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 Хелемендрик Павло Іванович
(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 " Кіберфізична система контролю мікроклімату готелів мережі Optima Hotel Group "
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Бешта Д.О.			
спеціальної частини	доц. Бешта Д.О.			
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 Хелемендрик П.І. **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 " Кіберфізична система контролю мікроклімату готелів мережі Optima Hotel Group "

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.05.2022 № 771–л

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 _____ доц. Бешта Д.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.01.2024

Дата подання до екзаменаційної комісії 14.06.2024

Прийнято до виконання _____ Хелемендрик П.І.

РЕФЕРАТ

Пояснювальна записка: 107 с., 35 рис., 4 табл., 1 дод., 17 джерел.

СИСТЕМА, МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об’єкт розробки: кіберфізична система контролю мікроклімату готелів мережі Optima Hotel Group з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: створення кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Здійснено розробку кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі..

Комп’ютерна система дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання наступних функцій:

– зайнята кімната, чи відкриті вікна;

– чи потрібно відрегулювати температуру навколишнього середовища, і вносять відповідні зміни:

– аналітика та штучному інтелекті інформує про більш широку картину прийняття рішень з точки зору енергетичної стратегії або інвестицій у модернізацію будівель.

Розроблена комп’ютерна мережа виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Робота системи перевірена за допомогою моделі схеми корпоративної мережі із застосуванням програми Cisco Packet Tracer.

Результати перевірки у вигляді таблиць та графіків описані і наводяться у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

Ethernet – технологія передачі даних по мережі;

Wi–Fi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

ВСТУП

Ідеальний індивідуальний мікроклімат у приміщенні потрібен для повного задоволення потреб клієнтів готелів.

У контексті проектів розвитку та реновації забезпечується енергоефективність, комфортабельність готелю. Подібні, системи як правило, відстежують стан душових кабін системи опалення та кондиціювання [3].

Кліматичні умови в Україні «суворіші», ніж у багатьох інших країнах Європи. Взимку температура може опускається до –30°С, а літом сягати до 45°С. Таким чином погодні умови роблять істотний вплив на можливість експлуатації складних кліматичних систем, які часто не розраховані виробником на такий «широкий» діапазон зміни клімату. Мультизональні системи кондиціонування являють собою інтелектуальні та кіберфізичні системи центрального кондиціонування, які дозволяють керувати повітрям у кількох приміщеннях та у всій будівлі завдяки можливості підключення понад декількох десятків внутрішніх блоків до одного зовнішнього блоку. Це одна з найбільш енергоефективних систем, яка може працювати як на охолодження, так і на нагрівання повітря, створюючи індивідуальний клімат в кожному приміщенні [11].

На таких конкурентних ринках, як туризм, готелі конкурують за гроші, пропонуючи диференційовану якість. Крім того, згідно з мікроекономічною теорією, виробник диференційованих товарів є не ціноутворювачем.

Аналіз відносної ефективності здійснюється за допомогою аналізу оболонки даних, який визначає групу аналогів і цільові показники для неефективних підрозділів. Динамічний аналіз ефектів у часі впроваджених політик здійснюється за допомогою методології системної динаміки [1].

Такий комбінований підхід допоможе виявити які готелі мережі будуть привабливими, а які ефективними.

Закриті, контрольовані середовища, що простягаються від місць споживання предметів розкоші до міського виробництва продуктів харчування, поширюються в містах по всьому світу, використовуючи все більш просунуті методи для відтворення та оптимізації мікрокліматичних умов для різних цілей.

Однак роль кіберфізичних систем управління – фільтрувати, переробляти і збирати атмосферні і метаболічні потоки зі зростаючою точністю – залишається недостатньо розвинутою та вивченою.

Важливо досліджувати феномен кіберфізичного контролю навколишнього середовища в ботанічних оранжереях, розкішних готелях та інших об’єктах. Ці дослідження показують, як контрольоване середовище конституюється через специфічні відносини між внутрішнім і зовнішнім, які вбудовані в невід'ємні за своєю суттю політичні міські контексти та процеси.

По–друге, визначається технічна та екологічна напруга та межі екологічного контролю в приміщеннях на кожному об'єкті, які обмежують сферу застосування кіберфізичних систем, а також значну кількість прихованої праці та енергії, необхідних для підтримки та стабілізації бажаних кліматичних умов [2].

Неможливо переоцінити переваги корпоративної мережі, особливо з точки зору підвищення продуктивності та спрощення корпоративних процесів.

Невелика фірма з простою мережею може обійтися лише маршрутизатором і достатнім покриттям Wi–Fi, але в міру того, як організація зростає і ускладняється, ефективність і продуктивність, безсумнівно, будуть знижуватися, що негативно позначиться на кінцевому результаті.

Власнику бізнесу було б розумно найняти професійного консультанта з нетворкінгу, який би допоміг у всьому: від проектування архітектури кабелів і придбання стандартного обладнання до впровадження та навіть підтримки системи. Зрештою, нашвидкуруч побудована мережа з невідповідним дизайном може принести більше шкоди, ніж користі.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі

Технологічно просунутими контрольовані середовища, які застосовують методи кіберфізичного мікрокліматичного контролю в закритих приміщеннях для створення штучних умов для різних цілей, стають все більш поширеними – готельний бізнес, туристичні криті гірськолижні траси та тропічні острови.

Поряд з цими вражаючими випадками, поширюються більш приземлені форми екологічного контролю. Наприклад, кондиціонування повітря має довгу історію від заводу до торгового центру, призначене для створення та підтримки оптимальних умов для виробництва та споживання.

Сьогодні кондиціонування повітря стає майже повсюдним явищем у певних міських контекстах і поширюється за межі окремих будівель на ширше зовнішнє середовище. Зростає системна та інфраструктурна логіка та імператив для асамбляжу науково–технологічного потенціалу контрольованих середовищ як стратегічної форми міської адаптації та імунізації перед обличчям дедалі більш непередбачуваної екології.

Як задокументовано у великій, але розрізненій літературі, відтворення природи в приміщенні пов'язане з проблемами, невизначеностями та особливостями. Природу важко контролювати та імітувати і зупинити зовнішнє проникнення всередину ніколи не буває просто. У відповідь на це використання передових кіберфізичних систем відіграє дедалі більшу роль у екстравагантних заявах про потенціал контрольованих середовищ для подолання природних обмежень.

Тим не менш, кіберфізичні системи має свої межі та протиріччя, і в міру того, як соціально–екологічні ставки стають вищими, вексельний перетин кіберфізичних систем та екологічного контролю вимагає більшої уваги як з боку критично налаштованих міських географів, так і з боку екологічних географів [2].

Відповідний мікроклімат в приміщенні позитивно впливає на стан здоров’я. Шлях до сприятливого клімату починається з моніторингу поточних умов.

Значна увага приділяється моніторингу мікроклімату приміщень готелів. Мотивацією для моніторингу температури повітря і температур поверхонь, відносної вологості повітря або повітряного потоку є установка систем опалення та кондиціювання.

Шляхом аналізу найбільш часто використовуваних ключових слів було виявлено сильний зв'язок, наприклад, між тепловим комфортом і готелем.

Важливу роль для проведення досліджень моніторингу мікроклімату в готельних спорудах мають комп’ютерні системи, які окрім функцій управління забезпечують інформацією, необхідною для оцінювання моніторингу з точки зору обраного періоду року, вимірюваних параметрів і тривалості інтервалу між записами величин.

Досить часто результати моніторингу використовуються для калібрування імітаційної моделі, що описує гідротермальну поведінку готельного об'єкта при різних альтернативних варіантах експлуатації – вплив вентиляції, зміна клімату, заповнюваність, тощо. Таким чином, можна тестувати різні інтелектуальні системи управління мікрокліматом у віртуальному світі без особливого ризику, перш ніж вони будуть використані в реальному додатку для готельного бізнесу [4].

Дані про події, пов'язані з кліматом, мають бути записані окремо, тому коли вони вводяться, у розрахунок, то є можливість вибрати ночівлю, якусь подію або всі види даних. Це визначає кілька основних наслідків для майбутніх досліджень контрольованих середовищ.

Важливість застосування комп’ютерних систем для розробки теоретичних робіт щодо взаємозв'язків між внутрішнім і зовнішнім середовищем у готельній індустрії дуже важливе. Часткова та вибіркова реконструкція мікроклімату всередині все частіше використовується для створення нових об'ємних просторів як стратегічних ресурсів для відтворення комфортних місць відпочинку.

Рисунок 1.1 – Кіберфізичні системи для готельного комплексу

Застосування комп’ютерних систем забезпечить розгортання інфраструктури контрольованого середовища як стратегічного потенціалу, який і надалі залишатиметься вибірковим, фрагментованим і нерівномірно розподіленим у мікрокліматичній забудові готелю.

1.2 Характеристика і структура об’єкта впровадження

1.2.1 Системи управління енергоспоживанням готелю

Системи управління енергоспоживанням готелю – це суттєва економія готельєрів на експлуатаційних витратах, так як типовий готельний номер може бути незайнятим майже 70% часу.

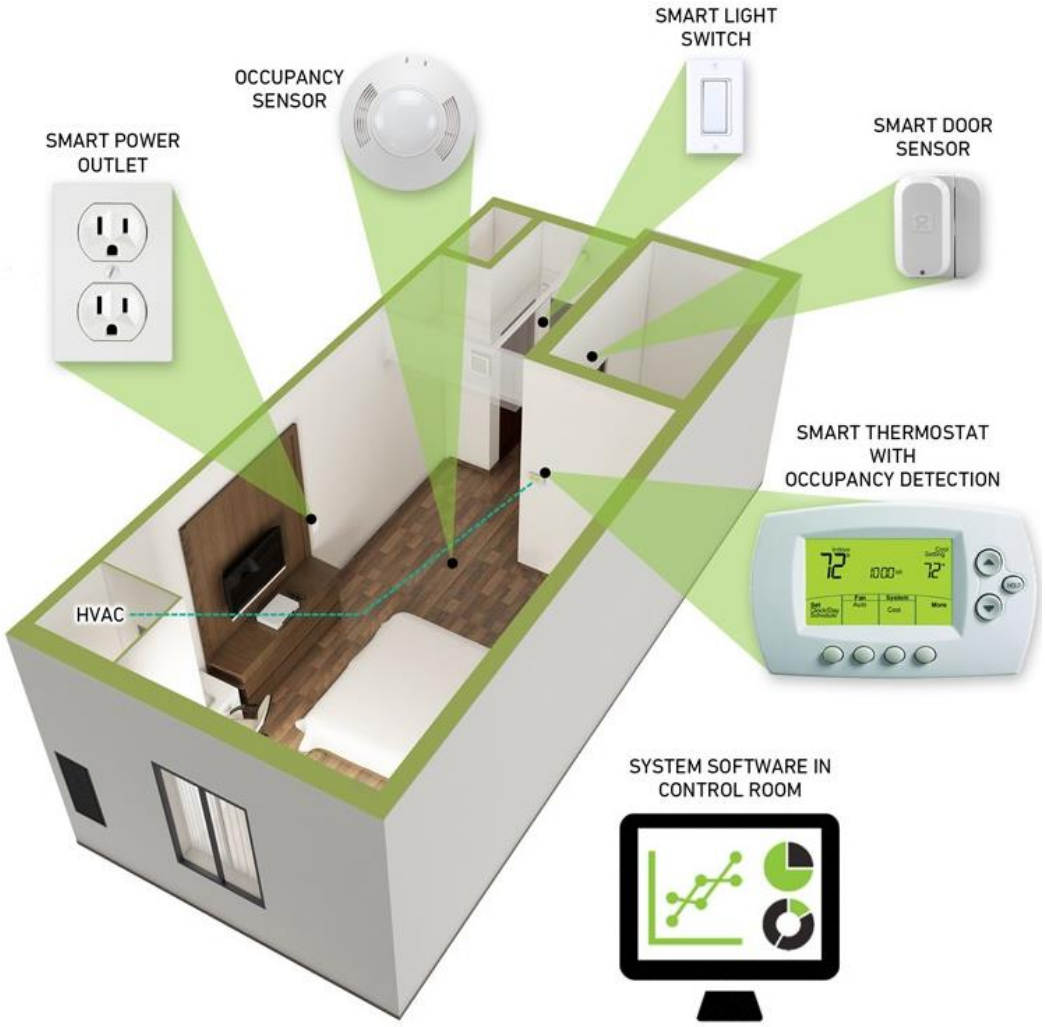


Рисунок 1.2 – Система енергетичного менеджменту для готелю

Крім того, постояльці готелю набагато менше турбуються про економію електроенергії у вашому готелі, ніж у себе вдома. Тому багато готельєрів платять за обігрів, охолодження, освітлення та живлення телевізорів для номера, в якому нікого немає. Одним з чудових рішень є системи енергетичного менеджменту (EMS).

EMS – це комбінація апаратного та програмного забезпечення (ПЗ), яка працює для зниження енергоспоживання готелю та покращення операцій з технічного обслуговування.

Ці системи використовують датчики присутності в номері, щоб визначити, чи присутній гість, а потім застосовують спеціальні профілі номерів, які регулюють освітлення відповідно до потужності.

EMS також використовує збір даних і планування програм для підвищення ефективності роботи та обслуговування готелю.

Загальна мета цих систем полягає в тому, що забезпечити комфортний мікроклімат, зменшити споживання енергії та технічне обслуговування, покращити умови проживання для гостей готелю.

Рисунок 1.3 – Зайнятий номер

Рисунок 1.4 – Вільний номер

Переваги використання системи енергетичного менеджменту для готелю:

1. Менше споживання енергії – Використовувані пристрої та освітлення в незайнятій кімнаті, такі як світло та телевізори, будуть вимкнені. Крім того, термостати можуть дрейфувати до температури, яка вимагає менших вимог до системи опалення, вентиляції та кондиціонування повітря.

2. Покращення якості обслуговування гостей – служба швидкої допомоги може підготувати номер під час реєстрації заїзду до стану прибуття. Цей параметр налаштовує термостат на комфортну температуру, вмикає привітну музику в кімнаті, забезпечує вітальне вітання на телевізорі та вмикає необхідне освітлення. Служба швидкої допомоги також розпізнає, коли в кімнаті проживає гість, що може допомогти уникнути непотрібних порушень прибирання.

3. Оптимізація профілактичного обслуговування – EMS може відстежувати час роботи системи опалення, вентиляції та кондиціонування повітря та повідомляти технічне обслуговування готелю, коли потрібне оновлення фільтрів та акумуляторів. Ця функція дозволяє проводити профілактичне обслуговування до скарг гостей і уникати типових непотрібних замін.

4. Прогнозування проблем з опаленням, вентиляцією, вентиляцією, вен Ця функція попереджає вас про термінові потреби в технічному обслуговуванні, наприклад, коли температура в приміщенні опускається занадто низько протягом зимового сезону [5].

1.3.1 Мережа готелів Optima Hotels & Resorts

Мережа готелів Optima Hotels & Resorts – це найбільша національна мережа готелів в Україні, ка нараховує більш ніж 40 готелів в 30 містах.

Рисунок 1.5 – Готелі мережа Optima Hotels & Resorts

Керуюча компанія мережі готелів, об'єднаних під зонтичним брендом Optima Hotel Group має готелі рівня 3, 4 зірки.

Мережа готелів Optima Hotels & Resorts складається з наступних брендів мережі: Optima Collection Hotel, Optima Hotels & Resorts, Vita Park, Raziotel [7].

Складові успіху мережі готелів Optima Hotels & Resorts:

– стандарти бренду та корпоративної культури;

– стандарти обслуговування та операційної діяльності4

– центральний відділ продажів і маркетингу;

– будівельний підрозділ, служба архітектури та дизайну.

– централізована система закупівель;

– єдина система адаптації, навчання та розвитку співробітників.

1.3.1 Готель Optima collection Дніпро

Готель Optima Collection Дніпро (вул. Шевченка 53 А), розташований в центральній частині м. Дніпро.

Рисунок 1.6 – Готель Optima Collection Дніпро

Номерний фонд готелю Optima Collection Дніпро становить 23 розкішних і комфортабельна мебльованих номерів: «Стандарт Твін», «Стандарт Double», «Суперіор Double», «Напівлюкс Double» і «Люкс Double».

Готель Optima Collection Дніпро має власний ресторан, бар і конференц–зал, повне покриття WI–FI, на території є кіберфізична система для парковки.

Рисунок 1.7 – Внутрішній простір готелю Optima Collection Дніпро

У готелі передбачено місце для перебування персоналу та гостей під час повітряної тривоги [6].

1.3 Технології збору та передачі інформації для систем управління мікрокліматом готельних комплексів

1.3.1 Сімейство пристроїв IoT від SensorFlow

Застосування продукції від SensorFlow, якій довіряють Accor, Marriott та інші бренди готельного бізнесу, може скоротити витрати на опалення, вентиляцію та кондиціонування повітря вдвічі завдяки своїм передовим технологіям. SensorFlow використовує бездротові датчики для визначення зайнятості номерів, які потім керують системою опалення, вентиляції та кондиціонування повітря в номері на основі різноманітних вхідних даних.

Якщо система виявляє, що кімната вільна, система вимикається або перемикається на більш енергоефективні налаштування, а коли гість знову входить до номера, система повертається до попередніх налаштувань, щоб гість залишався у комфортних умовах. SensorFlow пишається своєю зручною, інтуїтивно зрозумілою системою, і компанія підрахувала, що можна встановити їхні пристрої всього за п'ять хвилин у кожному номері.

За допомогою цифрового інтерфейсу можна налаштувати такі параметри, як години дії кіберфізичних систем, порогові значення та енергозберігаючі режими. Інформаційна панель також показує такі показники, як температура, вологість, поведінка гостей і тенденції використання, щоб ви могли оптимізувати економію коштів без шкоди для комфорту.

Сімейство пристроїв IoT від SensorFlow засновано на штучному інтелекті, SensorFlow поєднує бездротові рішення IoT та кіберфізичні системи, щоб зробити розумні будівлі реальністю. Це дозволяє адаптувати окремі будівлі, допомагаючи розкрити переваги щодо сталого розвитку, енергоефективності та економії коштів.

Рисунок 1.8– Пристроїв IoT від SensorFlow

Одним ранніх висновків компанії було те, що на ринку модернізації немає двох однакових будівель, тому ви повинні бути адаптивними. Ось чому компанія створила ціле сімейство пристроїв IoT, які можуть служити різним сценаріям

використання. Це модульний підхід, який означає, що можна швидко встановити датчики в місцях без необхідності закривати будівлю на будь–який період часу.

Встановлені датчики визначають, чи зайнята кімната, чи відкриті вікна або чи потрібно відрегулювати температуру навколишнього середовища, і вносять відповідні зміни. Завдяки аналітиці та штучному інтелекту в системі управління, система може інформувати про більш широку картину прийняття рішень з точки зору енергетичної стратегії або інвестицій у модернізацію будівель.

Штучний інтелект відіграє ключову роль у SensorFlow і є темою, яка особливо цікавить компанію. Компанія очікує, що сучасні розмовні моделі штучного інтелекту відкриють великі переваги, особливо коли йдеться про навчання та розвиток. Штучний інтелект замінить читання користувачами посібників та витрачати час на запам'ятовування всіх тонкощів того, як щось працює – продукт сам пояснить потрібно робити.

Великі готельні мережі мають команди інженерів і витрачають тижні на їх навчання, але бачать, що люди йдуть і їм доводиться починати процес спочатку. Інституційні знання падають, а величезна кількість часу та грошей витрачається даремно. Можливість зробити системи більш доступними за набагато коротший час дозволить людям використовувати переваги технологій і робити більше з меншими витратами [9].

1.3.2 Технології збору та передачі інформації для мережі готелів Optima Hotels & Resorts

Технології збору та передачі інформації для мережі готелів Optima Hotels & Resorts використовує технологію оптимізації стека програмного забезпечення для периферійної або хмарної аналітики. Програмний стек самої бази даних або екземплярів хмарних баз даних, може бути переналаштований в умовах швидко мінливих робочих навантажень IoT, як це зроблено для локальних NoSQL DBs або для хмарної або безсерверної інфраструктури в умовах мінливих робочих

навантажень. Ця реконфігурація може призвести до підвищення продуктивності як з точки зору більш традиційних метрик на основі пропускної здатності, так і з точки зору метрик на основі затримки. Ці системи часто розроблені, щоб допомогти досягти ефективності витрат і продуктивності баз даних, розміщених у хмарі, надаючи ресурси на користь як постачальникам хмарних послуг, яким не потрібно агресивно надмірно надавати свої сервери, розміщені в хмарі, для відмовостійких операцій, так і клієнтам, оскільки економія на центрах обробки даних може бути передана їм. Такі оптимізовані програмні стеки можуть покращити наскрізну продуктивність конвеєрів IoT.

Архітектура мережі складається з декількох сенсорних вузлів IoT, підключених бездротовим способом до периферійного сервера за допомогою мережі BLE або LoRa, як показано на рис. 1.9.

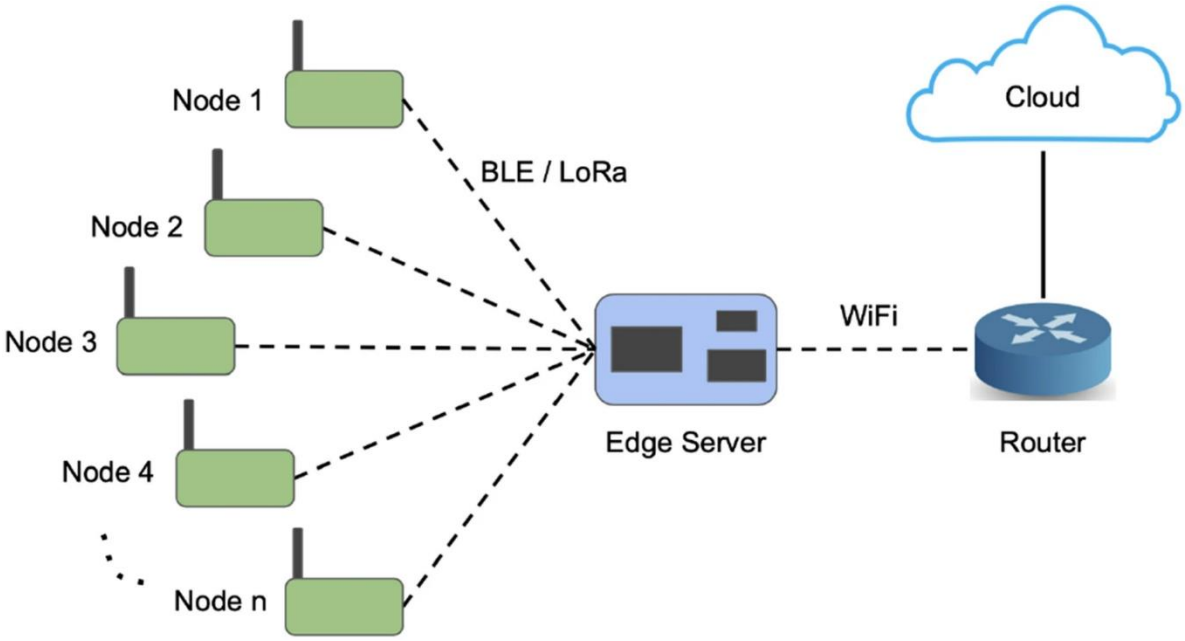


Рисунок 1.9– Архітектура мережі BLE або LoRa

Периферійний сервер, у свою чергу, підключений до хмари. Дані, зібрані сенсорними вузлами IoT, надсилаються на периферійний сервер для аналізу. З периферійного сервера дані можуть бути відправлені в хмару для зберігання та подальшого аналізу за потреби. Відтепер, коли ми говоримо про «сервер», ми маємо

на увазі периферійний сервер, а не хмарний сервер (якщо прямо не вказано інше) [10].

1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

Одним з найважливіших фінансових показників індустрії гостинності є коефіцієнт заповнюваності, тобто кількість зайнятих номерів в порівнянні із загальною кількістю доступних номерів. На цей показник безпосередньо впливає комфорт гостей готелю, так як задоволені гості з більшою ймовірністю повернуться. [10]

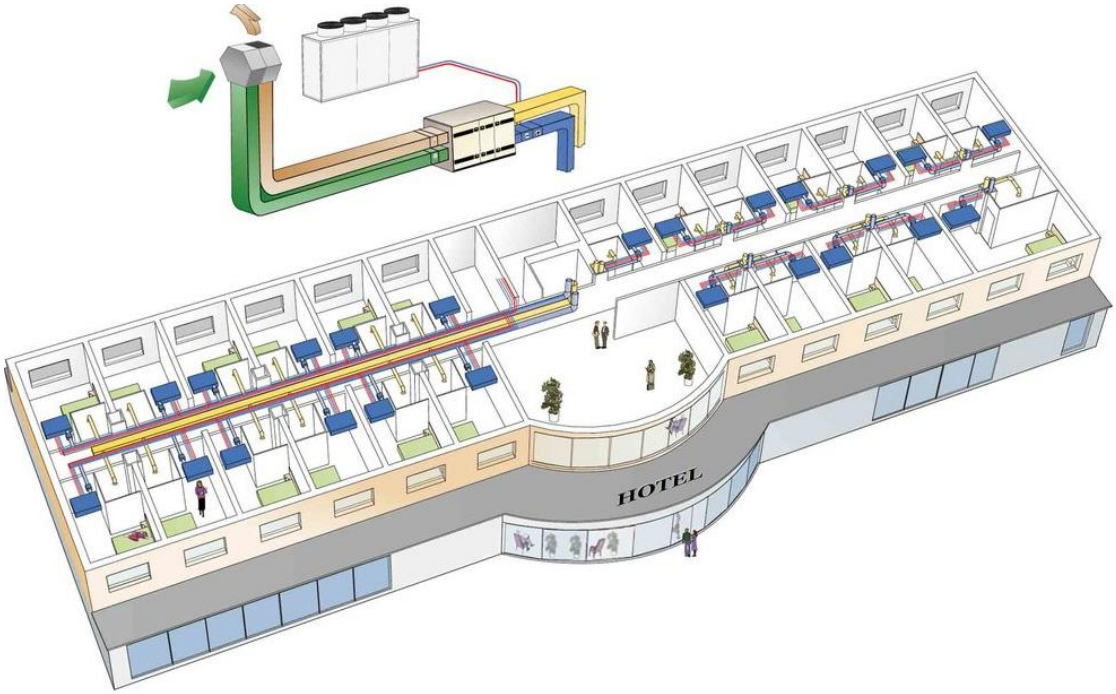


Рисунок 1.10– Розташування елементів системи контролю мікроклімату у готельному комплексі

Інформаційне забезпечення КС для кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group має забезпечувати підтримку та реалізацію наступних завдань:

1. Затишок – номери повинні бути чистими, свіжими, тихими і затишними – це головні вимоги гостей готелю. Майже усім доводилося погоджуватися на готельний номер з центральною вентиляцією, яку не можна було відрегулювати, яка хиталася або свистіла, і де температура була або занадто високою, або занадто низькою. Саме тому більшість гостей хочуть мати можливість самостійно контролювати клімат у своєму номері. Потреба в системному рішенні полягає у створенні індивідуально керованого мікроклімату в приміщенні з високою енергоефективністю та економічною експлуатацією одночасно.

2. Проблема вентиляційних каналів – готельні номери зазвичай розташовуються один за одним, тому вентиляційна система часто має великі розгалужені повітроводи. Це створює велику різницю тисків між першим і останнім припливним повітряним проходом. Це призводить до додаткового шуму. Коефіцієнт нерегулювання зростає. Чим нижчий тиск, що регулюється на виходах припливного повітря, тим тихіше працює система.

3. Комплексний підхід – при плануванні вентиляційної системи в готелі, потрібно враховувати всі фактори і застосовувати всі необхідні компоненти. Прикладом такого підходу є дизайн типового п'ятиповерхового готелю. Системне рішення полягає в поділі системи кондиціонування на дві підсистеми, що дає ряд переваг перед традиційними готельними рішеннями.

4. Розміщення дифузорів – конструкція конусів, їх тип і положення є одними з ключових факторів, які слід враховувати. При виборі типу дифузора і місця його установки важливо враховувати розташування меблів готельного номера. Треба знайти правильні рішення, щоб гості залишалися задоволеними. Треба мати на увазі, що будь–яка подальша перестановка меблів може вимагати переналаштування або перевибору дифузорів припливного повітря.

5. Модулі управління процесом охолодження і нагріву – кожен номер готелю кондиціонується і вентилюється компактним модулем комфорту, який управляється кіберфізичною системою вентиляційної установки. Мікроклімат в

громадських зонах, ресторанах, вестибюлях і переговорних кімнатах забезпечується модулями комфорту, що не обслуговуються. Керовані повітряні заслінки, підключені до системи управління вентиляційною установкою, оптимізують роботу всієї системи і підвищують енергоефективність.

7. Можливості для подальшої економії – завдяки сучасним датчикам руху та CO2, а також підключенню даних від рецепції готелю до системи кондиціонування, експлуатаційні витрати були значно знижені. Коли гостя немає в приміщенні, вентиляція зменшується, що призводить до значної економії. У порівнянні з постійним повітряним потоком, близько 80% електричної енергії, що використовується для роботи вентиляторів, і 40% енергії, що використовується для роботи опалення та охолодження, можна заощадити без шкоди для комфорту гостей готелю.

1.5 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань

Програмне забезпечення локальної КС має ієрархічну структуру та відповідає семи–рівневий моделі OSI. Така ситуація спрощує питання стандартизації ПЗ за загальноприйнятими протоколами. Основним завданням КС є забезпечення роботи прикладних процесів, реалізованих в кіберфізичних системах, включених до мереж. Реалізація прикладних процесів забезпечується за допомогою засобів мережевого прикладного програмного забезпечення (NSP), які реалізуються протоколами верхнього (прикладного) рівня моделі OSI і тим самим формують верхній рівень програмної структури локальних КС (LCN).

Обмін даними між процесами реалізації взаємодії та прикладними процесами різних АС реалізується за допомогою мережевих операційних систем (NSS) та мережевого обладнання. Як правило, додатки локальної мережі (LAN) реалізують протоколи трьох верхніх рівнів (рівень прикладної програми, рівень презентації та рівень сеансу) у моделі OSI. Чотири протоколи нижчого рівня (транспортний,

мережевий, канальний і фізичний) протоколи моделі OSI зазвичай реалізуються апаратним забезпеченням (мережевим адаптером).

Найбільша національна мережа розкішних готелів Optima Hotels & Resorts, яка нараховує більш ніж 40 готелів в 30 містах, та складається брендів мережі: Optima Collection Hotel, Optima Hotels & Resorts, Vita Park, Raziotel мають покладаються на сучасні інтелектуальні технології управління перш за все з використанням комп’ютерних систем з їх безмежними можливостями з інформаційного забезпечення різноманітних сфер і процесів.

Система бронювання має бути підключена до КС системи управління мікрокліматом готелю, завдяки такому зв'язку в кімнатах завжди буде комфортна і при цьому не буде споживано зайву енергію.

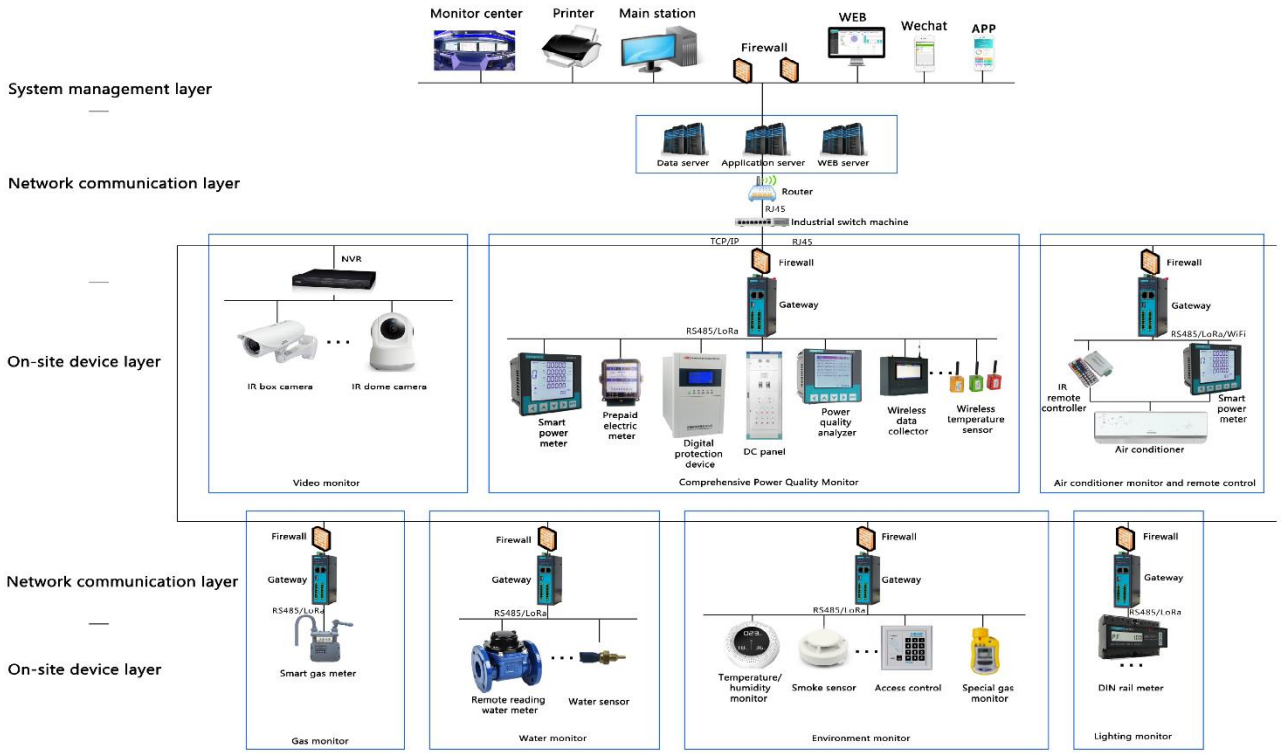


Рисунок 1.11 – Система енергетичного менеджменту

Крім комфорту, треба забезпечити профілактика і безпеку гостей готелю. Це включає профілактику проти хронічних хвороб, завдяки підключенню технологічних рішень до душових кабін та системи опалення та кондиціювання де

система управління отримуєте сповіщення, як тільки буде виявлено незвичайне відхилення від встановлених санітарних норм. Це гарантуватиме комфортний відпочинок для гостей готелю з дотриманням норм навколишнього середовища.

Система енергетичного менеджменту використовується для онлайн–моніторингу споживання електроенергії, води, газу, тепла тощо. Система енергетичного менеджменту може генерувати погодинний, щоденний, щотижневий, щомісячний, річний звіт про дані. Система енергетичного менеджменту також інтегрує функцію керування ланцюгом лічильника дистанційного керування та з функцією сигналізації про перевантаження тощо.

Система енергоменеджменту готелів має кілька поверхів, і на кожному поверсі, загальна кількість номерів може сягати декількох сотень [8].

Мультизональні системи кондиціонування включають в себе повітряні системи зі змінним повітряним потоком і інтегрованими системи управління, де надлишок тепла і основна вологість приміщення поглинається кімнатними кондиціонерами, а повітряне навантаження залишається на центральний кондиціонер або вентиляційну систему.

Мультизональна система кондиціонування призначена для управління вентиляцією і створення комфортного мікроклімату у всіх приміщеннях будівлі, яка складається з зовнішнього і внутрішнього блоків, з'єднаних трубами, по яких рухається теплоносій. В якості теплоносія використовується одна з марок фреону. На відкритому повітрі – створюється мікроклімат і циркуляція свіжого повітря. Температура регулюється індивідуальними пультами управління. Також вона може здійснюватися від станції управління через всю комп’ютерну систему управління і окремі елементи. Системи VRV або VRF є синонімом багато–зонної конфігурації, яка являє собою систему, в якій подачу холодоагентів кінцевому споживачеві диверсифікує сам споживач. Кліматичні умови кожного приміщення не залежать один від одного і контролюються всередині або з центральної станції [12].

1.6 Схема організаційної структури мережі готелів Optima Hotels & Resorts

Організаційна структура управління готельною мережею вимагає раціонального навчання і постійного вдосконалення, що робить цю діяльність складною і актуальною темою в управлінні. Взагалі, організаційна структура – це структура, фундамент і сутність всієї компанії, тому побудова організаційної структури – це дуже важливий процес.

Правильно побудована організаційна структура дозволяє компанії ефективно працювати, правильно управляти кожним відділом компанії, і тим самим визначати фінансовий успіх, так як грамотна організоване управління неминуче веде до зниження витрат і підвищення ефективності.

Менеджмент передбачає делегування прав і обов'язків для організації взаємодії органів управління і розподілу завдань, які необхідно вирішити різним працівникам. Керівники повинні наділити співробітників своїми правами і обов'язками, інакше необхідна робота не буде виконана. Таким чином, організація праці – це робота. Це те, що потрібно робити всім керівникам на всіх рівнях. Однак слід зазначити, що дане поняття передбачає делегування прав і обов'язків щодо поділу роботи по горизонталі і вертикалі, але рішення про вибір структури організації практично завжди приймає керівництво. При цьому керівники середньої і нижчої ланки допомагають йому тільки через засоби масової інформації, а у великих компаніях ще й пропонуючи структуру своїх підрозділів, що відповідає вже обраній вищим керівництвом загальній структурі організації. В цілому в широкому сенсі метою керівника в такій діяльності є вибір структури, яка максимально відповідає завданням і цілям організації, впливаючи на неї зовнішніми і внутрішніми факторами.

Найкраща структура – це та, яка найкращим чином дозволяє організації ефективно взаємодіяти із зовнішнім середовищем, продуктивна і швидко

розподіляти зусилля співробітників, а завдяки цим заходам задовольняти потреби клієнтів і виконувати поставлені завдання з високою ефективністю.

Робота готелю визначається його організаційною структурою, яка становить основу моделі управління готельною компанією. Це стосується і роботи готельної мережі. Організаційна структура керівництва – це система взаємовідносин, які працюють між підрозділами готелю, а також його співробітниками. Тобто адміністративна одиниця підрозділів строго підпорядкована і забезпечує взаємодію між керованою системою і системою, якою вона керує. Іншими словами, організаційна структура управління визначає сутність готелю і становить основу його діяльності.

Призначення організаційної структури управління готелем Optima Collection Дніпро виражається в забезпеченні раціонального розподілу і кооперації праці в готелі, у визначенні завдань і визначенні того, хто відповідає за їх вирішення, в розподілі функціональних обов'язків між співробітниками і в забезпеченні зв'язку між ними, а також в створенні і підтримці каналів зв'язку рис. 1.12.

Рисунок 1.12 – Організаційна структура управління готель Optima Collection Дніпро

Організаційна структура готелю Optima Collection Дніпро повинна забезпечувати виконання його основних завдань: ефективне функціонування закладу або установ і задоволення потреб співробітників і клієнтів.

Налагоджена організаційна структура є ключовим фактором ефективної роботи мережі готелів або готелів. Без такої умови навіть найпрофесійніші менеджери не можуть повноцінно розвинути свій лідерський потенціал. Все це вимагає постійного перегляду організаційної структури готелю або готельної мережі з метою постійної адаптації її до умов динамічного середовища.

Використання організаційної структури готелів мережі Optima Hotel Group вимагає поєднання команди IT–фахівців готелів мережі Optima Hotel Group та мережевого обладнання у комп’ютерну мережу.

Структура комп'ютерної системи кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group визначена завданням до кваліфікаційної роботи бакалавра.

Загальна структура кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group має вигляд такий, як наведено на рис. 1.13.

Параметри LAN для кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group наступні:

- блок адрес для виділення підмереж: 10.25.IPn.0/22;
- значення IPn блоку адрес виділення підмереж IPn: 120;
- кількості вузлів для мережі LAN1: 7;
- кількості вузлів для мережі LAN2, од.: 111;
- кількості вузлів для мережі LAN3, од.: 93;
- кількості вузлів для мережі LAN4, од.: 47;
- кількості вузлів для мережі LAN5, од.: 26;
- інтенсивність найбільшої мережі, μ (кадрів/с): 170.

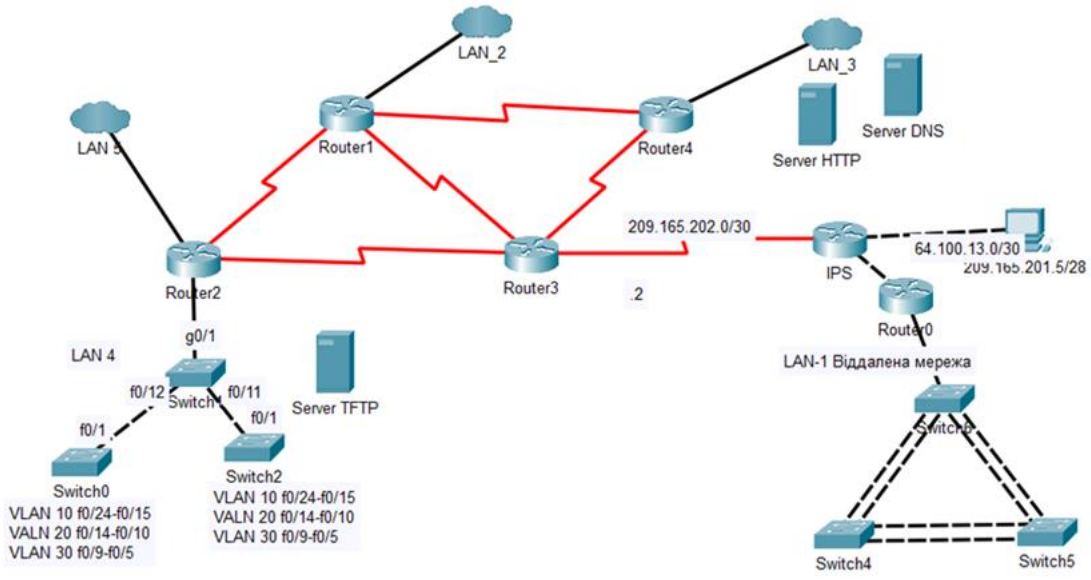


Рисунок 1.13 – Топологія мережі кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group

Розподіл мереж між маршрутизаторами (WAN):

- блок адрес для каналів між маршрутизаторами 10.0.№.0/24;
- номер варіанту № 15;
- перші можливі для використання IP–адреси призначати інтерфейсам і під–інтерфейсам маршрутизаторів у LAN;
- інші з можливих IP–адрес призначати комутаторам у LAN;
- адреса серверів: перший можливий адресу у мережі + 9 + №.
- адреса вузлів: інші з використаних;
- в мережах VLAN використовувати адресацію кінцевих пристроїв за протоколом DHCP.

1.7 Завдання і мета роботи

У кваліфікаційній роботі бакалавра необхідно розробити кіберфізичну система контролю мікроклімату готелів мережі Optima Hotel Group.

Треба щоб розроблена кіберфізична система контролю мікроклімату готелів мережі Optima Hotel Group мала значну надійність роботи, високу стійкість до

зростаючої кількості кіберзагроз та інцидентів, якій можуть підвергатися мережеві пристрої комп’ютерної системи, на якій базується побудова кіберфізичної системи контролю мікроклімату для готелів мережі Optima Hotel Group.

Враховуючи архітектуру кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group, потрібну кількість підмереж, та їх взаємозв’язок між собою, та необхідну кількість мережевих пристроїв управління мікрокліматом у кімнатах готелю, комп’ютерів для робочих станцій обслуговуючого персоналу для мережі Optima Hotel Group, перш за все треба виконати розрахунок налаштувань для визначеної топології комп’ютерної мережі, здійснити вибір інтерфейсу для каналів зв’язку між мережевими пристроями, визначитися з протоколом обміну даними між мережевими пристроями, провести необхідні розрахунки для топологічної схеми комп’ютерної системи, здійснити розрахунок налаштувань маршрутизації у комп’ютерній мережі, а також виконати подальше моделювання роботи мережі і перевірку її правильної роботи.

1.8 Визначення можливих напрямків рішення поставлених завдань

1.8.1 Загальна інформація про кіберзагрози

В умовах повної цифровізації бізнес–одиниці покладаються на багатофакторні зовнішні впливи, особливо в кіберпросторі. Пандемія та війна в Україні створили нові погляди на цифрові відносини, яке необхідно захищати від дезінформації, кібератак та кіберінцидентів.

Сьогодні готельні бренди також беруть участь в інформаційних війнах проти руйнівної російської агресії та переживають кризу нового виду, пов’язану з можливою уразливістю комп’ютерних систем від постійних кібератак, які постійно нарощують свій потенціал, вдосконалюючи свої можливості по враженню об’єкта атаки.

Тому кіберзахист став одним із стратегічних завдань фінансової безпеки готельного бренду, а його важливість полягає у визначенні його напрямків на часовому горизонті результатів.

Оскільки індустрія гостинності стає все більш залежною від технологій, важливість кібербезпеки важко переоцінити.

Оскільки системи онлайн–бронювання, обробка платежів та зручності в номерах покладаються на технології, готелі та курорти стали головними мішенями для кібератак.

Успішна кібератака може призвести до фінансових втрат, шкоди репутації та втрати довіри клієнтів.

Розглянемо найпоширеніші кіберзагрози, з якими стикається індустрія гостинності, визначити напрямки, як готелі можуть стати менш вразливими мішенями для хакерів.

Фінансові втрати можуть бути значними, оскільки хакери можуть отримати доступ до конфіденційних фінансових даних, таких як номери кредитних карток та інформація про банківські рахунки. Окрім фінансових втрат, кібератака також може призвести до шкоди репутації готелю та втрати довіри клієнтів.

Якщо системи готелю скомпрометовані, гості можуть бути не в змозі робити або змінювати бронювання, а готель може бути не в змозі обробляти платіжні транзакції.

Це може призвести до розчарування гостей і значного падіння доходу.

У деяких випадках кібератака також може порушити повсякденну роботу готелю, що призведе до додаткових витрат і створить незручності для гостей.

Загалом, наслідки кібератаки на готель можуть бути далекосяжними та довготривалими.

За останні роки відбулося кілька гучних кібератак на готелі. Ось кілька прикладів:

– готель Mandarin Oriental в Бангкоку (2014). Готель став жертвою кібератаки, в результаті якої було викрадено понад 500 000 номерів кредитних карток. Хакери отримали доступ до систем торгових точок готелю та змогли викрасти дані кредитних карток гостей, які робили покупки в ресторанах і магазинах готелю.

– готелі Трампа (2017). Мережа зазнала витоку даних, який торкнувся 14 об'єктів нерухомості в Сполучених Штатах. Хакери отримали доступ до платіжних систем готелів і змогли викрасти дані кредитних карток гостей, які робили покупки в готелях.

– готель Mariott International (2018). Вони стали жертвою масштабного витоку даних, від якого постраждали до 500 мільйонів гостей. Хакери отримали доступ до системи бронювання готелю та змогли викрасти конфіденційну інформацію, таку як імена, адреси та номери паспортів.

– InterContinental Hotels Group (2019). Група зазнала витоку даних, який вплинув на гостей 12 її готельних брендів. Хакери отримали доступ до платіжних систем готелів і змогли викрасти дані кредитних карток гостей, які робили покупки в готелях.

– невеликий готель в США (2019). Готель зазнав витоку даних, що призвело до крадіжки номерів кредитних карток та іншої конфіденційної інформації. Хакери отримали доступ до платіжних систем готелю та змогли викрасти дані гостей, які здійснювали покупки в готелі.

– бутік–готель в Канаді (2020). Стали жертвами фішингової атаки. Хакери розіслали фальшиві електронні листи нібито з системи бронювання готелю та обманом змусили співробітників розкрити облікові дані для входу. Отримавши облікові дані для входу, хакери змогли отримати доступ до систем готелю та викрасти конфіденційні дані.

Готелям важливо бути пильними та вживати заходів, щоб захистити себе та своїх гостей від кіберзагроз. Існує кілька поширених кіберзагроз:

1. Програми–вимагачі: цей тип атаки полягає в тому, що хакери шифрують дані готелю та вимагають викуп в обмін на ключ розшифровки.

2. Фішинг: цей тип атаки полягає в тому, що хакери надсилають підроблені електронні листи або текстові повідомлення, які нібито надходять із законних джерел, щоб обманом змусити людей розкрити конфіденційну інформацію або завантажити шкідливе програмне забезпечення.

3. Зловмисне програмне забезпечення: цей тип атаки полягає в тому, що хакери встановлюють шкідливе програмне забезпечення в системах готелю, щоб отримати доступ до конфіденційних даних готелю або порушити роботу.

4. Атаки типу "людина посередині": цей тип атаки полягає в тому, що хакери перехоплюють спілкування між двома сторонами, щоб отримати доступ до конфіденційної інформації.

5. Атаки типу «відмова в обслуговуванні» (DoS): цей тип атаки полягає в тому, що хакери перевантажують системи готелю трафіком, роблячи їх нездатними функціонувати належним чином.

6. Атаки на паролі: цей тип атаки полягає в тому, що хакери намагаються вгадати або зламати паролі, щоб отримати доступ до конфіденційних даних гостей.

Важливо, щоб готелі знали про ці загрози та вживали заходів, щоб захистити себе та своїх гостей від кібератак. Це може включати впровадження надійних паролів, регулярне оновлення програмного забезпечення та систем безпеки, а також навчання співробітників тому, як виявляти та запобігати кібератакам [13].

1.8.2 Найбільш уразливі місця в готелі:

Є кілька місць у готелях, які особливо вразливі до кібератак:

1. Мережі Wi–Fi: Загальнодоступні мережі Wi–Fi часто незахищені, і хакери можуть легко отримати до них доступ.

2. Системи торгових точок: Ці системи, які використовуються для обробки платіжних транзакцій, є поширеною мішенню для хакерів.

3. Системи онлайн–бронювання: Ці системи часто є першою точкою контакту для гостей і можуть бути вразливими до атак.

4. Зручності в номері: Смарт–телевізори, термостати та інші підключені пристрої можуть бути вразливими до злому, якщо вони не захищені.

5. Пристрої співробітників: Хакери можуть намагатися отримати доступ до систем готелю за допомогою пристроїв співробітників – ноутбуків та смартфонів.

6. Фізичні точки доступу: Хакери також можуть намагатися отримати фізичний доступ до систем готелю через незахищені двері або вікна.

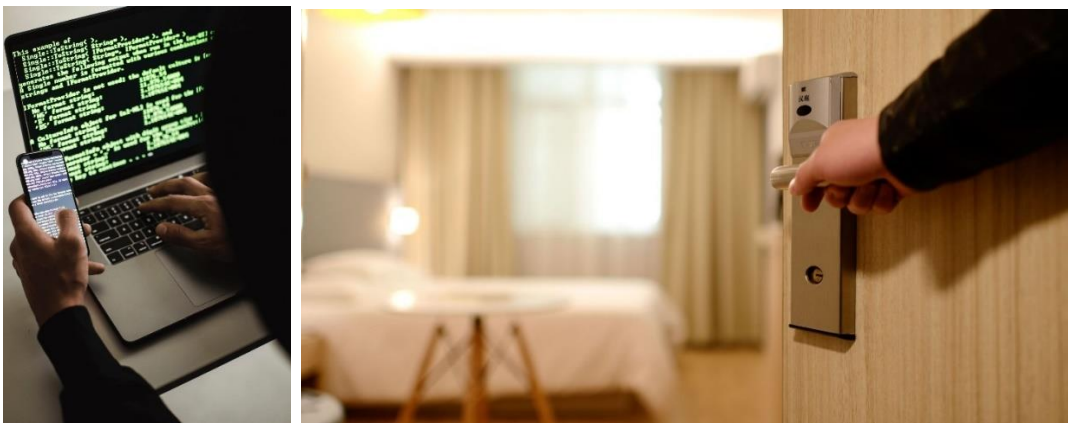


Рисунок 1.13 – Кіберзагроза фізичного проникнення в номер

Важливо, щоб готелі знали про ці вразливості та вживали заходів для їх захисту. Це може включати впровадження надійних паролів, регулярне оновлення програмного забезпечення та систем безпеки, а також навчання співробітників найкращим практикам кібербезпеки [13].

1.8.3 Методи захисту від кіберзагроз

Є кілька кроків для які готелів, щоб стати не вразливою мішенню для хакерів:

1. Надійні паролі – складні паролі, які хакерам важко вгадати або зламати. Заохочування співробітників робити те саме для своїх особистих пристроїв.

2. Регулярне оновлення ПЗ та системи безпеки – все програмне забезпечення та системи безпеки мають бути оновлені останніми виправленнями та оновленнями. Це виправить будь–які відомі вразливості, якими можуть скористатися хакери.

3. Ознайомлення співробітників із найкращими практиками кібербезпеки – протидія фішинговій електронній пошті, зловмисне програмне забезпечення.

3. Безпечні мережі Wi–Fi – надійні паролі та шифрування для захисту мереж Wi–Fi готелю, можливість використання віртуальної приватної мережі (VPN) для додаткового захисту онлайн–активності гостей.

4. Використання брандмауерів та антивірусного ПЗ, оновлення їх.

5. Регулярне відстеження комп'ютерної системи на предмет незвичайної активності, вживання відповідних заходів, якщо виявлено щось підозріле.

Рисунок 1.14 – Використання надійних секретних паролів

Ці кроки для готелів можуть значно знизити ризик стати мішенню хакерів і захистити себе та своїх гостей від кібератак [13].

1.9 Обґрунтування вибраного напрямку інженерного рішення

Розширення сфери та функціональності кіберфізичної система контролю мікроклімату готелів мережі Optima Hotel Group потребує надійної кібербезпеки.

Закон про цифрову операційну стійкість (DORA) – це нова правова база, створена Європейським Союзом для підвищення операційної стійкості фінансового сектору. Впровадження DORA має на меті гарантувати, що всі компанії в секторі фінансових послуг мають адекватні захисні заходи для зниження кіберризиків і підтримки безперебійної роботи у разі збоїв. DORA розширює та конкретизує

вимоги та посилює їх, зокрема, для компаній фінансового сектору та їхніх постачальників ІТ–послуг.

Основними складовими успіху є застосування директиви DORA, де дотримується цілісний підхід, спрямований на широко визначену цільову групу фінансових компаній, які в майбутньому підпадатимуть під сферу регулювання.

Фінансові установи: Розширення сфери діяльності банків та страхових компаній, які вже знайомі з рекомендаціями EBA/EIOPA щодо безпеки ІТ та аутсорсингу, на торгові платформи, професійні пенсійні установи, постачальників криптопослуг, страхових посередників та багато інших фінансових компаній, компаній готельного бізнесу та туризму.

Постачальники ІТ–послуг: Крім того, постачальники ІТ–послуг, які працюють у фінансових установах, тепер також підпадають під дію DORA, якщо вони класифікуються як «критично важливі постачальники ІТ». Критерії цієї класифікації, які мають бути додатково уточнені Європейськими наглядовими органами (ЄКА), залежать насамперед від того, наскільки критичними є послуги, що надаються для фінансового ринку, наскільки вони залежать від постачальника ІТ і наскільки легко їх можна замінити.

Ця широка сфера застосування має вирішальне значення, оскільки вона гарантує, що вся фінансова екосистема, включаючи допоміжну інфраструктуру ІКТ, дотримується послідовних стандартів стійкості. Це дозволить значно знизити системний ризик та підвищити стабільність фінансових ринків у межах Європейського Союзу.

Наріжні камені DORA. Для підвищення кібербезпеки фінансового сектору в Європейському Союзі DORA спирається на такі ключові моменти:

Управління ризиками ІТ: Розробка комплексної концепції та структури інформаційної безпеки, включаючи оцінку існуючої стійкості та налаштування систем безпеки для постійної ідентифікації.

Звітування про інциденти в ІТ: Розробка індикаторів раннього попередження та інструментів для класифікації, управління та відстеження інцидентів.

Цифрове тестування операційної стійкості: створення планів на випадок надзвичайних ситуацій, проведення регулярних тестів та їх оцінка (наприклад, наскрізний, ефективність, проникнення або сумісність), а також навчання співробітників.

Управління ризиками третіх сторін у сфері ІТ: оцінка обсягу, складності та актуальності залежностей, пов'язаних з ІТ, від постачальників послуг, включаючи договірні угоди та документацію до них.

Угоди про обмін інформацією: передача інформації про кіберзагрози в межах довірених мереж для підвищення безпеки та забезпечення захисту деталей і відповідності політикам конфіденційності та конкуренції.

Разом ці пункти зміцнюють цифрову інфраструктуру фінансового сектора і, таким чином, забезпечують ефективне вирішення збоїв у роботі, пов'язаних з проблемами ІТ. Це забезпечує цілісність ринків і зміцнює загальну довіру.

Роль обізнаності про кібербезпеку для готельєрів важко переоцінити.

Зробивши кібербезпеку пріоритетом і навчаючи співробітників найкращим практикам, готелі можуть значно знизити ризик стати мішенню для хакерів.

У разі кібератаки готелям важливо мати план відновлення та мінімізації збоїв [14].

Sbit Hospitality ICT Services може допомогти готелям запобігти кібератаці та впоратися з нею, надаючи низку рішень з кібербезпеки.

Ці рішення включають хмарне резервне копіювання, аварійне відновлення, мережу, а також віддалений моніторинг і керування.

Використовуючи ці рішення, готелі можуть краще захистити себе від кіберзагроз і швидше та ефективніше відновлюватися в разі атаки [12].

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Комп'ютерні системи (КС) – це з'єднання різної кількості комп'ютерів і периферійних пристроїв за допомогою ліній зв'язку (кабелів) в одну інформаційну мережу. Комп'ютерні мережі є дуже складними структурними системами, і їх коректна робота залежить від роботи кожного елемента мережі. Забезпечення інформаційної безпеки в глобальних (Інтернет) або локальних мережах є однією з найактуальніших проблем, що постають перед комп'ютерними фахівцями. Мережа – група комп’ютерів або інших пристроїв, з’єднаних будь–якими засобами з метою обміну інформацією та спільного використання ресурсів. Ресурси — це спільні програми, файли, принтери та інші периферійні пристрої в мережі.

2.1 Технічні вимоги до кіберфізичної системи контролю мікроклімату готелів мережі «Optima Hotel Group»

2.1.1 Вимоги до системи в цілому

КС має назву кіберфізична системи контролю мікроклімату готелів мережі «Optima Hotel Group», далі скорочено КФСМ. КФСМ повинна розроблятися і виготовлятися відповідно до вимог актуальних стандартів або технічних умов (ТУ) діючих на території України, або на технічне завдання на розробку конкретних спеціалізованих КС. КС розробляється для кіберфізичної системи контролю мікроклімату готелів мережі «Optima Hotel Group».

Виконання робіт має бути з робочими кресленнями, затвердженими в установленому порядку.

2.1.1.1 Вимоги до структури і функціонуванню

Сучасні готелі мережі «Optima Hotel Group» – це об'єднання підприємств, які мають систему управління і вирішують спільні завдання. Вони розкидані на дуже

великих територіях, а підприємства, що входять до них, можуть розташовуватися в областях України. Для забезпечення діяльності, управління та розвитку КС готелів мережі «Optima Hotel Group» необхідність створення корпоративного інформаційного простору, поєднаного КС.

КС є основою системної діяльності мережі готелів «Optima Hotel Group».

Сьогодні неможливо створити КС для великих корпорацій без застосування сучасних інформаційних технологій (ІТ). Об'єднання окремих ресурсів корпорацій з корпоративною інформаційно–комунікаційною системою виводить їх на корпоративний рівень. Кожен суб'єкт в корпорації створює через КС взаємні інформаційні зв'язки з іншими суб'єктами на різних рівнях. У результаті таких взаємодій відбувається процес поширення та обміну інформацією всередині корпорації.

КС КФСМ має представляти сукупність інформаційних ресурсів і систем, телекомунікаційних систем і мереж, що діють на основі єдиного принципу і загальних правил.

КС КФСМ це складна і багатопрофільна структура. З цієї причини він має розподілену ієрархічну систему управління. Крім того, до складу КС мережі готелів «Optima Hotel Group» має входять підприємства, відділи та адміністративні офіси, розташовані далеко один від одного.

Для централізованого управління такою спільнотою підприємств створюються КС. КС КФСМ це спеціальна мережа, призначена для підключення обчислювальних, комунікаційних та інформаційних ресурсів мережі готелів «Optima Hotel Group» має передавати електроні дані (електроні документи, голосу, відео тощо).

КС КФСМ має складатися з різних компонентів, таких як системне та прикладне ПЗ, мережеві адаптери, концентратори, комутатори, маршрутизатори та кабельна система.

2.1.1.2 Призначення КС КФСМ

2.1.1.2.1 Кіберфізична система контролю мікроклімату готелів

Кожен номер готелю кондиціонується і вентилюється за допомогою компактного модуля комфорту, керованого системою автоматики припливно–витяжної установки.

Мікроклімат в громадських зонах, ресторанах, вестибюлях і конференц–залах забезпечують модулі комфорту, що не потребують обслуговування.

Керовані повітряні заслінки, підключені до системи управління припливно–витяжною установкою, оптимізують роботу системи в цілому, покращуючи енергетичні показники.

Додатковими функціями КС КФСМ є надавання різних види послуг, які включають традиційну передачу даних, IP–телефонію, відео– та аудіоконференції та відеотрансляції, охорону та відеоспостереження.

Використання КС КФСМ має забезпечувати наступне:

– ефективну спільну роботу користувачів користувачів мережі;

– максимально ефективне використання комп'ютерів, периферійних пристроїв і програмного забезпечення;

– простоту, зручність і т.д. доступу до загальновживаних даних.

2.1.1.2.2 КС КФСМ

Метою КС є створення єдиного інформаційного простору всередині мережі готелів «Optima Hotel Group» – треба забезпечити взаємодію системних і прикладних програм, розташованих на різних вузлах, а також можливість їх використання користувачами, що знаходяться далеко від них. Забезпечити обмін інформацією через файлову систему, захищену електронну пошту, багатофункціональний телефонний зв'язок, консультації для вибору, відеоконференції тощо. послуги, такі як основним і першочерговим питанням у КС

є забезпечення ефективного функціонування працівників у системі корпоративного управління КФСМ.

Кабельна інфраструктура корпоративної мережі готелів «Optima Hotel Group» є важливою частино. Бізнес проєкту. Компанія «Optima Hotel Group» ризикує втратити гроші та продуктивність на цьому компоненті, якщо вона ретельно не продумає, не спланує та не передбачить майбутнє.

При проектуванні КФСМ слід зосередити увагу на наступному.

1. Непрофесійне прокладання кабелів може спричинити проблеми для компанії, такі як нестабільне покриття Wi–Fi, низька швидкість передачі даних і переривання дзвінків. Ці незручності призводять до втрати часу, неефективності та поганого обслуговування клієнтів.

2. Одним з найважливіших факторів, який слід враховувати, є потенціал для майбутнього розширення фірми. Після того, як бізнес запущений і працює, може бути складно переналаштувати кабельну інфраструктуру. З цієї причини бізнесу потрібне рішення, яке легко масштабувати в міру зростання мережі. Бувають випадки, коли це просто неможливо. Можливість додавати більше робочих станцій, кабелів або інших оновлень дозволяє побудувати добре спроектовану кабельну структуру спеціально для того, щоб пристосуватися до зростання організації. Завжди слід враховувати можливість вдосконалення.

3. Оскільки середовище компанії унікальне слід найняти групу мережевих професіоналів для обслуговування КС. Вони мають запропонувати рекомендації щодо обладнання, галузевих стандартів і методів, які відповідають цілям і бюджету фірми.

2.1.1.3 Вимоги до апаратних компонентів

2.1.1.3.1 Кіберфізична система контролю мікроклімату готелів

При підборі обладнання враховуються нормативні вимоги і категорія об'єкта.

У малих приміщеннях слід встановлювати механічну витяжну вентиляцію і децентралізовану припливну вентиляцію (клапани, фрамуги, провітрювачі). Використання кондиціонера в готелях 1 і 2 зірки рекомендується, але не є обов'язковим.

Центральні припливно–витяжні системи використовуються на об'єктах середньої і великої потужності.

У великих готельних комплексах економія на витратах на клімат–контроль відіграє важливу роль.

Вентиляція часто оснащується теплообмінником, що знижує витрати на опалення. У приміщення подається попередньо нагріте або охолоджене свіже повітря: для цього в повітроводах встановлюються канальні нагрівачі та охолоджувачі. Для зволоження повітря у вентиляційному каналі використовуються два види зволожувачів – паровий і випарний. Припливне і кондиціоноване повітря піддається багатоступеневому очищенню. Кондиціонер ефективно охолоджує повітря до заданої температури.

При монтажі вентиляційних систем в готелі звертається увага на характеристики повітроводів. Якщо стельовий простір обмежений, вибирають плоскі прямокутні вентиляційні канали. Для зниження рівня шуму встановлюються акустичні глушники і швидкість руху повітря знижується до 1–3 м/с.

2.1.1.3.2 КС КФСМ

Апаратна складова КС для керування бізнес–мережею є важливим компонентом. Це реальні інструменти та системи, які виконуватимуть більшу частину роботи.

Визначення технічних вимог дає можливість проектувальнику встановити обсяг проекту. Ці вимоги зумовлюють вибір технологій, обладнання та програмного забезпечення для управління.

Технічні вимоги включають, але не обмежуються наступним:

1. Покращення масштабованості мережі;

2. Підвищення доступності та продуктивності мережі;

3. Підвищення безпеки мережі;

4. Спрощення керування мережею та її підтримки.

Розробник мережі має вести цей список і може змінювати його, якщо будуть виявлені зміни в запропонованому дизайні в процесі проектування.

1. Маршрутизатор. Маршрутизатор – це пристрій, який встановлює з'єднання між двома або більше мережами. Це пристрій, який з'єднує локальну мережу (LAN) з Інтернетом або глобальну мережу (WAN) у середовищі SMB. Це дозволяє парку пристроїв, підключених до мережі, підключатися до Інтернету та обмінюватися інформацією та ресурсами один з одним. Маршрутизатор може використовуватися як у підключеній або дротовій установці, так і в бездротовій. В даний час бездротові з'єднання широко використовуються в більшості установ через їх доступність і простоту установки.

Wi–Fi маршрутизатори бізнес–класу відрізняються від моделей споживчого класу тим, що вони оснащені системами брандмауера, антивірусним програмним забезпеченням і функціями захисту від спаму. Крім того, на деяких моделях можна встановити VPN–сервер, який шифрує дані під час їх проходження мережею. Вони забезпечують захист мережі та зменшують її сприйнятливість до зовнішніх загроз так, як це не може зробити звичайний домашній маршрутизатор.

Маршрутизатори бізнес–класу також пропонують інші важливі переваги для бізнесу, деякі з яких включають:

а) Можливість керування налаштуваннями брандмауера та керування ними на підключених пристроях.

б) Заборона зловмисної діяльності з одного комп'ютера або мережевого пристрою, яка може поставити під загрозу мережу в цілому.

в) Можливість відсіювання небажаного інтернет–трафіку.

г) Довший термін служби, що пояснюється вищими цінами та довшими гарантіями, оскільки вони виготовлені з міцнішого обладнання та компонентів, які можуть витримувати несприятливі умови, такі як відключення електроенергії.

е) Додаткові параметри конфігурації, які можуть дозволити визначати пріоритети та контролювати пропускну здатність відповідно до різних потреб та використання.

2. Мережеві комутатори. Мережевий комутатор полегшує спільне використання ресурсів і обмін даними між двома або більше користувачами мережі, пристроями та програмами. Крім того, мережеві комутатори здатні підтримувати віртуальні мережі, що усуває потребу в дорогих, окремих фізичних мережах, дозволяючи величезним мережам пов'язаних пристроїв взаємодіяти, відокремлюючи одні групи пристроїв від інших з міркувань безпеки.

Тільки пристрої, підключені до локальної мережі (LAN), можна підключати через найпростіші комутатори LAN.

а) Некеровані комутатори. Некеровані комутатори – це прості пристрої plug–and–play, які не потребують складної конфігурації та параметрів налаштування. Некеровані комутатори дозволяють кільком пристроям взаємодіяти один з одним, що робить їх чудовим способом розширення мережі. Некеровані комутатори добре підходять для переговорних кімнат, конференц–залів, а також станцій друку або факсу.

б) Керовані комутатори. Керовані комутатори надають можливість контролювати не тільки те, хто може отримати доступ до даних, але й те, як вони протікають через мережу. Це керування можна застосувати до кожного порту комутатора.

Оскільки керовані комутатори не дуже зручні для не професіоналів, власникам мережі готелів «Optima Hotel Group», доведеться найняти IT–фахівця або скористатися послугами керування IT, щоб повною мірою скористатися перевагами безпеки керованого комутатора.

Для легкого керування в КС КФСМ мережевим трафіком слід обрати керований комутатор початкового рівня або розумний комутатор. Організація, яка використовує бездротові мережі, також може подумати про придбання керованого хмарою комутатора, який би забезпечував віддалений доступ до мережі та керування нею.

3. Точки доступу. Бездротова локальна мережа, або WLAN, створюється точкою доступу, яка також діє як шлюз для бездротового підключення користувачів до мережі. Вони також збільшують зону покриття мережі, а також діапазон кінцевих точок і користувачів, які можуть до неї підключитися.

Незважаючи на те, що існує багато різних типів точок доступу, точки доступу бізнес–класу рекомендуються для підприємств, оскільки вони мають такі характеристики, як більша пропускна здатність для обробки трафіку, більший радіус дії сигналу та функції безпеки порівняно з точками доступу споживчого класу.

Ще однією альтернативою є ретранслятори, але вони мають обмеження. Вони можуть підтримувати лише певну кількість пристроїв, і якщо їх використовувати неправильно, вони можуть навіть уповільнити роботу мережі.

Розміри та дизайн будівлі конкретного готелю «Optima Hotel Group», які безпосередньо впливають на ефективність та дальність доступності. Це включає в себе облік мережевих кабелів, які так само залежать від конструкції будівлі.

Використання мережі: приблизна загальна кількість кінцевих точок і користувачів, до яких потрібно буде підключитися як зараз, так і в майбутньому. Також важливо заздалегідь оцінити, наскільки добре точки доступу можуть витримувати сплески трафіку та використання.

Безпека: функції безпеки повинні бути достатніми щодо чутливості даних, що передаються мережею, оскільки точки доступу будуть передавати конфіденційні дані між користувачами мережі та програмами.

Простіші мережі можуть обійтися лише однією або двома встановленими точками доступу plug–and–play, але більші та складніші організації або організації з кількома відділами та користувачами, можливо, треба найняти IT–спеціаліста для проведення оцінки, оцінки мережі, збору організаційних даних та пропозиції індивідуального рішення.

4. Брандмауери. Першою лінією захисту мережі невеликої компанії від зловмисних атак є брандмауер. Це система мережевої безпеки, яка відстежує весь вхідний і вихідний мережевий трафік і визначає, чи слід дозволяти або блокувати трафік на основі заздалегідь визначеного набору правил безпеки.

Вони встановлюють бар'єр між ненадійними зовнішніми мережами та внутрішніми, керованими та захищеними мережами.

У мережі компанії готелів «Optima Hotel Group» брандмауер може бути встановлений як програмне забезпечення, апаратне забезпечення або як поєднання обох. Програмні брандмауери також можуть бути аутсорсинговими та хмарними.

5. Сервер. Простіше кажучи, сервер – це комп'ютерна система, яка розміщує та надає ресурси, дані, програми або інші послуги іншим комп'ютерам, які підключені до мережі (також відомі як клієнти) через цю мережу. Будь–яке комп'ютерне програмне або апаратне забезпечення, яке забезпечує функціональність інших додатків, може називатися «сервером».

Сервер допомагає оптимізувати та організувати керування IT–інфраструктурою малого та середнього бізнесу, керуючи програмним забезпеченням, програмами безпеки, а також процесами доступу та дозволів користувачів. Якщо в мережі є кілька клієнтів, це може допомогти підвищити продуктивність, запобігти порушенням безпеки та відновити дані в разі катастрофи.

Встановивши необхідне програмне забезпечення, звичайний комп'ютер, що відповідає набору мінімальних вимог до обладнання, можна перетворити на сервер. Однак цього недостатньо, щоб конкурувати з оптимізованою для сервера машиною,

і вона може бути небезпечною та нестабільною. Однак це може спрацювати, особливо для невеликих мереж з низькими вимогами до серверних додатків.

Апаратні компоненти з можливістю гарячої заміни, такі як жорсткі диски та блоки живлення, є особливістю серверів, яка дозволяє проводити технічне обслуговування та ремонт з мінімальним порушенням робочого процесу або без нього. У разі відмови компонента решта цих компонентів може підтримувати працездатність системи. Крім того, завдяки своїй індивідуальній технології вони обробляють дані значно швидше, ніж звичайний настільний комп'ютер, і призначені для постійної роботи.

Файлові сервери, сервери баз даних, Інтернет, пошта та друк – це лише деякі з серверів, які можуть використовувати малі та середні підприємства.

Незважаючи на те, що додавання сервера до мережі малого та середнього бізнесу пов'язане з певними витратами, загалом переваги переважують початкові інвестиції. Оскільки більшості малого та середнього бізнесу не вистачає досвідченого IT–персоналу та ресурсів, необхідних для створення адекватної IT–інфраструктури, вони можуть думати, що серверам не місце в їхніх мережах.

6. Кінцеві пристрої. По суті, це гаджети, які підключені до мережевих систем, включаючи принтери, камери, телефони, POS–системи, ПК, робочі станції та пристрої Інтернету речей.

Як і будь–яка інша технологія, кінцеві точки, зокрема ПК, мають конфігурації, які ідеально підходять як для домашнього, так і для комерційного використання. Можливість оптимізації та модифікації апаратного та програмного забезпечення під конкретні потреби є однією з переваг комп'ютерів бізнес–класу. Наприклад, ноутбук офіс–менеджера та ноутбук польового інженера можуть мати різні технічні характеристики.

Комп'ютери бізнес–класу розроблені таким чином, щоб витримувати інтенсивні робочі навантаження та служити довше, ніж ПК споживчого класу. Крім того, комп'ютери бізнес–класу можуть бути оснащені вбудованими заходами

безпеки, такими як зчитувачі відбитків пальців і інструменти шифрування, через характер і чутливість їх передбачуваного використання.

Найбільші ризики для бізнес–мереж або будь–яких інших мереж насправді походять від кінцевих пристроїв. Тому, коли справа доходить до створення та впровадження на практиці заходів кібербезпеки, вони повинні бути першочерговим рішенням.

Пріоритет критеріїв вимог:

1. Підвищення доступності на 40% – підтримка доступності мережі 24x7 для підключення до Інтернету, та застосування продуктивності;

2. Підтримка доступності мережі 24x7 для безпеки додатків, відео телефонної системи;

3. Гарантія якості обслуговування;

4. Підвищення безпеки на 30% з додаванням фільтрації, брандмауери та IDS;

5. Централізація серверів і керування;

6. Безпека бездротової мережі – покращення підтримки мережі 50% зростання запропонованої мережі на 20%;

7. Масштабованість кількості користувачів і сайтів протягом наступних двох років – підтримка 75% зростання пропонованої мережі в бездротовому зв'язку, зона покриття.

2.1.1.4 Вимоги до експлуатації

Стійкість до впливу зовнішніх кліматичних факторів під час експлуатації КС КФСМ має бути наступною:

– діапазон температур навколишнього середовища, °С: 5…40;

– діапазон відносної вологості навк. середовища, %: 40...80 (25°С);

– діапазон атмосферного тиску навк. середовища, кПа: 84... 107;

Живлення здійснюється від однофазної мережі змінного струму напругою 220 В ± 10% і частотою 50 Гц.

Комп'ютер і його периферійні пристрої повинні бути підключені до електричної мережі через спеціальні розетки із заземлюючими контактами. Заземлюючі контакти повинні забезпечувати надійне заземлення. Опір контуру заземлення має бути не більше 4 Ом. Забороняється використовувати в якості заземлення водогазопровідні труби, радіатори та інші парові опалювальні агрегати.

Від розетки, до якої підключений комп'ютер, не рекомендується подавати живлення на пристрої, що створюють великі імпульсні перешкоди в електричній мережі під час роботи (кондиціонери, пилососи, вентилятори і так далі). Це може спричинити збої в роботі комп'ютера та призвести до втрати інформації.

2.1.1.5 Вимоги до надійності

КС КФСМ повинна нормально працювати з безперебійною роботою комп'ютера. У разі апаратного збою нормальну роботу системи необхідно відновити після: перезавантаження операційної системи; Запустіть виконуваний файл платформи, для якої розробляється система, відкличте розроблену систему та повторно введіть втрачені дані.

КС КФСМ повинна залишатися працездатною та забезпечувати відновлення своїх функцій у разі виникнення надзвичайної ситуації:

а) у разі несправності апаратної системи живлення, що призводить до перезавантаження операційної системи, програма відновлюється після перезавантаження операційної системи та виконання виконуваного файлу;

б) у разі виникнення помилок у роботі апаратного забезпечення (за винятком носіїв інформації та програм) відновлення системної функції покладається на операційну систему;

в) При виникненні помилок, пов'язаних з програмним забезпеченням (операційною системою і драйверами пристроїв), відновлення працездатності необхідно віднести до операційної системи.

Час відновлення після відмови має бути таким: при перезавантаженні операційної системи користувачем; Час, коли користувач запустив виконуваний файл, час виклику системи, що розробляється, і час, необхідний для повторного введення втрачених даних.

Надійність розроблюваної системи повинна забезпечуватися:

а) підбір відмовостійкого обладнання та його конструктивної резервованості;

а) використання джерел безперебійного живлення;

б) вибір топології телекомунікаційних і локальних мереж, що забезпечують варіативність маршрутизації інформаційних потоків;

в) дублювання носіїв інформації;

г) використання програмних методів забезпечення цілісності даних.

2.1.1.6 Вимоги до патентної чистоти

Програмно–апаратні засоби, технології, алгоритми обробки даних та інші компоненти інтегрованої системи запатентовані на території України.

Інсталяція системи в цілому, а також інсталяція окремих компонентів системи не повинні пред'являти додаткових вимог до придбання ліцензій на стороннє програмне забезпечення, за винятком програмного забезпечення, зазначеного в пункті.

КС КФСМ повинна мати патентну чистоту на території України.

2.1.2 Вимоги та функцій КФСМ

Кіберфізична система контролю мікроклімату готелів мережі «Optima Hotel Group» буде оснащена сучасними сенсорними технологіями, розумні номери готелю надають цілодобову інформацію про мікроклімат.

1. Моніторинг мікроклімату. Зібрані дані можуть бути проаналізовані платформою IoT і автоматично скориговані в разі відхилень від встановленої норми. Виконання певних операції, таких як обігрів, охолодження, вентиляція, на

вимогу клієнта мають здійснюватися одним натисканням кнопки. Має бути постійний моніторинг даних, що сприятиме розробці прогностичних моделей для оцінки ризиків захворювань та інфекції.

2. Підтримання ідеальних мікрокліматичних умов. Провайдери збирають дані з безпрецедентною деталізацією та надають персоналу інформацію про ключові кліматичні фактори в режимі реального часу. Ці дані аналізуються та коригуються відповідно до заздалегідь визначених налаштувань системи опалення, вентиляції та кондиціонування повітря, забезпечуючи клієнтам готелю найбільш комфортні умови проживання. Основними контрольованими показниками є вологість і температура повітря. Контроль температури і вологості – одна з найважливіших функцій. Ці дані найчастіше збираються за допомогою датчика температури та вологості.

Кіберфізичні системи контролю мікроклімату готелів мережі «Optima Hotel Group» мають не тільки контролювати кліматичні параметри, але і автоматично їх обслуговувати. Підтримувати температуру в допустимих межах можна за допомогою кондиціонера або системи опалення.

2.1.3 Види забезпечення КС КФСМ

Основним видом забезпечення КС для кіберфізичної системи контролю мікроклімату готелів мережі «Optima Hotel Group» є мережева операційна система, яка керує процесами, об’єднаними спільною архітектурою, певними протоколами зв’язку та механізмами взаємодії обчислювальних процесів кіберфізичної системи контролю мікроклімату готелів мережі «Optima Hotel Group». Ця система дозволяє користувачам використовувати різні мережеві ресурси за стандартними правилами і легко, як правило, з високим рівнем прозорості.

На верхньому рівні прозорості, необхідно забезпечити ізоляцію фізичних параметрів, усіх різних аспектів і особливостей, пов’язаних із процесами, які

застосовуються до оброблених ресурсів від користувачів (тобто користувачів КС не залучених до вирішення цих питань).

Операційна система (ОС), яка керує роботою КС, має бути розподіленою системою. Ця система має розподіляти всі ресурси мережі між КС і організовувати обмін між комп'ютерами кіберфізичної системи кіберфізичної системи контролю мікроклімату готелів мережі «Optima Hotel Group».

ОС локальної мережі має бути побудована на базі ОС однієї машини (мережі Ethernet, Arcnet і Token Ring), або бути перероблена як окрема повна операційна система.

Для КС КФСМ можливі наступні варіанти структури:

– кожен компонент мережі реалізує всі функції ОС, тобто розміщує резидентну частину ОС у своїй робочій пам’яті (в ОЗП) і може посилатися на довільні нерезидентні частини, розташовані на зовнішніх носіях;

– у кожному компоненті мережі розміщуються лише швидкості програм, які забезпечують регулярно реалізовані функції ОС, тоді як копії програм, які забезпечують функції, які час від часу необхідно реалізовувати, зберігаються в пам'ять лише однієї або кількох компонентів;

– кожен компонент мережі виконує певну частину набору функцій ОС, причому кількість таких функцій (тобто набір функцій операційної системи, що виконується на цьому комп'ютері) або індивідуальна, або кількість функцій є спільними для кількох компонентів.

Відмінності в обраному напрямку побудови структури КС КФСМ визначаються прийнятими методами управління (централізоване і децентралізоване управління) КС. Головною відмінною рисою кіберфізичної системи контролю мікроклімату готелів мережі «Optima Hotel Group» є те, що тут є певний рівень ОС, який забезпечує обмін інформацією між компонентами КС, що входять до мережі.

2.1.4 Вимоги до інформаційного забезпечення КС КФСМ

Комп'ютерна система визначається як програмне забезпечення, програмне забезпечення або людино–машинна система. Це складна і структурована система, а системні вимоги є підмножиною функціональних вимог продукту і включають в себе програмне забезпечення, прошивку, інші інструменти,

Вимоги до програмного забезпечення, як окрема підмножина системних вимог, які зосереджені тільки на програмних компонентах системи, роботі, пов'язаної з системою в цілому і з програмним забезпеченням, віднесені до окремих груп, прикладна програмна система (особливо інформація) до середовища, в якій вона функціонує.

Вимоги до РГК повинні відповідати наступним критеріям:

1. Єдність завдання для всіх елементів системи.

2. Повнота, після чого немає необхідності змінювати систему.

3 Реальність завдань, які повинні бути досяжними і не суперечливими.

4. Актуальність – систему не потрібно оновлювати відразу після розгортання.

5. Ефективність. – відсутність постійних проблеми має бути включена;

6. Інтелектуальна власність – якщо існують будь–які вимоги до інтелектуальної власності, що випливають із бізнес–процесів або чинного законодавства, їх слід розглянути;

6. Перевірюваність – рішення поставлених завдань має бути перевірено в процесі аудиту.

2.1.5 Вимоги до програмного забезпечення

Основною функцією програмного забезпечення КС КФСМ є регулювання мікроклімату в готельних приміщеннях та регулювання необхідних теплообмінних процесів , що здійснюються у вузлах комп'ютерних мереж і між елементами мережі. Іншою важливою функцією програмного забезпечення КС є організація

розподіленого колективного використання мережевих ресурсів користувачами мережі з метою досягнення високої ефективності.

Мережеве ПЗ КС для КФСМ має складатися з трьох компонентів:

– загального ПЗ;

– системне ПЗ;

– індивідуального ПЗ по підтримці заданого мікроклімату;

– контроль за роботою елементів мережі та забезпечення достовірності вхідної та вихідної інформації;

– захист даних і мережевих ресурсів від інших зовнішніх програм;

– надання довідок про інформаційні, програмні та технічні ресурси, що використовуються в мережі.

ПЗ КС забезпечує організацію колективного доступу до комп'ютерних і мережевих інформаційних ресурсів, динамічний розподіл і перерозподіл мережевих ресурсів з метою підвищення ефективності обробки інформації і максимального навантаження на апаратні засоби, а також при виникненні поломок і відмов окремих технічних засобів і т.д.

ПЗ КС КФСМ складається з трьох компонентів:

– загальне програмне забезпечення, що складається з базового програмного забезпечення окремих комп'ютерів, що входять до складу мережі;

– спеціальне програмне забезпечення, що складається з прикладного програмного забезпечення, що відображає специфіку сфери діяльності користувачів при реалізації завдань управління;

Системне мережеве ПЗ, що представляє собою сукупність програмних засобів, що підтримують і координують взаємодію всіх мережевих ресурсів комп'ютера в єдину систему.

Системне мережеве ПЗ, функції якого реалізовані у вигляді розподіленої мережевої операційної системи.

Мережева операційна система КС КФСМ включає в себе набір програм контролю і обслуговування, які забезпечують:

– метод між–програмного доступу (можливість організації зв'язку між окремими прикладними програмами комплексу, реалізованими в різних вузлах мережі);

– доступ окремих прикладних програм до мережевих ресурсів (особливо пристроїв введення–виведення);

– синхронізацію роботи прикладного програмного забезпечення за умов їх доступу до одного і того ж комп'ютерного ресурсу;

– обмін інформацією між програмами за допомогою мережевих «поштових скриньок»;

– виконання команд оператора з терміналу, підключеного до одного з вузлів мережі на будь–якому пристрої, підключеному до іншого віддаленого вузла комп'ютерної мережі;

– віддалене введення заданих завдань з будь–якого терміналу і виконання на будь–якому комп'ютері в пакетному або онлайн режимі;

– обмін наборами даних (файлами) між комп'ютерами в мережі;

– доступ і обробка файлів, що зберігаються на віддалених комп'ютерах;

– захист мережевих даних та IT–ресурсів від несанкціонованого доступу;

– видавати різні види сертифікатів про використання інформаційних, програмних і технічних засобів мережі;

– пересилання текстових повідомлень з одного пристрою користувача на інший (e–mail).

Мережеву операційна система забезпечує виконання наступних функцій:

– визначається послідовність розв'язання задачі користувача.

– завдання користувача отримують необхідні дані, що зберігаються в різних вузлах мережі;

– контролюється працездатність мережевого обладнання та програмного забезпечення;

Плановий і оперативний розподіл ресурсів забезпечується відповідно до виникаючих потреб різних користувачів комп'ютерної мережі.

Адміністрування за допомогою мережевої операційної системи включає: планування, коли і коли отримувати та розповсюджувати інформацію серед учасників; розподіл розв'язуваних завдань у комп'ютерній мережі; Пріоритезує завдання та результати. зміна конфігурації комп'ютерної мережі; Розподіл мережевих інформаційних обчислювальних ресурсів для вирішення завдань користувачів.

Оперативне управління процесом обробки інформації за допомогою мережевої операційної системи дає можливість організувати збір даних про виконані роботи в мережі.

Операційні системи окремих комп'ютерів, що входять до складу комп'ютерної мережі, задовольняють потреби користувачів у всіх видах традиційного обслуговування: засоби автоматизації, програмування та налагодження, доступ до пакетів прикладних програм та інформації локальних баз даних тощо.

2.2 Розробка апаратної частини комп’ютерної системи

Вентиляційні системи управління мікрокліматом готелів мережі «Optima Hotel Group» призначені для відслідковування та регулювання низки показників за допомогою яких досягаються ті чи інші необхідні умови для комфортної праці, та інших процесів життєдіяльності людини в приміщенні. Загалом, зовнішнє повітря, яке надходить в систему проходить через необхідне обладнання але через значну інерційність необхідних мікрокліматичних показників та високу залежність від погодних умов та пори року показники мають не завжди досягають необхідної якості. Аналіз існуючих кіберфізичних систем для мікроклімату показав, що задані

характеристики для припливного повітря досягаються за рахунок додаткового обладнання, що в свою чергу збільшує необхідну кількість використовуваної енергії для системи. Аналіз систем показує – на сьогоднішній час, в цій сфері кіберфізичних систем майже не використовуються новітні методи та принципи будування кіберфізичних систем управління. Для надання повітрю необхідних показників використовуються різні за комплектацією та алгоритмами роботи системи. Схема кіберфізичної системи управління мікрокліматом в приміщенні готельного номеру зображена на рис. 2.1.

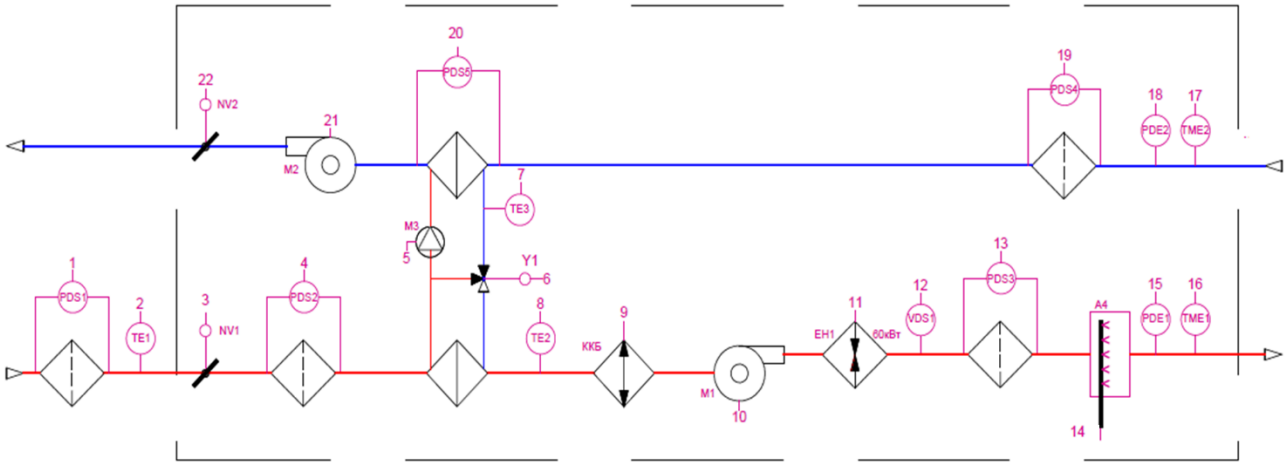


Рисунок 2.1 – Схема КФСМ в приміщенні готельного номеру

КС кіберфізичної системи контролю мікроклімату готелів мережі «Optima Hotel Group» має SCADA–систему (рис 2.2).

SCADA–систему має необхідний набор типових функцій: відображення стану системи, задати необхідні уставки, переглянути тренди основних показників. Такого набору функцій кіберфізичних систем вже не вистачає для підтримання необхідних мікрокліматичних умов.

Зазвичай, кіберфізичні системи з використанням технологій машинного навчання використовують для підвищення продуктивності технологічного процесу за рахунок підбору оптимальних режимів роботи обладнання, завантажень сировини, підвищення якості продукції шляхом виявлення критичних факторів у виробничому процесі, що впливають на кінцевий

результат; оптимізація технологічного обслуговування та ремонту дорогого виробничого обладнання, прогноз поломок та деградації обладнання.

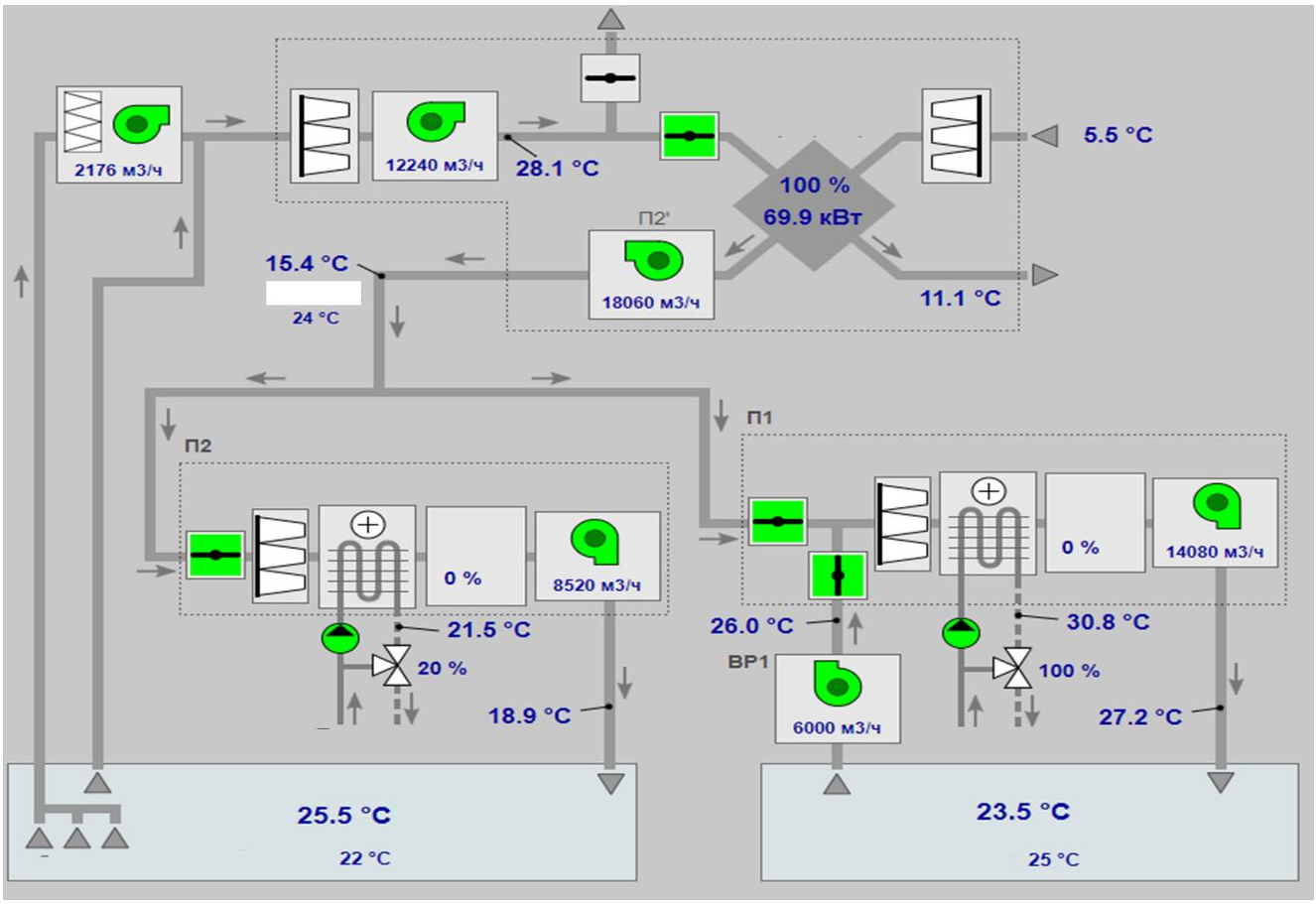


Рисунок 2.2 – SCADA–система керування мікрокліматом для КФСМ

Основна перевага систем, заснованих на машинному навчанні, полягає в тому, що вони охоплюють набагато ширше коло можливих варіантів подій. Удосконалена система на основі машинного навчання здатна швидше відреагувати на зміни вхідних даних, що дозволяє забезпечити більшу гнучкість системи. [3].

Отже, використання технологій машинного навчання в кіберфізичних системах керування мікрокліматом допоможе системам, наприклад, у визначенні слабких місць, спираючись на необхідну вибірку даних з роботи системи, зменшенні використання енергетичних ресурсів та несе більшу точність в необхідні показники мікроклімату.

2.2.1 Вимоги до розміщення структурних підрозділів підприємства

На сервері КС управління мікрокліматом готелів мережі «Optima Hotel Group» встановлюється база даних. Всі сервери додатків підключені до бази даних.

Кожен сервер КС КФСМ додатків може бути встановлений на одному сервері (фізичній або віртуальній машині) або на окремому сервері для прискорення клієнтських додатків.

Пов'язані сервери мають бути розташовані в одній локальній мережі.

Має бути один сервер, для забезпечення шлюзу між зовнішніми ресурсами і базою даних. До зовнішніх джерел, характерних для системи управління мікрокліматом готелів мережі «Optima Hotel Group» можна віднести:

– інтернет–ресурси (сторінки), які забезпечують купівлю та бронювання номерів, програм, резервування послуг та повернення коштів через мережу Інтернет;

– термінали самообслуговування, які необхідні для друку замовлення, чеків на послуги придбані онлайн;

– термінали збору даних, які необхідні для організації контролю доступу (входу та виходу) співробітників та відвідувачів на територію готелю за допомогою мобільних пристроїв.

2.2.2 Розробка загальної архітектура мережі підприємства

Загальна архітектура КС КФСМ включає: елементи функціональної структури кіберфізичних систем управління мікрокліматом; кіберфізичні функції систем управління мікрокліматом; сукупність заходів, пов'язаних з виконанням функцій кіберфізичних систем, які здійснюються виключно технічними засобами або тільки програмними; інформаційні зв'язки між елементами КС, які пов'язані із зовнішнім середовищем, з коротким оглядом зв'язку між собою, змісту повідомлень та / або сигналів, що передаються через мережу КС; і, при необхідності, інші види

зв'язку вхідних, зв’язку підпорядкованих і т.п.; детальні схеми компонентів функціональної структури.

Схема функціональної структури КС КФСМ розробляється на етапі інженерного проектування. Система складається з наступних функціональних підсистем:

– підсистема збору, обробки та вилучення даних, яка призначена для виконання процедури збору даних з інших вихідних систем та перетворення їх у форму, необхідну для наповнення підсистеми зберігання даних;

– підсистема зберігання даних, яка призначена для зберігання даних у структурі прийняття рішень;

– підсистема звітності та візуалізації, яка призначена для формування бізнес–орієнтованих даних та презентацій звітів.

КС КФСМ включає п’ять підмереж з загальною кількістю ПК 7+111+93+47+26=284 одиниці.

2.2.3 Вибір і обґрунтування структурної схеми КС КФСМ

2.2.3.1 Заходи захисту КС КФСМ

Захист КС КФСМ визначаються технічним відділом експлуатації готелю.

Типові заходи безпеки щодо забезпечення інформаційної безпеки в автоматизованих системах управління виробничо–технологічними процесами на критичних об'єктах, потенційно небезпечних об'єктах, а також об'єктах, що становлять підвищену небезпеку для життя і здоров'я людей і для навколишнього природного середовища», включають такі комплекси вимог:

– ідентифікація та автентифікація суб'єктів доступу та об'єктів доступу;

– управління доступом суб'єктів доступу до об'єктів доступу;

– обмеження програмного середовища;

– захист носіїв комп'ютерної інформації, на яких зберігається і (або) обробляється інформація, що захищається;

– ведення журналу подій безпеки;

– антивірусний захист;

– виявлення вторгнень (профілактика);

– контроль (аналіз) безпеки інформації, що захищається;

– забезпечення цілісності автоматизованої системи управління технологічними процесами та інформації, що захищається;

– забезпечення доступності інформації, що охороняється;

2.2.3.2 Захист технічних засобів КС КФСМ

Захист кіберфізичної системи контролю мікроклімату готелю мережі Optima Hotel Group, її об'єктів, систем зв'язку та передачі даних вимагає проведення наступних кроків:

– розробка розробником безпечного додатку та спеціального ПЗ;

– управління оновленнями програмного забезпечення;

– планування заходів щодо забезпечення інформаційної безпеки;

– забезпечення дій у надзвичайних (непередбачених) ситуаціях;

– інформування та навчання користувачів;

– аналіз загроз інформаційній безпеці та ризиків від їх реалізації;

– виявлення інцидентів та реагування на них;

– управління конфігурацією інформаційної системи та системою її захисту.

2.2.3.3 Політика Cisco для побудови відмовостійких і надійних мереж

Компанія Cisco приділяє велику увагу як питанням побудови відмовостійких і надійних мереж для кіберфізичних системи, так і пов'язаним з цим питанням забезпечення інформаційної безпеки на критично важливих об'єктах клієнтів. Для цього компанія багато років тому створила спеціалізовану CIAG (Critical Infrastructure Assurance Group), яка згодом була реорганізована в окремий фокус–підрозділ Cisco Connected Industries Group. Зовсім недавно цей підрозділ було

значно розширено і перейменовано в Cisco Internet of Things Group, зоною впливу якої стали не тільки рішення в області побудови надійних і безпечних мереж на промислових об'єктах, але і всі інші сценарії міжмашинної взаємодії, описані терміном «Інтернет всього». Протягом останнього десятиліття експерти Cisco брали активну участь у роботі різних консультативно–експертних рад, а також робочих груп, що займаються безпекою критично важливих об'єктів у різних галузях економіки, що дозволяє пропонувати рішення, що враховують специфіку конкретної галузі або сегменту ринку.

2.2.4 Специфікація апаратної частини КС КФСМ

Розробимо специфікацію апаратних засобів для КС КФСМ.

В якості робочого місця користувача КС КФСМ оберемо ASUS A3402WVA – 23,8–дюймовий моноблочний комп’ютер, який працює на основі процесорів Intel® нової лінійки Core™ Series 1 (Raptor Lake–U Refresh) [18].

Рисунок 2.3 – Зовнішній вигляд комп’ютера ASUS A3402WVA

Моноблок оснащений високоякісним IPS–дисплеєм із широкими кутами огляду й частотою оновлення 100 Гц. Він має сучасний мінімалістичний дизайн з оригінальною вбудованою підставкою. Завдяки витонченому зовнішньому вигляду й двом варіантам кольору цей моноблок ідеально впишеться в будь–який інтер’єр сучасного дому або офісу.

Наступним компонентом КС КФСМ оберемо сервер двох–процесорний Alfa Server #224. Переваги Alfa Server Сервери Alfa Server відзначаються високою продуктивністю, надійністю та гнучкістю налаштувань, що робить їх відмінним вибором для вирішення задач управління даними та обробки великих обсягів інформації. Модель #224 з подвійними процесорами Intel Xeon, розширеною оперативною пам'яттю та високопродуктивною графікою забезпечує відмінну продуктивність для складних завдань [19].

Рисунок 2.4 – Зовнішній вигляд сервера двох–процесорного Alfa Server #224

Наступним компонентом КС КФСМ оберемо комутатор Catalyst 2960 Plus 48 10/100 + 2 T/SFP LAN Lite (WS–C2960+48TC–S) [20].

Керований комутатор Catalyst 2960 Plus 48 10/100 + 2 T/SFP LAN Lite (WS–C2960+48TC–S) з 48 портами Fast Ethernet і 2 комбінованими гігабітними портами SFP. Cisco Catalyst 2960–Plus – це серія комутаторів Fast Ethernet фіксованої конфігурації, які забезпечують комутацію рівня 2 для філій, традиційних робочих місць і нетрадиційних застосувань, таких як будівельна інфраструктура. Вони забезпечують надійну та безпечну роботу з низькою сукупною вартістю володіння (TCO) завдяки програмним функціям Cisco IOS, таким як Cisco Catalyst SmartOperations. Переваги 2960–Plus включають високу якість QoS, гнучкі функції безпеки, а також спрощені операції та інструменти автоматизації [21].

Рисунок 2.5 – Зовнішній вигляд комутатора Catalyst 2960 Plus 48 10/100 + 2 T/SFP LAN Lite (WS–C2960+48TC–S)

Наступним компонентом КС КФСМ оберемо маршрутизатор Cisco ISR4331–VSEC/K9, який Підтримує різноманітні функції, такі як маршрутизація на основі політик, фільтрація вмісту, балансування навантаження тощо. Його також можна використовувати для налаштування віртуальних приватних мереж (VPN), що дозволяє користувачам безпечно підключатися до віддалених ресурсів. Пристрій також має вбудовані механізми безпеки, такі як брандмауер, перевірка пакетів та аутентифікація користувача. Всі ці функції допомагають забезпечити високий рівень безпеки в мережі [22].

Рисунок 2.6 – Зовнішній вигляд маршрутизатора Cisco ISR4331–VSEC/K9

Наступним компонентом КС КФСМ оберемо джерело безперебійного живлення FSP iFP 800VA/480W [22].

Рисунок 2.7 – Зовнішній вигляд джерела безперебійного живлення FSP iFP 800VA/480W

Кількість таких пристроїв на розрахована як сума ПК, серверів, комутаторів та маршрутизаторів в корпоративній мережі.

Специфікація основних обраних пристроїв для КС КФСМ наведена в табл. 2.1.

Таблиця 2.1 – Специфікація апаратних засобів КС КФСМ

№ п/п	Найменування	Тип	Одиниці виміру	Кількість	Технічні характеристики
1	23,8" Lenovo ThinkCentre M90a Gen 3 Intel Core i5–12400 RAM 16GB SSD 512GB Windows 11	Моноблочний комп'ютер	одиниці	284	Процесор – Intel Core i7–1255U, кількість ядер – 10 ядер, 1,7 (4,7) ГГц; Об'єм ОЗП – 16 ГБ DDR4, тип накопичувача SSD 512 ГБ; Відеокарта Intel UHD Graphics, нтегрована; Екран – 23,8', 1920x1080 Full HD, LCD, 60 Гц; Інтерфейси – LAN, Wi–Fi
2	TOWER PowerUp #60 Xeon E5 2699 v4 x2/256 GB/HDD 6 TB/SSD 512GB x2 Raid/Int Video	Сервер двох–процесорний	одиниці	3	2x Intel Xeon E5–2667v4, 16 ядер, 32 потока, ОЗП 128GB, QUADRO RTX A4000 16GB
3	Catalyst 2960 Plus 48 10/100 + 2 T/SFP LAN Lite (WS–C2960+48TC–S)	Комутатор	одиниці	6	48 портів Fast Ethernet, порти Uplink SFP і Gigabit Ethernet, підтримка IEEE 802.3af PoE, програмне забезпечення LAN Base або LAN Lite. Технологія Cisco EnergyWise забезпечує контроль енергоспоживання підключених пристроїв.
4	Cisco ISR4331–VSEC/K9	Маршрутизатор	одиниці	6	3 порти GigabitEthernet (10/100/1000), Bundle with UC & Sec Lic, PVDM4–32, CUBE–10;
5	FSP iFP 2000VA	Джерело безперебійного живлення	одиниці	284+3+6+6+1=300	Лінійно–інтерактивна, апроксимована синусоїда, макс. вихідна потужність 800 ВА.

2.2.5 Структурна схеми комплексу технічних засобів КС КФСМ

КС КФСМ має відмінності від корпоративних мереж передачі даних, а саме:

– найменша пауза в роботі мережі може привести до зупинки складного технологічного процесу;

– наслідки збою в мережі можуть бути катастрофічними;

Дуже часто в таких мережах до сих пір все ж використовуються пропрієтарні технологічні протоколи виробників обладнання, які чреваті важко детективними вразливостями, які складно вчасно закрити виробникам традиційних систем захисту інформації і виробникам самого обладнання.

Мережа кіберфізичної системи контролю мікроклімату готелю повинна бути максимально доступною, іноді навіть на шкоду безпеці. Помилкові спрацьовування, що призводять до відключення сегментів мережі або перебоїв у нормальному функціонуванні технологічних процесів, неприпустимі

Обмін даними з корпоративною мережею з метою експлуатації MES, ERP та інших систем, а також забезпечення віддаленого доступу та управління мережею кіберфізичної системи контролю мікроклімату готелю, в тому числі через мережу Інтернет, не може бути заблокований і тому повинен здійснюватися за суворими правилами побудови так званих буферних, демілітаризованих зон, і в повній відповідності з галузевими нормами і рекомендаціями.

Беручи до уваги всі перераховані вище та інші особливості, характерні для мереж кіберфізичної системи контролю мікроклімату готелю загальна структура мережі отелів Optima Hotel Group має вигляд такий, як наведено на рис. 2.8.

Структура кіберфізичної системи контролю мікроклімату готелю мережі отелів Optima Hotel Group виконана за рекомендаціями компанії Cisco спільно з одним зі світових лідерів з виробництва промислового обладнання Rockwell Automation. Алгоритм побудови архітектури Conwerged Plantwide Ethernet описує всі нюанси створення промислових мереж, включаючи питання забезпечення їх безпеки. В рамках цієї архітектури враховуються і вимоги до відмовостійкості, і обмеження топології будівель, і протоколи, що використовуються промисловим обладнанням, і багато інших питань.

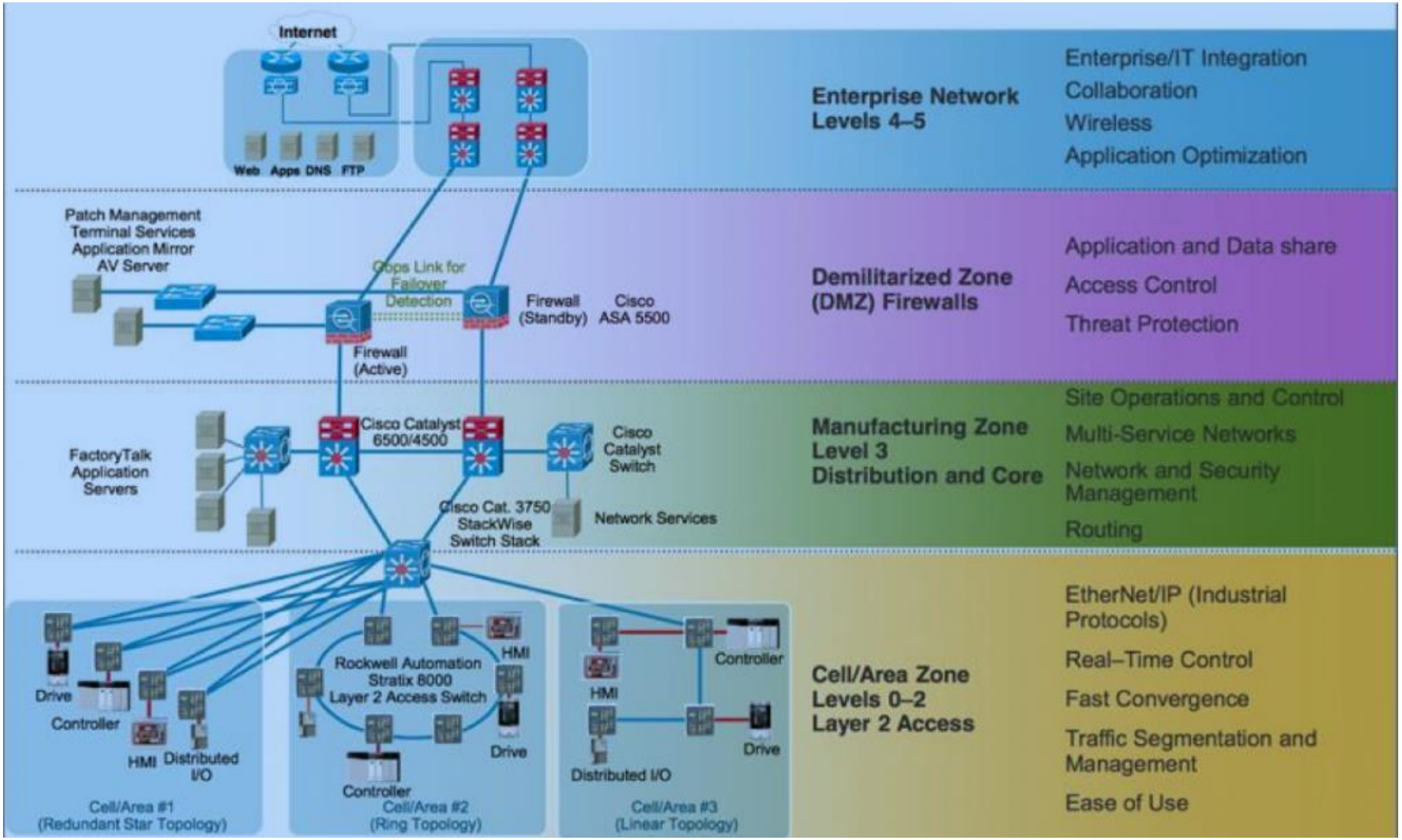


Рисунок 2.8 – Структура кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group

Підвищена увага до питань інформаційної безпеки кіберфізичної системи контролю мікроклімату готелю Optima Hotel Group викликана переходом промислових рішень з пропрієтарних протоколів на TCP/IP і активним впровадженням нових технологій (в тому числі віддаленого доступу і бездротових рішень) в процесі обробки і передачі команд управління, а також зберігання діагностичної та іншої історичної інформації.

Проблемою також є витончені, цілеспрямовані атаки, метою яких є порушення нормального функціонування технологічних процесів, що може призвести навіть до екологічних катастроф та людських жертв. При цьому проблема полягає не стільки в самих атаках, скільки в змінах в мережі кіберфізичної системи контролю мікроклімату готелю, які вже фізично не ізольовані від зовнішнього світу.

Віддалений доступ до кіберфізичної системи контролю мікроклімату готелю Optima Hotel Group передають інформацію в диспетчерські центри. Розроблена модель інформаційної безпеки, орієнтована на широкий спектр різних загроз, дозволяє здійснювати моніторинг і контроль кіберфізичної системи контролю мікроклімату готелю, а також захищати їх від несанкціонованого втручання будь–якого типу у всіх напрямках, причому постійно, в будь–який час.

Для того щоб надійно захиститися від всіляких атак з усіх напрямків, необхідно знати і розуміти сучасне мережеве середовище кіберфізичної системи контролю мікроклімату готелю Optima Hotel Group, використовувані в ній пристрої (контролери і виконавчі механізми), а також використовувані промислові протоколи. Особливо важливо розуміти цілі захисту кіберфізичної системи контролю мікроклімату готелю Optima Hotel Group, які відрізняються від аналогічних завдань в корпоративних мережах. Не менш важливо розуміти та аналізувати мислення зловмисників при створенні комплексної системи захисту кіберфізичної системи контролю мікроклімату готелю Optima Hotel Group.

Портфоліо інтегрованих рішень Cisco досягає цих цілей, забезпечуючи безпрецедентну видимість і безперервний захист від найскладніших атак. Це дозволяє державним і комерційним клієнтам і операторам кіберфізичних систем діяти швидше і розумніше до, під час і після атаки. І при цьому в повній відповідності з вимогами українського законодавства.

2.2.6 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Найбільша підмережа LAN2 КС КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group має максимальну кількість комп'ютерів, як становить 111 од.. Ця підмережа має комутатори та маршрутизатори Cisco, які об'єднують всі ці 111 ПК користувачів в єдину КМ.

Вихідний трафік підмережі LAN2 пересилається на маршрутизатор Cisco в лінію зв'язку з максимальною пропускною здатністю у 1 000 Мбіт/с. Для того, щоб комутатор Cisco не був перенавантажений і працював без виникнення черги, швидкість надходження інформаційних пакетів з лінії зв'язку не має перевищувати швидкість їх відправлення.

Послугами КС можуть одночасно користуватися 111 користувачів підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group, де середня інтенсивність інформаційного трафіку становить $\mu = 170$ кадрів/с, а середня довжина інформаційного повідомлення має значення у 650 байт.

Розрахуємо пропускну здатність підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group, припускаючи, що послугами одночасно користуються всі 100% користувачів.

Так як у нас є один комутатор рівня доступу, а загальна кількість користувачів підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі

Optima Hotel Group дорівнює 111, то пропускна здатність цієї підмережі на рівні доступу і може бути розрахована за наступною формулою:

$$Pp.p = \mu * n * N * 8 \text{ , Мбіт/с,} \quad (2.1)$$

де Pp.p – пропускна здатність, біт/с; μ – інтенсивність інформаційного трафіку, кадрів/с; n – кількість комутатор рівня доступу, од.; N – кількість користувачів, од.

Pp.p = 170 * 1 * 650 * 111 * 8 = 98,2 Мбіт/с.

Результати розрахунку пропускної здатності підмережі на рівні доступу не перевищують задані параметри мережі у 1 000 Мбіт/с. Отже, перевантажень у підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group для обраного мережевого обладнання не трапиться.

Комутатор рівня доступу в підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group пересилає трафік на маршрутизатор через вихідну інформаційну лінію також з пропускною здатністю у 1 000 Мбіт/с. Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = F / (l * 8) \quad (2.2)$$

де $\mu_{вих}$ – навантаження на комутатор, пакетів/с; F – пропускна здатність, біт/с; l – довжина повідомлення, байт.

$\mu_{вих}$ = 1 000 000 000 / (650 * 8) = 43 333 пакетів/с.

Оскільки робоче місце в підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group виробляє в середньому 111 пакетів/с, то є обмеження з приєднання комутатора рівня доступу до максимальної кількості робочий станцій:

$$N_{max} = \mu_{вих} / \mu, \text{ од.,} \quad (2.3)$$

де N_{max} – максимум інформаційних джерел, од.; μ – інтенсивність інформаційного трафіку, кадрів/с.

N_{max} = 43 333 / 121 = 359 од.

Отриманий результат розрахунку максимальної кількості інформаційних джерел повністю і значним зі запасом перевищує у існуючу кількість робочий станцій у 111 од. в підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group.

Кожен зі 111 ПК підмережі LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group посилає потік заявок з інтенсивністю 170 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів можна розрахувати за наступною формулою:

$$\lambda = N * \mu, \text{ пакетів/с.,} \quad (2.4)$$

де λ – інтенсивність трафіку всіх користувачів, пакетів/с; N – кількість користувачів, од.; μ – інтенсивність інформаційного трафіку, кадрів/с.

$\lambda = 111 * 170 = 18\,870$, пакетів/с.

Розрахуємо коефіцієнт затримки на рівні розподілу, тобто показник, що показує завантаженість вихідного каналу зв'язку, який впливає на час очікування черги:

$$\rho = \lambda / \mu_{вих}, \quad (2.5)$$

де ρ – коефіцієнт затримки на рівні розподілу; λ – інтенсивність трафіку всіх користувачів, пакетів/с; $\mu_{вих}$ – навантаження на комутатор, пакетів/с;

$\rho = 18\,870 / 43\,333 = 0{,}44$.

Коефіцієнт зайнятості комутатора рівня розподілу розрахуємо наступним чином:

$$r = \rho / (1 - \rho), \quad (2.6)$$

де r – коефіцієнт зайнятості комутатора рівня розподілу; ρ – коефіцієнт затримки на рівні розподілу.

$r = 0{,}44 / (1 - 0{,}44) = 0{,}79$.

Середня затримка кадру, що пов’язана з можливою чергою M/M/1, буде розрахована наступним чином:

$$T = 1 / (\mu - \lambda), \text{ с} \quad (2.7)$$

T – середня затримка кадру, с; μ – інтенсивність інформаційного трафіку, кадрів/с; λ – інтенсивність трафіку всіх користувачів, пакетів/с.

T = 1 / (43 333 – 18 870) = 40,9 мкс.

Середня довжина можливої черги становитиме значення:

$$\mathscr{L}_{чер} = \rho * \rho / (1 - \rho), \quad (2.8)$$

де $\mathscr{L}_{чер}$ – середня довжина черги; ρ – коефіцієнт затримки на рівні розподілу;

$\mathscr{L}_{чер}$ = 0,44 * 0,44 / (1 – 0,44) = 0,35.

Отримане в результаті розрахунку значення середньої довжини черги може бути корисною при налаштуванні черг на обраному мережевому обладнанні. Згідно цього значення в апаратурі можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні умовне значення черги значно втричі менше ніж один пакет. Таким чином черги в найбільшій підмережа LAN2 КМ кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group зовсім не очікується.

3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Розрахунок схеми адресації корпоративної мережі компанії «Optima Hotel Group»

Корпоративна мережа компанії «Optima Hotel Group» складається з двох окремих мереж. Мережа головної будівлі готелю, яка розташована в чотирьох поверховій будівлі та мережа малого готельного комплексу, в якому реалізована IoT–система.

У головній будівлі готелю з центральним офісом використовується деревоподібна топологія на логічному рівні для комутованого середовища рівня ядра, яка також відома як ієрархічна зірка. Вузлами цієї структури є різні види комутаційного обладнання, що встановлюються у технічних приміщеннях і з'єднуються між собою та з інформаційними розетками на робочих вузлах за допомогою електричних і оптичних мережних кабелів.

Зірка є базовою топологією комп'ютерної мережі, в якій усі комп'ютери підключені до центрального вузла, зазвичай мережевого комутатора, утворюючи фізичний сегмент локальної мережі. Такий сегмент може функціонувати як самостійно, так і бути частиною складної мережної топології, наприклад, «дерева». Весь обмін інформацією відбувається виключно через центральний маршрутизатор, на який лягає навантаження з маршрутизації трафіку. Конфлікти у мережі з топологією зірка практично неможливі, оскільки управління повністю централізоване.

При побудові топології мережі потрібно дотримуватись технічних вимог.

Таблиця 3.1 – Вихідні дані мережі компанії «Optima Hotel Group»

LAN1	LAN2	LAN3	LAN4	LAN5
7	111	93	47	26

Для розрахунків використаний метод VLSM (Variable Length Subnet Masking) є потужним інструментом для ефективного планування та управління корпоративною мережею готельного комплексу, оскільки забезпечує оптимальне використання IP–ресурсів та підвищує загальну продуктивність і безпеку мережі. VLSM особливо корисний для підприємств з численними готелями та їхніми організаційними підрозділами, оскільки дозволяє виділяти підмережі відповідного розміру відповідно до потреб кожного підрозділу.

Метод VLSM сприяє створенню більш гнучкої структури мережі, що полегшує адаптацію до змін у кількості або розташуванні готелів. Це значно спрощує процес розширення мережі та впровадження нових готелів. Крім того, VLSM дозволяє більш ефективно використовувати доступні IP–адреси, уникаючи надмірного витрачання ресурсів, що є важливим для забезпечення стабільної та надійної роботи мережі.

За допомогою VLSM можна легко управляти підмережами різних розмірів, що дозволяє адаптувати мережу до специфічних вимог кожного готельного підрозділу. Це включає можливість швидкого та безболісного додавання нових підрозділів до мережі без необхідності суттєвої перебудови існуючої інфраструктури.

Додатково, застосування VLSM сприяє покращенню безпеки мережі, оскільки дозволяє чітко розмежувати підмережі та обмежити доступ до різних частин мережі, що знижує ризик несанкціонованого доступу та покращує загальний рівень захисту інформації.

Lan1 – Адміністративний відділ.

Lan2 – Фінансовий відділ (підрозділи: фінансове планування, бюджетування, облік).

Lan3 – Відділ інформаційних технологій.

Lan4 – Відділ обслуговування клієнтів.

Lan5 – Адміністративний відділ готелю 2 (віддалена мережа).

Виділений блок IP–адрес – 10.25.120.0/22.

Таблиця 3.2 – Схема адресації мереж компанії «Optima Hotel Group»

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN2	128	10.25.120.0	255.255.255.128	10.25.120.1 – 10.25.120.126
LAN3	128	10.25.120.128	255.255.255.128	10.25.120.129 – 10.25.120.254
LAN4	64	10.25.121.0	255.255.255.192	10.25.121.1 – 10.25.121.62
LAN5	32	10.25.121.64	255.255.255.224	10.25.121.65 – 10.25.121.94
LAN1	16	10.25.121.96	255.255.255.240	10.25.121.97 – 10.25.121.110
WAN1	2	10.10.15.0	255.255.255.252	10.10.15.1 – 10.10.15.2
WAN2	2	10.10.15.4	255.255.255.252	10.10.15.5 – 10.10.15.6
WAN3	2	10.10.15.8	255.255.255.252	10.10.15.9 – 10.10.15.10
WAN4	2	10.10.15.12	255.255.255.252	10.10.15.13 – 10.10.15.14
WAN5	2	10.10.15.16	255.255.255.252	10.10.15.17 – 10.10.15.18
WAN IPS	2	209.165. 202.0	255.255.255.252	209.165.202.1– 209.165.202.2
WAN Remout	2	64.100.13.0	255.255.255.252	64.100.13.1– 64.100.13.2
LAN IPS	2	209.165.201.0	255.255.255.240	209.165.200.1 – 209.165.200.16

Отримані дані табл. 3.2 застосовані для виконання адресації пристроїв в підмережах компанії «Optima Hotel Group».

Таблиця 3.3 – Схема адресації маршрутизаторів

Ім'я пристрою	Інтер–фейс	IP–адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Helemendruk_R1	G0/2	10.25.120.129	/25	–	—	G0/2
	S0/0/1	10.10.15.2	/30	–	–	S0/1/0
	S0/0/0	10.10.15.9	/30	–	–	S0/0/0
	S0/1/1	10.10.15.13	/30	–	–	S0/1/1
Helemendruk_R2	G0/2	10.25.121.97	/28	–	–	G0/2
	S0/0/1	10.10.15.1	/30	–	–	S0/0/1
	S0/0/0	10.10.15.5	/25	–	–	S0/0/0
	G0/1.1	10.25.120.1	/27	–	25	G0/1.1
	G0/1.2	10.25.120.33	/27	–	35	G0/1.2
	G0/1.2	10.25.120.65	/27	–	45	G0/1.2
	G0/1.99	10.25.120.96	/28		99	G0/1.99
Helemendruk_R0	G0/2	10.25.121.65	/27	–	–	G0/2
	G0/0	64.100.13.2	/30	–	–	G0/0
Wireless_R0	Internet	10.25.121.66	/27	10.25.121.65	–	F0/24
DCL–100	Internet	10.25.121.67	/27	10.25.121.65	–	F0/23
Helemendruk_R3	S0/1/1	10.10.15.6	/30	–	–	S0/1/1
	S0/1/0	10.10.15.10	/30	–	–	S0/1/0
	S0/0/0	10.10.15.17	/30	–	–	S0/0/0
	S0/2/0	209.165.202.2	/30	–	–	S0/2/0
WireR	Internet	10.24.58.21	/26	–	–	G0/2
Rout_IPS	S0/2/0	209.165.202.1	/28	–	–	S0/2/0
	G0/0	64.100.13.1	/30	–	–	G0/0
	G0/1	209.165.201.1	/28	–	–	G0/1
Helemendruk_R4	G0/2	10.25.121.1	/26	–	–	S0/0/1
	S0/1/0	10.10.15.18	/30	–	–	S0/1/0
	S0/0/0	10.10.15.14	/30	–	–	S0/0/0

Таблиця 3.4 – Схема адресації комутаторів

Ім'я пристрою	Інтер–фейс	IP–адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Helemendruk_Sw1	Vlan1	10.25.121.98	/28	10.24.58.1	–	G0/2
Helemendruk_Sw3	Vlan1	10.25.120.130	/25	10.25.120.129	–	G0/2
Helemendruk_Sw4	Vlan1	10.25.121.2	/26	10.25.121.1	–	G0/1
Helemendruk_Sw21	Vlan99	10.25.120.98	/28	10.25.121.98	99	G0/1
Helemendruk_Sw22	Vlan99	10.25.120.99	/28	10.25.121.98	99	Fa0/1
Helemendruk_Sw23	Vlan99	10.25.120.100	/28	10.25.121.98	99	Fa0/2
Helemendruk_Sw51	G0/1	10.25.121.100	/27	10.25.121.98	–	G0/1
Helemendruk_Sw52	G0/2	10.25.121.101	/27	10.25.121.98	–	G0/2
Helemendruk_Sw53	G0/1	10.25.121.102	/27	10.25.121.98	–	G0/1

3.2 Розробка топологічної схеми корпоративної мережі

Логічна топологія мережі компанії «Optima Hotel Group» об’єднує п’ять підмереж, що відповідають організаційним підрозділам зазначеної компанії.

Тип архітектури мережі, що складається з п'яти підмереж, де одна підмережа є віддаленою та підключена через обладнання провайдера, є ієрархічною архітектура. На рівні ядра чотири маршрутизатори, забезпечують маршрутизацію та управління трафіком між підмережами. Кожен маршрутизатор має зв'язки з іншими трьома, що створює повно–зв’язну топологію, підвищуючи надійність і швидкість передачі даних.

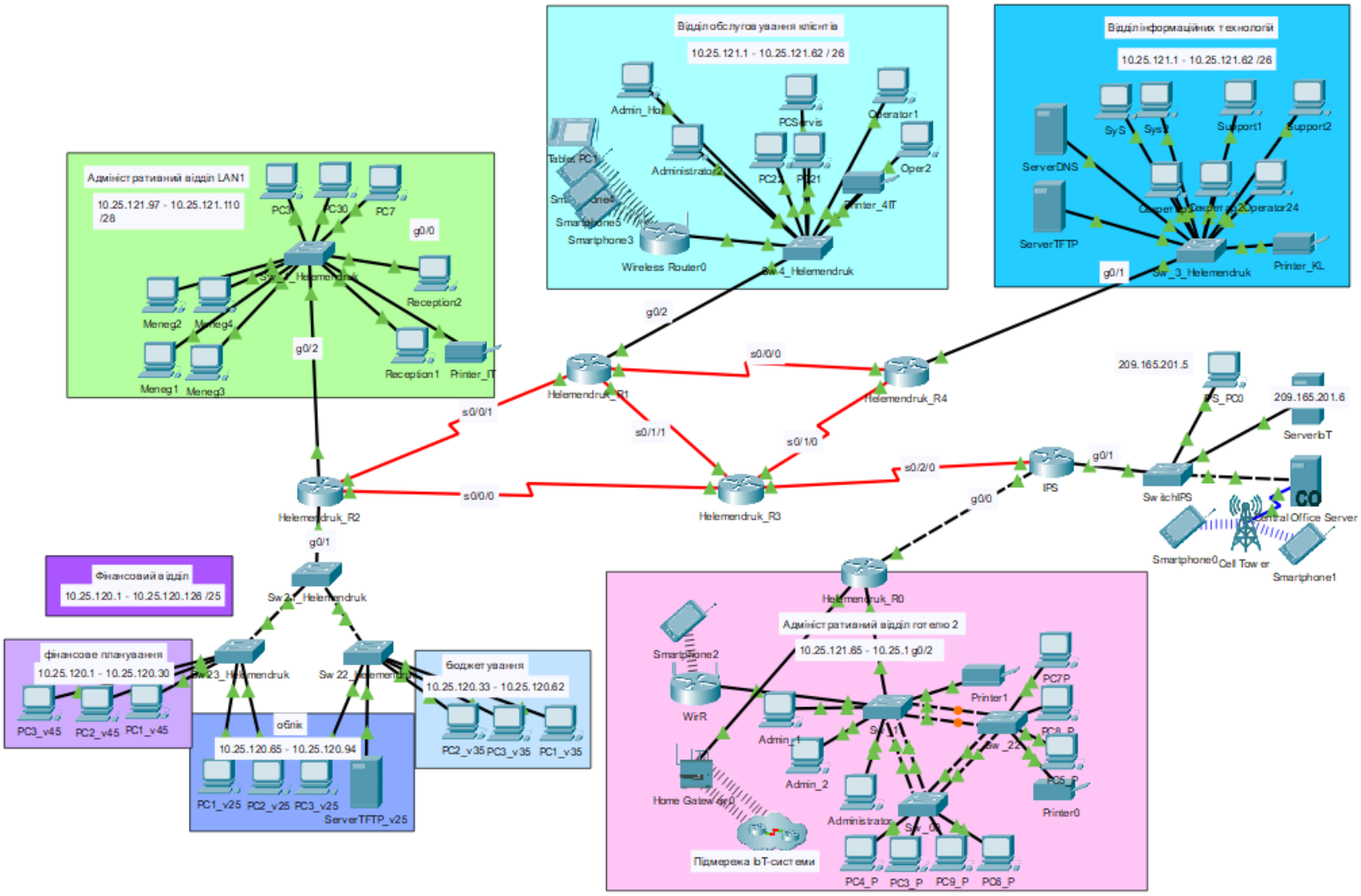


Рисунок 3.1 – Архітектура КС компанії «Optima Hotel Group»

3.3 Проектування комп’ютерної мережі та розрахунок її налаштувань

3.3.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації мережних пристроїв є критичним етапом у створенні надійної, безпечної та продуктивної мережевої інфраструктури. Правильна конфігурація дозволяє запобігти багатьом проблемам і забезпечити ефективну роботу всієї мережі.

Базове налаштування маршрутизаторів корпоративної мережі компанії «Optima Hotel Group», профілем якої є готельний бізнес, включає елементи, наведені на рис. 3.2.

```
Router(config)#hostname Helemendruk_R1

Helemendruk_R1(config)#no ip domain-lookup
Helemendruk_R1(config)#ip domain-name Helemendruk.123-20-1.com
Helemendruk_R1(config)#crypto key generate rsa
% You already have RSA keys defined named Helemendruk_R1.Helemendruk.123-20-1.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: Helemendruk_R1.Helemendruk.123-20-1.com
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Helemendruk_R1(config)#username Helemendruk secret cisco
*Mar 1 3:1:17.470: %SSH-5-ENABLED: SSH 1.99 has been enabled
Helemendruk_R1(config)#enable secret cisco
Helemendruk_R1(config)#service password-encryption
Helemendruk_R1(config)#line console 0
Helemendruk_R1(config-line)#password cisco
Helemendruk_R1(config-line)#login
Helemendruk_R1(config-line)#exit
Helemendruk_R1(config)#line vty 0 15
Helemendruk_R1(config-line)#password cisco
Helemendruk_R1(config-line)#login local
Helemendruk_R1(config-line)#trans input ssh
Helemendruk_R1(config-line)#exit
Helemendruk_R1(config)#banner motd #123202 Helemendruk This is SEKURE area#
```

Рисунок 3.2 – Базове налаштування роутера Helemendruk_R1

```
Helemendruk_R1(config)#int g0/2
Helemendruk_R1(config-if)#description TO LAN3
Helemendruk_R1(config-if)#ip add 10.25.120.129 255.255.255.128
Helemendruk_R1(config-if)#no shutdown
```

Рисунок 3.3 – Базове налаштування інтерфейсу роутера Helemendruk_R1

3.3.2 Налаштування маршрутизаторів корпоративної мережі

На маршрутизаторах корпоративної мережі компанії «Optima Hotel Group» для маршрутизації пристроїв використовується протокол динамічної маршрутизації EIGRP з параметром 15.

Правильно створені таблиці маршрутизації в мережі формують маршрути що вказують на правильний інтерфейс, який пов'язаний з цільовою мережею, а також таблиця маршрутизації містить записи для всіх мереж в складі корпоративної мережі компанії «Optima Hotel Group».

```
Helemendruk_R2(config)#router eigrp 15
Helemendruk_R2(config-router)#redistribute static
Helemendruk_R2(config-router)#network 110.25.121.96 0.0.0.15
Helemendruk_R2(config-router)#network 10.25.120.0 0.0.0.31
Helemendruk_R2(config-router)#network 10.25.120.32 0.0.0.31
Helemendruk_R2(config-router)#network 10.25.120.64 0.0.0.31
Helemendruk_R2(config-router)#network 10.10.15.0 0.0.0.3
Helemendruk_R2(config-router)#network 10.10.15.4 0.0.0.3
Helemendruk_R2(config-router)#pas g0/1.25
Helemendruk_R2(config-router)#pas g0/1.35
Helemendruk_R2(config-router)#pas g0/1.45
Helemendruk_R2(config-router)#pas g0/1.99
Helemendruk_R2(config-router)#exit
```

Рисунок 3.4 – Налаштування маршрутизації на Helemendruk_R2

При налаштуванні маршрутизації відповідні інтерфейси роутера містять налаштування пропускної здатності та метрики маршрутів.

```
Helemendruk_R1(config)#int s0/0/1
Helemendruk_R1(config-if)#description to R2
Helemendruk_R1(config-if)#ip add 10.10.15.2 255.255.255.252
Helemendruk_R1(config-if)#no shutdown

Helemendruk_R1(config-if)#clock rate 128000
Helemendruk_R1(config-if)#bandwidth 128
```

Рисунок 3.5 – Налаштування інтерфейсу роутера Helemendruk_R4

Результат реалізації процесу динамічної маршрутизації КС компанії «Optima Hotel Group» виконаний за допомогою діагностичних команд *show ip route ma show ip protocol* наведено на рис. 3.6 та рис. 3.7.

```
Kupchuk_R2#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 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 18 subnets, 4 masks
C       10.10.7.0/30 is directly connected, GigabitEthernet0/2
L       10.10.7.1/32 is directly connected, GigabitEthernet0/2
C       10.10.7.4/30 is directly connected, Serial0/1/0
L       10.10.7.5/32 is directly connected, Serial0/1/0
D       10.10.7.8/30 [90/20512256] via 10.10.7.2, 00:08:13, GigabitEthernet0/2
D       10.10.7.12/30 [90/21024000] via 10.10.7.6, 00:08:05, Serial0/1/0
C       10.24.56.0/27 is directly connected, GigabitEthernet0/1.17
L       10.24.56.1/32 is directly connected, GigabitEthernet0/1.17
C       10.24.56.32/27 is directly connected, GigabitEthernet0/1.27
L       10.24.56.33/32 is directly connected, GigabitEthernet0/1.27
C       10.24.56.64/27 is directly connected, GigabitEthernet0/1.37
L       10.24.56.65/32 is directly connected, GigabitEthernet0/1.37
C       10.24.56.96/27 is directly connected, GigabitEthernet0/1.99
L       10.24.56.97/32 is directly connected, GigabitEthernet0/1.99
C       10.24.57.0/25 is directly connected, GigabitEthernet0/0
L       10.24.57.1/32 is directly connected, GigabitEthernet0/0
D       10.24.57.128/25 [90/21536512] via 10.10.7.6, 00:08:05, Serial0/1/0
D       10.24.58.64/27 [90/3072] via 10.10.7.2, 00:08:13, GigabitEthernet0/2
     64.0.0.0/30 is subnetted, 1 subnets
D       64.100.13.0/30 [90/21536256] via 10.10.7.6, 00:08:05, Serial0/1/0
     209.165.201.0/28 is subnetted, 1 subnets
D       209.165.201.0/28 [90/21536256] via 10.10.7.6, 00:08:05, Serial0/1/0
     209.165.202.0/30 is subnetted, 1 subnets
D       209.165.202.0/30 [90/21536000] via 10.10.7.6, 00:08:05, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.6 – Таблиця маршрутизації на Helemendruk_R2

```
Helemendruk_R4# show ip protocols

Routing Protocol is "eigrp  15 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 15
  EIGRP-IPv4 Protocol for AS(15)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.10.15.14
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     10.25.121.0/26
     10.10.15.16/30
     10.10.15.12/30
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.15.13     90            4176776
  Distance: internal 90 external 170
```

Рисунок 3.7 – Результат налаштування маршрутизації на Helemendruk_R4

У підмережах компанії «Optima Hotel Group» налаштований DHCP–сервіс на роутерах для автоматичної видачі налаштувань TCP/IP хостам в цих підмережах. Як приклад, можна розглянути налаштування DHCP–пулу для підмережі «Відділ фінансовий», де додатково реалізовані віртуальні мережі для різних груп цього відділу.

Для налаштування DHCP на роутері, спочатку визначається пул IP–адрес, які будуть призначатися пристроям у підмережі. Далі конфігуруються додаткові параметри, такі як шлюз за замовчуванням, DNS–сервери та інші налаштування.

Для «Відділу фінансового» створено кілька віртуальних мереж (VLAN), кожна з яких має свій власний DHCP–пул. Це дозволить розділити трафік між різними групами в межах відділу, забезпечуючи при цьому централізоване управління IP–адресами.

```
Helemendruk_R2(config)#ip dhc ex 10.25.120.1 10.25.120.10
Helemendruk_R2(config)#ip dhc ex 10.25.120.33 10.25.120.43
Helemendruk_R2(config)#ip dhc ex 10.25.120.65 10.25.120.75
Helemendruk_R2(config)#ip dhc pool POOL_VLAN25
Helemendruk_R2(dhcp-config)#net 10.25.120.0 255.255.255.224
Helemendruk_R2(dhcp-config)#def 10.25.120.1
Helemendruk_R2(dhcp-config)#dns 10.25.121.10
Helemendruk_R2(dhcp-config)#ip dhc pool POOL_VLAN35
Helemendruk_R2(dhcp-config)#net 10.25.120.32 255.255.255.224
Helemendruk_R2(dhcp-config)#def 110.25.120.33
Helemendruk_R2(dhcp-config)#dns 10.25.121.10
Helemendruk_R2(dhcp-config)#ip dhc pool POOL_VLAN45
Helemendruk_R2(dhcp-config)#net 10.25.120.64 255.255.255.224
Helemendruk_R2(dhcp-config)#def 10.25.120.65
Helemendruk_R2(dhcp-config)#dns 10.25.121.10
Helemendruk_R2(dhcp-config)#int g0/2
Helemendruk_R2(config-if)#no shut

Helemendruk_R2(config-if)#ip add 10.25.121.97 255.255.255.240
Helemendruk_R2(config-if)#description to LAN1
Helemendruk_R2(config-if)#ex
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
```

Рисунок 3.8 – Приклад налаштування DHCP

```
Helemendruk_R2# show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.25.120.11     000D.BD1E.46C0           --                     Automatic
10.25.120.12     0002.17C4.7695           --                     Automatic
10.25.120.13     0060.2F89.5961           --                     Automatic
10.25.120.44     0001.4309.76BB           --                     Automatic
10.25.120.45     000D.BD36.750D           --                     Automatic
10.25.120.76     0001.C905.B3C9           --                     Automatic
10.25.121.108    0060.7033.5458           --                     Automatic
10.25.121.103    000A.4193.60CA           --                     Automatic
10.25.121.104    0002.17AB.2C8E           --                     Automatic
10.25.121.109    000A.F343.AAC1           --                     Automatic
10.25.121.106    0050.0F03.67B2           --                     Automatic
10.25.121.110    00E0.F716.C4D2           --                     Automatic
10.25.121.101    0001.6319.81EE           --                     Automatic
10.25.121.105    00E0.F917.735C           --                     Automatic
10.25.121.107    00D0.58C7.0365           --                     Automatic
10.25.121.102    0001.9744.514E           --                     Automatic
Helemendruk_R2#
```

Рисунок 3.9 – Результат налаштування DHCP

3.3.3 Налаштування роботи Інтернет

На прикордонному маршрутизаторі компанії «Optima Hotel Group» налаштовано NAT (Network Address Translation) відповідно до вимог. Це налаштування дозволяє перетворювати внутрішні IP–адреси мережі, які знаходяться в діапазоні 10.25.120.0/22, на глобальні IP–адреси з діапазону 209.165.202.1 – 209.165.202.30.

Конфігурація NAT забезпечує наступні функції:

– перетворення адрес (IP Address Translation). Внутрішні приватні IP–адреси замінюються на глобальні IP–адреси, що дозволяє внутрішнім хостам здійснювати з'єднання з зовнішніми мережами;

– захист мережі (Network Security). Внутрішні IP–адреси приховані від зовнішніх мереж, що підвищує рівень безпеки;

– збереження IP–адрес (IP Address Conservation). Використання обмеженого діапазону глобальних IP–адрес для великої кількості внутрішніх хостів.

Дані для застосування:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 10.25.121.10/26 – адреса Server HTTP;

- номер списку доступу: 15;
- ім'я пулу: Internet.

```
Helemendruk_R3(config)#access-list 15 permit 10.25.120.0 0.0.3.255
Helemendruk_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask
255.255.255.224
Helemendruk_R3(config)#ip nat inside source list 15 pool Internet
Helemendruk_R3(config)#ip nat inside source static 10.25.120.10 209.165.200.5
Helemendruk_R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
Helemendruk_R3(config)#ip route 10.25.120.0 255.255.252.0 GigabitEthernet0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance
Helemendruk_R3(config)#interface Serial0/2/0
Helemendruk_R3(config-if)#ip nat outside
Helemendruk_R3(config-if)#interface Serial0/0/0
Helemendruk_R3(config-if)#ip nat inside
Helemendruk_R3(config-if)#interface Serial0/1/1
Helemendruk_R3(config-if)#ip nat inside
Helemendruk_R3(config-if)#interface Serial0/1/0
Helemendruk_R3(config-if)#ip nat inside
```

Рисунок 3.10 – Налаштування NAT на Helemendruk_R3

Даним набором команд на маршрутизаторі Helemendruk_R3 виконані наступні дії: створено список контролю доступу (ACL), який дозволяє всі адреси внутрішньої мережі, а також створено пул для динамічного виділення IP–адрес для доступу до Інтернету; задано статичну адресу NAT для HTTP–сервера; призначено інтерфейси як вихідні для трафіку з приватної мережі, а також інтерфейси як вхідні для трафіку з приватної мережі.

```
Helemendruk_R3#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.10:1  10.25.120.141:1    209.165.201.6:1    209.165.201.6:1
icmp 209.165.202.11:5  10.25.120.142:5    209.165.201.6:5    209.165.201.6:5
icmp 209.165.202.11:6  10.25.120.142:6    209.165.201.6:6    209.165.201.6:6
icmp 209.165.202.12:1  10.25.121.12:1     209.165.201.6:1    209.165.201.6:1
icmp 209.165.202.5:5   10.25.121.105:5    209.165.202.1:5    209.165.202.1:5
icmp 209.165.202.6:6   10.25.120.76:6     209.165.201.6:6    209.165.201.6:6
icmp 209.165.202.7:3   10.25.120.13:3     209.165.201.6:3    209.165.201.6:3
icmp 209.165.202.8:1   10.25.121.10:1     209.165.201.6:1    209.165.201.6:1
icmp 209.165.202.9:9   10.25.121.11:9     209.165.201.6:9    209.165.201.6:9
---  209.165.200.5     10.25.120.10       ---                ---

Helemendruk R3#
```

Рисунок 3.11 – Таблиця перетворювань NAT на Helemendruk_R3

3.3.4 Перевірка роботи моделі комп'ютерної системи компанії «Optima Hotel Group»

Виконання команди Ping між хостами з підмереж комп'ютерної системи компанії «Optima Hotel Group» та доступності віддалених ресурсів.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	Operator24	ServerIoT	ICMP		0.000
	Successful	Support1	IPS_PC0	ICMP		0.000
	Successful	Reception2	Support1	ICMP		0.000
	Successful	PC3_v45	Reception2	ICMP		0.000

Рисунок 3.12 – Результат команди «ping»

Для перевірки протоколу SSH, що надає зашифрований віддалений доступ до активного мережного обладнання, зробимо підключення з командного рядка PC Сектетар з підмережі «Фінансове планування» до маршрутизатора Helemendruk_R2 від користувача Helemendruk з паролем admincisco123201.

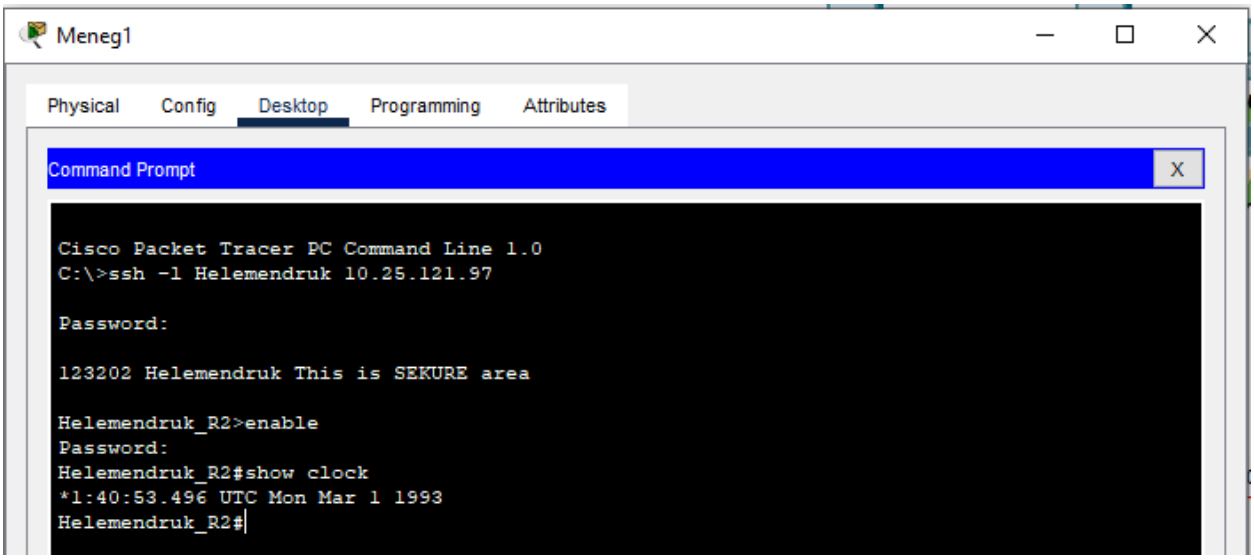


Рисунок 3.13– Перевірка підключення до маршрутизатора Helemendruk_R2 за SSH

```
line vty 0 4
 password 7 0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
```

Рисунок 3.14– Перевірка захищеного доступу VTY 0 4 на Helemendruk_R4

```
banner motd ^C123202 Helemendruk This is SEKURE area^C
ip domain-name Helemendruk.123-20-1.com
username Helemendruk secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
hostname Helemendruk_R4
!
interface Serial0/0/0
 description to R1
 bandwidth 128
 ip address 10.10.15.14 255.255.255.252
 clock rate 128000
!
```

Рисунок 3.15– Перевірка базових налаштувань на Helemendruk_R4

3.4 Захист інформації в комп'ютерній системі від несанкціонованого доступу

У мережі компанії «Optima Hotel Group» для забезпечення безпеки застосовуються наступні методи:

– віртуальні мережі (VLAN) у підмережі 10.25.120.1 – 10.25.121.127 для сегментації трафіку та підвищення безпеки внутрішньої мережі;

– RADIUS використаний для централізованої аутентифікації та авторизації користувачів, забезпечуючи єдиний контроль доступу.

– AAA (Authentication, Authorization, Accounting) застосований для забезпечення трьох–факторного контролю доступу на всіх маршрутизаторах

компанії. Це включає аутентифікацію (перевірка особи), авторизацію (надання прав доступу) та облік (реєстрація дій користувачів);

– безпека портів комутатора Helemendruk_Sw_4, до якого підключені сервери компанії, налаштовані механізми безпеки для запобігання несанкціонованому доступу;

– шифрування даних для захисту інформації під час передачі, забезпечуючи конфіденційність і цілісність даних.

```
Helemendruk_R4(config)#aaa new-model
Helemendruk_R4(config)#aaa authentication login default local
Helemendruk_R4(config)#aaa authentication login Login group radius local
Helemendruk_R4(config)#line vty 0 4
Helemendruk_R4(config-line)#login authentication default
Helemendruk_R4(config-line)#radius-server host 10.25.121.10 auth-port 1645
%New type server exists with same address port combination.
Helemendruk_R4(config)#radius-server key RadiuS123
Helemendruk_R4(config)#exit
Helemendruk_R4#
%SYS-5-CONFIG_I: Configured from console by console

Helemendruk_R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Helemendruk_R4(config)#aaa authentication login SSH-LOGIN local
Helemendruk_R4(config)#line vty 0 4
Helemendruk_R4(config-line)#login authentication SSH-LOGIN
Helemendruk_R4(config-line)#transport input ssh
Helemendruk_R4(config-line)#exit
Helemendruk_R4(config)#radius-server host 10.25.121.10
%New type server exists with same address port combination.
Helemendruk_R4(config)#radius-server key RadiuS123
Helemendruk_R4(config)#aaa authentication login default group radius local
Helemendruk_R4(config)#exit
Helemendruk_R4#
```

Рисунок 3.16 – Налаштування AAA на Helemendruk_R4

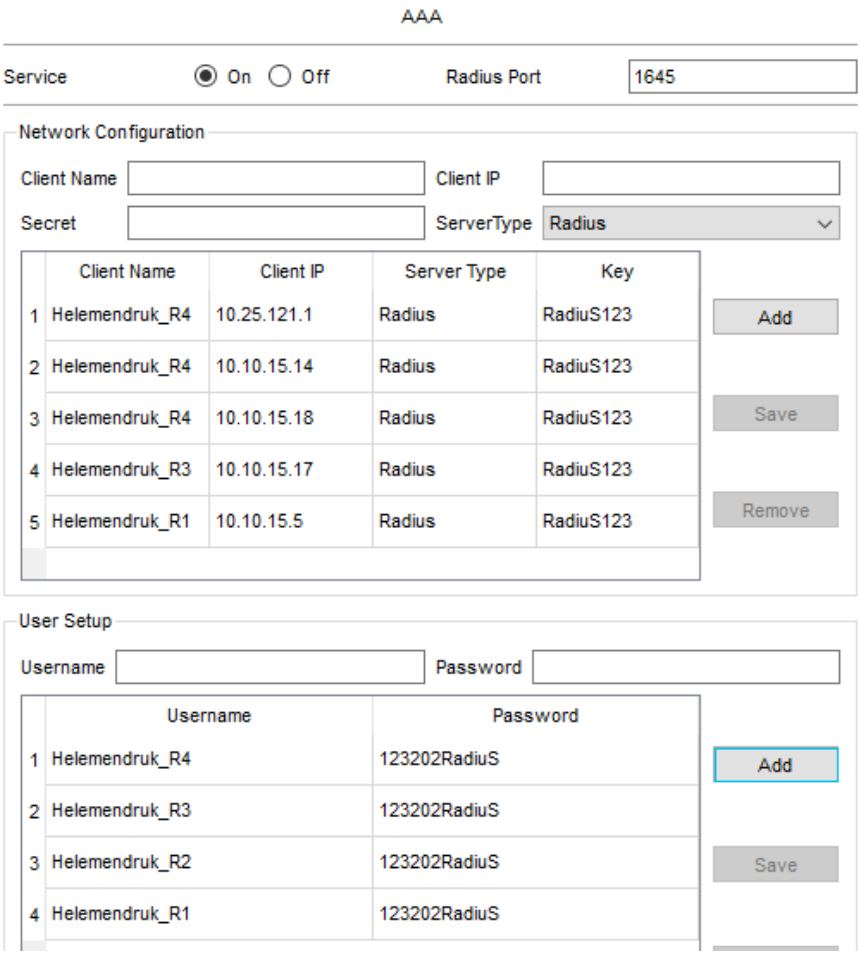


Рисунок 3.17 – Налаштування RADIUS на сервері

```
123202 Helemendruk This is SEKURE area

User Access Verification

Username: Helemendruk_R4
Password:
Helemendruk_R4>enable
Password:
Helemendruk_R4#show ip prot
Helemendruk_R4#show ip protocols

Routing Protocol is "eigrp  15 "
  Outgoing update filter list for all interfaces is not set
```

Рисунок 3.18 – Перевірка централізованої аутентифікації та авторизації на Helemendruk_R4

В підмережі «Відділ фінансування» створені 3 віртуальні підмережі VLAN на базі комутаторів Sw21_Helemendruk, Sw22_Helemendruk, Sw23_Helemendruk та маршрутизатора Helemendruk_R2.

Таблиця 3.5 – Назви VLAN в підмережі

Номер VLAN	Ім’я VLAN	Примітка
1	Default	Не використовується
17	vlan25	Фінансовий відділ
27	vlan35	Відділ обліку
37	vlan45	Відділ бюджетування
99	Management	Управління пристроями
100	Native	Власна

Таблиця 3.6 – Схема адресування VLAN

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
VLAN25	32	10.25.120.0	255.255.255.224	10.25.120.1 – 10.25.120.30
VLAN35	32	10.25.120.32	255.255.255.224	10.25.120.33 – 10.25.120.62
VLAN45	32	10.25.120.64	255.255.255.224	10.25.120.65 – 10.25.120.94
VLAN99	16	10.25.120.96	255.255.255.240	10.25.120.97 – 10.25.120.110

```
Sw21_Helemendruk(config)#vlan 25
*Mar 1 2:37:52.392: %SSH-5-ENABLED: SSH 1.99 has been enabled
Sw21_Helemendruk(config-vlan)#name vlan25_Budget
Sw21_Helemendruk(config-vlan)#vlan 35
Sw21_Helemendruk(config-vlan)#name vlan35_Oblik
Sw21_Helemendruk(config-vlan)#vlan 45
Sw21_Helemendruk(config-vlan)#name vlan45_FinPlan
Sw21_Helemendruk(config-vlan)#vlan 99
Sw21_Helemendruk(config-vlan)#name Management
Sw21_Helemendruk(config-vlan)#vlan 100
Sw21_Helemendruk(config-vlan)#name Native
Sw21_Helemendruk(config-vlan)#exit
```

Рисунок 3.19 – Створення VLAN

```
Sw21_Helemendruk(config)#int fa0/1
Sw21_Helemendruk(config-if)#no shut

Sw21_Helemendruk(config-if)#sw m t

Sw21_Helemendruk(config-if)#sw t n v 100
Sw21_Helemendruk(config-if)#switchport trunk allowed vlan 25,35,45,99-100
Sw21_Helemendruk(config-if)#no shutdown
Sw21_Helemendruk(config-if)#exit

Sw21_Helemendruk(config)#int g0/1
Sw21_Helemendruk(config-if)#switchport mode trunk

Sw21_Helemendruk(config-if)#switchport trunk native vlan 100
Sw21_Helemendruk(config-if)#switchport trunk allowed vlan 25,35,45,99-100
Sw21_Helemendruk(config-if)#no shutdown
```

Рисунок 3.20 – Налаштування портів TRANK

```
Sw21_Helemendruk(config)#int vlan 99
Sw21_Helemendruk(config-if)#description LAN Vnutr_99
Sw21_Helemendruk(config-if)#ip add 10.25.120.98 255.255.255.240
Sw21_Helemendruk(config-if)#no shut
Sw21_Helemendruk(config-if)#ip default-gateway 10.25.120.97
Sw21_Helemendruk(config)#exit
```

Рисунок 3.21 – Налаштування Management керування VLAN

```
Sw21_Helemendruk(config-if-range)#sw m a
Sw21_Helemendruk(config-if-range)#sw a v 45
Sw21_Helemendruk(config-if-range)#exit
Sw21_Helemendruk(config)#int r f0/15-24
Sw21_Helemendruk(config-if-range)#sw m a
Sw21_Helemendruk(config-if-range)#no shut
Sw21_Helemendruk(config-if-range)#sw a v 25
Sw21_Helemendruk(config-if-range)#int r f0/10-14
Sw21_Helemendruk(config-if-range)#sw m a
Sw21_Helemendruk(config-if-range)#no shut
Sw21_Helemendruk(config-if-range)#sw a v 35
Sw21_Helemendruk(config-if-range)#int r f0/5-9
Sw21_Helemendruk(config-if-range)#no shut
Sw21_Helemendruk(config-if-range)#sw m a
Sw21_Helemendruk(config-if-range)#sw a v 45
```

Рисунок 3.22 – Налаштування режиму роботи портів комутатора з VLAN

```
Sw21_Helemendruk#sh vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/3, Fa0/4, Gig0/2
25   vlan25_Budget                       active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Fa0/24
35   vlan35_Oblik                        active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14
45   vlan45_FinPlan                      active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9
99   Management                          active
100  Native                              active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
25   enet  100025     1500  -      -      -        -    -        0      0
35   enet  100035     1500  -      -      -        -    -        0      0
45   enet  100045     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
```

```
Device Name: Helemendruk_R2
Device Model: 2911
Hostname: Helemendruk_R2

Port                    Link   VLAN   IP Address
GigabitEthernet0/0      Down   --     <not set>
GigabitEthernet0/1      Up     --     <not set>
GigabitEthernet0/1.25   Up     --     10.25.120.1/27
GigabitEthernet0/1.35   Up     --     10.25.120.33/27
GigabitEthernet0/1.45   Up     --     10.25.120.65/27
GigabitEthernet0/1.99   Up     --     10.25.120.97/28
GigabitEthernet0/2      Up     --     10.25.121.97/28
Serial0/0/0             Up     --     10.10.15.5/30
Serial0/0/1             Up     --     10.10.15.1/30
```

Рисунок 3.23 – Перевірка налаштування створених віртуальних мереж

```
Sw_3_Helemendruk#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
------------------------------------------------------------------------
        Fa0/1        2           0                0         Restrict
       Fa0/23        2           0                0         Restrict
------------------------------------------------------------------------
```

Рисунок 3.24 – Перевірка на Sw_3_Helemendruk

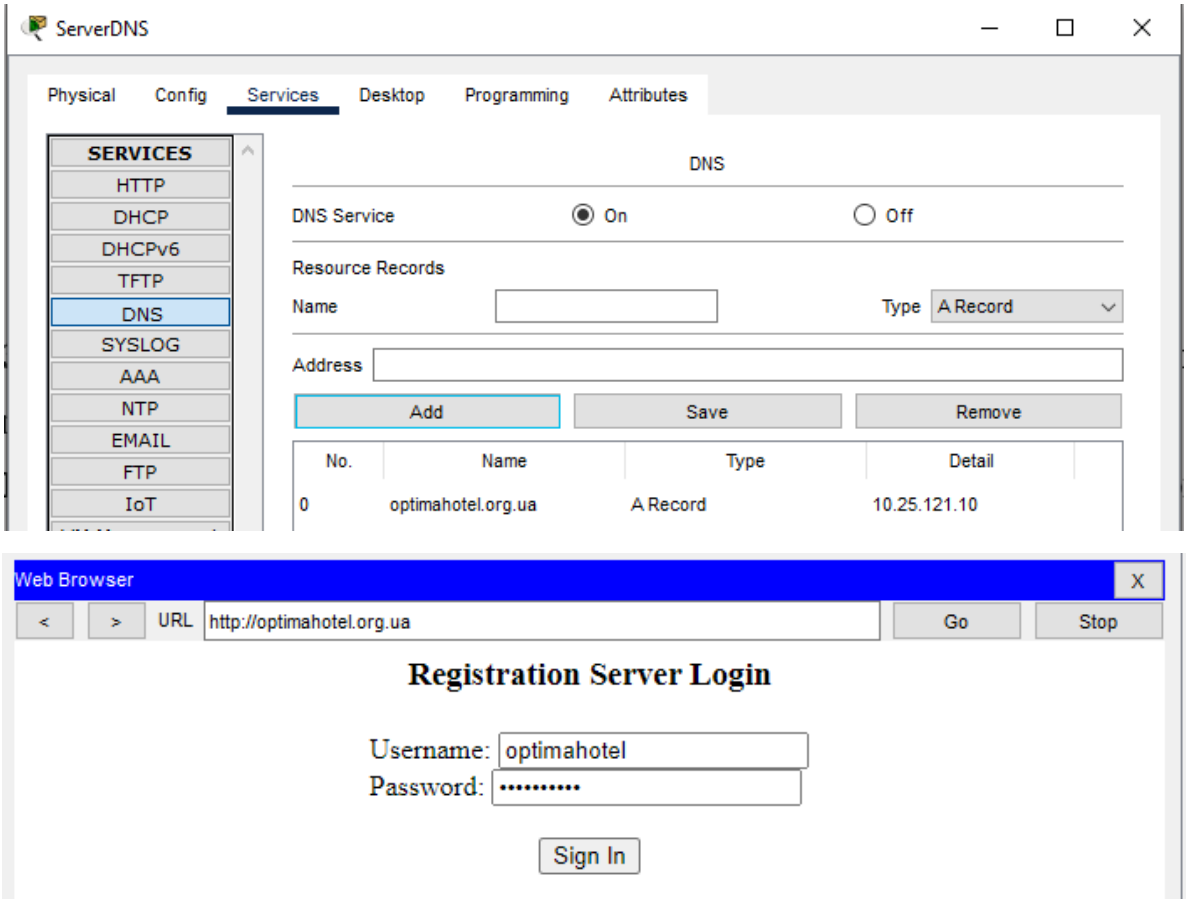


Рисунок 3.25 – Перевірка DNS Server

Віддалена підмережа групи «Адміністративний відділ готелю 2» (IP 10.25.121.64/27) пов'язана з підмережою «Відділ обслуговування клієнтів» (IP 10.25.120.128/25) тунелем VPN.

```
Helemendruk_R0(config)#access-list 110 permit ip 10.25.121.64 0.0.0.31 10.25.120.128 0.0.0.127
Helemendruk_R0(config)#crypto isakmp policy 10
Helemendruk_R0(config-isakmp)#encryption aes
Helemendruk_R0(config-isakmp)#authentication pre-share
Helemendruk_R0(config-isakmp)#group 2
Helemendruk_R0(config-isakmp)#ex
Helemendruk_R0(config)#crypto isakmp key cisco address 209.165.202.2
Helemendruk_R0(config)#crypto ipsec transform-set VPN-CONF esp-3des esp-sha-hmac
Helemendruk_R0(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Helemendruk_R0(config-crypto-map)#description VPN connection to Helemendruk_R3
Helemendruk_R0(config-crypto-map)#set peer 209.165.202.2
Helemendruk_R0(config-crypto-map)#set transform-set VPN-CONF
Helemendruk_R0(config-crypto-map)#match address 110
Helemendruk_R0(config-crypto-map)#ex
Helemendruk_R0(config)#interface GigabitEthernet 0/0
Helemendruk_R0(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Рисунок 3.26 – Налаштування VPN на роутері Helemendruk_R0

```
Helemendruk_R0#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: VPN-MAP, local addr 64.100.13.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.25.121.64/255.255.255.224/0/0)
   remote  ident (addr/mask/prot/port): (10.25.120.128/255.255.255.128/0/0)
   current_peer 209.165.202.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 64.100.13.1, remote crypto endpt.:209.165.202.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x0(0)
```

Рисунок 3.27 – Перевірка стану IPSec SA на роутері Helemendruk_R2

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Об’єкт та тип впроваджуваного компоненту системи

Другий готель компанії «Optima Hotel Group» обладнаний IoT–системою «Hotel2». IoT–система призначена для запобігання аварійних ситуацій, таких як: протікання води в номерах, контроль зачинених вікон та дверей, моніторинг задимлення.

Система IoT побудована відповідно до еталонної архітектури IoT та складається з рівнів: пристроїв, комунікацій, хмарних сервісів та додатків. Компоненти проектованої системи розташовані в коридорах готельного комплексу (протипожежна безпека) та в гостьових кімнатах (небезпека затоплення та задимлення). Система IoT «Hotel2» включає наступні компоненти та розумні речі рівня пристроїв: датчики протікання (2 од.), датчик виявлення диму (2 од.), датчик відкриття вікна (7 од.), сирена (2 од.), вентилятор (5 од.), розумне вікно (7 од.). Для доступу в мережу застосований маршрутизатор DLC–100. На рівні хмарних сервісів розташований віддалений сервер в підмережі «LAN 4 Відділ IT» з підтримкою IoT сервісу. В якості технології передачі даних обрана WiFi IEEE 802.11g з швидкістю з'єднання до 54 Мбіт/с.

Принцип роботи датчика протікання: у сухому стані пристрій не активний, але при потраплянні вологи на його поверхню полюси електродів замикаються. Це викликає відправку сигналу на сервер IoT для перекриття подачі води та звукове оповіщення про інцидент.

Система IoT «Hotel2» інтегрується з існуючою інфраструктурою готелю, забезпечуючи централізоване управління та моніторинг. Це дозволяє оперативно реагувати на аварійні ситуації та забезпечувати комфорт і безпеку гостей.

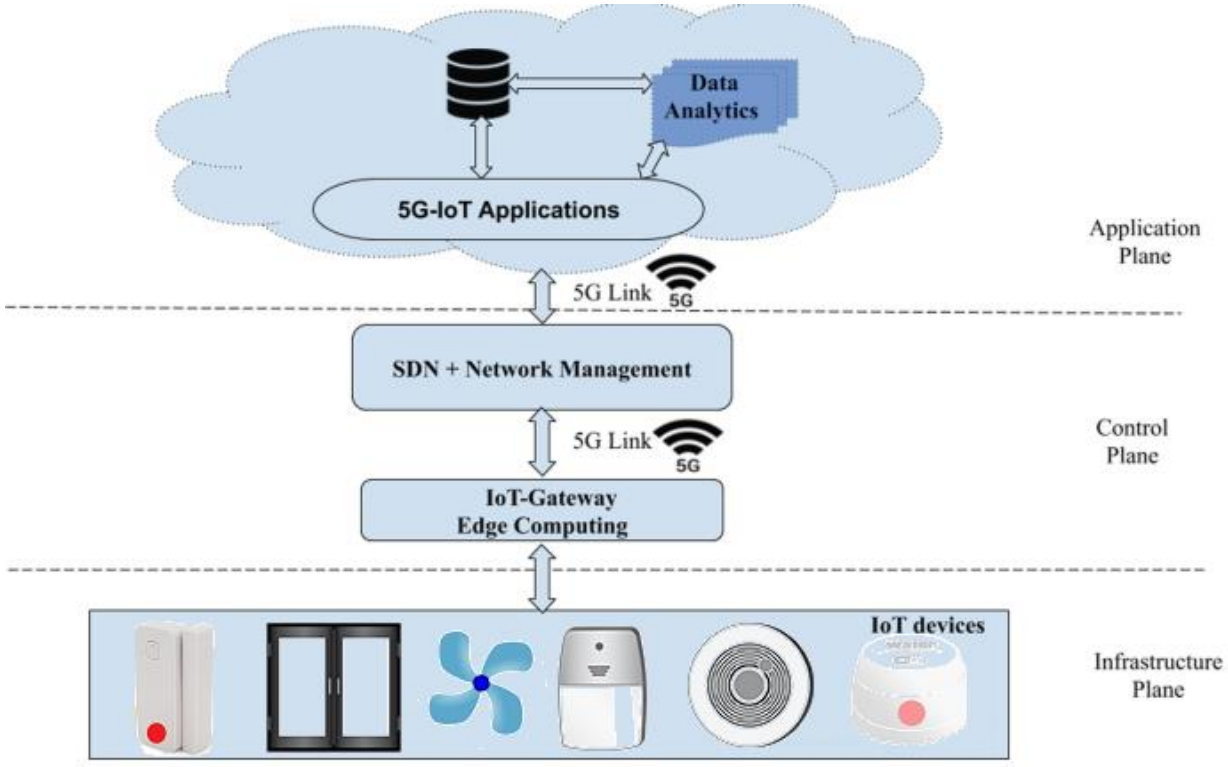


Рисунок 4.1 – Архітектура IoT–системи «Hotel2»

Функціонал IoT–системи.

1. Встановлені в ванних кімнатах датчики протікання води фіксують наявність води на підлозі, та передають стан датчика на хмарний сервіс і за наявності води вмикається звуковий сигнал.

2. Виконується постійний моніторинг диму. При показниках датчика вище 40% вмикаються вентилятори і відчиняються вікна.

3. Для комфорту та безпеку гостей виконується контроль зачинених вікон.

4. За допомогою розумних вікон виконується керування вентиляцією та віддалене керування зачиненням/відчиненням.

4. Дані про стан датчиків протікання води та відчинення вікон, показники датчиків диму передаються на хмарну платформу для подальшого аналізу та управління виконавчими пристроями.

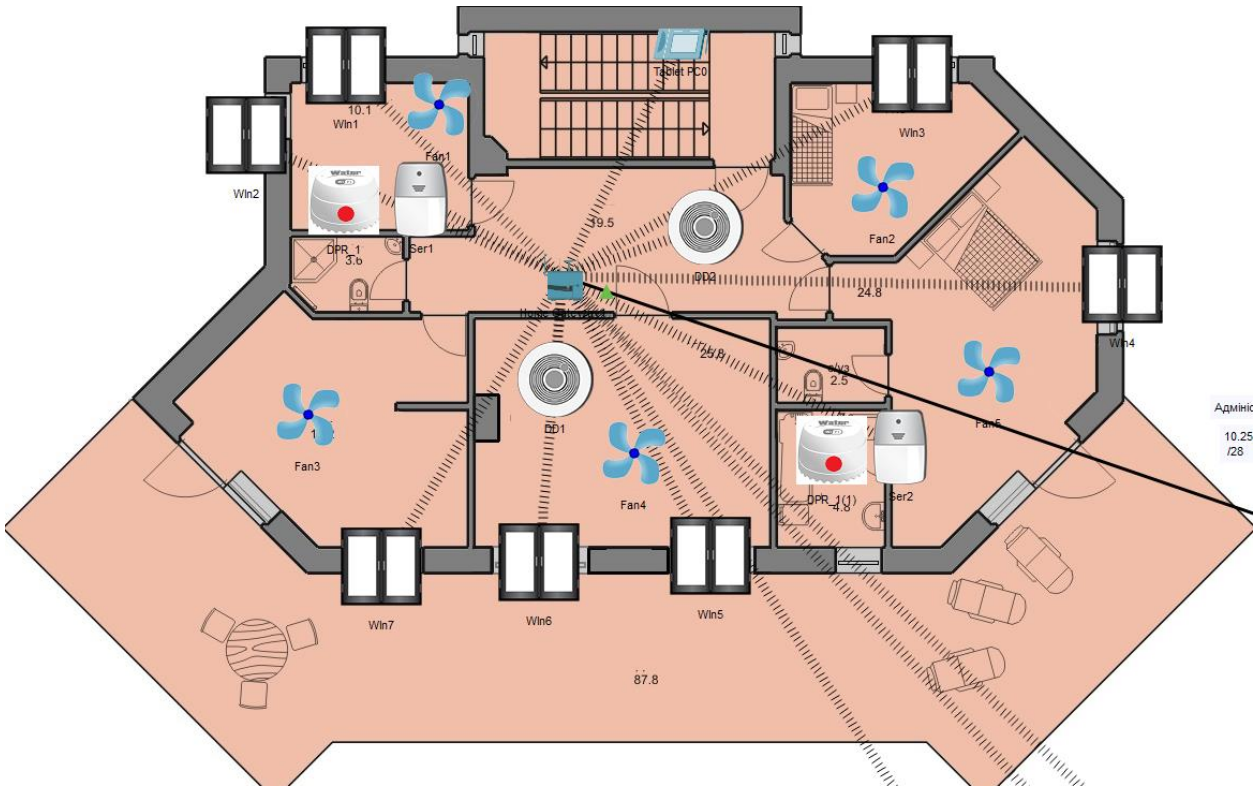


Рисунок 4.2 – План розміщення пристроїв IoT «ClamatAtlant»

4.2 Налаштування IoT–системи

Налаштування IoT–системи умовно поділені на чотири етапи.

Етап 1. Налаштування роутера DLC100/ На цьому етапі роутер налаштовується на підтримку бездротової мережі та забезпечення безпеки і включає: вибір та конфігурацію SSID (назва бездротової мережі), налаштування параметрів безпеки WiFi, таких як WPA2 або WPA3, для захисту мережі, встановлення надійного пароля для доступу до мережі, конфігурацію DHCP для автоматичного призначення IP–адрес пристроям IoT, налаштування брандмауера та мережевих фільтрів для обмеження несанкціонованого доступу.

Цей етап забезпечує стабільну та безпечну роботу бездротової мережі, на яку будуть підключатися пристрої IoT. на підтримку бездротової мережі та забезпечення безпеки.

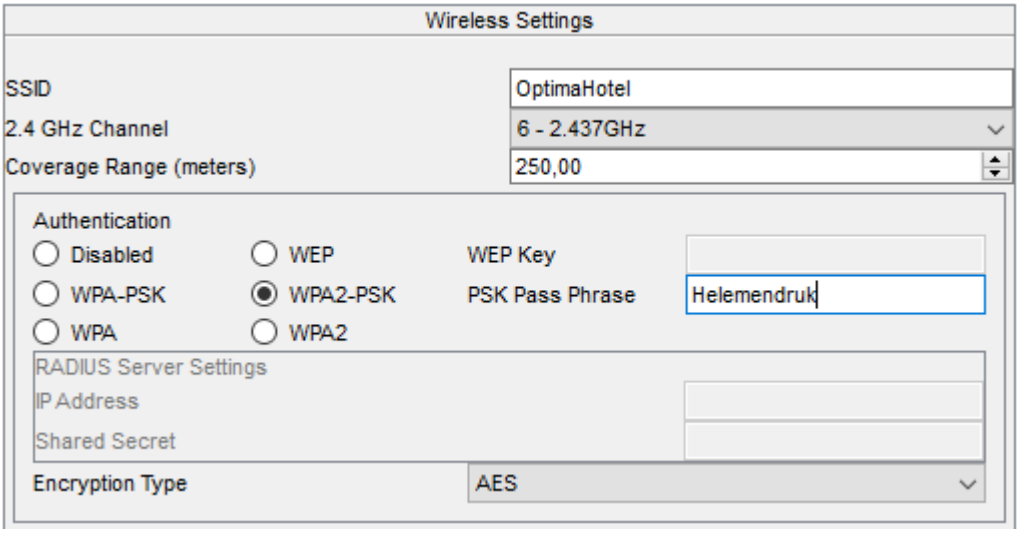


Рисунок 4.3 – Реалізація етапу 1

Етап 2. На цьому етапі встановлюються та підключаються всі IoT–пристрої, такі як датчики, сирени, вентилятори та розумні вікна. Підключення пристроїв до бездротової мережі та перевірка їх працездатності.

Віддалений сервер IoT має IP–адресу 10.25.121.0/27 та налаштовано обліковий запис Helemendruk pass Uotel123211. Конфігурація хмарних сервісів:

– налаштування віддаленого сервера, який розташований у підмережі «LAN 4 Відділ IT», з підтримкою IoT–сервісу;

– налаштування розумних речей для обміну даними та доступу розумних речей до бездротової мережі, що підтримує DLC100.

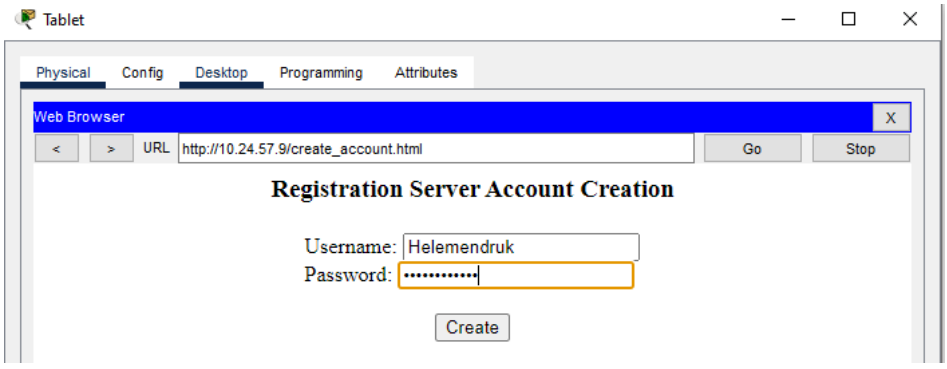


Рисунок 4.4 – Доступ до відділеного сервера

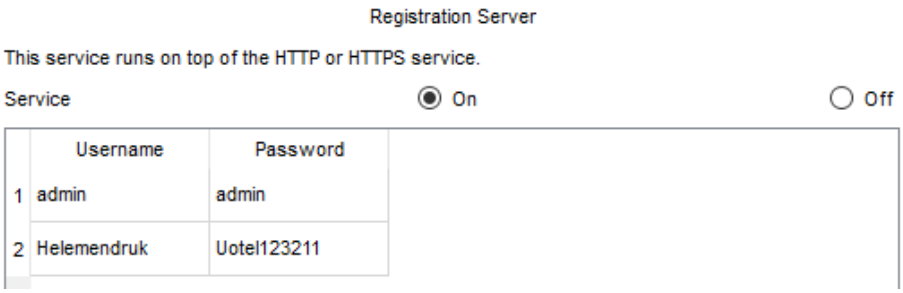


Рисунок 4.5 – Сервіс IoT на відділеному сервері

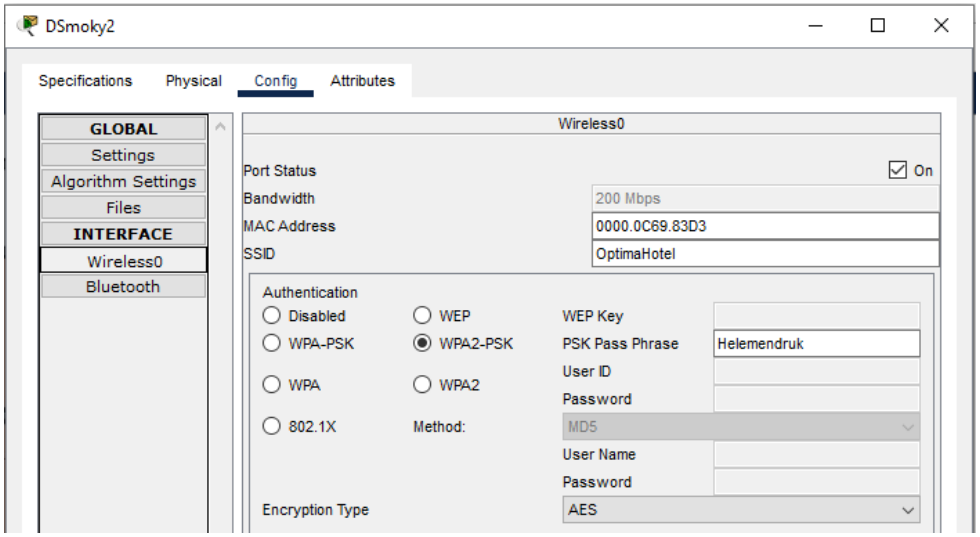


Рисунок 4.6 – Налаштування розумних речей

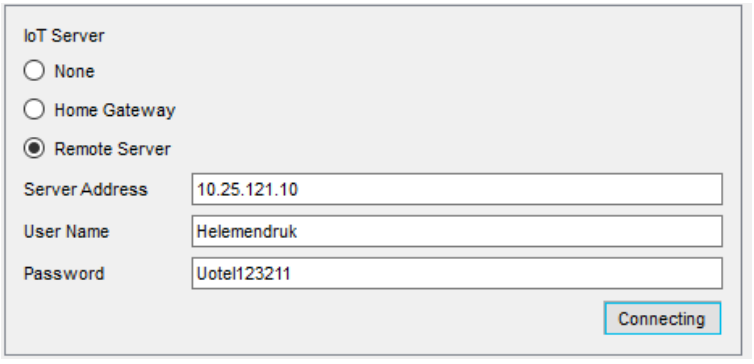


Рисунок 4.7 – Налаштування розумних речей на зв’язок з віддаленим сервером

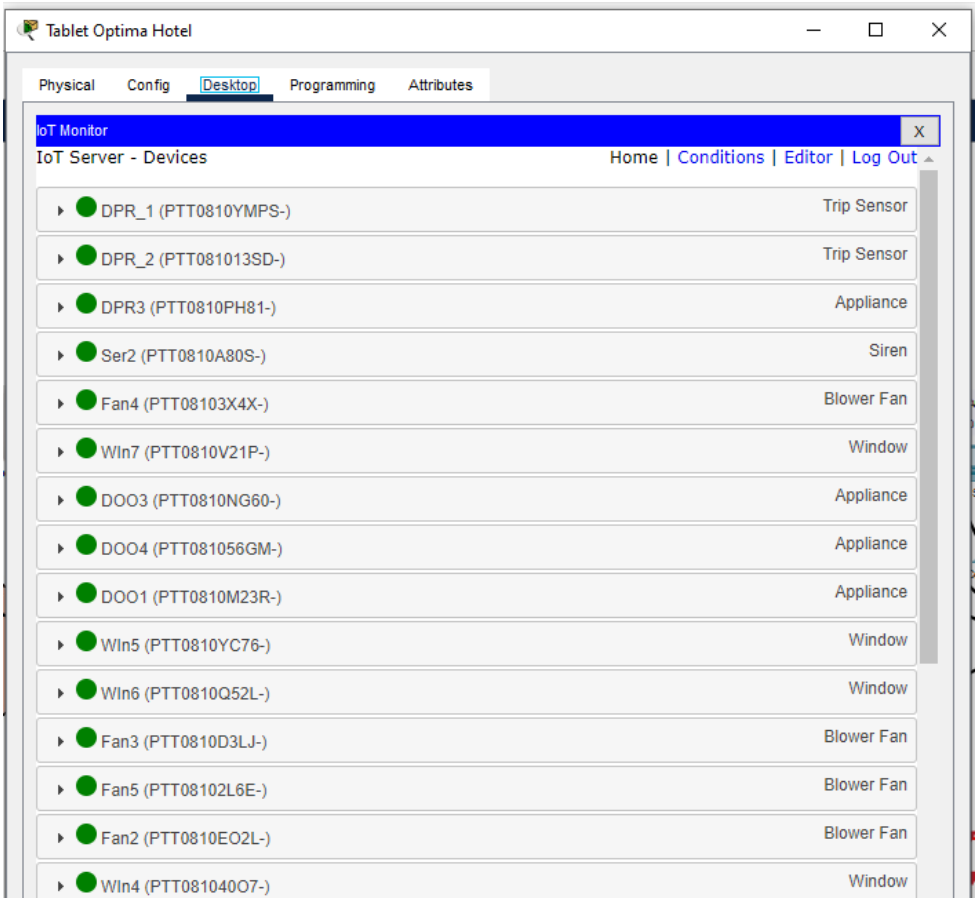
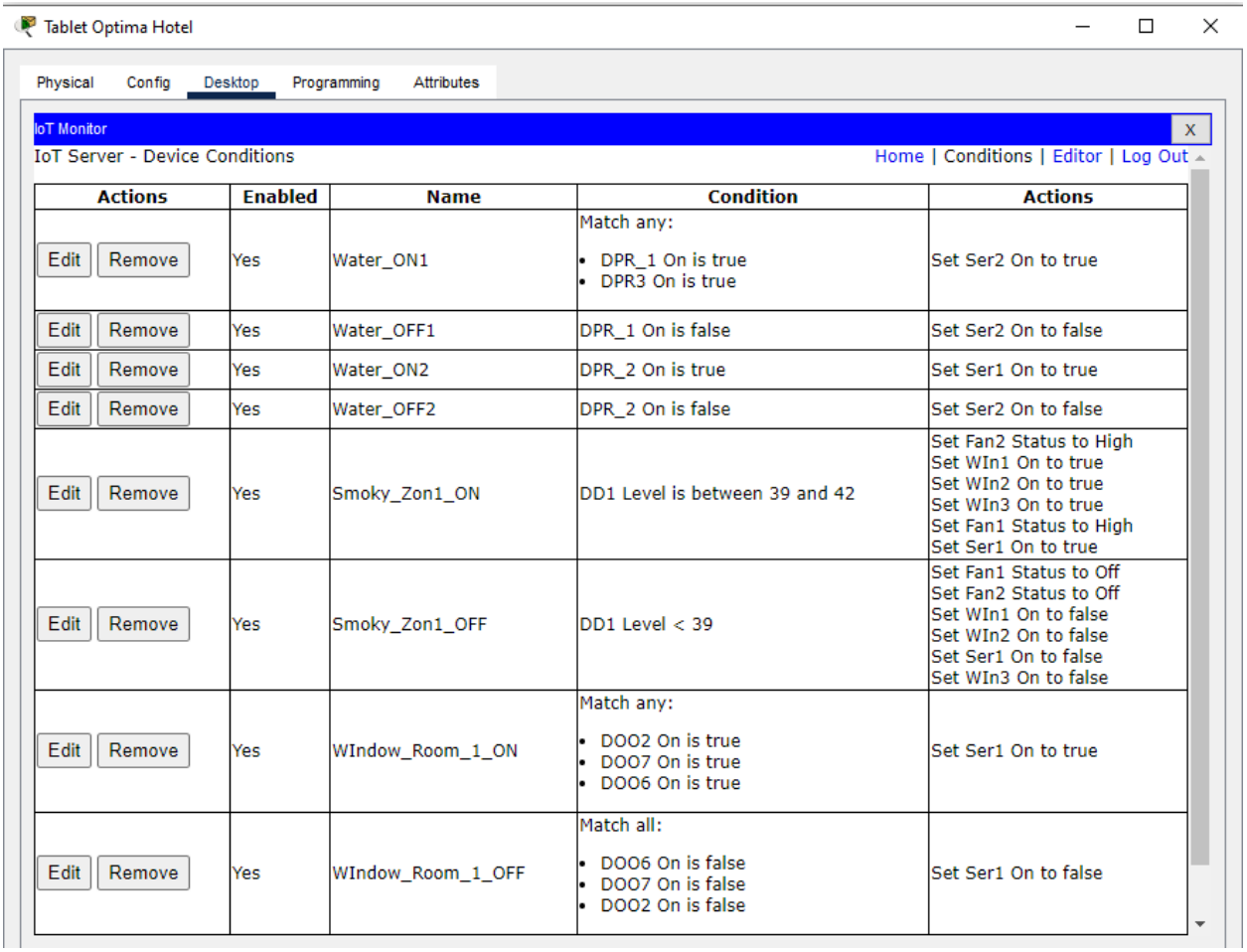


Рисунок 4.8 – Підключені на сервері розумні речі

Етап 3. Створення та налаштування правил і сценаріїв для автоматизованого керування пристроями, таких як автоматичне відключення подачі води при виявленні протікання або включення вентилятора при виявленні диму.

Також виконується інтеграція з додатками – зв'язок хмарних сервісів з мобільними або веб–додатками для керування пристроями та отримання сповіщень у режимі реального часу.



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Water_ON1	Match any: • DPR_1 On is true • DPR3 On is true	Set Ser2 On to true
Edit Remove	Yes	Water_OFF1	DPR_1 On is false	Set Ser2 On to false
Edit Remove	Yes	Water_ON2	DPR_2 On is true	Set Ser1 On to true
Edit Remove	Yes	Water_OFF2	DPR_2 On is false	Set Ser2 On to false
Edit Remove	Yes	Smoky_Zon1_ON	DD1 Level is between 39 and 42	Set Fan2 Status to High Set WIn1 On to true Set WIn2 On to true Set WIn3 On to true Set Fan1 Status to High Set Ser1 On to true
Edit Remove	Yes	Smoky_Zon1_OFF	DD1 Level < 39	Set Fan1 Status to Off Set Fan2 Status to Off Set WIn1 On to false Set WIn2 On to false Set Ser1 On to false Set WIn3 On to false
Edit Remove	Yes	WIndow_Room_1_ON	Match any: • DOO2 On is true • DOO7 On is true • DOO6 On is true	Set Ser1 On to true
Edit Remove	Yes	WIndow_Room_1_OFF	Match all: • DOO6 On is false • DOO7 On is false • DOO2 On is false	Set Ser1 On to false

Рисунок 4.9 – Реалізація сценарію на сервері для автоматизованого керування розумними речами

4.3 Моделювання IoT–системи

Модель IoT–системи «Hotel2» створена за допомогою симулятора Cisco Packet Tracer. Результати перевірки реалізації роботи «Hotel2» наведена на рисунках 4.10–4.12. На рисунку 4.10 показано спрацювання сценарію з протіканням води в ванній кімнаті готельного номеру.

На рис. 4.11 показано спрацювання сценарію з перевіркою відкритих вікон в кімнаті готельного номеру.

На рис. 4.12 показано спрацювання сценарію з перевіркою наявності диму в кімнаті готельного номеру.

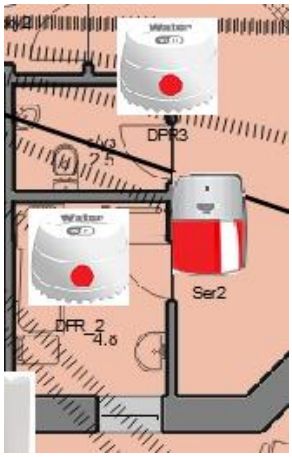


Рисунок 4.10 – Результат сценарію з протіканням води в ванній кімнаті готельного номеру

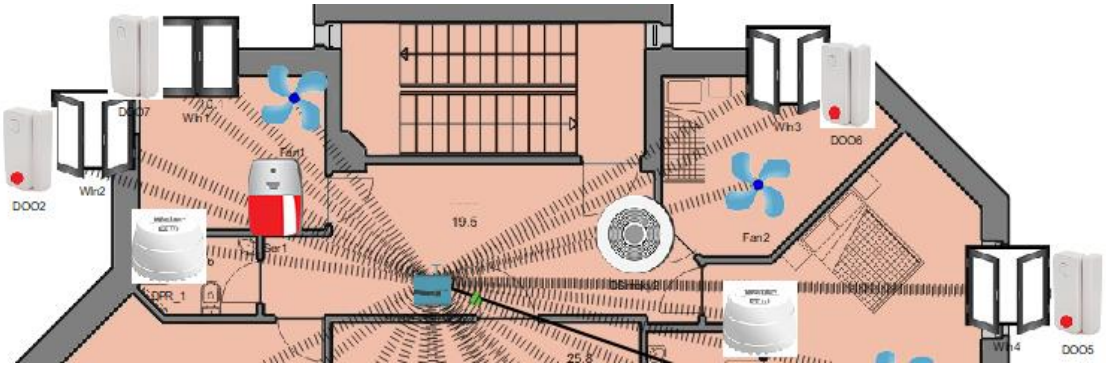


Рисунок 4.11 – Результат сценарію з з перевіркою відкритих вікон в кімнаті готельного номеру

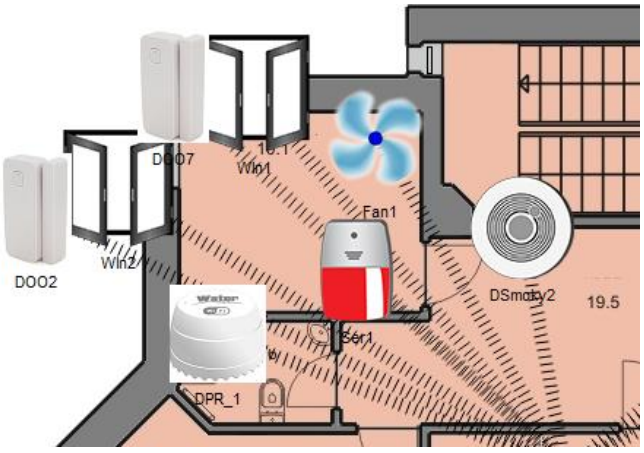


Рисунок 4.12 – Результат сценарію з перевіркою наявності диму в кімнаті готельного номеру

ВИСНОВКИ

Згідно до завдання розроблена кіберфізична система контролю мікроклімату готелів мережі Optima Hotel Group з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Архітектура кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group визначила необхідну наявність підмереж та їх внутрішні взаємозв'язки. Для визначеної у завданні кількості комп'ютерів в КС здійснено розрахунок налаштувань КС, визначено інтерфейс каналів зв'язку між мережевими пристроями та необхідний протокол для обміну інформацією, також здійснено налаштування параметрів маршрутизації.

Конфігурація налаштування маршрутизаторів та комутаторів корпоративної мережі кіберфізичної системи контролю мікроклімату готелів мережі Optima Hotel Group належним чином забезпечує повну відповідність заданого адресного простору до поставлених вимог та варіанту завдання. Динамічну маршрутизацію в КС виконано за допомогою протоколу EIGRP. Впровадження віртуальних локальних мереж та тунельного VPN–з'єднання необхідно для забезпечення належного рівня інформаційної безпеки в КС.

В кваліфікаційній роботі бакалавра було здійснено налаштування динамічної трансляції адрес, як необхідна для забезпечення виходу користувачів робочих місць локальних мереж в глобальну мережу Інтернет. Обране серверне обладнання та та налаштування його конфігурації дає змогу для роботи сервісів HTTP, DNS та AAA.

Моделювання роботи комп'ютерної системи та перевірка її роботи на коректність заданим показникам здійснено у симуляторі Cisco Packet Tracer, а результати цієї перевірки у представлені у вигляді таблиць, графіків і описані у пояснювальній записці та додатках.

Для підвищення функціоналу побутового середовища та зручності керування в кваліфікаційній роботі бакалавра також розроблено компонент керування IoT–

системою призначеною для запобігання аварійних ситуацій таких як: протікання води в номерах, контроль зачинених вікон та дверей, моніторинг задимлення.

Система IoT побудована відповідно до еталонної архітектури IoT та складається з різних рівнів: пристроїв, комунікацій, хмарних сервісів та додатків. Компоненти проектованої системи розташовані в коридорах готельного комплексу (протипожежна безпека) та в гостьових кімнатах (небезпека затоплення та задимлення).

ПЕРЕЛІК ПОСИЛАНЬ

1. An Optimized System Dynamics Approach for a Hotel Chain Management. Режим доступу: https://www.researchgate.net/publication/232956610

2. Microclimates of Urban Reproduction: The Limits of Automating Environmental Control. Режим доступу: https://onlinelibrary.wiley.com/doi/full/10.1111/anti.12566

3. Contrôle climatique dans les hôtels pour un séjour sain et confortable. Режим доступу: https://www.priva.com/fr/blog/batiments/controle–climatique–hotels

4. Microclimates of Urban Reproduction: The Limits of Automating Environmental Control. Antipode, Volume52, Issue 3, May 2020, Pages 637–659. Режим доступу: https://onlinelibrary.wiley.com/doi/10.1111/anti.12566/

5. Hotel energy management systems – saving hoteliers on operating costs. Режим доступу: https://www.base–4.com/hotel–energy–management–systems–2/

6. Optima Collection Dnipro. Режим доступу: https://optimahotels.com.ua/en/hotels/collection–dnipro/

7. Optima Hotels & Resorts. Режим доступу: https://www.linkedin.com/company/optima–hotels–resorts/

8. Hotel energy management system. Режим доступу: https://www.comperepower.com/solutions/hotel.html#

9. Max Pagel, SensorFlow: Amplifying Advancement with AI. Режим доступу: https://aiven.io/blog/sensorflow–amplifying–advancement–with–ai

10. Система мікроклімату для готелів. Режим доступу: https://ecoclimate.com.ua/solutions/hotels/

11. Бондарь Е., Гордиенко В. Михайлов Г. Автоматизація систем вентиляції та кондиціонування. Київ: ТОВ «Аванпост – Прим», 2005.

12. Що таке VRF/VRV мультизональна система кондиціонування. Режим доступу: https://klimat–center.cv.ua/shcho–take–vrf–vrv

13. Hotel Cyber Security: all you need to know. Режим доступу: https://sbit–hospitality.com/hotel–cyber–security–all–you–need–to–know/

14. Alles, was Sie über Cybersecurity wissen müssen – NIS2, DORA, NIST CSF 2.0, ISO27001 und BSI IT–Grundschutz. Режим доступу: https://www.boc–group.com/de/

15. Свистунов В.М., Пушняков Н.К. 2007. Опалення, вентиляція та кондиціювання повітря. Об'єктів агропромислового комплексу та житлово–комунального господарства. 2–ге вид. СПб.: Політехніка.

16. Пупена О.М. 2020. Розроблення людино–машинних інтерфейсів та систем збирання даних з використанням програмних засобів SCADA/HMI.: Навч.посіб. Київ : Видавництво Ліра–К.

17. Глибовець М.М. 2002. Штучний інтелект. Підручник для студентів вищих навчальних закладів, які навчаються за спеціальностями “Комп’ютерні науки” та “Прикладна математика”. Вид. дім: “Академія”.

18. ASUS A3402WVA – 23,8–дюймовий моноблочний комп’ютер з 3–річною гарантією. Режим доступу: https://broadcast.net.ua/ru/equipment/11414–asus–a3402wva–23–8–diuimovyi–monoblochnyi–kompiuter–z–3–richnoiu–harantiieiu.

19. Сервер двопроцесорний Alfa Server #224, 2x Intel Xeon E5–2667v4, 16 ядер, 32 потока, ОЗП 128GB, QUADRO RTX A4000 16GB. Режим доступу: https://alfa–server.com.ua/server–dvoprotsesornyi–alfa–server–224–2x–intel–xeon–e5–2667v4–16–yader–32–potoka–ozp–128gb–quadro–rtx–a4000–16gb//

20. Комутатор Cisco Catalyst 2960 Plus 48 10/100 + 2 T/SFP LAN Lite (WS–C2960+48TC–S). Режим доступу: https://networkdiscount.com.ua/ua/p2214589313–kommutator–cisco–catalyst.html?source=merchant_center&utm_term=&utm_campaign=&utm_source=adwords&utm_medium=ppc&hsa_acc=2700887574&hsa_cam=20983840971&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad

_source=1&gclid=CjwKCAjwhIS0BhBqEiwADAUhc5J98qYrII3SBjuRqjsmYovCclIUnwW_XDxjrvjytaJmd8BcW4xJ7hoCmKQQAvD_BwE.

21. Маршрутизатор Cisco ISR4331–VSEC/K9. Режим доступу: https://nexen.com.ua/uk/goods/marshrutizator–cisco–isr4331–vsec–k9?gclid=CjwKCAjwhIS0BhBqEiwADAUhc–OtEy3VeGm4bwKnNgcFDhmdIq0rWfMXTTjjBHykRX_899dS–zC–NxoCpi8QAvD_BwE.

22.

ДОДАТОК А – ТЕКСТ ПРОГРАМИ

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.20015–01 12 01

Листів 6

2024

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи. Програма призначена для забезпечення налаштування IP, DHCP, VLSM, EtherCanel, AAA, інтерфейсів, протоколу маршрутизації, NAT, консольних і vty ліній та створення мереж VPN, домену и ssh комп’ютерної системи.

ЗМІСТ

1. Налаштування роутера Helemendruk R2

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password–encryption
!
hostname Helemendruk_R2
!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded–address 10.25.120.1 10.25.120.10
ip dhcp excluded–address 10.25.120.33 10.25.120.43
ip dhcp excluded–address 10.25.120.65 10.25.120.75
ip dhcp excluded–address 10.25.121.97 10.25.121.100
!
ip dhcp pool POOL_VLAN25
 network 10.25.120.0 255.255.255.224
 default–router 10.25.120.1
 dns–server 10.25.121.10
ip dhcp pool POOL_VLAN35
 network 10.25.120.32 255.255.255.224
 default–router 110.25.120.33
 dns–server 10.25.121.10
ip dhcp pool POOL_VLAN45
 network 10.25.120.64 255.255.255.224
 default–router 10.25.120.65
 dns–server 10.25.121.10
ip dhcp pool POOL_LAN1
 network 10.25.121.96 255.255.255.240
 default–router 10.25.121.97
 dns–server 10.25.121.10
!
!
username Helemendruk secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO2911/K9 sn FTX15246078–
!
no ip domain–lookup
ip domain–name Helemendruk.123–20–1.com
!
spanning–tree mode pvst
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.25
 encapsulation dot1Q 25
 ip address 10.25.120.1 255.255.255.224
!
interface GigabitEthernet0/1.35
 encapsulation dot1Q 35
 ip address 10.25.120.33 255.255.255.224
!
interface GigabitEthernet0/1.45
 encapsulation dot1Q 45
 ip address 10.25.120.65 255.255.255.224
!
interface GigabitEthernet0/1.99
 encapsulation dot1Q 99
 ip address 10.25.120.97 255.255.255.240
!
interface GigabitEthernet0/2
 description to LAN1
 ip address 10.25.121.97 255.255.255.240
 duplex auto
 speed auto
!
interface Serial0/0/0
 description to R3
 bandwidth 128
 ip address 10.10.15.5 255.255.255.252
!
interface Serial0/0/1
 description to R1
 bandwidth 128
 ip address 10.10.15.1 255.255.255.252
!
!
router eigrp 15
 redistribute static
 passive–interface GigabitEthernet0/1.25
 passive–interface GigabitEthernet0/1.35
 passive–interface GigabitEthernet0/1.45
 passive–interface GigabitEthernet0/1.99
 network 110.25.121.96 0.0.0.15
 network 10.25.120.0 0.0.0.31
```

```
 network 10.25.120.32 0.0.0.31
 network 10.25.120.64 0.0.0.31
 network 10.10.15.0 0.0.0.3
 network 10.10.15.4 0.0.0.3
 network 10.25.121.96 0.0.0.15
 network 10.25.120.96 0.0.0.15
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow–export version 9
!
!
banner motd #123202 Helemendruk This is SEKURE area#
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
end
```

Налаштування роутера Helemendruk _R3

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password–encryption
!
hostname Helemendruk_R3
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524ZW69–
license boot module c2900 technology–package securityk9
!
spanning–tree mode pvst
!
!
interface Serial0/0/0

 ip address 10.10.15.6 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/1/0
 ip address 10.10.15.17 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/1/1
 ip address 10.10.15.10 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/2/0
 ip address 209.165.202.2 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 15
 network 209.165.202.0 0.0.0.3
 network 10.10.15.16 0.0.0.3
 network 10.10.15.8 0.0.0.3
 network 10.10.15.4 0.0.0.3
!
ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224
ip nat inside source list 15 pool Internet
ip nat inside source static 10.25.120.10 209.165.200.5
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 10.25.120.0 255.255.252.0 GigabitEthernet0/1
!
ip flow–export version 9
!
access–list 15 permit 10.25.120.0 0.0.3.255
!
```

```
no cdp run
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

3. Налаштування комутатора Sw21_Helemendruk

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password–encryption
!
hostname Sw21_Helemendruk
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip domain–name Helemendruk.123–20–1.com
!
username Helemendruk privilege 1 password 7 0822455D0A16
!
spanning–tree mode pvst
spanning–tree extend system–id
!
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 25,35,45,99–100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 100
 switchport trunk allowed vlan 25,35,45,99–100
 switchport mode trunk
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!

interface FastEthernet0/5
 switchport access vlan 45
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 45
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 45
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 45
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 45
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 35
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 35
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 35
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 35
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 35
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 25
 switchport mode access
```

```
!
interface FastEthernet0/17
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 25
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 25,35,45,99–
100
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 description LAN Vnutr_99
 ip address 10.25.120.98 255.255.255.240
!
ip default–gateway 10.25.120.97
!
banner motd #123202 Helemendruk This is
SEKURE area#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
end
```

ВІДГУКИ КОНСУЛЬТАНТІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ