відповідному сигналі з датчика система запускає спринклери, які усувають аварійну ситуацію. Задача підсистеми:

- постійне стеження за інфрочервоним діапазоном;
- виведення стану системи на дисплеї;
- запуск спринклерів при аварійній ситуації;
- безперервний моніторинг;
- виявлення полум’я з точністю 95%;
- оновлення зображення стану системи кожні 5 секунд.

Підсистема контролю доступу до приміщення налаштовується на головному вузлі. Складається з дверей, Rfid зчитувачів та міток . де мітки виконуються функцію картки доступу. Задача підсистеми:

- забезпечення уникання несанкціонованого проникнення;
- організація доступу для персоналу підприємства;
- налаштування карток доступу та зчитувачів;
- постійний моніторинг;
- надійне зчитування та перевірка карток;
- миттєве відкриття дверей.

Підсистема контролю вологості складається з : датчиків вологості та вентиляції. Вентиляція має декілька режимі : вимкнений/середній/посилений. Задачі підсистеми:

- моніторинг рівня вологості;
- управління режимами вентиляції;
- передача даних у хмару для моніторингу персоналом;
- вимірювання з точністю ±2%.

### 2.1.3 Вимоги до видів забезпечення

#### 2.1.3.1 Інформаційне забезпечення

– дані про температурні та вологісні параметри;

– дані про ідентифікатор на картці доступу персоналу;

– дані про стан обладнання;

– дані про розташування обладнання;

– інформаційний зв’язок виконується за допомогою головного шлюзу;

– використання мережевих протоколів HTTP для передачі даних між ioT пристроїв;

– обмін даних відбувається у режимі реального часу.

#### 2.1.3.2 Технічне забезпечення

У системі припустимо використовувати такі технічні засоби:

– датчики температури;

– датчики вологості;

– інфрачервоні датчики;

– датчики руху;

– RFID зчитувачі;

– RFID мітки;

– камери спостереження;

– центральний шлюз;

– контролери ESP8266;

– кабелі;

– сервери;

– маршрутизатор;

– кабельний модем.

Датчики забезпечують точні вимірювання температури та вологості з найменшою похибкою.

RFID зчитувачі та мітки працюють на частоті 1- 5.

Камери відеоспостереження та датчики руху працюють цілодобово.

Камери та датчики захищенні від пилу та вологи.

Обладнення системи SWMS має низьке енергоспоживання та використовує енергоефективні компоненти.

### 2.1.3.3 Організаційне забезпечення

Задля забезпечення безпеки системи кожен співробітник проходить інструктаж та йому надають логін та пароль для автентифікації в системі та отримати можливість моніторингу й налаштування системи.

Інформація підсистем зберігається на центральному шлюзі, який також використовує хмарні технології для обробки даних. На ньому виконуються резервне копіювання конфігурації системи.

Щоб уникнути від помилкових дій персоналу впроваджено такі методі:

– тільки старші працівники мають доступ до системи;

– проходження курсів CCNA, що надають базові навичкі налаштування iot систем;

– кожен користувач має унікальний логін і пароль, який змінюється кожні півроку;

– проведення вебінарів з техніки безпеки системи.

### 2.1.3.4 Методичне забезпечення

Міжнародні стандарти:

ISO 9001: Стандарт системи управління якістю, що забезпечує високу якість обслуговування та управління процесами.

ISO 27001: Стандарт системи управління інформаційною безпекою, що забезпечує захист даних і кібербезпеку.

ISO 28000: Стандарт системи управління безпекою для ланцюга постачання.

ISO 22301: Стандарт системи управління безперервністю бізнесу, що забезпечує стійкість до збоїв і надзвичайних ситуацій.

Галузеві стандарти:

GS1: Стандарти для автоматичної ідентифікації та збору даних, зокрема RFID.

WMS (Warehouse Management System): Стандарти для управління складськими процесами.

Технічні стандарти:

IEEE 802.11: Стандарт для бездротових мереж (Wi-Fi).

IEEE 802.3: Стандарт для дротових мереж (Ethernet).

ISO/IEC 19762: Стандарт для RFID та безконтактних смарткарт.

### 2.1.3.5 Вимоги до модернізації

Система SWMS повинна інтегруватись до мережі організації складського підприємства Landlord. Доступ до системи можна отримати у відділі керування складом. Для цього було проведено повний цикл тестування системи перед впровадженням.

Параметри впровадження система:

– до мережі забезпечено доступ лише авторизованим користувачам;

– впроваджено систему моніторингу для відстеження активності IoT системи;

– використовуються загальноприйняті протоколи HTTP/HTTPS;

– мережа організації підключена до SWMS віддалено;

– SWMS не може впливати на мережу організації.

### 2.1.4 Мережа організації

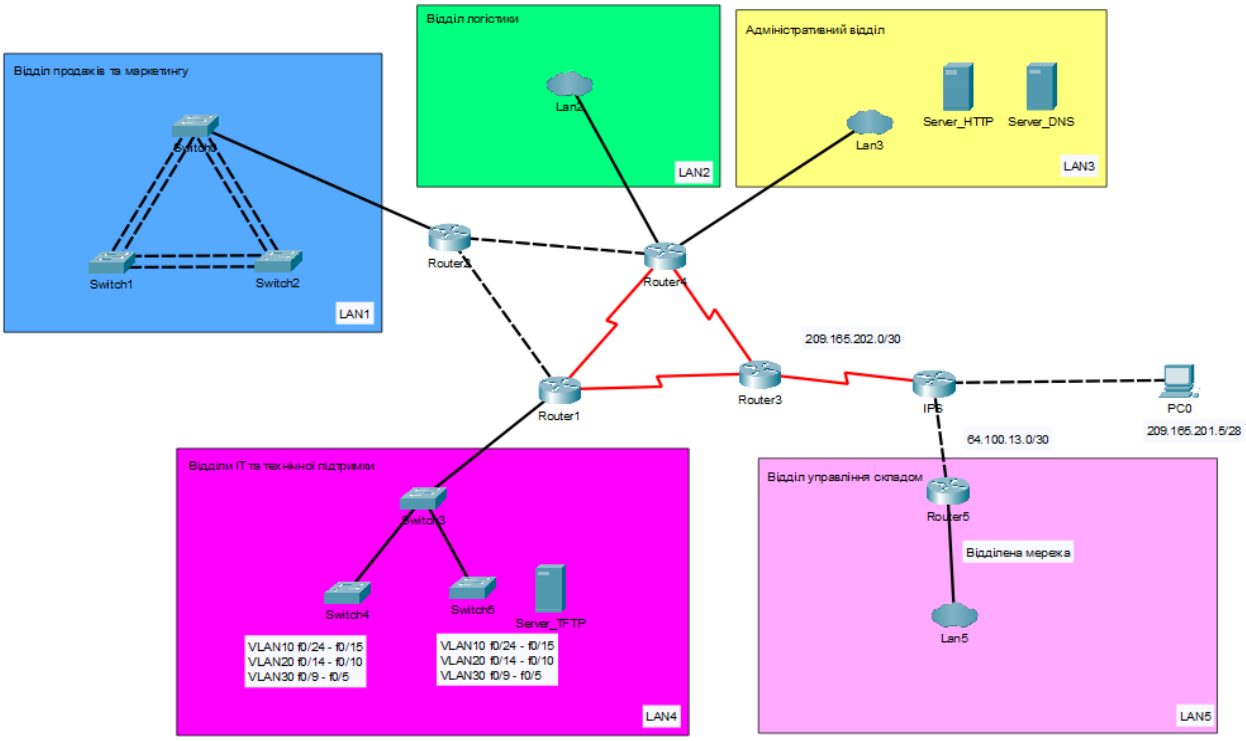



Рисунок 2.1 – Топологія мережі підприємства за завданням

Мережа підприємства LANDLORD складається з п'яти основних відділів, кожен з яких має свою підмережу. Всі підмережі з'єднані через маршрутизатори, що дозволяє ефективно обмінюватися даними між різними відділами.

Мережа побудована за зірковою топологією, де маршрутизатори відіграють роль центральних елементів. Всі маршрутизатори підключені один до одного, що забезпечує швидкий і надійний обмін даними між відділами. Віддалене складське приміщення підключене через захищене VPN-з'єднання. Основні з'єднання здійснюються через Router1, Router2, Router3, Router4 та Router5.

Для налаштування та роботи мережі використовувалися такі протоколи і технології:

– HTTP/HTTPS для безпечного доступу до мережевих ресурсів.

– VPN для захищеного підключення віддалених підрозділів.

– IEEE 802.11 (Wi-Fi) для бездротових з'єднань.

– IEEE 802.3 (Ethernet) для дротових з'єднань.

– DHCP для автоматичного призначення IP-адрес пристроям у мережі.

– NAT для трансляції приватних IP-адрес у публічні та забезпечення доступу до інтернету.

– VLAN для сегментації мережі та підвищення її безпеки та ефективності.

– OSPF для динамічної маршрутизації даних між підмережами.

### 2.1.5 Визначення обсягу та інтенсивності вихідного трафіку для найбільшої корпоративної локальної мережі

Задані умови, згідно варіанту завдання:

– кількість підмереж та кількість вузлів: Lan1 – 38, Lan2 – 109, Lan3 – 237, Lan4 – 33 , Lan5 – 10;

– середня інтенсивність трафіку 200 кадрів/с;

– середня довжина повідомлення в найбільшій мережі (Lan3) 650 байт;

– затримка передачі пакету ≤6 мс.

Для того щоб розрахувати інтенсивність трафіку вихідного трафіку мережі Lan3 потрібно спочатку розрахувати пропускну здатність мережі.

Розрахунок пропускної здатності мережі рівня доступу: Pp.p = 200*l*n8 , де n – кількість доступних портів комутатора

Pp.p = 200 * 650 * 48 * 8 = 49 920 000 = 49.92 ( Мбіт/с)

Далі потрібно розрахувати загальне навантеження на комутатор при підключенні через лінію 1000 Мбіт/с:

μв = 1000000000 / 8 / 650 = 192307 (пакетів/с)

Розрахунок максимуму вузлів для комутатора розподілу:

N = μв / 200 = 192307 / 200 = 961 вузлів

Далі потрібно розрахувати інтенсивність трафіку, який йде від всіх користувачів:

$\lambda = N_{вуз} * \mu = 237 * 200 = 47400$ (пакетів/с)

Розрахунок коефіцієнту затримки:

$p = 47400 / 192307 = 0.25$

Коефіцієнт зайнятості комутатора дорінює:

$R = p/(1-p) = 0.25/(1-0.25) = 0.33$

Також розрахуємо середню затримку кадру:

$T = 1 / (\mu_в – \lambda) = 1 / (192307 – 47400) = 0.000007$

Середня довжина черги:

$L_{чер} = p^2 / (1 - p) = 0.25^2 / (1 – 0.25) = 0.08$

Середній час перебування пакетів трафіку в черзі:

$T_{оч} = L_{чер} / \lambda = 0.08 / 47400 = 1.68$ мс.

За умовою Затримка передачі пакету ≤6 мс тому значення 1.68 підходить

Насамперед потрібно розрахувати пропускну здатність каналу:

$B = \lambda \cdot l = (47400 * 650 * 8) * 10^{-6} = 246.4$ Мбіт/с

Беручи до уваги що вихідний канал – 1000 Мбіт/с , пропускна здатність каналу задовільняє умові

## 2.2 Розробка апаратної частини системи

### 2.2.1 Вибір технічних засобів для реалізації системи

#### 2.2.1.1 Вибір датчиків

Датчики вологості Honeywell HumidIcon™ серії HIH6100 - це цифрові датчики відносної вологості з вихідним сигналом, об'єднані в одному корпусі. Ці датчики забезпечують рівень точності ±4,0 % відносної вологості і рівень точності вимірювання температури ±0,5 °C. [13]

Особливості:

– найкраща в галузі довгострокова стабільність;

– цифровий вихід I2C або SPI з температурною компенсацією;

– найкраща в галузі надійність;

– енергоефективність;

– рішення з найнижчою загальною вартістю;

– надмалий розмір корпусу та безліч опцій.

Тепловий датчик Dallas DS18B20 забезпечує вимірювання температури в діапазоні від 9 до 12 біт за Цельсієм і має функцію сигналізації з енергонезалежними програмованими користувачем верхньою і нижньою точками спрацьовування. [14]

Особливості:

– не потребує зовнішніх компонентів;

– живлення від лінії передачі даних. Діапазон живлення 3,3 В;

– не потребує живлення в режимі очікування;

– вимірює температуру від -55°C до +125°C.;

– точність ±0,5°C від -10°C до +85°C;

– перетворює 12-бітну температуру в цифрове слово за 750 мс (макс.).

Датчик освітлювання TSL2561 - перетворює інтенсивність світла в цифровий сигнал, що виводиться через інтерфейс I2C. Він також стійкий до шуму та вібрацій, що робить його ідеальним для використання в складських приміщеннях. [15]

Особливості:

– запатентована архітектура з двома діодами;

– динамічний діапазон 1M:1;

– програмована функція переривання;

– цифровий інтерфейс I²C.

Датчик руху Parallax PIR Motion Sensor піроелектричний пристрій, який виявляє рух, вимірюючи зміни рівня інфрачервоного (теплового) випромінювання, що випускається навколишніми об'єктами. При виявленні руху PIR-сенсор видає високий рівень сигналу на свій вихідний вивід. [16]

Особливості:

– виявлення людини на відстані до 30 футів або до 15 футів у режимі зниженої чутливості;

– перемичка вибирає нормальну роботу або знижену чутливість;

– струм джерела до 12 мА при 3 В, 23 мА при 3.3 В;

– монтажні отвори для гвинтів 2-56;

– 3-контактний SIP-роз'єм, готовий для макетних або наскрізних проектів.

Попередні обрані датчики були відносно дешеві від своїх аналогів на ринку , але щодо датчику диму було вирішено обрати за вищою ціною ніж середня на ринку та з більшою ефективністю - First Alert SA320FF. [17]

Найважливішою особливість цього датчика є зона покриття на 360 градусів , на висока надійність.

Інфрочервоний датчик було обрано Артон-ДЛ 1477, який використовується для великих закритих приміщень.[18]

**2.2.1.2 Вибір периферійних пристроїв**

Для створення наприклад підсистеми пожежогасіння або освітлення необхідно використати реле яке буде підтримувати напругу у 3.3V та 10A що дозволить використовувати прилади саме від контролера.

У зв’язку з заданими умовами було обрано реле Element з чотирма каналами. [19]

Щодо оприскувачів (sprinklers) було обрано варіант американської компанії Viking VK1021 , який якраз розроблений для автоматизованих систем пожежогасіння. [20]

Його перевагою є те що він може використовувати декілька видів розпилювачів, що дозволить у разі аварійної ситуації ефективно потушити палаючу ділянку.

Також було обрано комплект Rfid міток та зчитувачів компанії Impinj , основною причиною обрання саме цього комплекту висока швидкість та 17 пар міток та зчитувачів. [21]

Сигналізацію та відекамеру було обрано Ajax тому що вони легка у використанні та продається за доступними цінами , а також підтримує моніторинг 24/7 , хоча і не підтримує резервне живлення , але в даному випадку це не потрібно.

Також у системі використовується вентиляція компанії Vents, яка має 3 режими використання. [22]

Таблиця 2.1 – Специфікація обладнання

| **Позиція** | **Найменування і технічна характеристика** | **Тип, марка, позначення документа, опитувального листа** | **Одиниці виміру** | **Кількість** | **Примітки** |
|---|---|---|---|---|---|
| 1 | Датчик вологості | Honeywell HIH6100 | шт. | 12 | Цифровий вихід I2C або SPI |
| 2 | Тепловий датчик | Dallas DS18B20 | шт. | 12 | від -55°C до +125° |

Продовження таблиці 2.1

| | | | | | |
|---|---|---|---|---|---|
| 3 | Датчик освітлення | TSL2561 | шт. | 6 | Цифровий інтерфейс I2C |
| 4 | Датчик руху | Parallax PIR Motion Sensor | шт. | 10 | Виявлення руху до 30 футів, струм джерела до 12 мА |
| 5 | Датчик диму | First Alert SA320FF | шт. | 12 | Зона покриття 360 градусів, |
| 6 | Реле | Element | шт. | 10 | Напруга 3.3V, струм 10A |
| 7 | Оприскувач | Viking VK1021 | шт. | 12 | Система пожежогасіння |
| 8 | Комплект RFID міток та зчитувачів | Impinj RFID Kit | Комплект | 17 | Висока швидкість роботи |
| 9 | Інфрочервонй датчик | Артон 1477 | шт. | 6 | Вимірює інфрочервоний діапазон |
| 10 | Сигналізація | Ajax | шт. | 2 | Звукове оповіщення |
| 11 | Вентиляція | Vents | шт. | 9 | Провітрення приміщення |
| 12 | Відео-камери | Ajax | шт. | 12 | Відеоспостереження |

### 2.2.2 Розробка переліку вхідних та вихідних сигналів

У таблиці 2.2 представлено таблицю вхідних сигналів системи складського приміщення

Таблиця 2.2 – Вхідни сигнали

| **№** | **Найменування інформації** | **Ідентифікатор** | **Функція** | **Вид** | **Тип сигналу** |
|---|---|---|---|---|---|
| 1 | Датчик вологості | DUBV | Контроль | Аналоговий | 3.3 В |
| 2 | Датчик температури | DTS | Контроль | Аналоговий | 3.3 В |
| 3 | Датчик освітлення | DLS | Контроль | Аналоговий | 3.3 В |
| 4 | Інфрочервоний датчик | DLI | Контроль | Аналоговий | 3.3 В |
| 5 | Датчик руху | DMP | Контроль | Дискретний | 3.3 В |
| 6 | Датчик диму | DDS | Контроль | Дискретний | 3.3 В |
| 7 | RFID-мітка | DRID | Ідентифікація | Дискретний | Частота (HF) |

У таблиці 2.3 представлено таблицю вихідних сигналів системи складського приміщення

Таблиця 2.3 – Вихідні сигнали

| № | Найменування інформації | Ідентифікатор | Функція | Вид | Тип сигналу |
|---|---|---|---|---|---|
| 1 | Реле | NR | Управління | Дискретний | 3.3 В |
| 3 | Сигналізація | NAL | Попередження | Дискретний | 3.3 В |
| 4 | Оприскувач | NV | Управління | Дискретний | 3.3 В |
| 5 | Світло | NS | Управління | Дискретний | 3.3 В |
| 6 | Вентиляція | VENT | Управління | Дискретний | 3.3 В |

### 2.2.3 Вибір пристрою керування

У системі IoT складського підприємства використовується Homegateway та три контролери esp8266.

DLC-100 – це бездротовий контролер, який контролює широкий спектр пристроїв для виявлення пожежної (датчики диму і CO) та охоронної (датчики відчинення дверей/вікон, датчики руху) тривог. Після встановлення та активації DLC-100 постійно контролює детектори диму та чадного газу і автоматично повідомляє про тривоги на пульт централізованого спостереження на IoT моніторі. Коли система перебуває під охороною, DLC-100 автоматично повідомляє про тривоги вторгнення в центральний моніторинговий центр.

ESP8266EX від Espressif – це високоінтегроване рішення Wi-Fi SoC, що відповідає постійним вимогам до ефективного енергоспоживання, компактного дизайну та надійної роботи в галузі. Завдяки повним і автономним мережевим можливостям Wi-Fi, він може працювати як автономний додаток або як підлеглий до головного MCU. Коли ESP8266EX розміщує додаток, він швидко завантажується із зовнішнього флеш-накопичувача. Вбудований високошвидкісний кеш допомагає збільшити продуктивність системи та оптимізувати системну пам'ять. Крім того, ESP8266EX може бути застосована до будь-яку мікроконтролеру конструкцію в якості Wi-Fi адаптера через інтерфейси SPI/SDIO або I2C/UART.

Мережевим адаптером для esp8266EX було обрано ESP-07, він є одним з найпопулярніших виборів для ESP контролерів.

### 2.2.4 Вибір джерела живлення

Для підключення живлення у SWMS використовуються живлення 220V. Враховуючи що IoT система має 3 підсистеми було вирішено придбати Liitokala та стабілізатор AMS1117.

Liitokala має такі характеристики:

– ac 100-240В 50-60Гц;

– usb DC 5V 2A.

AMS1117 використовується для передачі на контролер на 3.3V згідно характеристики обраної моделі. Стабілізатор має такі параметри:

– ams1117-3.3;

– вихідна напруга 3.3 В;

– вхідний струм 1А;

– макс. вхідна напруга 15 В.

Для того щоб підключити DLC100 Home Gateway до джерела живлення було обрано адаптер LEDTech 12v 2a 24w. Параметри адаптеру:

– вхідна напруга 220V;

– вихідний струм 2А;

– вихідна напруга 12В.

### 2.2.5 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Структурна схема комплексу технічних засобів комп'ютерної IoT системи складається з трьох рівнів:

Нижній рівень – датчики вологості , тепла , освітлення , руху , диму , реле.

Середній рівень – мережеве обладнення та мікроконтролер для оброблення інформації отриманої з датчиків

Верхній рівень – сервери – для обробки та зберігання інформації , прилади для моніторингу стану системи

Система забезпечує ефективний моніторинг складського приміщення підприємства Landlord , контроль вологості , освітлення , тепла та руху реалізовано по площині території складського приміщення. Для запобігання аварійних ситуацій потрібно регулярно проводити ревізію заданих параметрів на приладах.

Структурна схема комплексу технічних засобів комп'ютерної системи складскього приміщення наведена на рисунку 2.3.

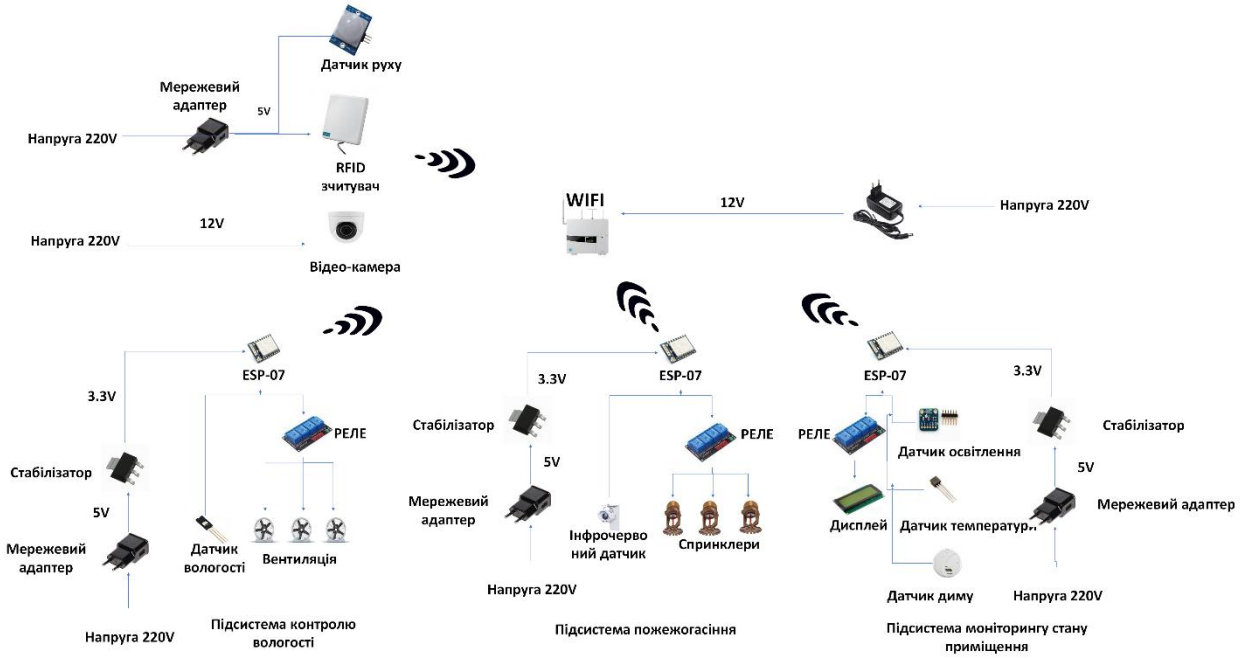



Рисунок 2.3 - Структурна схема комплексу технічних засобів комп’ютерної системи складського приміщення

# 3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

## 3.1 Проектування мережі підприємства

### 3.1.1 Мережеве обладнання

Модель маршрутизатора , яку було обрано для маршрутизаторів центральної частини системи (тобто роутери 1 – 4) – Cisco ISR4300 . Цей маршрутизатор підтримує роботу таких протоколів, як : EIGRP, OSPF, BGP, IPv4 та IPv6 адресацію.

Для підмереж Lan1, Lan2, Lan4 та Lan5 обрано модель комутаторів Cisco Catalyst 9200L-48P-4x, який гарно підходить для мереж середнього розміру

Для найбільшої мережі Lan3 підійде Cisco Catalyst 9300-24P-A. Він підтримує високу масштабованість та має велику швидкість переадрисації трафіку.

Як маршрутизатор з доступом в інтернет було обрано модель Asus RT-AX1800U, він обладнаний технологією покриття великих будинків та має високу швидкість передачі даних.

Також варто придбати ДБЖ Powercom Macan MAC-6000 LCD , який використовується як аварійне джерело живлення при наприклад відключенні електроенергії на підприємстві. Його перевагою є постійна вихідна частота 50/60 ГЦ.

Розрахунки обладнання мережі розрахована на можливість масштабування, використання гігабітної швидкості обміну інформацією в мережі офісної будівлі та складської частини підприємства , тому в обох випадках будуть використовуватись однакові моделі та виробники обладнання.

Враховуючи розміри складського приміщення було також додано два Wifi роутери TP-LINK TL-WR841N та чотири UniFi U6-LR точки доступу

Таблиця 3.1 – Перелік мережевого обладнання

| № | Назва в топології | Модель | Одиниці виміру | Кількість |
|---|---|---|---|---|
| 1 | Router_Router1-5 | Cisco ISR4300 | шт. | 5 |
| 2 | Hrachov_RouterISP | Asus RT-AX1800U | шт. | 1 |
| 3 | Switch | Catalyst 9200L-48P-4x | шт. | 12 |
| 4 | Server Dns/HTTP | Dell | шт. | 2 |
| 5 | AccesPoint-PT | UniFi U6-LR | шт. | 3 |

### 3.1.2 Серверне обладнення

У офісній частині підприємства розміщено 3 сервери: HTTP, TFTP та DNS, HTTP – це головний сервер який використовується для зберігання даних. Обрано модель серверів – DELL T330, який має такі характеристики : Оперативна пам'ять 8GB DDR4 ECC, 1 x Intel XEON 4 Core E3-1225 V5 3.30GHz, RAID-контроллер DELL PERC H330 RAID PCI 12GB SAS, Блок живлення DELL 350-Watts T330, 240гб SSD , LAN, USB, VGA.

### 3.1.5 Розрахунок ір адресації мережі підприємства

Мережа підприємства – це дві окремі мережі , офісна мережа яка розташована в трьох поверховій будівлі та мережа складського приміщення в якій реалізована IoT система.

При побудові топології мережі потрібно дотримуватись вимог виданого завдання

Таблиця 3.2 – Кількість вузлів у підмережах

| Lan1 | Lan2 | Lan3 | Lan4 | Lan5 |
|---|---|---|---|---|
| 38 | 109 | 237 | 33 | 10 |

Lan1 – Відділ продажів та маркетингу.

Lan2 – Відділ логістики.

Lan3 – Адміністративний відділ.

Lan4 – Відділ іт та технічної підтримки.

Lan5 – Відділ управління складом (Віддалена мережа).

Виділений блок адрес – 10.25.24.0/22.

Таблиця 3.3 – Адресація мереж

| **Ім'я мережі** | **Кількість вузлів** | **Адрес мережі** | **Маска мережі** | **Діапазон адрес** |
|---|---|---|---|---|
| LAN1 | 38 | 10.25.24.0 | /26 | 10.25.24.1 - 10.25.24.62 |
| LAN2 | 109 | 10.25.24.64 | /25 | 10.25.24.65 - 10.25.24.190 |
| LAN3 | 237 | 10.25.25.0 | /24 | 10.25.25.1 - 10.25.25.254 |
| LAN4 | 33 | 10.25.26.0 | /26 | 10.25.26.1 - 10.25.26.62 |
| LAN5 | 10 | 10.25.26.64 | /27 | 10.25.26.65 - 10.25.26.70 |
| LAN6 | 40 | 192.168.25.0 | /24 | |
| WAN1 | 2 | 10.1.3.0 | /30 | 10.1.3.1- 10.1.3.2 |
| WAN2 | 2 | 10.1.3.4 | /30 | 10.1.3.5- 10.1.3.6 |
| WAN3 | 2 | 10.1.3.8 | /30 | 10.1.3.9- 10.1.3.10 |
| WAN4 | 2 | 10.1.3.12 | /30 | 10.1.3.13- 10.1.3.14 |

Продовження таблиці 3.3

| | | | | |
|---|---|---|---|---|
| WAN5 | 2 | 10.1.3.16 | /30 | 10.1.3.17-10.1.3.18 |
| WAN6 | 2 | 209.165.202.0 | /30 | 209.165.202.1-209.165.202/2 |
| WAN7 | 2 | 209.165.201.5 | /28 | 209.165.201.6-209.165.201.7 |
| Hrachov_PC_1.1 | 7 | 10.25.24.0 | /26 | 10.25.24.2 – 10.25.24.8 |
| Hrachov_PC_1.2 | 7 | 10.25.24.0 | /26 | 10.25.24.9 – 10.25.24.15 |
| Hrachov_PC_1.3 | 7 | 10.25.24.0 | /26 | 10.25.24.16 – 10.25.24.22 |
| Hrachov_PC_1.4 | 7 | 10.25.24.0 | /26 | 10.25.24.23 – 10.25.24.29 |
| Hrachov_PC_1.5 | 7 | 10.25.24.0 | /26 | 10.25.24.30 – 10.25.24.36 |
| Hrachov_PC_1.6 | 7 | 10.25.24.0 | /26 | 10.25.24.37 – 10.25.24.43 |
| Hrachov_PC_1.7 | 7 | 10.25.24.0 | /26 | 10.25.24.44 – 10.25.24.50 |
| Hrachov_PC_1.8 | 7 | 10.25.24.0 | /26 | 10.25.24.51 – 10.25.24.57 |
| Hrachov_PC_1.9 | 6 | 10.25.24.0 | /26 | 10.25.24.58 – 10.25.24.64 |
| Hrachov_PC_2.1 | 31 | 10.25.24.64 | /25 | 10.25.24.66 – 10.25.24.96 |

Продовження таблиці 3.3

| | | | | |
|---|---|---|---|---|
| Hrachov_PC_2.2 | 31 | 10.25.24.64 | /25 | 10.25.24.97 – 10.25.24.127 |
| Hrachov_PC_2.3 | 31 | 10.25.24.64 | /25 | 10.25.24.128 –10.25.24.158 |
| Hrachov_PC_2.4 | 31 | 10.25.24.64 | /25 | 10.25.24.159 –10.25.24.189 |
| Hrachov_PC_3.1 | 63 | 10.25.25.0 | /24 | 10.25.25.2 – 10.25.25.65 |
| Hrachov_PC_3.2 | 63 | 10.25.25.0 | /24 | 10.25.25.66 – 10.25.25.129 |
| Hrachov_PC_3.3 | 63 | 10.25.25.0 | /24 | 10.25.25.130 –10.25.25.193 |
| Hrachov_PC_3.4 | 58 | 10.25.25.0 | /24 | 10.25.25.194 –10.25.25.252 |
| Hrachov_PC_4.1 | 5 | 10.25.26.0 | /26 | 10.25.26.2 – 10.25.26.6 |
| Hrachov_PC_4.2 | 5 | 10.25.26.0 | /26 | 10.25.26.7 – 10.25.26.11 |
| Hrachov_PC_4.3 | 5 | 10.25.26.0 | /26 | 10.25.26.12 – 10.25.26.16 |
| Hrachov_PC_4.4 | 5 | 10.25.26.0 | /26 | 10.25.26.17 – 10.25.26.21 |
| Hrachov_PC_4.5 | 5 | 10.25.26.0 | /26 | 10.25.26.22 – 10.25.26.26 |
| Hrachov_PC_4.6 | 5 | 10.25.26.0 | /26 | 10.25.26.30 – 10.25.26.34 |
| Hrachov_PC_4.7 | 5 | 10.25.26.0 | /26 | 10.25.26.35 – 10.25.26.39 |

Продовження таблиці 3.3

| | | | | |
|---|---|---|---|---|
| Hrachov_PC_4.8 | 5 | 10.25.26.0 | /26 | 10.25.26.40 – 10.25.26.44 |
| Hrachov_PC_4.9 | 5 | 10.25.26.0 | /26 | 10.25.26.45 – 10.25.26.49 |
| Hrachov_PC_4.10 | 5 | 10.25.26.0 | /26 | 10.25.26.50 – 10.25.26.54 |
| Hrachov_PC_4.11 | 5 | 10.25.26.0 | /26 | 10.25.26.55 – 10.25.26.59 |
| Hrachov_PC_4.12 | 3 | 10.25.26.0 | /26 | 10.25.26.60 – 10.25.26.62 |
| Hrachov-PC_5.1 | 1 | 10.25.26.64 | /27 | 10.25.26.66 |
| Hrachov-PC_5.1 | 1 | 10.25.26.64 | /27 | 10.25.26.67 |
| Hrachov-PC_5.1 | 1 | 10.25.26.64 | /27 | 10.25.26.68 |
| Hrachov-PC_5.1 | 1 | 10.25.26.64 | /27 | 10.25.26.69 |

Далі необхідно виконати налаштування ip-адрес на мережевих приладах та їх інтерфейсах

Таблиця 3.4 – Адреси пристроїв

| **Ім`я пристрою** | **Інтерфейс** | **Ip адреса** | **Маска** | **Інтерфейс підключеного пристрою** |
|---|---|---|---|---|
| Hrachov_Router1 | Gig0/0/0 | 10.1.3.1 | /30 | Hrachov_Router1 Gig0/0/0 |
| | Serial0/1/0 | 10.1.3.5 | /30 | Hrachov_Router1 Serial0/1/0 |
| | Serial0/2/0 | 10.1.3.18 | /30 | Hrachov_Router3 Serial0/1/0 |

Продовження таблиці 3.4

| | | | | |
|---|---|---|---|---|
| Hrachov_Router2 | Gig0/0/0 | 10.1.3.2 | /30 | Hrachov_Router1 Gig0/0/0 |
| | Gig/0/0/1 | 10.1.3.13 | /30 | Hrachov_Router4 Gig0/0/1 |
| | Gig/0/0/2 | 10.25.24.1 | /26 | Hrachov_SW_1.2 Gig0/1 |
| Hrachov_Router3 | Gig0/0/0 | 10.25.26.1 | /26 | Gig0/1 Hrachov_SW_4.3 |
| | Serial0/1/0 | 10.1.3.17 | /30 | Hrachov_Router1 Serial0/1/0 |
| | Serial0/1/1 | 10.1.3.9 | /30 | Hrachov_Router4 Serial0/1/1 |
| | Serial0/2/0 | 209.165.202.1 | /30 | Hrachov_IPS Serial0/1/0 |
| Hrachov_IPS | Serial0/1/0 | 209.165.202.1 | /30 | Hrachov_Router3 Serial0/2/0 |
| | Gig0/0/0 | 64.100.13.1 | /30 | Hrachov_Router0 Gigo/0/0 |
| Hrachov_Router0 | Gig0/0/0 | 64.100.13.1 | /30 | Hrachov_IPS Gig0/0/0 |
| | Gig0/0/1 | 10.25.26.65 | /27 | Hrachov_SW_5.1 |
| Hrachov_Router4 | Gig0/0/1 | 10.1.3.14 | /30 | Hrachov_Router2 Gig0/0/1 |
| | Serial0/1/0 | 10.1.3.6 | /30 | Hrachov_Router1 Serial0/1/0 |
| | Serial0/1/1 | 10.1.3.10 | /30 | Hrachov_Router3 Serial0/1/1 |
| | Gig0/0/0 | 10.25.24.66 | /26 | Hrachov_SW_2.1 Gig0/1 |
| | Gig0/0/2 | 10.25.25.1 | /24 | Hrachov_SW_3.1 Gig0/1 |

Продовження таблиці 3.4

| | | | | |
|---|---|---|---|---|
| Hrachov_SW_1.1 | Fa0/1 | | | Hrachov_SW_1.2 Fa0/1 |
| | Fa0/2 | | | Hrachov_SW_1.2 Fa0/2 |
| | Fa0/4 | | | Hrachov_SW_1.3 Fa0/6 |
| | Fa0/3 | | | Hrachov_SW_1.3 Fa0/5 |
| Hrachov_SW_1.2 | Fa0/1 | | | Hrachov_SW_1.1 Fa0/1 |
| | Fa0/2 | | | Hrachov_SW_1.1 Fa0/2 |
| | Fa0/3 | | | Hrachov_SW_1.3 Fa0/3 |
| | Fa0/4 | | | Hrachov_SW_1.3 Fa0/4 |
| Hrachov_SW_4.3 | Fa0/1 | | | Hrachov_SW_4.1 Fa0/1 |
| | Fa0/2 | | | Hrachov_SW_4.2 Fa0/1 |
| Hrachov_SW_5.1 | Gig0/1 | | | Hrachov_Router0 Gig0/0/1 |

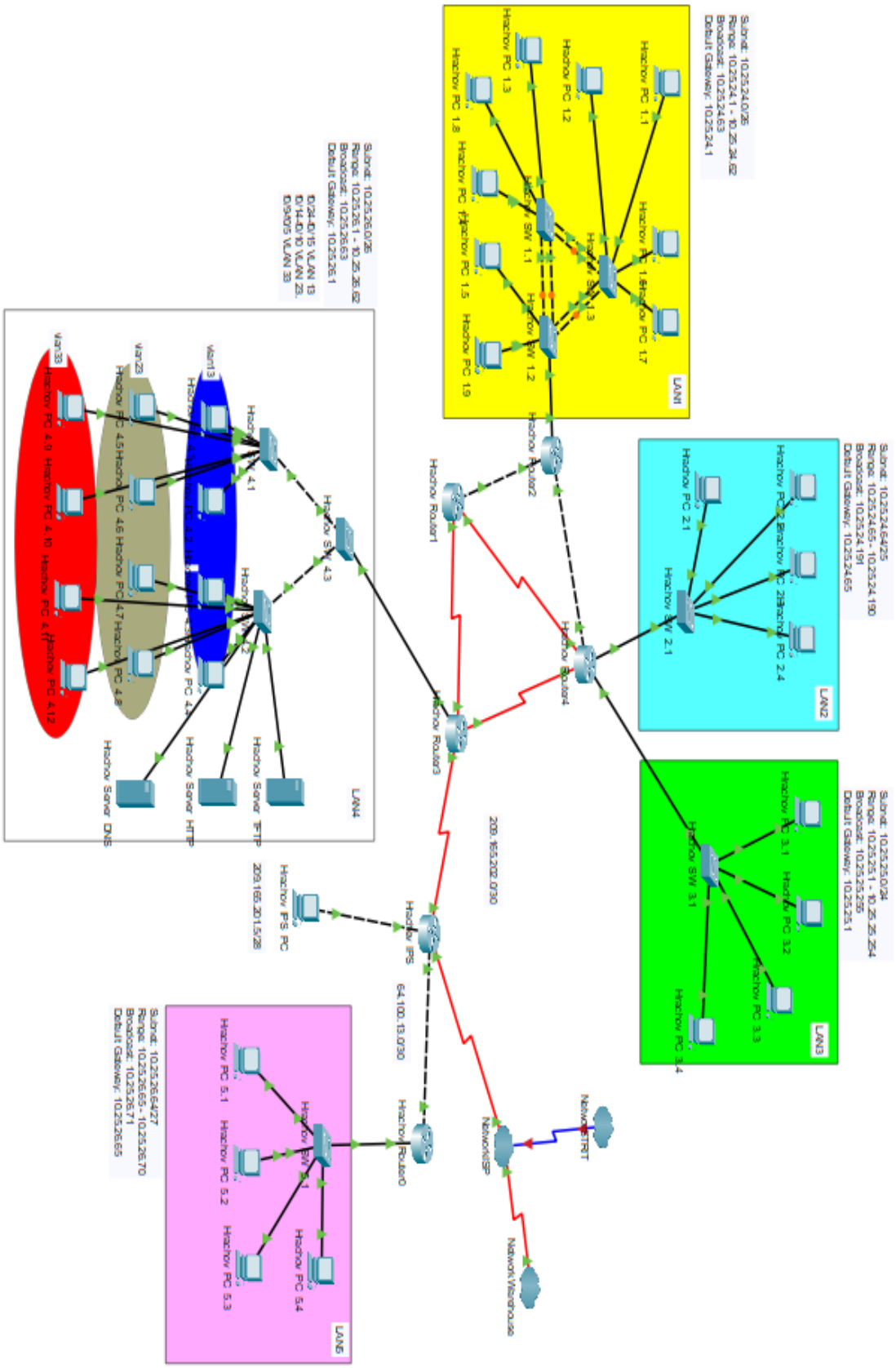
### 3.1.6 Розробка логічної топології мережі підприємства Landlord

На основі таблиць 3.3 та 3.4 за допомогою програми Cisco Packet Tracer побудовано комп’ютерна модель мережі підприємства Landlord (див. рисунок 4.1)

Для налаштування IP-адрес на кінцевих пристроях були використанні можливості як і графічного інтерфейсу так и командної строки.

Налаштування комутаторів та маршрутизаторів виконувалось виключно за допомогою командної строки.

Рисунок 3.1 – Побудована мережа підприємства Landlord



### 3.1.7 Базове налаштування пристроїв

Як приклад базового налаштування пристроїв буде наведене налаштування Hrachov_Router4 .

Переходить в режим конфігурації консолі - Hrachov_Router4(config)#line console 0.

Встановлює пароль "hrachov123" для доступу до консолі - Hrachov_Router4(config-line)#password hrachov123.

Дозволяє використання встановленого паролю для входу в консоль - Hrachov_Router4(config-line)#login.

Переходить в режим конфігурації віртуальних термінальних ліній (VTY) з 0 по 4 - Hrachov_Router4(config-line)#line vty 0 4.

Встановлює пароль "hrachov123" для VTY ліній - Hrachov_Router4(config-line)#password hrachov123.

Дозволяє використання встановленого паролю для входу по VTY лініях - Hrachov_Router4(config-line)#login.

Встановлює захищений (шифрований) пароль "privilaged_hrachov123" для доступу до привілейованого режиму - Hrachov_Router4(config-line)#enable secret privilaged_hrachov123.

Вмикає шифрування всіх паролів, що зберігаються у відкритому вигляді в конфігурації - Hrachov_Router4(config)#service password-encryption.

Встановлює банер повідомлення дня (MOTD), який відображається під час входу на пристрій - Hrachov_Router4(config)#banner motd #HRACHOV DIPLOM 123 AUTORIZATION#.

Створює користувача "hrachov" з привілеєм 15 (максимальні права) і шифрованим паролем "hrachov123" - Hrachov_Router4(config)#username hrachov privilege 15 secret hrachov123.

Встановлює доменне ім'я "Hrachov_Router4" для пристрою - Hrachov_Router4(config)#ip domain-name Hrachov_Router4.

Запускає процес генерації ключа RSA для використання протоколу SSH - Hrachov_Router4(config)#crypto key generate rsa.

Повертається до конфігурації VTY ліній (0-4) - Hrachov_Router4(config)#line vty 0 4.

Обмежує віддалений доступ до пристрою лише за допомогою протоколу SSH - Hrachov_Router4(config-line)#transport input ssh.

Налаштовує аутентифікацію для VTY ліній з використанням локальної бази користувачів - Hrachov_Router4(config-line)#login local.

Вихід з режиму конфігурації ліній VTY - Hrachov_Router4(config-line)#exit.

Переходить в режим конфігурації інтерфейсу для серійного інтерфейсу se0/1/0 - Hrachov_Router4(config)#interface se0/1/0.

Встановлює тактову частоту 128000 для серійного інтерфейсу se0/1/0 - Hrachov_Router4(config-if)#clock rate 128000.

Вихід з режиму конфігурації інтерфейсу - Hrachov_Router4(config-if)#exit.

Переходить в режим конфігурації інтерфейсу для серійного інтерфейсу Serial0/1/1 - Hrachov_Router4(config)#interface Serial0/1/1.

Встановлює тактову частоту 128000 для серійного інтерфейсу Serial0/1/1 - Hrachov_Router4(config-if)#clock rate 128000.

Вихід з режиму глобальної конфігурації та повернення в привілейований режим - Hrachov_Router4(config-if)#end.

Зберігає поточну конфігурацію в пам'ять - Hrachov_Router4#write memory.

На рисунку 3.2 виконано команду show running-config.


Рисунок 3.2 – Базова конфігурація роутера

### 3.1.8 Налаштування маршрутизації

Між EIGRP та OSPF було обрано протокол динамічної маршрутизації OSPF , тому що він краще підходить для великих мереж. OSPF швидко адаптується до змін у топології мережі, мінімізуючи час простою і втрату пакетів. Він використовує алгоритм Dijkstra для обчислення найкоротшого шляху, що забезпечує швидку і точну маршрутизацію. OSPF добре підходить для великих і складних мереж. Він підтримує концепцію областей (areas), що дозволяє зменшити обсяг трафіку маршрутних оновлень і розділити мережу на більш керовані сегменти. Налаштування маршрутизації для роутера 4 зображено на рисунку 3.2.

```
Hrachov_Router4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
O       10.1.3.0/30 [110/2] via 10.1.3.13, 01:10:24, GigabitEthernet0/0/1
C       10.1.3.4/30 is directly connected, Serial0/1/0
L       10.1.3.6/32 is directly connected, Serial0/1/0
C       10.1.3.8/30 is directly connected, Serial0/1/1
L       10.1.3.10/32 is directly connected, Serial0/1/1
C       10.1.3.12/30 is directly connected, GigabitEthernet0/0/1
L       10.1.3.14/32 is directly connected, GigabitEthernet0/0/1
O       10.1.3.16/30 [110/66] via 10.1.3.13, 00:04:26, GigabitEthernet0/0/1
C       10.25.24.0/25 is directly connected, GigabitEthernet0/0/0
L       10.25.24.65/32 is directly connected, GigabitEthernet0/0/0
C       10.25.25.0/24 is directly connected, GigabitEthernet0/0/2
L       10.25.25.1/32 is directly connected, GigabitEthernet0/0/2
O       10.25.26.0/26 [110/65] via 10.1.3.9, 00:03:05, Serial0/1/1
```

Рисунок 3.3 – Перевірка командою sh ip route роутера Hrachov_Router4

На рисунку 3.3 можна побачити , що все необхідні мережі додано , тому маршрутизація налаштована правильно. Також протокол ICMP успішно доходить з мережі в мережу

Sending 5, 100-byte ICMP Echos to 10.1.3.9, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/20 ms

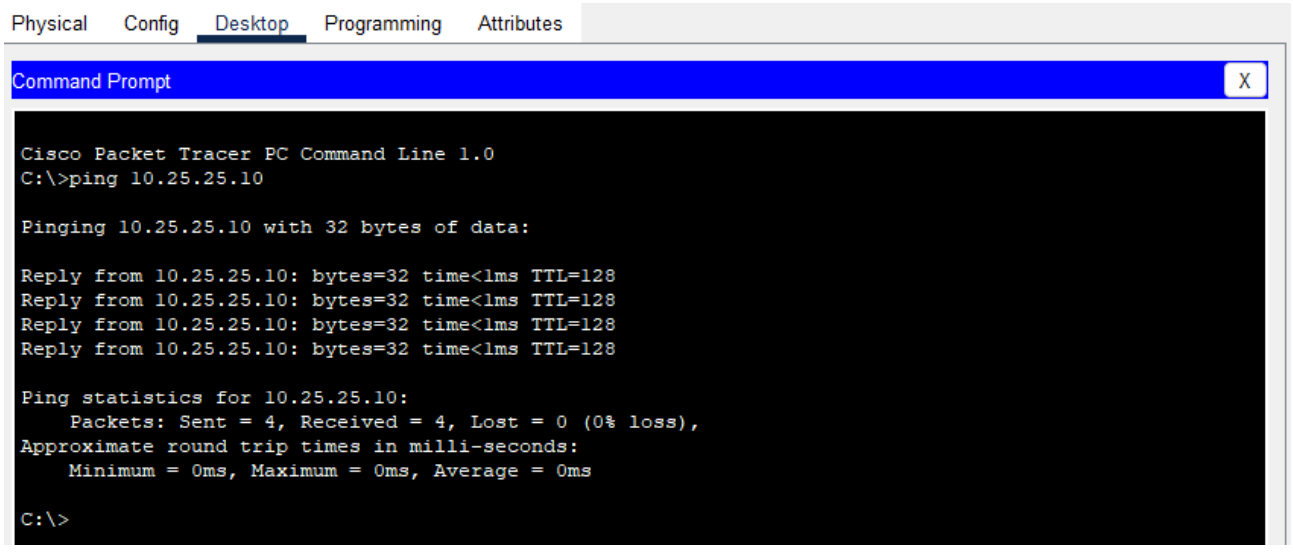



Рисунок 3.4 – Виконання команди Ping з ПК мережі Lan1 до ПК мережі Lan2

### 3.1.9 Налаштування роботи Провайдера

Компанію провайдера було обрано “НТУ Інтернет” бо вони спеціалізуються на рішення для підприємств, мають безкоштовне підключення та забезпечують високошвидкісний інтернет швидкість до 500Мбіт/с.

Потрібно підключити сервіс DNS на DNS сервері як на рисунку 3.4.

DNS сервер виконує роль перекладача між зрозумілими для людей іменами хостів та IP-адресами, які розуміють комп'ютери.

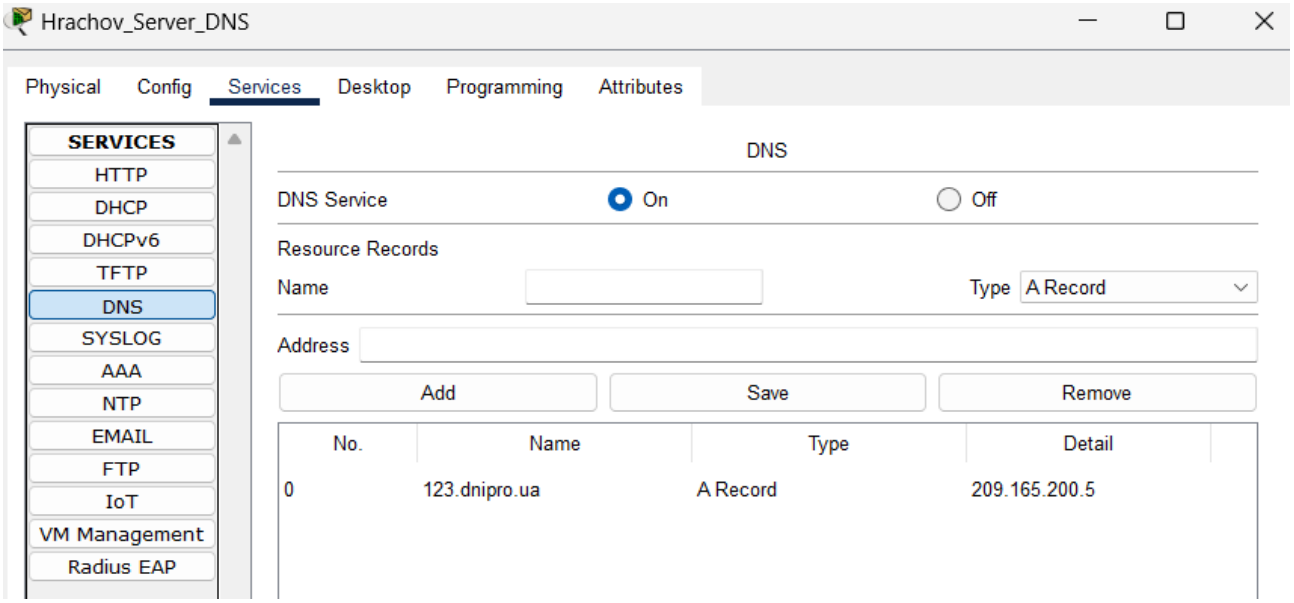



Рисунок 3.5 – Включено сервіс DNS

Також було включено сервіс HTTP на пристрої HTTP_Server , який виконує роль представлення теми роботи за допомогою html та DNS сервера , який представляє адресу HTTP сервера як 123.dnipro.ua

На рисунку 3.5 представлено налаштування NAT на маршрутизаторі провайдера

```
Router#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/0/0
Inside Interfaces: GigabitEthernet0/0/1
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool Internet refCount 0
 pool Internet: netmask 255.255.255.224
       start 209.165.200.5 end 209.165.200.30
       type generic, total addresses 26 , allocated 0 (0%), misses 0
```

Рисунок 3.6 – Налаштування NAT на маршрутизаторі Router_IPS

Далі потрібно налаштувати VPN канал

Налаштування ISAKMP (IKE) політики :

crypto isakmp policy 10 - Створює або налаштовує політику ISAKMP з пріоритетом 10.

encr aes 256 - Встановлює AES-256 як алгоритм шифрування для IKE.

hash sha256 - Встановлює SHA-256 як алгоритм хешування для IKE.

authentication 1234 - Встановлює попередньо узгоджений ключ як метод аутентифікації.

group 14 - Встановлює групу 14 для обміну ключами.

lifetime 86400 - Встановлює час життя політики ISAKMP на 86400 секунд

На рисунку 3.7 зображено налаштування isakmp політики

```
Router>enable
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                86400 seconds, no volume limit
```

Рисунок 3.7 – Виконання команди show crypto isakamp policy

Визначення попередньо узгодженого ключа:

crypto isakmp key 1234 address 64.100.13.1 - Встановлює попередньо узгоджений ключ для з'єднань з віддаленим маршрутизатором, який має IP-адресу 64.100.13.1.

Налаштування списку доступу для трафіку, що підлягає шифруванню:

access-list 110 permit ip 64.100.13.0 0.0.0.3 10.25.26.65 0.0.0.21 - Створює список доступу з номером 110, який дозволяє IP-трафік між локальною мережею 64.100.13.0/30 та віддаленою мережею 10.25.26.64/27.

Налаштування трансформаційного набору:

crypto ipsec transform-set ESP-AES256-SHA256 esp-aes 256 esp-sha256-hmac - Створює набір трансформацій під назвою ESP-AES256-SHA256, який використовує шифрування AES-256 та аутентифікацію HMAC-SHA-256.

Mode tunnel - Встановлює тунельний режим для набору трансформацій.

Налаштування криптографічного списку :

crypto map VPN-MAP 10 ipsec-isakmp - Створює або налаштовує криптографічну карту з ім'ям VPN-MAP та пріоритетом 10 для використання з IPsec та ISAKMP.

set peer 64.100.13.1 - Встановлює IP-адресу віддаленого VPN-партнера.

set transform-set ESP-AES256-SHA256 - Вказує набір трансформацій, який буде використовуватися.

match address 110 - Вказує, що цей криптографічний список буде застосовуватись до трафіку, що відповідає списку доступу 110.

Прив'язка криптографічного списку до інтерфейсу:

interface GigabitEthernet0/0 - Входить в режим конфігурації інтерфейсу GigabitEthernet0/0.

crypto map VPN-MAP - Прив'язує криптографічну карту VPN-MAP до інтерфейсу.

```
Router#show crypto ipsec transform-set
Transform set VPN-SET: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },

Router#
```

Рисунок 3.8 – Перевірка трансформаційних наборів

Протестуємо за допомогою команди ping досяжність пакетів з підмережі Lan1 да Lan6. Результат тестування зображено на рисунку 3.9.

```
C:\>ping 10.25.26.70

Pinging 10.25.26.70 with 32 bytes of data:

Reply from 10.25.26.70: bytes=32 time<1ms TTL=128
Reply from 10.25.26.70: bytes=32 time=1ms TTL=128
Reply from 10.25.26.70: bytes=32 time<1ms TTL=128
Reply from 10.25.26.70: bytes=32 time<1ms TTL=128

Ping statistics for 10.25.26.70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Рисунок 3.9 – Виконання команди ping з ПК Lan1 до ПК у віддаленій мережі

### 3.2 Захист інформації в комп’ютерній або кіберфізичній системі від несанкціонованого доступу

Потрібно створити та налаштувати комутатори так щоб було створено нові Vlan :

vlan 13 - Accounting

vlan 23 - Resources_Department

vlan 33 - Guest

vlan 99 - Management

vlan 100 – Native

Зробити це можна за допомогою таких команд в командному рядку комутатора:

vlan 13 name Accounting

vlan 23 name Resources_Department

vlan 33 name Guest

vlan 99 name Management

vlan 100 name Native

де команда vlan – створює нову підмережу , а команда name – додає назву цій віртуальній підмережі

Також потрібно налаштувати транкові порти, які будуть передавати трафік Vlan.

interface range fa0/3 - 10

switchport mode access

switchport access vlan 13

interface range fa0/11 - 18

switchport mode access

switchport access vlan 23

interface range fa0/19 - 24

switchport mode access

switchport access vlan 33

На маршрутизаторі потрібно налаштувати маршрутизацію між Vlan

interface gig0/1.13

encapsulation dot1Q 13

ip address 10.25.26.1 255.255.255.192

interface gig0/1.23

encapsulation dot1Q 23

ip address 10.25.26.65 255.255.255.192

interface gig0/1.33

encapsulation dot1Q 33

ip address 10.25.26.129 255.255.255.192

interface gig0/1.99

encapsulation dot1Q 99

ip address 10.25.26.193 255.255.255.192

interface gig0/1.100

encapsulation dot1Q 100 native

ip address 10.25.26.225 255.255.255.192

```
Switch#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Gig0/1, Gig0/2
13   Accounting                       active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
23   Resources_Department             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
33   Guest                            active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
99   Management                       active
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Рисунок 3.10 – Вивід команди sh vlan br на одному з комутаторів

Для атвоматичної адресації пристроїв на Vlan потрібно налаштувати DHCP, попередньо виключивши перші 10 адрес з пулу

ip dhcp excluded-address 10.25.26.1 10.25.26.10

ip dhcp excluded-address 10.25.26.65 10.25.26.74

ip dhcp excluded-address 10.25.26.129 10.25.26.138

ip dhcp excluded-address 10.25.26.193 10.25.26.202 ip dhcp excluded-address 10.25.26.225 10.25.26.234

ip dhcp pool poolvlan13

network 10.25.26.0 255.255.255.192

default-router 10.25.26.1

dns-server 209.165.200.1

ip dhcp pool poolvlan23

network 10.25.26.64 255.255.255.192

default-router 10.25.26.65

dns-server 209.165.200.1

ip dhcp pool poolvlan33

network 10.25.26.128 255.255.255.192

default-router 10.25.26.129

dns-server 209.165.200.1

ip dhcp pool poolvlan99

network 10.25.26.192 255.255.255.192

default-router 10.25.26.193

dns-server 209.165.200.1

ip dhcp pool poolvlan100

network 10.25.26.224 255.255.255.192

default-router 10.25.26.225

dns-server 209.165.200.1

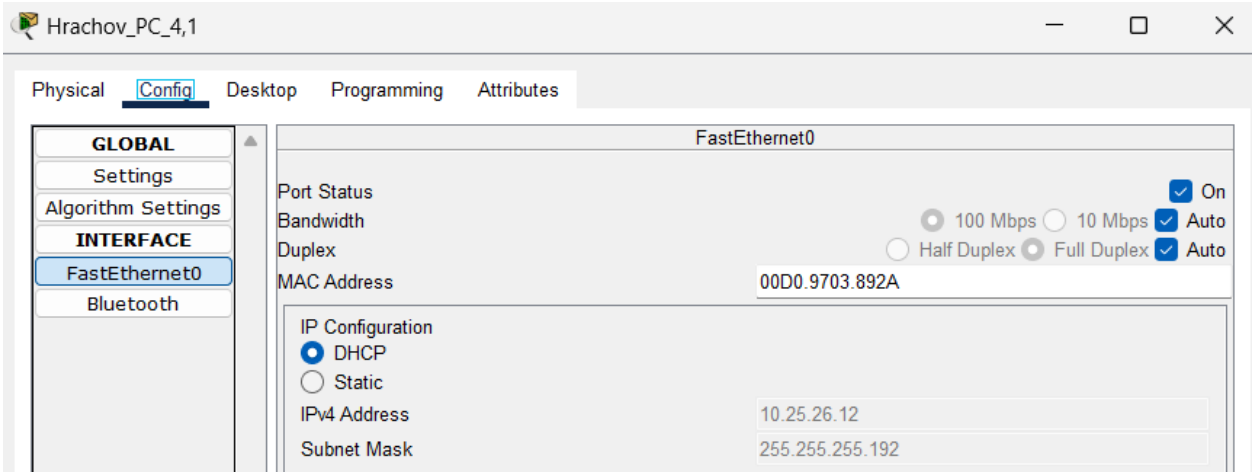
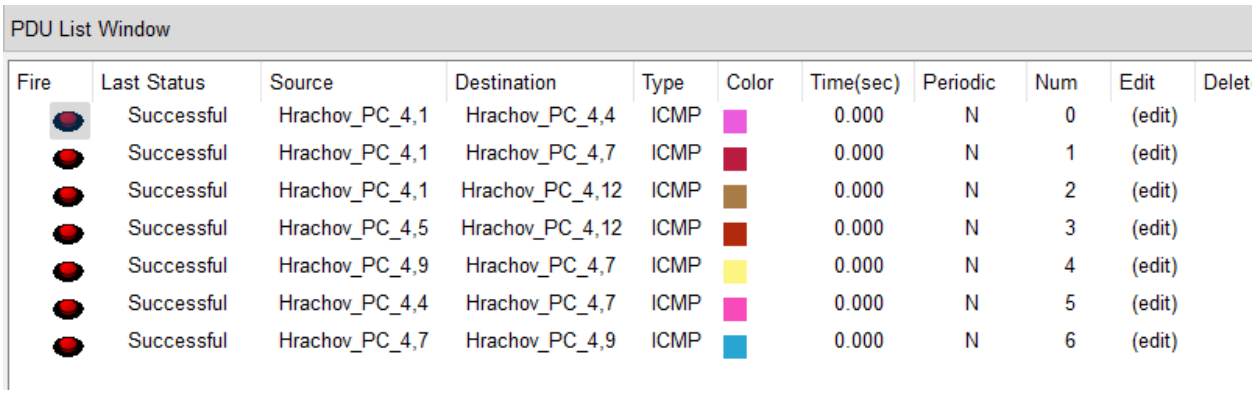



Рисунок 3.11 – Приклад використання DHCP на пристрої Lan4

Після налаштування DHCP протестуємо досяжність пристроїв різних Vlan один до одного. Тестування налаштування Lan4 зображено на рисунку 3.12.


PDU List Window

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delet |
|---|---|---|---|---|---|---|---|---|---|---|
| | Successful | Hrachov_PC_4,1 | Hrachov_PC_4,4 | ICMP | | 0.000 | N | 0 | (edit) | |
| | Successful | Hrachov_PC_4,1 | Hrachov_PC_4,7 | ICMP | | 0.000 | N | 1 | (edit) | |
| | Successful | Hrachov_PC_4,1 | Hrachov_PC_4,12 | ICMP | | 0.000 | N | 2 | (edit) | |
| | Successful | Hrachov_PC_4,5 | Hrachov_PC_4,12 | ICMP | | 0.000 | N | 3 | (edit) | |
| | Successful | Hrachov_PC_4,9 | Hrachov_PC_4,7 | ICMP | | 0.000 | N | 4 | (edit) | |
| | Successful | Hrachov_PC_4,4 | Hrachov_PC_4,7 | ICMP | | 0.000 | N | 5 | (edit) | |
| | Successful | Hrachov_PC_4,7 | Hrachov_PC_4,9 | ICMP | | 0.000 | N | 6 | (edit) | |

Рисунок 3.12 – Тестування роботи програми

Також налаштуєму безпеку для пристроїв , щоб задовільняло умові :

– тільки двом унікальним пристроям був дозволений доступ до порту.

– MAC-адрес пристрою розпізнавався динамічно і додавався в поточну конфігурацію.

– під час порушенні системи безпеки з’являлося повідомлення, порт залишався включеним.

```
interface range fa0/1 - 2
    switchport mode access
    switchport port-security
    switchport port-security maximum 2
    switchport port-security mac-address sticky
    switchport port-security violation restrict
```

```
Router#show ip dhcp pool

Pool poolvlan13 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.25.26.1           10.25.26.1       - 10.25.26.62      0    / 5     / 62

Pool poolvlan23 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.25.26.65          10.25.26.65      - 10.25.26.126     0    / 5     / 62

Pool poolvlan33 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.25.26.129         10.25.26.129     - 10.25.26.190     0    / 5     / 62

Pool poolvlan99 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.25.26.193         10.25.26.193     - 10.25.26.254     0    / 5     / 62
```

Рисунок 3.14 – Вивід команди show ip dhcp pool на маршрутизаторі

# 4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

## 4.1 Структура IoT системи SWMS складського приміщення

Систему складського приміщення підприємства Landlord було побудовано у програмі Cisco Packet Tracer. Система буде складатись з трьох трьох мереж:

1.Network Strit:

– smartphone (x2): Портативні пристрої для здійснення зв'язку, доступу до Інтернету та використання різних додатків;

– tablet (x2): Планшети для мобільного доступу до інформації та виконання завдань;

– cell Tower: Вежа для забезпечення стільникового зв'язку та покриття мережі в певній області;

– central Office Server: Сервер, що використовується для приєднання мережі Strit до маршрутизатора провайдера.

2.Network Provider:

– server_DNS: Сервер доменних імен для перетворення доменних імен в IP-адреси;

– server_IOT: Сервер для обробки даних від пристроїв Інтернету речей;

– cisco Catalyst 2960: Комутатор для забезпечення локального мережевого з'єднання та комутації даних між серверами;

– router_ISP_Warehouse: Маршрутизатор для маршрутизації даних між різними мережами та забезпечення доступу до Інтернету;

– pt-cloud Device: Пристрій, можливо, пов'язаний із хмарними послугами, такий як обчислення в хмарі або зберігання даних в хмарі.

3.Network Warehouse:

– підсистема пожежогасіння : використовує датчик інфрочервоного діапазону з спринклерами;

– підсистема контролю вологості : використовує датчик вологості та вентиляцію;

– підсистема контролю доступу : використовує RFID технологію;

– виконує моніторинг стану середовища підприємства.

## 4.2 Розробка Network Strit

Додамо до кластеру Network Strit необхідні пристрої та підключемо на них інтерфейси 3g/4g cell. Ця мережа потрібна для віддаленого моніторингу системи , також з цієї мережі можна підключитись з відділу керування складом в офісному приміщенні підприємства. На рисунку 4.1 можна побачити побудовану мережу та підключення пристроїв до вежі.

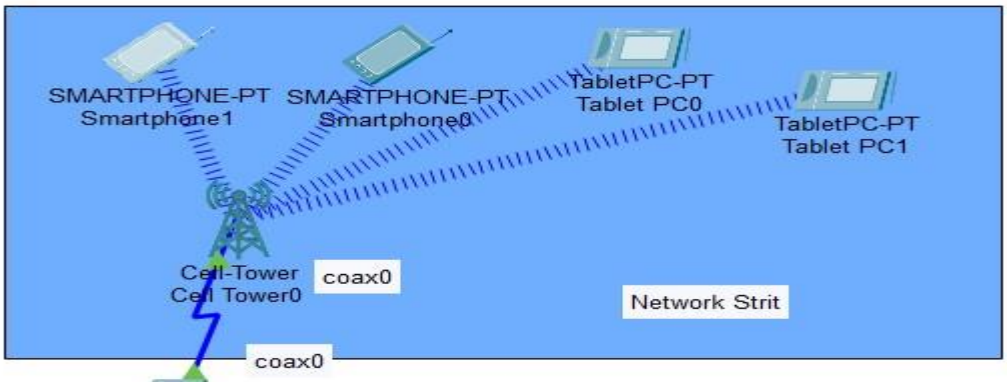



Рисунок 4.1 – Побудована мережа Network Strit

Щоб підключити прилади до вежі стільникового зв’язку потрібно ввімкнути інтерфейс 3g/4g, як зображено на рисунку 4.2, та налаштувати зону покриття 1000 футів , що як раз задовільняє розташуванню офісу та складського приміщення підприємства.

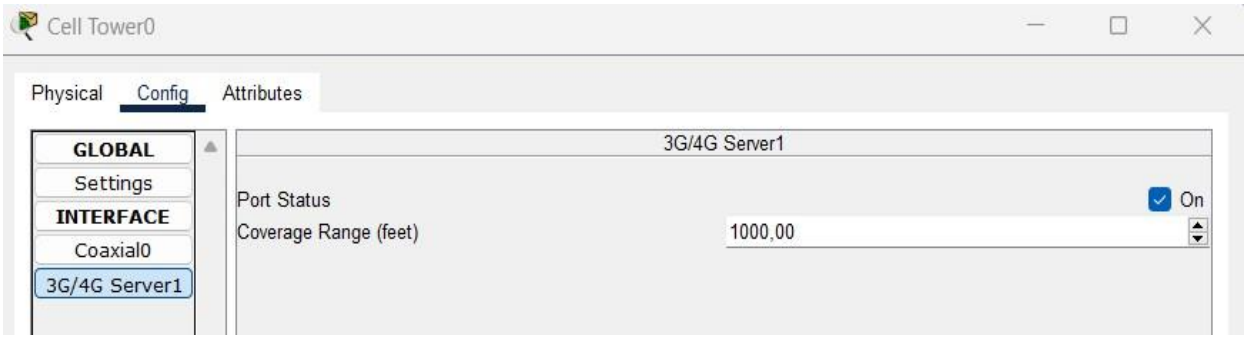



Рисунок 4.2 – Ввімкнено інтерфейс 3g/4g звязку та обрано зону покриття – макс(1000)

Щоб підключити мережу до роутеру Rout_ISP_Warehouse потрібно підключити Cell Tower до Central Office-Server за допомогою коаксіального кабелю.

Основне призначення коаксіального кабелю – передача сигналу в різних областях техніки:

- системи зв'язку;
- мовленнєві мережі;
- комп'ютерні мережі;
- системи дистанційного управління, вимірювання та контролю;
- системи сигналізації й автоматики;
- системи об'єктивного контролю та відеоспостереження.

## 4.3 Налаштування Network_Provider

Прилади мережі Network_Provider будуть реалізовувати підключення з віддаленої частини системи до IoT системи складського приміщення, також містить сервери в яких налаштовано DNS та IoT сервіси. На таблиці 4.1 зображена адресація інтерфейсів цієї мережі.

Таблиця 4.1 – Адресація інтерфейсів в мережі Network_Provider

| Пристрій | Інтерфейс | IP-адреса | Префікс | Підключення | |
|---|---|---|---|---|---|
| | | | | Назва пристрою | Інтерфейс |
| Rout_ISP | G0/0 | 20.3.201.225 | /27 | Central Office Server | Backbone |
| | G0/1 | 10.3.0.1 | /24 | Sw_ISP | G0/1 |
| | G0/2 | 20.3.200.225 | /27 | Cloud_WAN | Eth6 |
| Server_DNS | NIC | 10.3.0.203 | /24 | Sw_ISP | F0/1 |
| Server_IoT | NIC | 10.3.0.202 | /24 | Sw_ISP | F0/2 |

Підключення з мережі до IoT системи виконано зо допомогою кабеля, що надасть більшу щвидкість та захищеність для системи загалом. На рисунку 4.3 зображено підключення приладів в мережі Network_Provider

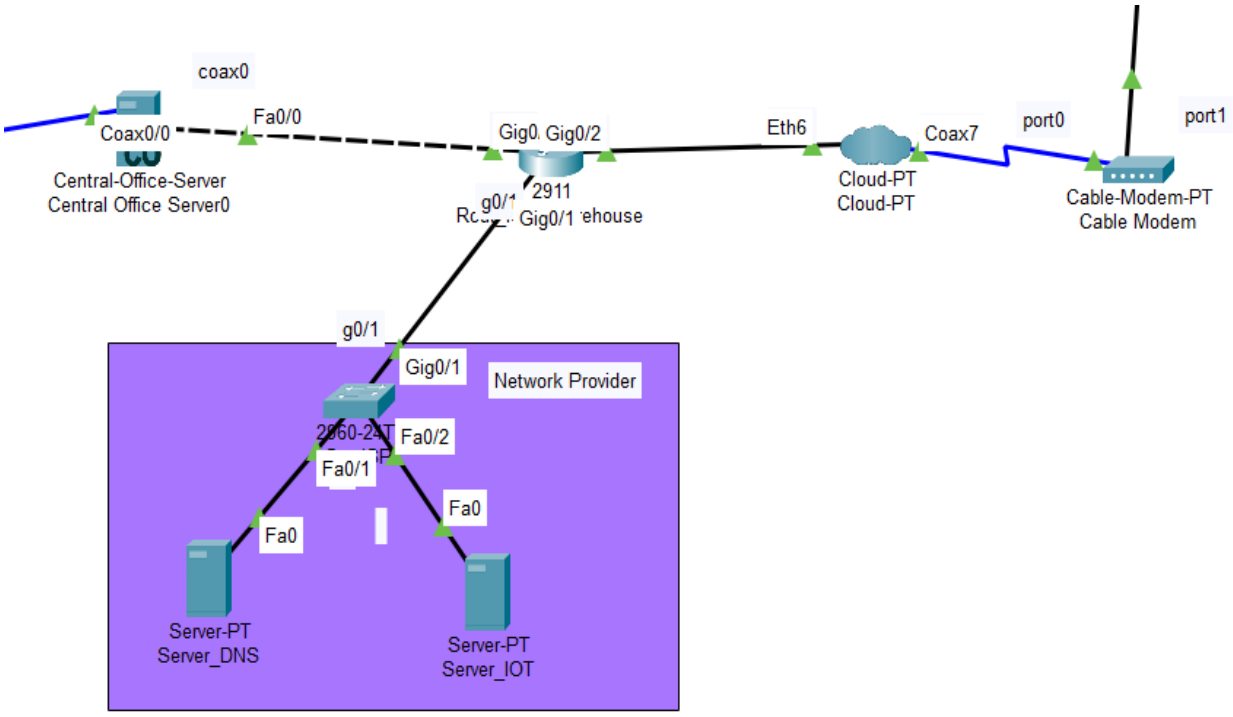



Рисунок 4.3 – Побудована мережа Network_Isp

### 4.3.1 Базові налаштування маршрутизатора

Отже виконаємо базові налаштування на роутері.

enable: Переходить у режим привілеї. В цьому режимі можна виконувати привілейовані (адміністративні) команди.

configure terminal: Входить у режим глобальної конфігурації, де можна налаштовувати різні параметри роутера.

hostname Hrachov_Rout_ISP: Встановлює ім'я хоста (hostname) роутера на "Hrachov_Rout_ISP".

enable secret hrachov: Встановлює захищений пароль для входу в режим привілеї.

line con 0: Входить у конфігураційний режим для консольного порту.

password cisco: Встановлює пароль для входу через консольний порт.

line vty 0 4: Входить у конфігураційний режим для віртуальних терміналів. password cisco: Встановлює пароль для входу через віртуальні термінали.

banner motd # [Banner on Router] #: Встановлює банер яке виводиться при вході в систему.

ip domain-name admin: Встановлює доменне ім'я для роутера.

crypto key generate rsa: Генерує RSA ключі для шифрування трафіку.

username hrachov password hrachov: Створює користувача з ім'ям "hrachov" і паролем "hrachov".

ip ssh version 2: Встановлює версію SSH для забезпечення безпечного з'єднання.

line vty 0 15: Знову входить у конфігураційний режим для віртуальних терміналів.

transport input ssh: Вказує, що можна використовувати лише SSH для віддаленого входу.

login local: Встановлює локальний метод аутентифікації для віртуальних терміналів.

### 4.3.2 Налаштування DHCP на роутері провайдера

ip dhcp excluded-address 20.3.201.225 20.3.201.229: визначає діапазон IP-адрес, які не будуть доступні для динамічного присвоєння DHCP-клієнтам у пулі STRIT.

20.3.201.225 - це перша IP-адреса в діапазоні.

20.3.201.229 - це остання IP-адреса в діапазоні.

ip dhcp pool STRIT: створює пул DHCP під назвою STRIT.

network 20.3.201.224 255.255.255.224: Ця команда визначає мережу для пулу DHCP STRIT.

20.3.201.224 - це IP-адреса мережі.

255.255.255.224 - це маска підмережі для мережі.

default-router 20.3.201.225: визначає шлюз для пулу DHCP STRIT.

20.3.201.225 - це IP-адреса шлюзу за замовчуванням.

dns-server 10.3.0.203: визначає DNS-сервер для пулу DHCP STRIT.

10.3.0.203 - це IP-адреса DNS-сервера.

service DHCP: включає службу DHCP` на маршрутизаторі.

ip dhcp excluded-address 20.3.200.225 20.3.200.229: визначає діапазон IP-адрес, які не будуть доступні для динамічного присвоєння DHCP-клієнтам у пулі WAREHOUSE.

20.3.200.225 - це перша IP-адреса в діапазоні.

20.3.200.229 - це остання IP-адреса в діапазоні.

ip dhcp pool WAREHOUSE: створює пул DHCP під назвою WAREHOUSE.

network 20.3.200.224 255.255.255.224: визначає мережу для пулу DHCP WAREHOUSE.

20.3.200.224 - це IP-адреса мережі.

255.255.255.224 - це маска підмережі для мережі.

default-router 20.3.200.225: визначає шлюз за замовчуванням для пулу DHCP WAREHOUSE.

20.3.200.225 - це IP-адреса шлюзу за замовчуванням.

dns-server 10.3.0.203: визначає DNS-сервер для пулу DHCP WAREHOuSE.

10.3.0.203 - це IP-адреса DNS-сервера

### 4.3.3 Налаштування DNS та IOT серверів

Тепер потрібно налаштувати сервери Server_DNS та Server_IOT , ведемо потрібну ip конфігурацію згідно таблиці 4.1 та підключемо сервіс DNS та IOT.

Створено домен www.hrachov.org

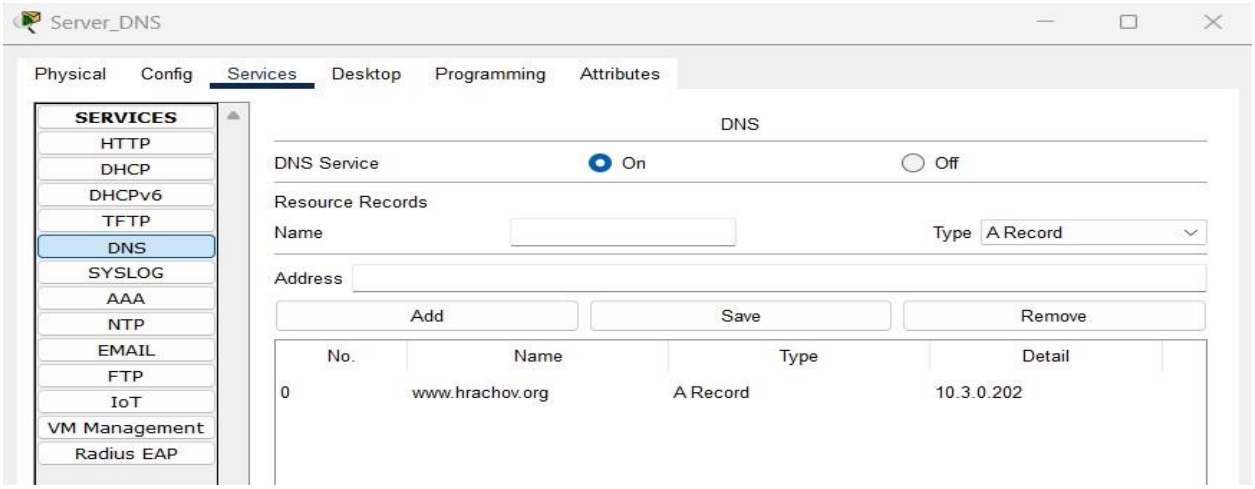



Рисунок 4.4 – Включення сервісу DNS

Також на сервері Server_IOT потрібно додати користувача системою:

Username : Hrachov

Password: hrachov

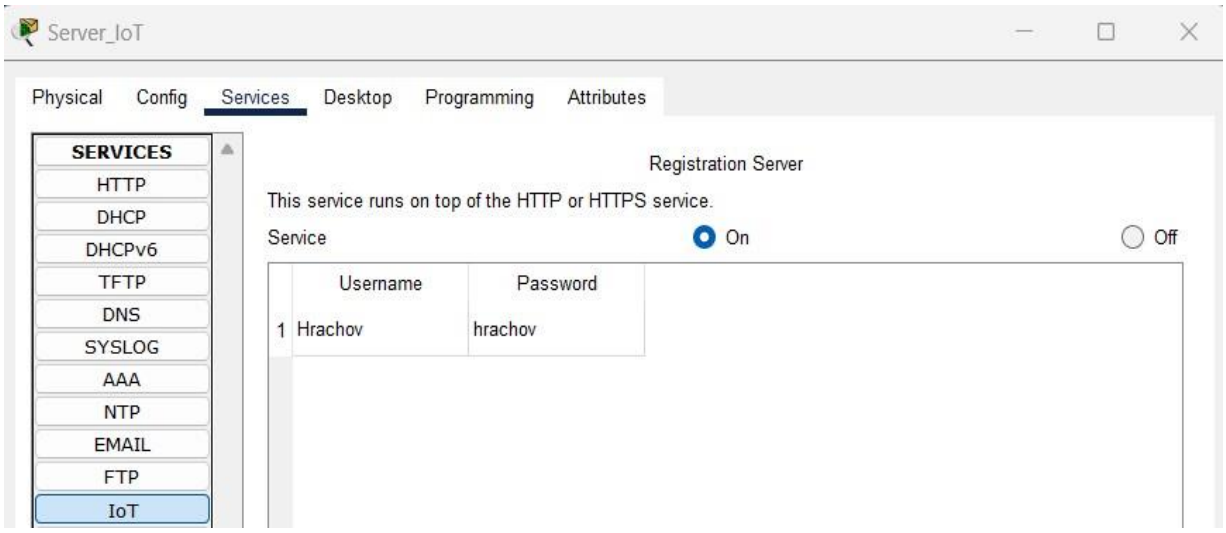



Рисунок 4.5 – Додання користувача Hrachov та ввімкнення сервісу IOT

Перевіримо підключення Центрального сервера за допомогою DHCP

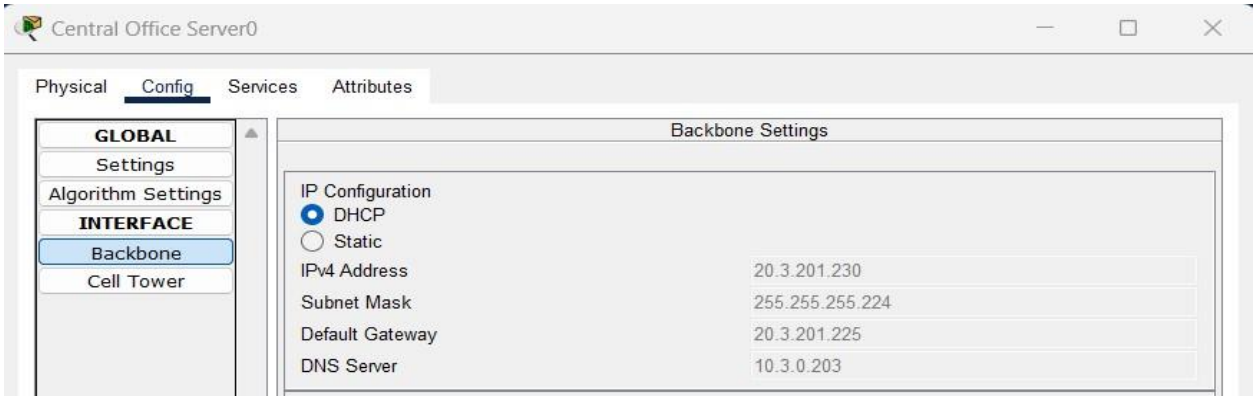



Рисунок 4.6 – DHCP успішно працює

На пристрої cloud-pt оберемо вид підключення – cable , як показано на рисунку 4.7.

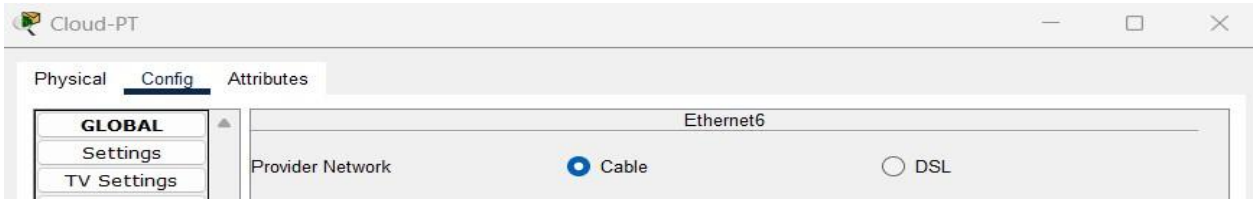



Рисунок 4.7 – Тип підключення – кабель

На кабелі зробимо асоціацію портів coaxial7 - ethernet6

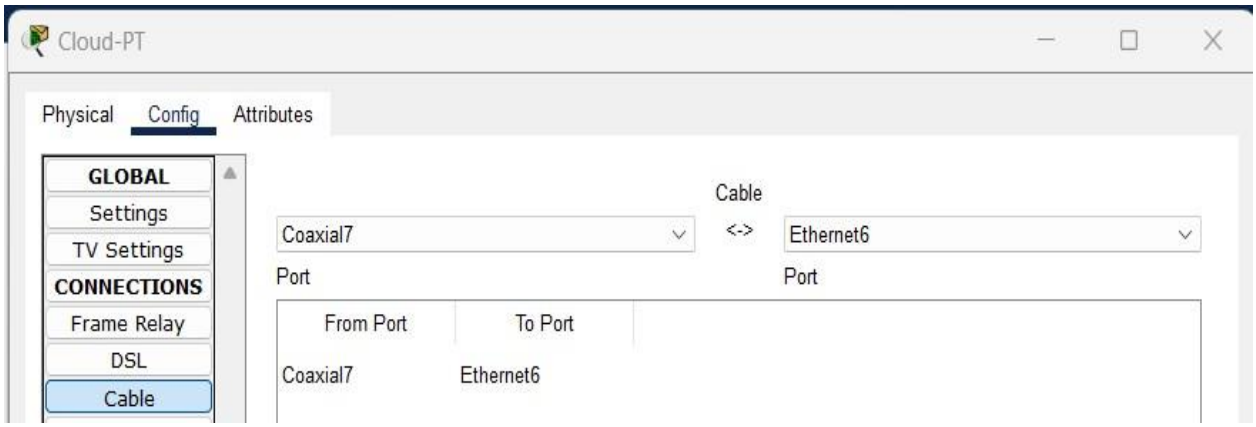



Рисунок 4.8 – успішно виконано асоціацію

## 4.4 Налаштування мережі складського приміщення

Головним маршрутизатором є пристрій DLC 100 , який є головним вузлом системи складського приміщення , налаштуємо його:

SSID – назва мережі (Hrachov) , WPA2-psk – спросіб аутентифікації який дозволяє додати пароль (hrachov123)

На рисунку 4.9 зображено налаштування бездротової мережі Homegateway

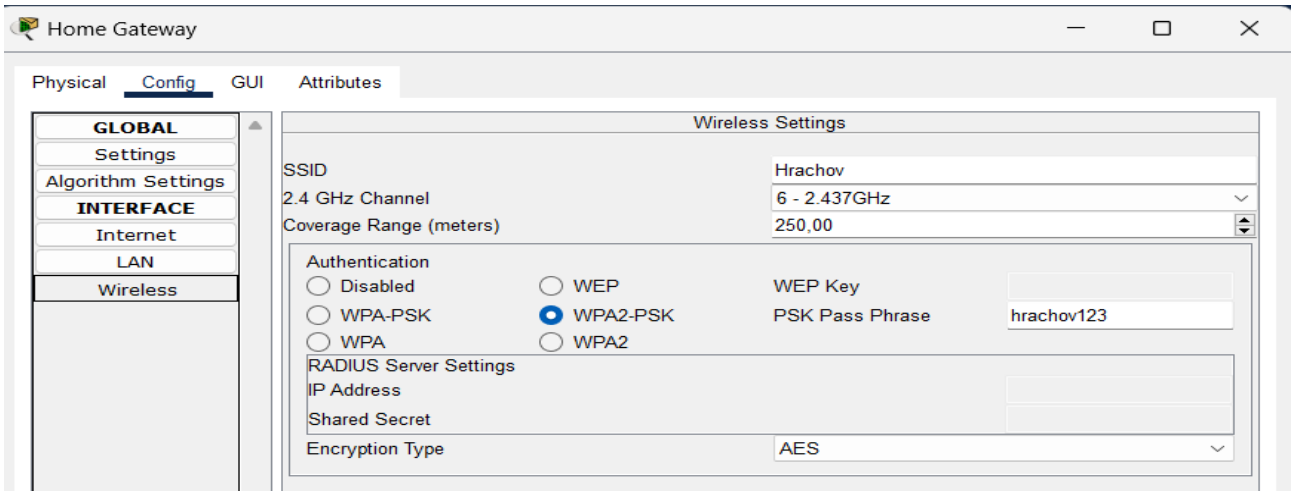



Рисунок 4.9 – Налаштування Wireless інтерфейсу на HomeGateway

Так як HomeGateway дозволяє під’єднати iot пристрої до одної мережі потрібно перевірити чи на всіх пристроях , які ми будемо під’єднувати до маршрутизатора є мережевий адаптер наприклад – PT-IOT-NM_1W

Також при підключенні пристрою до бездротової мережі необхідно переконатися що працює DHCP та чи проходить підключення до серверу IOT за допомогою попередньо створеного доменого ім’я www.hrachov.org

На рисунку 4.10 можна побачити що вдаось підключитися до маршрутизатора та DHCP успішно працює.

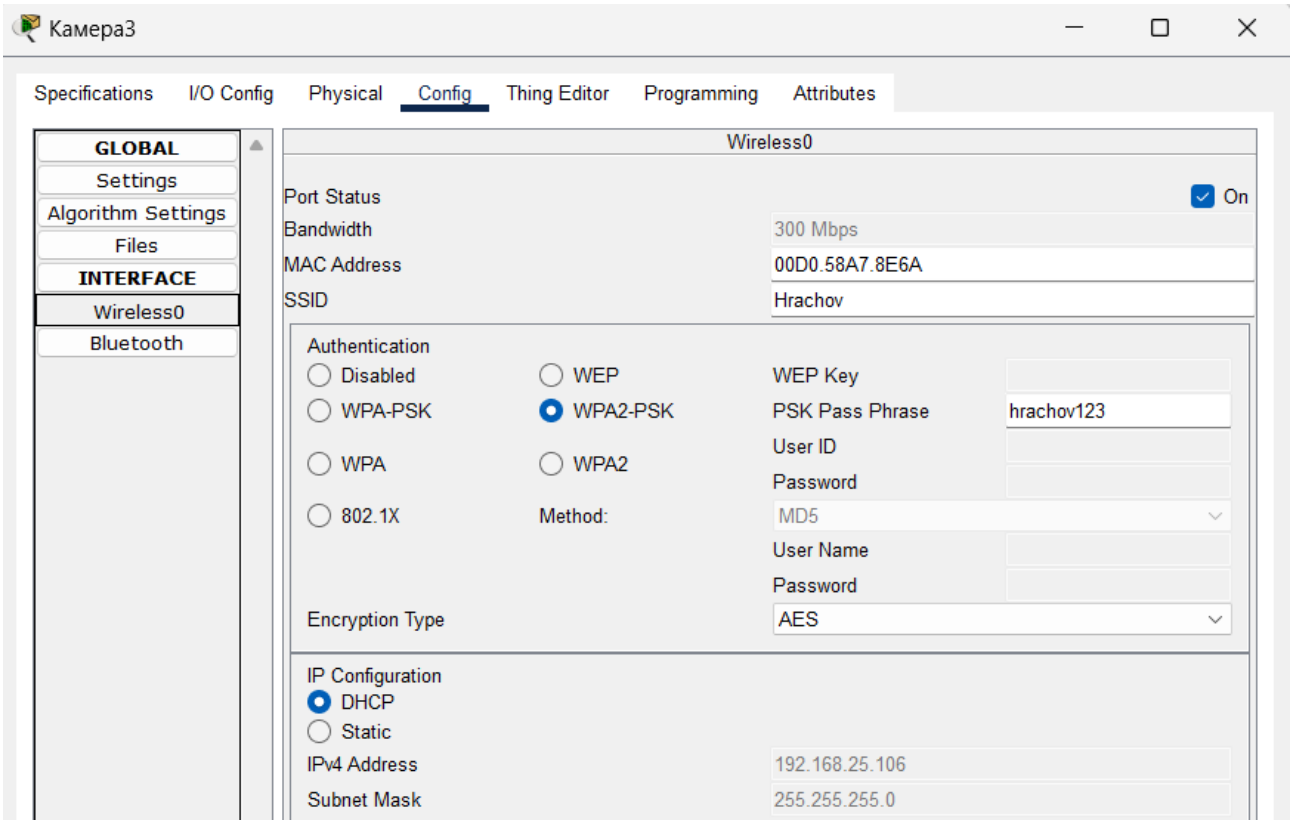



Рисунок 4.10 – Приклад налаштування IoT пристрою

## 4.5 Налаштування безпеки складського приміщення

### 4.5.1 Налаштування доступу до приміщення

Система дозволяє контролювати доступ до складського підприємства за допомогою Rfid міток та Rfid зчитувачів.

У програмі Packet Tracer було додано 5 дверей та 5 Rfid зчитувачів , а також картку доступу у вигляді Rfid Card – яку будемо налаштовувати на відповідні частоти за допомогою яких можна буде отримати доступ до приміщення.

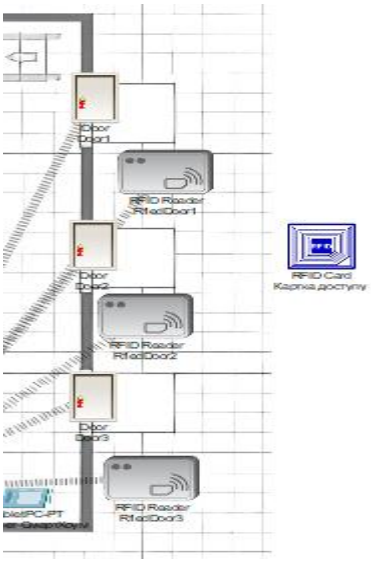


Рисунок 4.11 – Додання пристроїв контролю доступу до топології

Як можна побачити на рисунку 4.11 Rfid зчитувач та Двері знаходяться поряд , це зроблена для імітації реальних дверей з зчитувачами, які активно використовуються на автоматизованих складських приміщенням , як в компанії Amazon.

Далі необхідно додати логіку до користування Rfid технологією. Додаток IoT monitor, який містить інформацію про підключенні пристрої та їх статус, також можливість створення сценаріїв для зареєстрованих користувачів, створення сценаріїв зображено на рисунку 4.12.

Тому за допомогою попередньо створеного домену перейдемо до адреси www.hrachov.org , та авторизуэмось користувачем

Логін – Hrachov

Пароль – hrachov

ПланшетWarehouse

Physical | Config | Desktop | Programming | Attributes

IoT Monitor

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

| Actions | Enabled | Name | Condition | Actions |
|---|---|---|---|---|
| Edit Remove | Yes | ВідчинитиDoor1 | RfiedDoor1 Card ID = 1 | Set Door1 Lock to Unlock |
| Edit Remove | Yes | ВідчинитиDoor2 | RfiedDoor2 Card ID = 2 | Set Door2 Lock to Unlock |
| Edit Remove | Yes | ВідчинитиDoor3 | RfiedDoor3 Card ID = 3 | Set Door3 Lock to Unlock |
| Edit Remove | Yes | ВідчинитиDoor4 | RfiedDoor4 Card ID = 4 | Set Door4 Lock to Unlock |
| Edit Remove | Yes | ВідчинитиDoor5 | RfiedDoor5 Card ID = 5 | Set Door5 Lock to Unlock |
| Edit Remove | Yes | ЗачиненняDoor1 | RfiedDoor1 Card ID != 1 | Set Door1 Lock to Lock |
| Edit Remove | Yes | ЗачиненняDoor2 | RfiedDoor2 Card ID != 2 | Set Door2 Lock to Lock |
| Edit Remove | Yes | ЗачиненняDoor3 | RfiedDoor3 Card ID != 3 | Set Door3 Lock to Lock |
| Edit Remove | Yes | ЗачиненняDoor4 | RfiedDoor4 Card ID != 4 | Set Door4 Lock to Lock |
| Edit Remove | Yes | ЗачиненняDoor5 | RfiedDoor5 Card ID != 5 | Set Door5 Lock to Lock |

Рисунок 4.12 – Створенні сценарії для контролю доступу входу до приміщення

На рисунку 4.13 зображено алгоритм використання Rfid карток для відчинення дверей

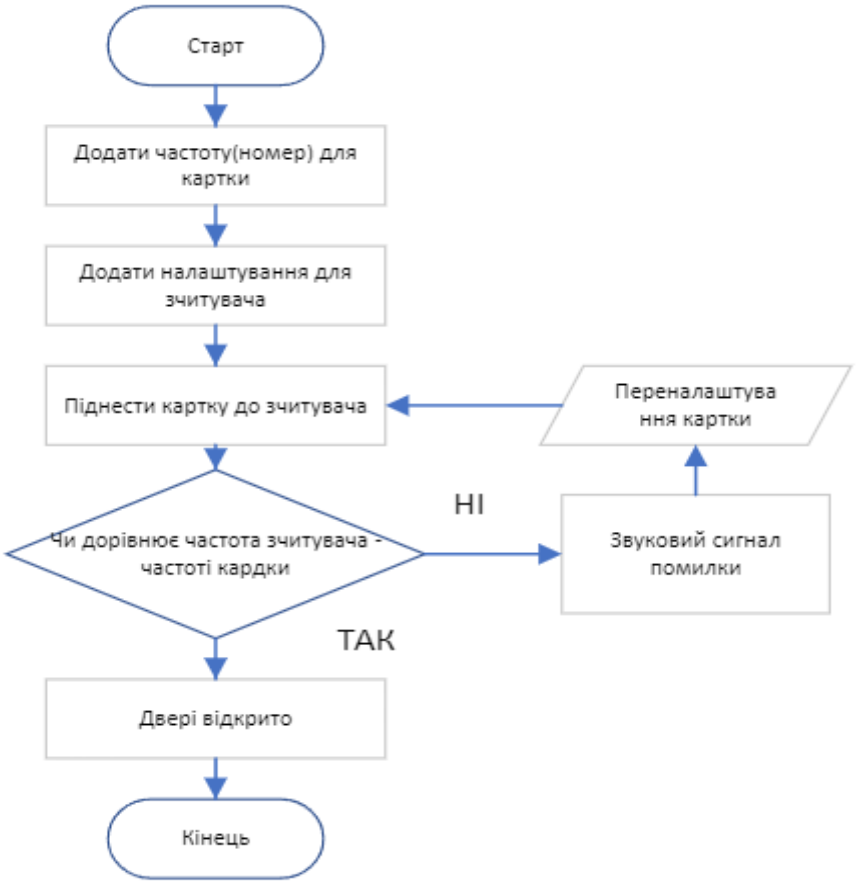



Рисунок 4.13 – Алгоритм використання Rfid карток з зчитувачем

### 4.5.2 Налаштування сигналізації

Також потрібно створити систему сигналізації для забезпечення безпеки приміщення , це буде реалізовано за допомогою 4 Веб-камер 3 датчиків руху та двох сирен. Виконати базове налаштування конфігурації та підключення до серверу та за допомогою IoT монітору створити сценарій роботи сигналізації

На рисунку 4.14 можна побачити, що сценарій спрацьовує при перетині датчику руху, що запускає Веб-камери та сирени.

| | | | | |
|---|---|---|---|---|
| Edit Remove | Yes | СистемаОхорониДругийПоверх | Match any:<br>• ДатчикРуху1 On is true<br>• ДатчикРуху3 On is true | Set Камера5 On to true<br>Set Камера6 On to true<br>Set Камера4 On to true<br>Set СигналізаціяПоверх2 On to true |
| Edit Remove | Yes | СистемаОхорониПершийПоверх | ДатчикРуху2 On is true | Set Камера1 On to true<br>Set Камера2 On to true<br>Set Камера3 On to true<br>Set СигналізаціяПоверх1 On to true |

Add

Рисунок 4.14 – Налаштування сигналізації за допомогою сценарію

Розташуємо отриману системи на схемі топології , зображення системи безпеки складського підпри’ємтсва реалізовано на рисунку 4.15.

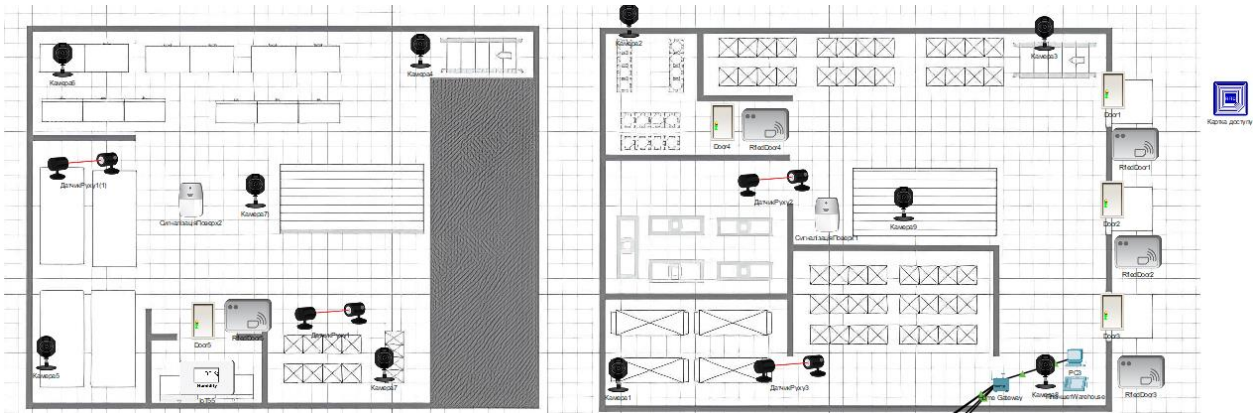


Рисунок 4.15 – Розташування системи безпеки складу

### 4.5.3 Тестування роботи системи безпеки

За допомогою кнопки ALT + Mouse1 можно ввійти в режим тестування та керувати роботою пристроїв. Для тестування доступу до приміщення необхідно спочатку налаштувати картку на необхідну частоту та піднести до

необхідного зчитувача. Якщо у картки та зчитувача одна частота то замок на двері буде відкрито, що дозволить увійти до складського приміщення.

На рисунку 4.16 наведено приклад доступу до Door1, при тому що частота картки (CardID) налаштована на 1 та в сценарії описано що зчитувач реагує на частоту 1.

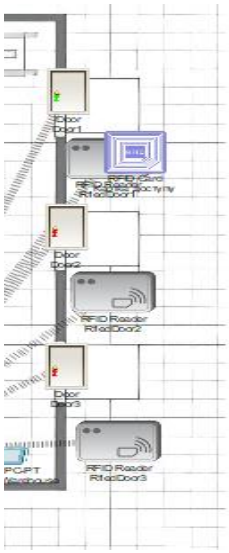


Рисунок 4.16 – Доступ до Дверей дозволено

Тепер можна змінити частоту наприклад на 99 , та перевірити чи залишиться доступ до дверей , на рисунку 4.17 можна побачити що після зчитування карту зчитувач передає сигнал на двері та зачиняє їх, тобто сценарії відпрацьовують правильно.

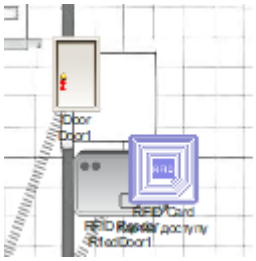


Рисунок 4.17 – Доступ до дверей відхилено

Щоб перевірити сигналізацію потрібно активувати один з датчиків руху за допомогою кнопки Alt та переміщенням по датчику з натиснутою кнопкою Mouse1. На рисунку 4.18 показано використання сигналізації.

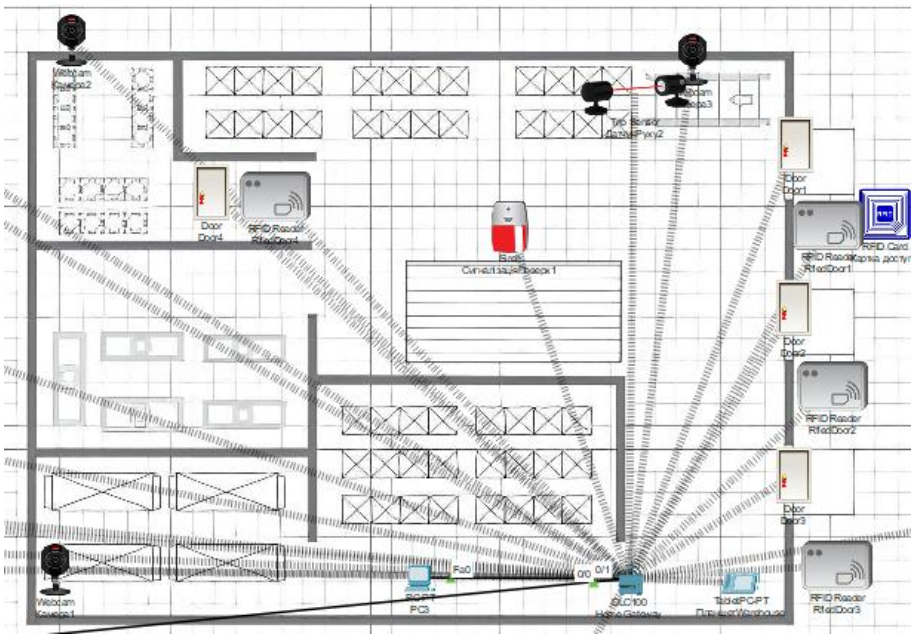


Рисунок 4.18 – Результат тестування сигналізації першого поверху

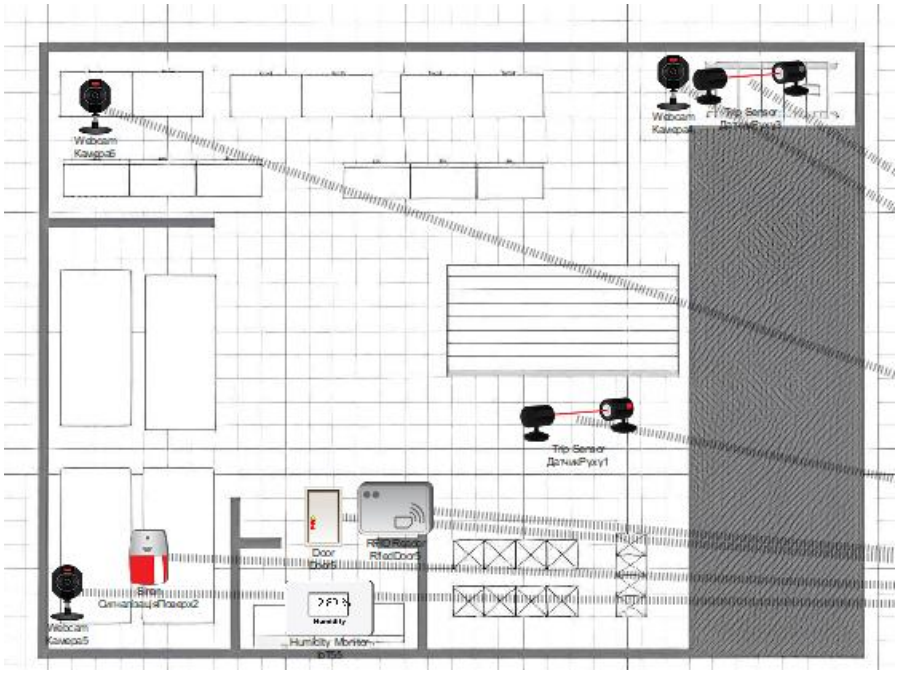


Рисунок 4.19 – Результат тестування сигналізації другого поверху

Як можна побачити з рисунку 4.18 при перетині пристрою ДатчикРуху3 ввімкнулись сирени та Веб камери, тобто сигналізація працює як треба. На рисунку 4.19 вигляд iot монітора при активації сигналізації.

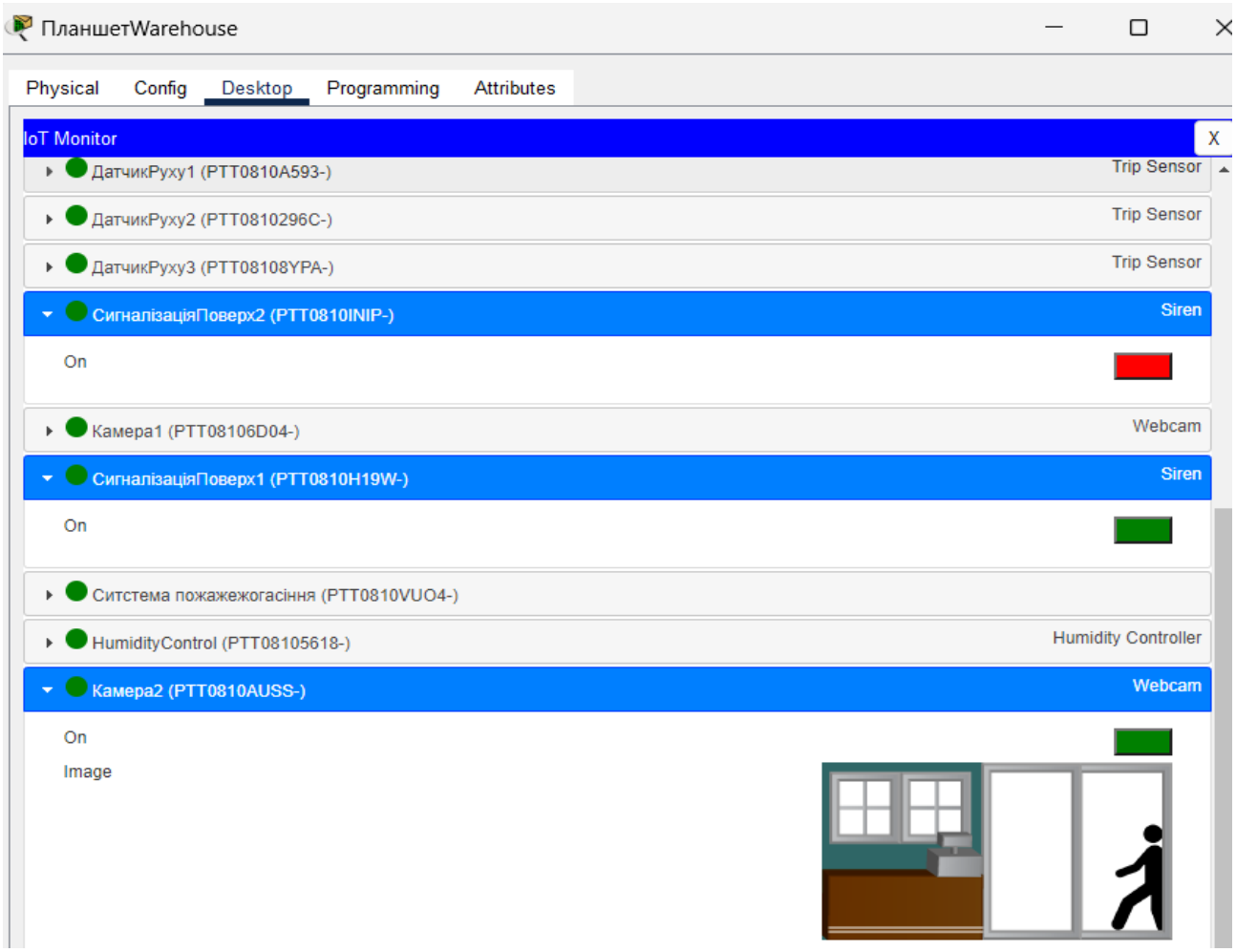



Рисунок 4.20 – Сценарій для сигналізації працює

## 4.6 Налаштування підсистеми пожежогасіння

Для налаштування системи пожежогасіння потрібно додати контролер mcu, датчик полум'я, три спринклери та LCD екран для зображення стану системи. Пристрої необхідні для цієї системи підключемо до контролеру за допомогою спеціального IoT кабелю. Також для підключення до загальної мережі до контролеру необхідно додати мережевий адптер. На рисунку 4.20 можна побачити підключення необхідних пристроїв до контролеру.

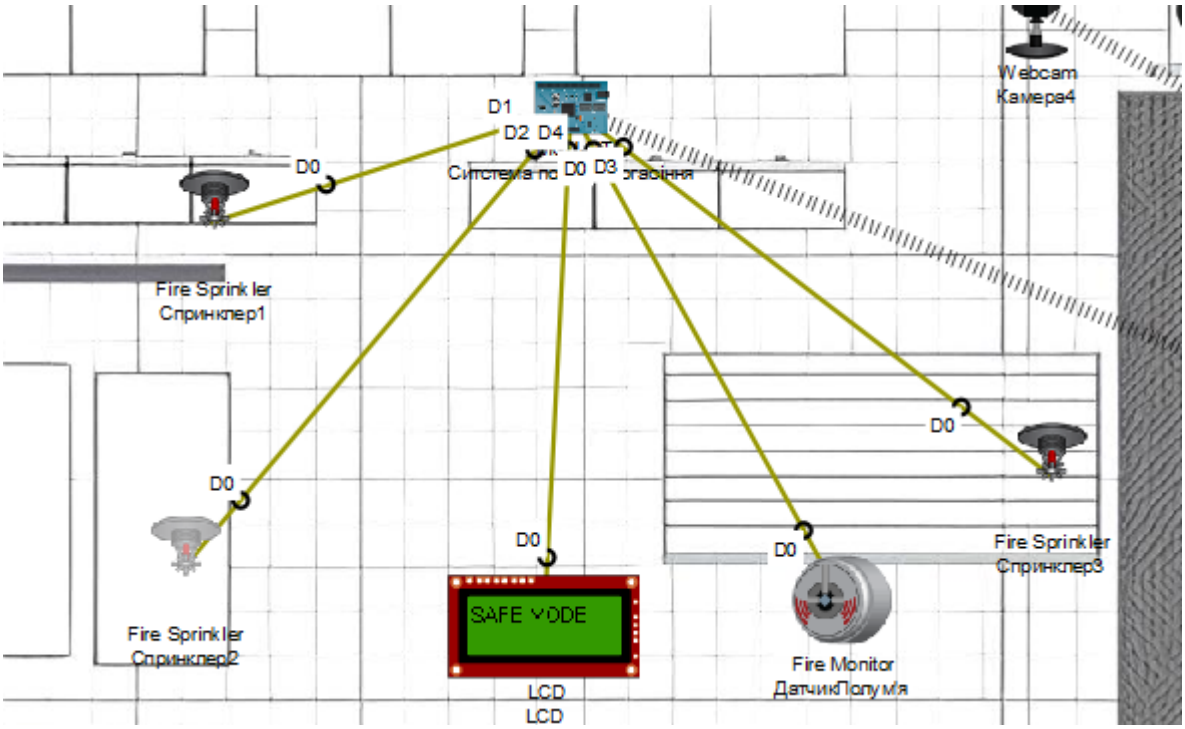



Рисунок 4.20 – Підключення пристроїв до системи пожежогасіння

Пояснення використання Fire Monitor - об'єкти, які можуть бути у вогні, повинні мати властивість пристрою «IR» зі значенням. ІЧ-діапазон, який буде визначено як пожежу, вказується у скрипті. Все, що знаходиться поблизу кінця датчика, буде перевірено на наявність пожежі, і буде надіслано цифровий сигнал HIGH або LOW, залежно від поточного виявлення.

Для того щоб датчик полум’я міг зчитувати інформацію потрібно додати об’єкт, який може підняти значення інфрочервоного діапазону. Для цього використаємо можливість програми Cisco Packet Tracer створювати свої об’єкти , прейдемо на вкладку Components -> Things , додамо відповідне зображення об’єкта та додами невеликий код на python, який як раз так й буде змінювати інфрочервоний діапазон в найближчих пристроях.

```
function setup()
{
 setDeviceProperty(getName(), 'IR', 900)
}
```

Далі необхідно написати на мові програмування python код , який зможе задовільняти вимогам системи пожежогасіння , тобто :

- Зчитування інформації з монітору
- Налаштування пінів входу та виходу
- Запуск спринклерів
- Вивід тексту на екран LCD

Також враховуючи розмір приміщення. пропускну здатність стін та зону покриття HomeGateway було вирішено додати до кожної підсистеми точку доступу що дозволить реалізувати SWMS на більшу площину.

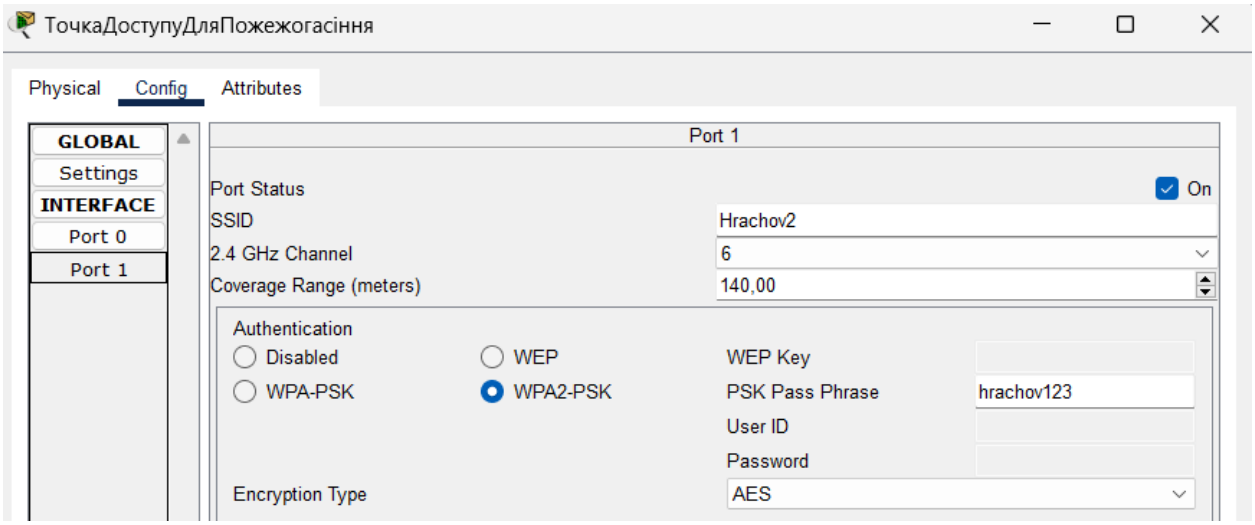



Рисунок 4.21 – Налаштування точки доступу для системи пожежогасіння

Виконаємо підключення точки доступу до контролера та правильно розташуємо прилади підсистеми, зображено на рисунку 4.22.

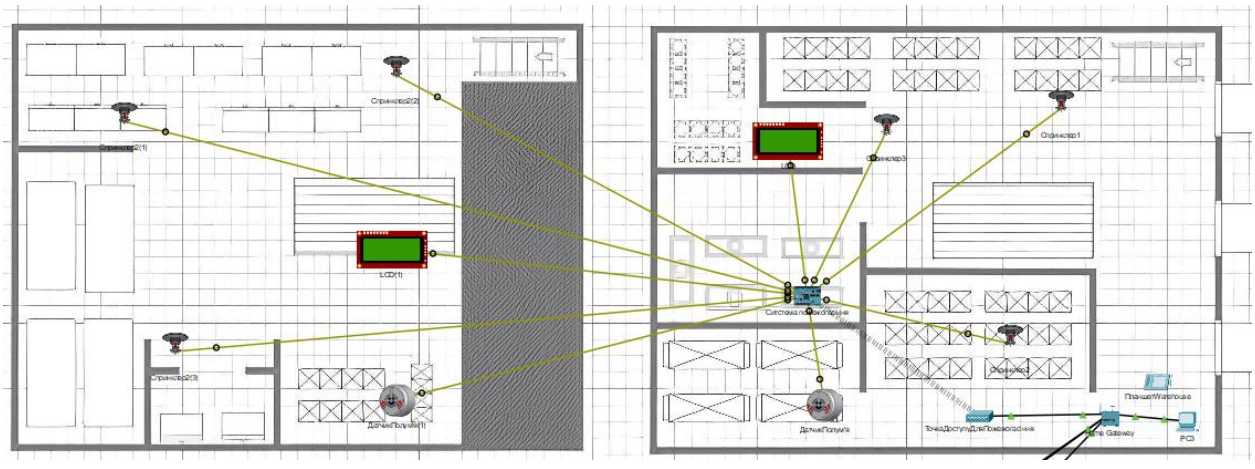


Рисунок 4.22 – Розташування підсистеми пожежогасіння

## 4.7 Тестування підсистеми пожежогасіння

Для тестування системи пожежогасіння необхідно спочатку запустити програму попередньо створеного об’єкта полум’я та піднести його до монітору. При умові що монітор незафіксує зміни повинен залишитись підпис “Safe mode” на LCD дисплеї, але якщо зміниться інфрочервоний діапазон та монітор це побачить – ввімкнуться спринклери та на LCD екрані з’явиться підпис “Fire Detected!”. На рисунку 4.23 продемонстровано тестування роботи контролера. Код програми додано до додатку Б.

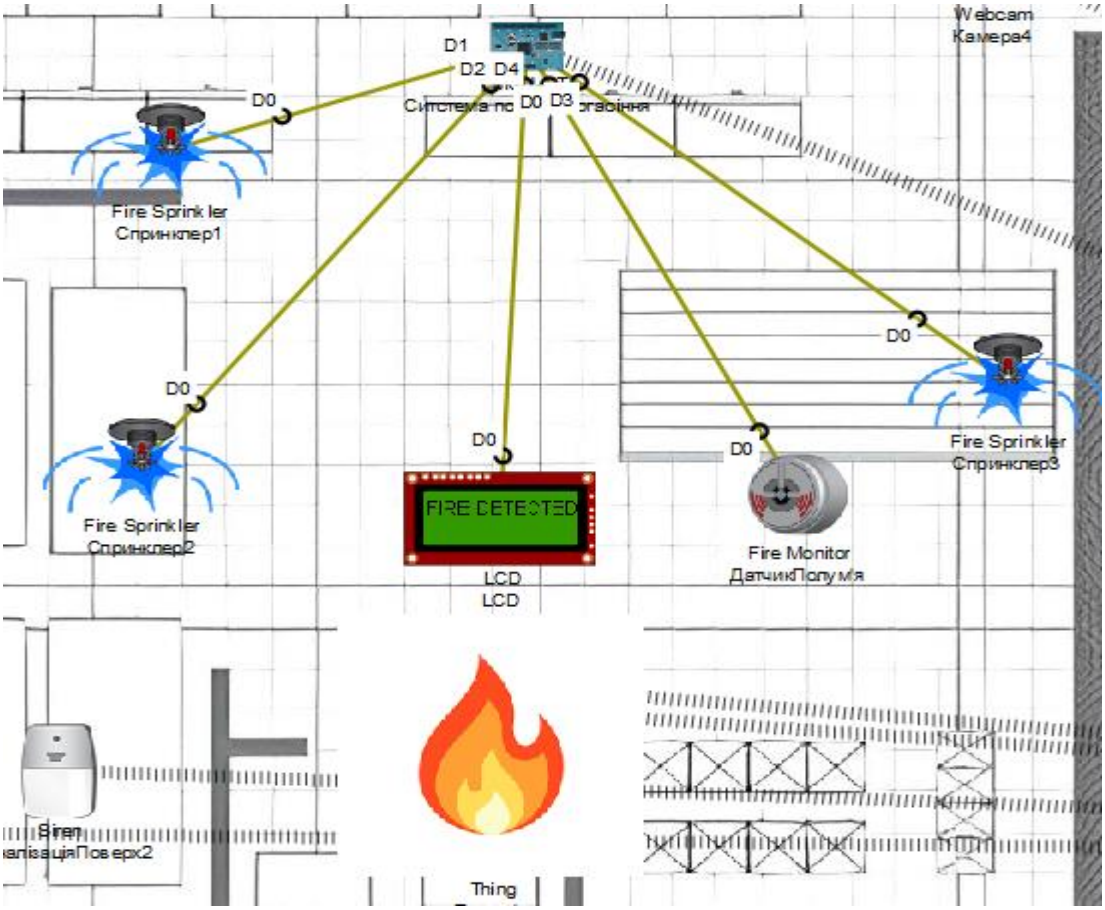



Рисунок 4.23 – Правильне спрацювання підсистеми пожежогасіння

## 4.8 Налаштування підсистеми контролю вологості

У складського підприємства виконують зберігання різних видів товарів, деякі з них потребують чіткого дотримання вологості тому, що якщо вологість сильно збільшиться такі товари як:

– Ліки;

– Меблі;

– Палети;

– Електроніка.

Можуть бути пошкодженні через що підприємство може втрати не тільки гроші а й партнерів з якими воно веде стосунки. Тому необхідно впровадити систему контролю вологості.

Для цього потрібно додати контролер, дві вентиляції, монітор вологості та датчик вологості. З’єднати їх спеціальним IoT кабелем та додати до контролер мережевий адаптер для підключення до маршрутизатора. Також буде реалізован моніторинг стану приладів на IoT моніторі. На рисунку 4.24 зображено підключення пристроїв до контролера.

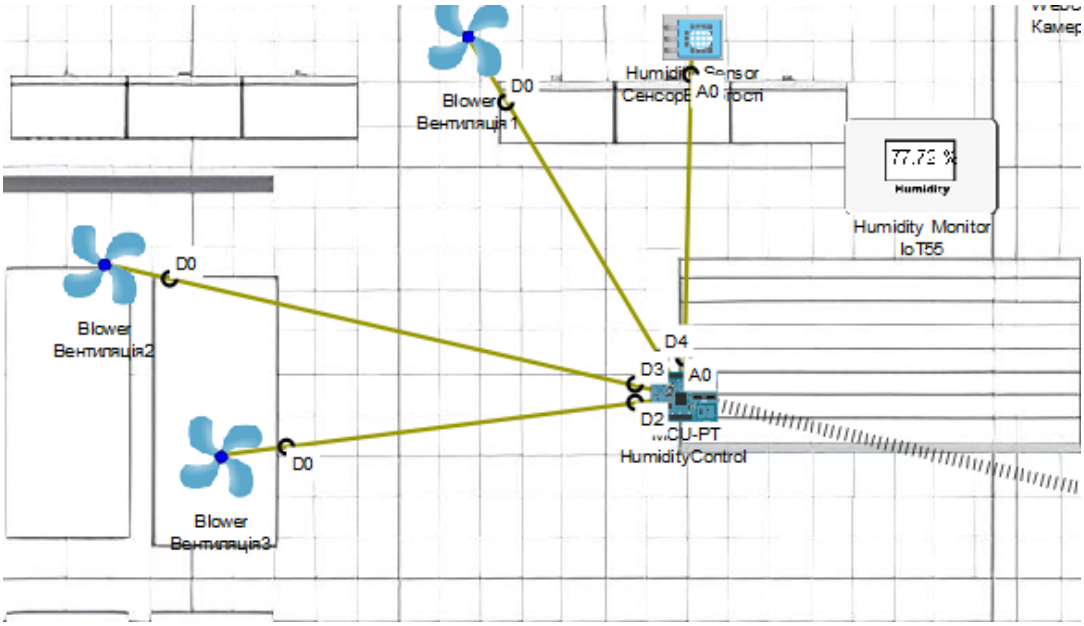



Рисунок 4.24 – Підключення підсистеми контролю вологості

Система постійно проводить моніторинг вологості на складу та при досягненні границі дозволеної вологості запускає три пристрої вентиляції на максимальну подужність та поступово понижає рівень вологості, також при досягненні закладеного мінімуму вологості вентиляція переходить до автономної роботи.

На рисунку 4.25 зображено підключення точки доступу до контролеру та розташування пристроїв у приміщені.

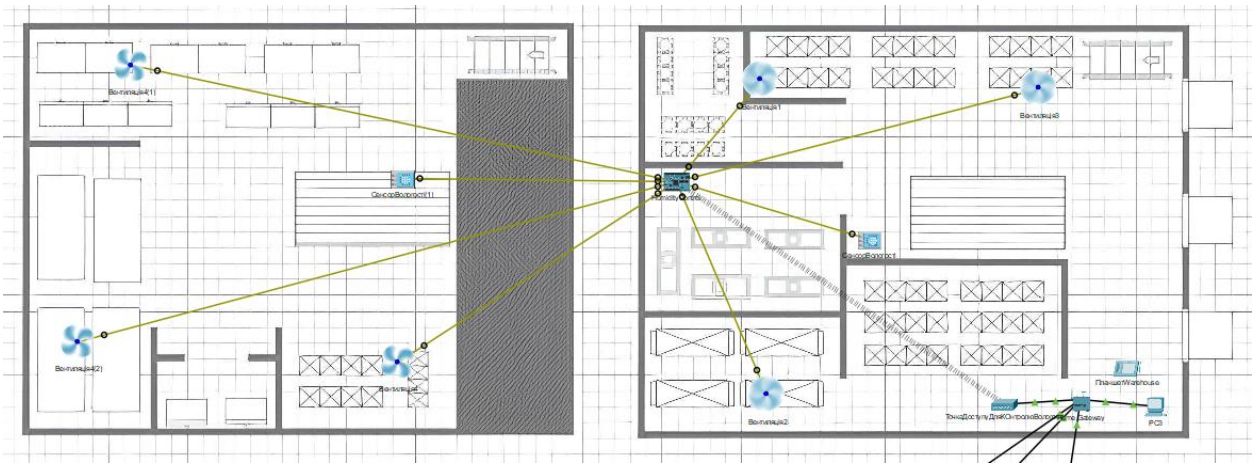


Рисунок 4.25 – Розташування підсистеми контролю вологості

## 4.9 Тестування роботи підсистеми контролю вологості

Для тестування системи контролю вологості запустимо програму контролеру , початкова вологість становить 72 -77 %. При запуску програми контролеру очікується запуск посиленого режима вентиляції та позавершеню роботи перехід до середнього режиму. Також передбачено моніторинг системи на додатку IoT монітор. На рисунку 4.26 зображено запуск програми контролера.

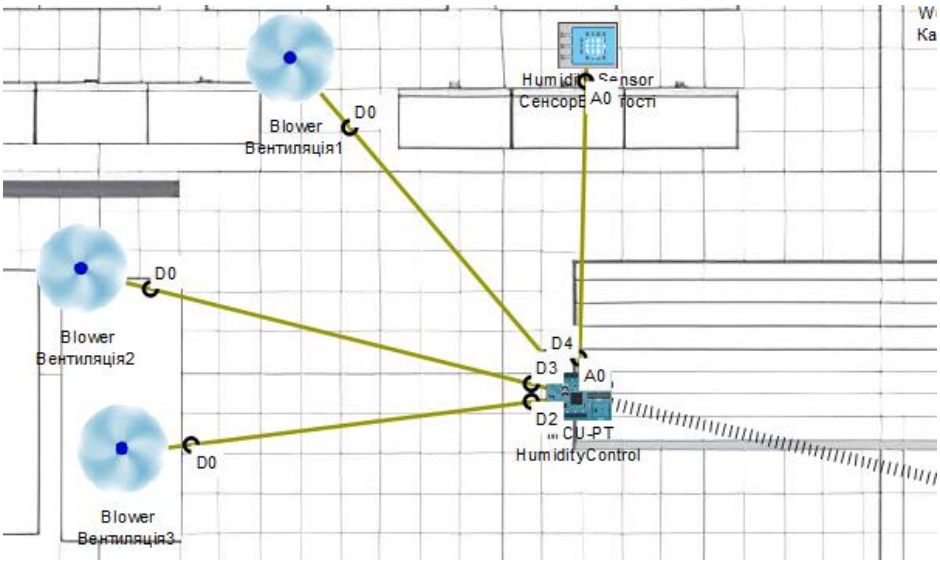



Рисунок 4.26 – Запущено посилений режим вентиляції

При досяганні значення вологості 20% програма переводить вентиляцію до середнього режиму це можна побачити на рисунку 4.27. Код програми представлено у додатку В.

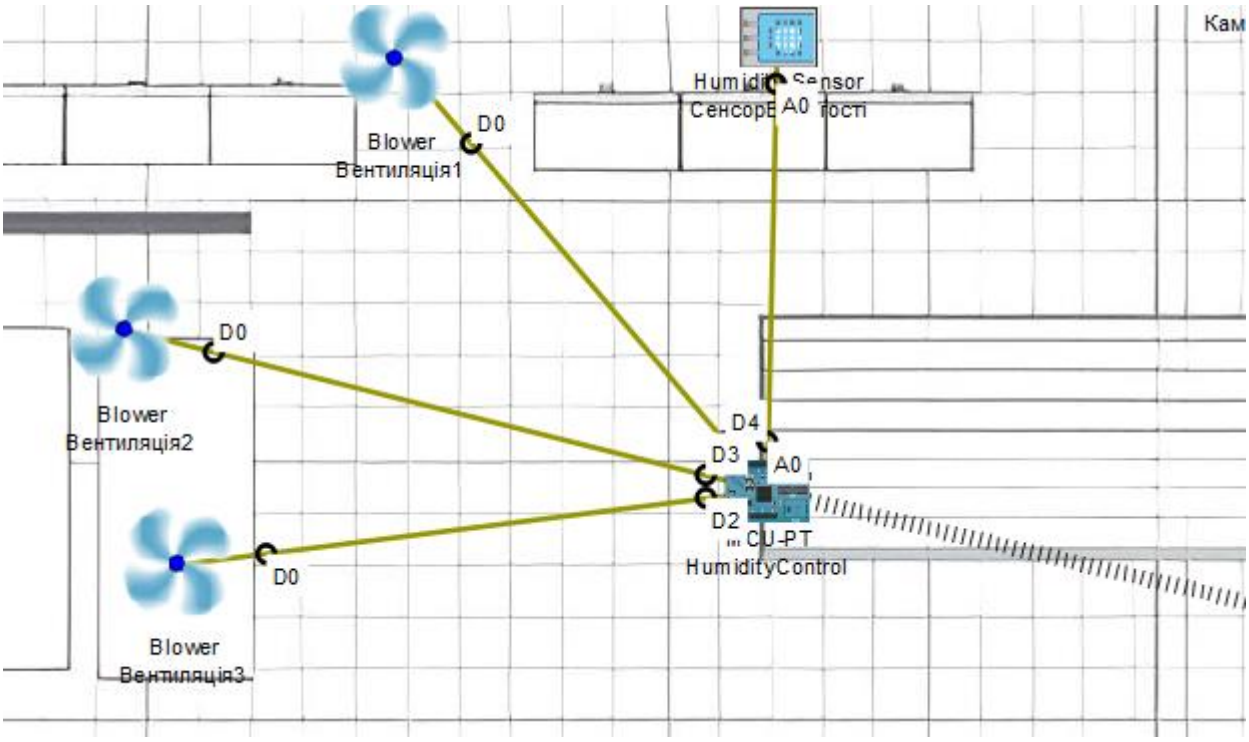



Рисунок 4.27 – Завершення роботи програми

Тепер якщо перейти до Iot монітору можна побачити що контролер передає чтан присроїв системи контролю вологості. На рисунку 4.28 можна побачити активний контролер HumidityControl.

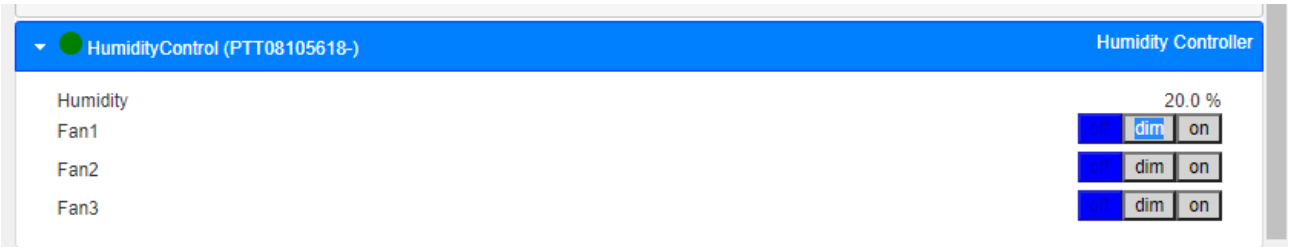



Рисунок 4.28 – Стан пристроїв системи контролю вологості

## 4.10 Налаштування моніторингу стану середовища

За допомогою датчиків диму, світла та температури, а також використовуючи LCD дисплеїв виведемо значення датчиків основних станів середовища. Також за допомогою мови програмування Python напишемо програму на контролері, яка буде у режимі реального часу оновлювати дані не тільки на дисплеях, а й у хмарі в програмі IoT монітор. Код програми наведено у додатку Г. На рисунку 4.29 показано підключення пристроїв до контролера.

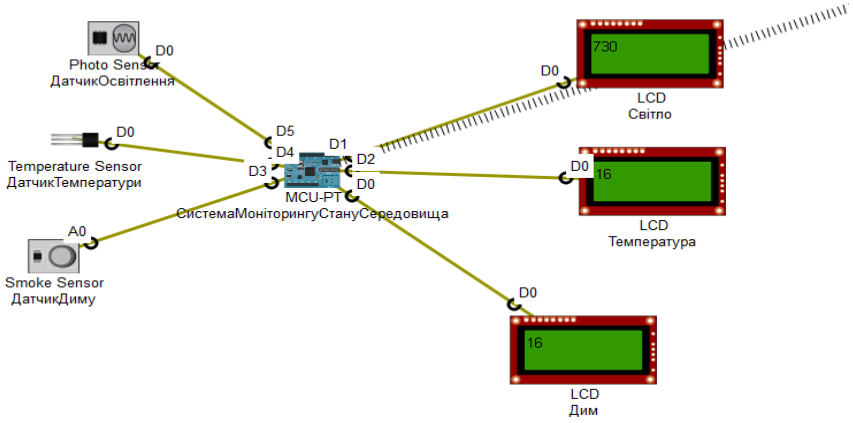



Рисунок 4.29 – Підключення пристроїв до контролера

Далі розташуємо пристрої моніторингу на схемі приміщення, зображено на рисунку 4.30.

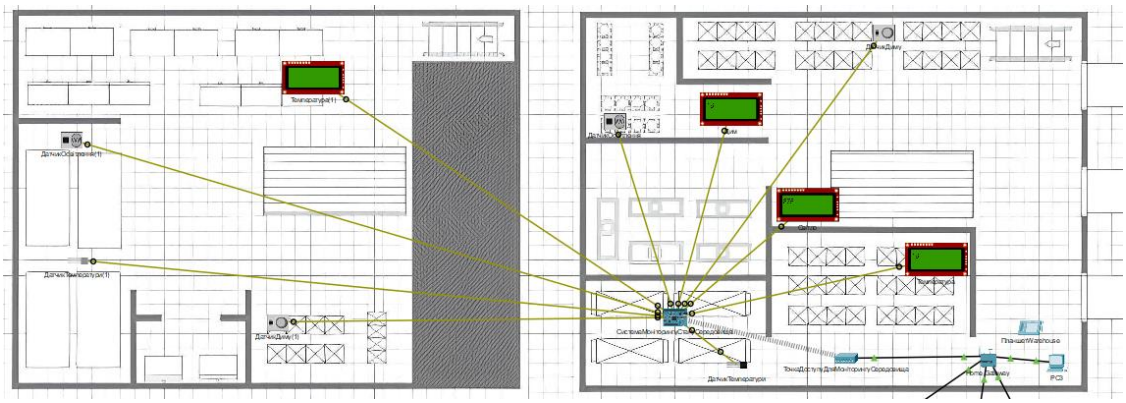


Рисунок 4.30 – Розташування пристроїв моніторингу стану середовища на схемі приміщення

Перейдемо наприклад з планшета до застосунку IoT монітор та переглянемо стан приладів як і зображено на рисунку 4.31.

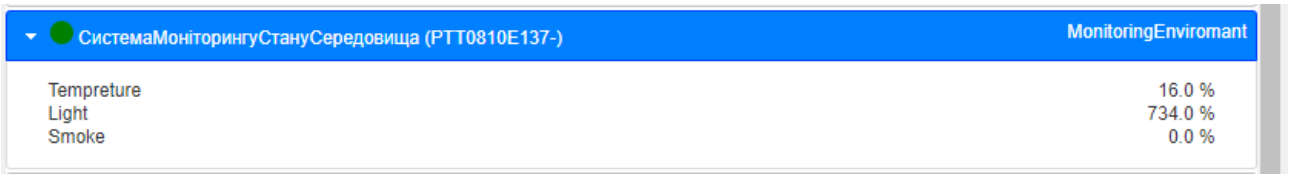



Рисунок 4.31 – Стан системи на моніторі

У додатку А наведена загальна система SWMS складського приміщення підприємства Landlord

# ВИСНОВКИ

Розроблена система управління складськими приміщеннями на базі IoT, відома як SWMS, була впроваджена з використанням таких технологій, як WiFi та RFID. Ця система відповідає сучасним вимогам до автоматизації, забезпечуючи надійний моніторинг пристроїв, контроль доступу та безпеку у випадках аварій.

Отримані результати можуть бути корисними для управління складськими приміщеннями великих підприємств і в логістиці для оптимізації процесів зберігання та транспортування товарів. Система також може бути інтегрована в інші промислові комплекси, де потрібен автоматизований контроль і моніторинг стану приміщень та обладнання.

Науково-технічна значущість роботи полягає в розробці ефективної системи моніторингу та управління складськими приміщеннями з використанням сучасних IoT технологій. Соціально-економічна значущість полягає в потенціалі зниження витрат на обслуговування складів, підвищенні безпеки та ефективності їх роботи, що може позитивно вплинути на економічні показники підприємств.

Подальші дослідження у напрямку вдосконалення IoT систем для промислових застосувань є доцільними, зокрема дослідження можливостей інтеграції додаткових сенсорів та модулів, а також розробка методів оптимізації обробки і аналізу даних для підвищення ефективності системи.

Робота досягла своєї мети: створена система SWMS відповідає сучасним стандартам і може бути успішно впроваджена у промислову експлуатацію. Дослідження та розробки у цьому напрямку мають значний потенціал для подальшого розвитку.

# ПЕРЕЛІК ПОСИЛАНЬ


1. IBM [Веб-сайт] URL: https://www.ibm.com/topics/internet-of-things
2. Cogniteq [Веб-сайт] URL: https://www.cogniteq.com/blog/iot-warehouse-management-solutions-and-use-cases
3. Lumive [Веб-сайт] URL: https://lumivestore.com/zigbee-vs-wifi-choosing-the-right-smart-home-protocol/
4. Amazon [Веб-сайт] URL: https://aws.amazon.com/ru/iot/
5. ResearchGate [Веб-сайт] URL: https://www.researchgate.net/publication/368591935_Research_on_Impact_of_IoT_on_Warehouse_Management
6. ResearchGate [Веб-сайт] URL: https://www.researchgate.net/publication/363923299_To_Design_A_Smart_Framework_With_Integration_Of_Iot_For_Warehouse
7. ResearchGate [Веб-сайт] URL: https://www.researchgate.net/publication/358164276_Smart_Warehouse_Monitoring_Using_Iot
8. ResearchGate [Веб-сайт] URL: https://www.researchgate.net/publication/322175801_RFID_IoT-enabled_warehouse_for_safety_management_using_product_class_based_storage_and_potential_fields_methods
9. Linkedin [Веб-сайт] URL: https://www.linkedin.com/pulse/application-rfid-technology-intelligent-warehousing-various-industries-d4yhc/
10. RFIDJournal [Веб-сайт] URL: https://www.rfidjournal.com/rfid-journal-live-2024-rfid-iot-in-warehouse-and-inventory-management-sessions
11. Wifirst [Веб-сайт] URL: https://www.wifirst.com/en/blog/connected-logistics-importance-of-wifi-in-warehouses
12. Invertia [Веб-сайт] URL: https://inveritasoft.com/blog/implementation-of-iot-in-your-smart-warehouse

13. Hineywell [Веб-сайт] URL: https://sps.honeywell.com/us/en/products/advanced-sensing-technologies/healthcare-sensing/humidity-with-temperature-sensors/honeywell-humidicon-hih6100-series

14. Maxintegrated [Веб-сайт] URL: https://www.stg-maximintegrated.com/en/products/sensors/DS18B20.html

15. 1wire [Веб-сайт] URL: https://1wire.com.ua/tsl2561-cifrovoj-datchik-osveshhennosti.html

16. Parallax [Веб-сайт] URL: https://www.parallax.com/product/pir-sensor-with-led-signal/

17. FirstAlert [Веб-сайт] URL: https://support.firstalert.com/s/active-product/a3J4x0000020RY8EAM/sa320cn-sa320-sa320b

18. Secure [Веб-сайт] URL: https://secur.ua/signalizatsii/datchiki/pozharnye-datchiki/datchik-dyma-arton-dl

19. Kosmodrom [Веб-сайт] URL: https://kosmodrom.ua/ru/releynye-moduli-arduino/4-channel-3-3v-relay-module-for-arduino.html

20. Viking [Веб-сайт]: URL: https://www.vikinggroupinc.com/products/pendent/vk1021-standard-response-pendent-sprinkler-k56

21. Impinj [Веб-сайт] URL: https://www.impinj.com/products/readers

22. Climatinvest[Веб-сайт] URL: https://climatinvest.net/p531189089-stenovoj-provetrivatel-pritochnyj

23. TFP1 [Веб-сайт] URL: https://www.tfp1.com/blog/smart-iot-fire-protection-systems/

24. Arduino [Веб-сайт] URL: https://arduino.ua/ru/prod980-wifi-modyl-esp8266

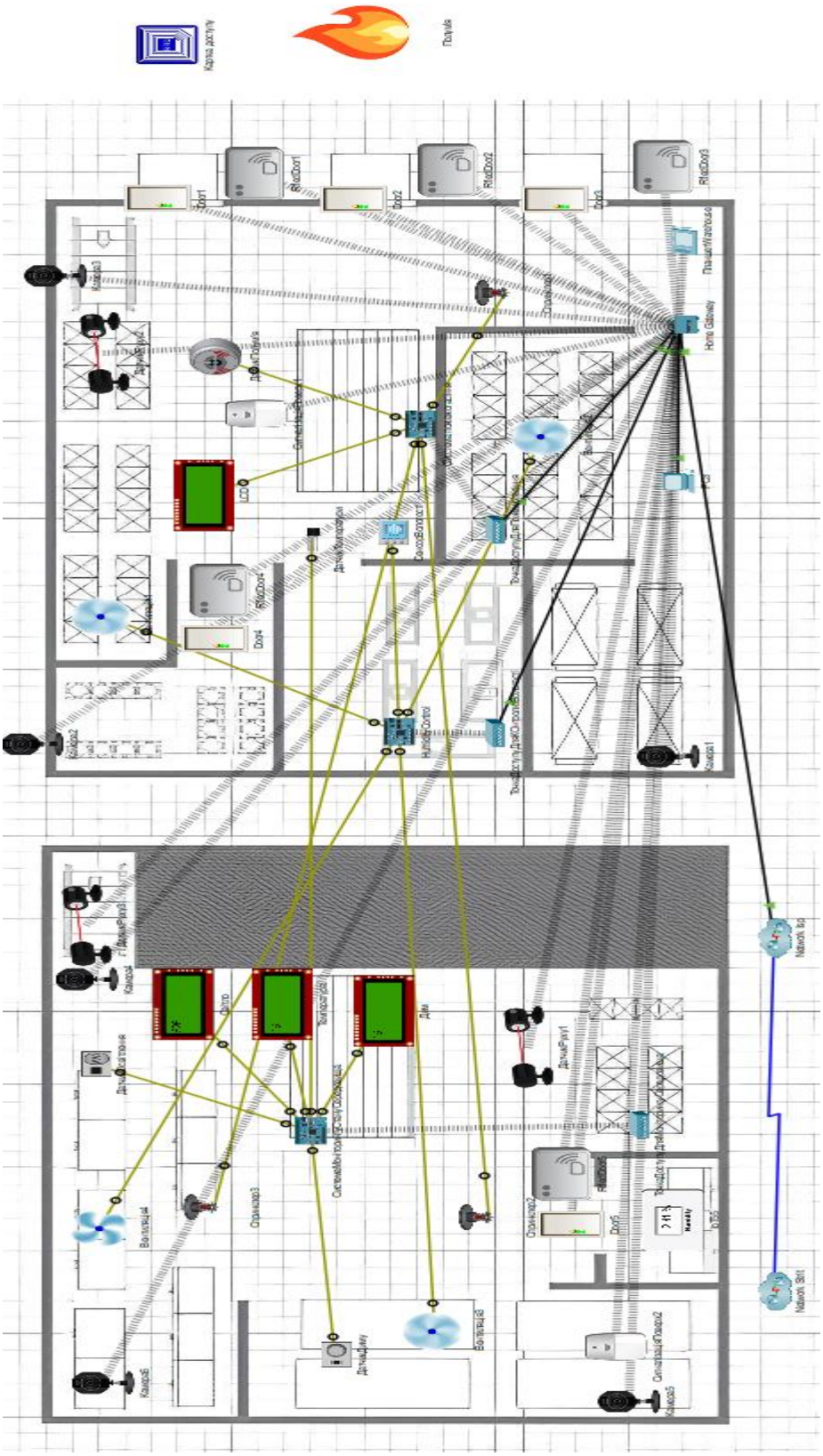
25. Linkedin [Веб-сайт] URL: https://www.linkedin.com/pulse/how-combine-solar-panels-iot-devices-fieldproxy/

26. Artel [Веб-сайт] URL: https://www.artel.com/wp-content/uploads/products/manuals/legacy-digilink-manuals/DLC100_Guide_AR200_008015_B00_K_HiRes.pdf

27. Цвіркун Л.І. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи магістра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, В.В. Гнатушенко, С.М. Ткаченко ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2023. – 43 с

# Додаток А

загальна система SWMS складського приміщення підприємства Landlord



Додаток Б

Текст програми налаштування IoT підсистеми пожежогасіння

```
from gpio import *
from time import *
def main():
    pinMode(0, INPUT)
    pinMode(1, OUT)
    print("Fire Alarm System")
    while True:
        fire = digitalRead(0)
        if fire == 1023:
            customWrite(1, "1")
            customWrite(4, "FIRE DETECTED!!")
            customWrite(3, "1")
            customWrite(2, "1")
            customWrite(6, "0")
            customWrite(7, "0")
            customWrite(8, "0")
            print("FIRE!")
        else:
            customWrite(1, "0")
            customWrite(4, "SAFE MODE")
            customWrite(3, "0")
            customWrite(2, "0")
            customWrite(6, "0")
            customWrite(7, "0")
            customWrite(8, "0")
            print("Normal")
        delay(1000)
```

```
if __name__ == "__main__":
    main()
```

Додаток В

Текст програми налаштування підсистеми контролю вологості

```
from gpio import *
from time import *
from ioeclient import *

def setup():
    pinMode(A0, IN)  # Humidity Sensor вхід
    pinMode(2, OUT)  # Fan1 вихід
    pinMode(3, OUT)  # Fan2 вихід
    pinMode(4, OUT)  # Fan3 вихід

# Ініціалізація IoEClient
IoEClient.setup({
    "type": "Humidity Controller",
    "states": [
        {
            "name": "Humidity",
            "type": "number",
            "unit": "%",
            "decimalDigits": 1
        },
        {
            "name": "Fan1",
            "type": "options",
            "options":{
                    "0":"off",
                    "1":"dim",
                    "2":"on"
```

```
            },
        "controllable":True
    },
    {
        "name": "Fan2",
        "type": "options",
        "options":{
            "0":"off",
            "1":"dim",
            "2":"on"
            },
        "controllable":True
    },
    {
        "name": "Fan3",
        "type": "options",
        "options":{
            "0":"off",
            "1":"dim",
            "2":"on"
            },
        "controllable":True
    }
  ]
})

# Початкова вологість (імітація)
initial_humidity = 70
```

```
# Функція для зниження вологості
def decrease_humidity(target_humidity):
    global initial_humidity
    while initial_humidity > target_humidity:
        print("Turning on fans to decrease humidity")
        customWrite(2, "2")
        customWrite(3, "2")
        customWrite(4, "2")
        report_states()
        sleep(5)  # Вентилятори працюють протягом 5 секунд

        # Імітація зниження вологості
        initial_humidity -= 5

        print("Current Humidity: {:.2f} %".format(initial_humidity))
        sleep(2)  # Зачекайте деякий час перед повторною перевіркою

# Функція для звітування станів пристроїв
def report_states():
    IoEClient.reportStates([
        initial_humidity,
        digitalRead(2),
        digitalRead(3),
        digitalRead(4)
    ])

# Основний цикл програми
def main():
    setup()
```

```
    while True:
        # Імітація читання вологості з датчика
        humidity = initial_humidity

        # Умова для зниження вологості до 20%
        if humidity > 20:
            decrease_humidity(20)

        customWrite(2, "1")
        customWrite(3, "1")
        customWrite(4, "1")
        report_states()

        # Затримка між вимірюваннями
        sleep(2)

if __name__ == "__main__":
    main()
```

Додаток Г

Текст програми налаштування моніторингу стану середовища

```
from gpio import *
from time import *
from ioeclient import *

def main():
        pinMode(0, OUT)
        pinMode(1, OUT)
        pinMode(2, OUT)
        pinMode(3, IN)
        pinMode(4, IN)
        pinMode(5, IN)

IoEClient.setup({
        "type": "MonitoringEnviromant",
        "states": [
                {
         "name": "Tempreture",
         "type": "number",
         "unit": "%",
         "decimalDigits": 1
      },
      {
         "name": "Light",
         "type": "number",
         "unit": "%",
         "decimalDigits": 1
      },
      {
         "name": "Smoke",
         "type": "number",
         "unit": "%",
         "decimalDigits": 1
      }
   ]
})
def report_states():
   IoEClient.reportStates([
      digitalRead(3),
      digitalRead(4),
      digitalRead(5)
   ])
```

```
while True:
        light = digitalRead(5)
        tempreture = digitalRead(4)
        smoke = digitalRead(3)
        customWrite(0 , smoke)
        customWrite(1 , tempreture)
        customWrite(2 , smoke)
        report_states()
        print(smoke)
        print(tempreture)
        print(light)

if __name__ == "__main__":
main()
```

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

# ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ IOT СИСТЕМИ

Текст програми
804.02070743.2403-01 12 01

Листів 8

**2024**

# АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування IoT-системи та моделювання в Packet Tracer. Програмний код створений мовою Python для контролерів системи SWMS.

# ЗМІСТ

Додаток Д

Налаштування мережевих пристроїв мережі організації

```
configure terminal
line console 0
password hrachov123
login
line vty 0 4
password hrachov123
login
enable secret privilaged_hrachov123
service password-encryption
banner motd #HRACHOV DIPLOM 123 AUTORIZATION#
username hrachov privilege 15 secret hrachov123
ip domain-name Hrachov_Router4
crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit
interface se0/1/0
clock rate 128000
exit
interface Serial0/1/1
clock rate 128000
end
write memory
ip dhcp excluded-address 10.25.26.1 10.25.26.10
ip dhcp excluded-address 10.25.26.65 10.25.26.74
ip dhcp excluded-address 10.25.26.129 10.25.26.138
ip dhcp excluded-address 10.25.26.193 10.25.26.202 ip dhcp excluded-address 10.25.26.225 10.25.26.234
ip dhcp pool poolvlan13
network 10.25.26.0 255.255.255.192
default-router 10.25.26.1
dns-server 209.165.200.1
ip dhcp pool poolvlan23
network 10.25.26.64 255.255.255.192
default-router 10.25.26.65
dns-server 209.165.200.1
```

```
ip dhcp pool poolvlan33
network 10.25.26.128 255.255.255.192
default-router 10.25.26.129
dns-server 209.165.200.1
ip dhcp pool poolvlan99
network 10.25.26.192 255.255.255.192
default-router 10.25.26.193
dns-server 209.165.200.1
ip dhcp pool poolvlan100
network 10.25.26.224 255.255.255.192
default-router 10.25.26.225
dns-server 209.165.200.1
crypto isakmp policy 10
encr aes 256
hash sha256
authentication pre-share
group 14
lifetime 86400
vlan 13
 name Accounting
vlan 23
 name Resources_Department
vlan 33
 name Guest
vlan 99
 name Management
vlan 100
 name Native
interface range fa0/3 - 10
 switchport mode access
```

```
 switchport access vlan 13
interface range fa0/11 - 18
 switchport mode access
 switchport access vlan 23
interface range fa0/19 - 24
 switchport mode access
 switchport access vlan 33
interface gig0/1.13
 encapsulation dot1Q 13
 ip address 10.25.26.1 255.255.255.192
interface gig0/1.23
 encapsulation dot1Q 23
 ip address 10.25.26.65 255.255.255.192
interface gig0/1.33
 encapsulation dot1Q 33
 ip address 10.25.26.129 255.255.255.192
interface gig0/1.99
 encapsulation dot1Q 99
 ip address 10.25.26.193 255.255.255.192
interface gig0/1.100
 encapsulation dot1Q 100 native
 ip address 10.25.26.225 255.255.255.192
```

# Додаток Е

## Налаштування мережевих пристроїв мережі складського приміщення

```
configure terminal
hostname Hrachov_Rout_ISP
enable secret hrachov
line con 0
password cisco
login
line vty 0 4
password cisco
login
banner motd # [Banner on Router] #
ip domain-name admin
crypto key generate rsa
username hrachov password hrachov
ip ssh version 2
line vty 0 15
transport input ssh
login local
ip dhcp excluded-address 20.3.201.225 20.3.201.229
ip dhcp pool STRIT
 network 20.3.201.224 255.255.255.224
 default-router 20.3.201.225
 dns-server 10.3.0.203
service dhcp
ip dhcp excluded-address 20.3.200.225 20.3.200.229
ip dhcp pool WAREHOUSE
 network 20.3.200.224 255.255.255.224
 default-router 20.3.200.225
 dns-server 10.3.0.203
```