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

здобувача Риндіна Артема Юрійовича
(ПІБ)

академічної групи 123-21-2
(шифр)

спеціальності 123 «Комп'ютерна інженерія»
(код і назва спеціальності)

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

на тему «Комп'ютерна система торгово-розважального центру з детальним налаштуванням мережі організації»
(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.			
розділу розробка корпоративної мережі	ас. Панферова Я.В.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

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

"__" ____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Риндіна. А.Ю. **академічної групи** 123-21-2
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»
(код і назва спеціальності)

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

на тему «Комп'ютерна система торгово-розважального центру з детальним налаштуванням мережі організації»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-С

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2025
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2025
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2025
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2025

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

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Риндін А.Ю.

РЕФЕРАТ

Пояснювальна записка: 88 с., 41рис., 10 табл., 1 дод., 27 джерел.

КОМП’ЮТЕРНА СИСТЕМА, ТРЦ, МЕРЕЖЕВІ ЗАСОБИ, CISCO, DHCP, VLAN, IOT

Об’єкт розробки – комп’ютерна система торгово-розважального центру з побудовою повноцінної локальної мережі

Мета роботи – спроєктувати, реалізувати, та налаштувати сучасну комп’ютерну систему для ТРЦ з урахуванням потреб у розподілі доступу між відділами, організації централізованих сервісів, а також інтеграції інтелектуальних підсистем.

У процесі роботи було розроблено логічну структуру локальної мережі з підтримкою VLAN для відділів, реалізовано маршрутизацію з використанням протоколу OSPF, а також забезпечено вихід до інтернету за допомогою NAT. Основні серверні служби, налаштовані для забезпечення стабільної роботи мережі, включають DNS, HTTP, AAA, IoT.

Крім того, проєкт має систему безпеки, яка включає відеоспостереження, автоматичне реагування на пожежні загрози, контроль доступу до критично важливих приміщень та систему клімат-контролю приміщень.

Функціональність і працездатність мережі перевірено в середовищі Cisco Packet Tracer. Результати надані у вигляді схем, таблиць та графічних матеріалів, що підтверджують відповідність рішення сучасним вимогам до корпоративних систем автоматизації.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ,УМОВНИХ ПОЗНАК,ОДИНИЦЬ І ТЕРМІНІВ

ТРЦ – торгово-розважальний центр;

SMM – маркетинг у соціальних мережах;

Event – подія;

HVAC – система опалення, вентиляції та відводу вологості в будівлі;

HPE – IT-компанія;

IoT – інтернет речей;

RFID – технологія автоматичної ідентифікації об’єктів;

КС – комп’ютерна система;

Single-Mode Fiber – оптичне волокно для передачі світла на великі відстані;

CRM – система для управління взаємовідносинами з клієнтами;

HTTPS – захищений протокол обміну даними;

TCP/IP – набір мережевих протоколів;

UDP – протокол швидкої передачі даних без перевірки доставки;

DHCP – протокол, який автоматично видає IP-адреси;

DNS – система, яка переводить доменні імена у IP-адреси;

HR – відділ компанії, який займається управлінням персоналом;

VLAN – розподіл мережі на віртуальні підмережі;

Wi-Fi – технологія бездротового зв’язку;

СКС – структурована кабельна система;

ПЗ – програмне забезпечення;

AES – Advanced Encryption Standart;

PoE – передача живлення і даних через Ethernet-кабель;

MAC – унікальна адреса мережевого пристрою;

ОС – операційна система;

DDR – тип оперативної пам’яті;

UTF-8 – стандарт кодування символів;

VLSM – підмережі змінної довжини.

ВСТУП

Сьогодні торгово-розважальні центри, стали невід'ємною частиною міської інфраструктури. Це складні багатофункціональні об'єкти, які поєднують в собі торгівлю, розваги, сфери послуг та громадське харчування. Ефективне функціонування об'єкта неможливе без сучасної комп'ютерної системи, яка буде забезпечувати взаємозв'язок між підрозділами, забезпечувати безпеку, контроль обладнання та автоматизацію процесів.

Відомі компанії та спеціалісти галузі, як-от Cisco, HPE, Siemens активно впроваджують рішення для побудови та налаштування інтегрованих комп'ютерних мереж у комерційній нерухомості. Разом із цим, в університетах і технічних інститутах постійно досліджуються способи та методи покращення кібербезпеки, розширення пропускної здатності мереж і оптимізації обслуговування користувачів.

На глобальному рівні спостерігається тенденція переходу до гнучких, масштабованих та захищених комп'ютерних систем з використанням хмарних технологій, IoT-рішень та віртуалізації. Як приклад, у більшості європейських країн у ТРЦ одразу створюється багаторівнева інфраструктура з можливістю керування кондиціонуванням, безпекою, освітленням та рекламними екранами з однієї керуючої платформи.

Значимість цієї роботи полягає в тому, що правильно спроєктована комп'ютерна система є основою для ефективної роботи ТРЦ. Створення системи, яка одночасно є безпечною, зручною та гнучкою для всіх користувачів, є важливою інженерною задачею в умовах зростаючих вимог до безпеки, автоматизації та сервісу.

Отримані результати можуть бути корисними для проєктування, розробки та побудови подібних систем у майбутньому, як для дійсних комерційних проєктів, так і для досліджень у галузі мережевих технологій.

1. СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп'ютерної системи ТРЦ

Торгово-розважальні центри займають важливе місце в інфраструктурі міста, об'єднуючи в собі торгові площі, кінотеатри, заклади харчування, супермаркети, зони для відпочинку, дитячі зони, технічні відділи, адміністративні приміщення та об'ємні паркінги, які необхідні для зручності відвідувачів ТРЦ. Всі ці об'єкти розраховані на обслуговування великої кількості відвідувачів щодня, серед яких є як покупці, так і орендарі магазинів. Для забезпечення цілодобової, безпечної та комфортної роботи такого об'єкту, необхідна ефективно організована комп'ютерна система.

З кожним роком галузь комерційної нерухомості розвивається все активніше, і разом із цим зростають вимоги до технічного забезпечення торгових об'єктів. Успішне функціонування ТРЦ вже неможливо уявити без комп'ютерних технологій, які впроваджують практично в кожній частині його роботи. Саме комп'ютерна система дозволяє забезпечити ефективну взаємодію між усіма структурними підрозділами та учасниками внутрішніх процесів ТРЦ.

Комп'ютерні технології у ТРЦ використовуються не лише для офісної роботи чи обліку. Вони відповідають за безпеку, управління ресурсами, внутрішні комунікації, збір і аналіз даних про потік відвідувачів і навіть автоматизацію різних побутових процесів. Ця система, подібна до нервової мережі, приховано підтримує роботу всього торгово-розважального центру, що робить його ефективним.

З часом технічне оснащення торгових центрів стає все більш складним. Це пов'язано з високими вимогами відвідувачів і необхідністю для власників швидко реагувати на різні ситуації. Без сучасної комп'ютерної системи неможливо забезпечити комфортну навігацію, оперативне реагування на проблеми чи гнучке керування простором. Вона стає головним інструментом для контролю, аналізу і прийняття рішень як у щоденній роботі, так і у планування майбутнього розвитку.

Таким чином, комп'ютерна система у торгово-розважальному центрі є не

просто середовищем для роботи офісного персоналу, а є комплексною системою, що забезпечує функціонування всього об’єкта. Від її якості залежить ефективність управління внутрішніми процесами, та зручність перебування для відвідувачів. Саме тому, правильне проєктування та налаштування системи, з урахуванням всіх нюансів та особливостей, має важливе значення в умовах сучасного ТРЦ.

1.2 Огляд сучасних технічних рішень у сфері комп’ютерних систем для торгово-розважальних центрів та аналіз можливих шляхів реалізації

Для створення ефективних комп’ютерних систем у торгово-розважальних центрах, використовуються спеціалізовані підходи для побудови мережевої інфраструктури, до якої входять налаштування мережних пристроїв, організацію безпеки даних, налаштування серверного обладнання, IoT-пристроїв та забезпечення бездротового доступу для відвідувачів ТРЦ. Комп’ютерна система включає в себе ряд компонентів, які працюють разом у комплексі, від серверної інфраструктури та локальних мереж, до пристроїв які забезпечують безпеку та бездротової мережі для відвідувачів. Останніми роками підхід до створення таких систем суттєво змінився, від простого забезпечення офісних комп’ютерів та Wi-Fi, до комплексних цифрових рішень, які містять системи аналітики, автоматизації, безпеки та інтеграцію з мобільними платформами.

В більшій частині сучасних ТРЦ застосовують трьохрівневу модель побудови мережі:

- ядро;
- агрегація;
- доступ.

Така мережа дає змогу керувати даними централізовано та забезпечити надійність при великому навантаженні. На рівні ядра використовуються маршрутизатори таких відомих компаній, як: «Cisco», «MikroTik» та «Juniper», вони дають змогу зробити резервування шляхів передачі даних, що є дуже важливим для великих площ. Для внутрішнього з’єднання активно використовуються оптоволоконні кабелі типу «Single-Mode Fiber», які забезпечують високу швидкість

передачі (до 10 Гбіт/с) на великі відстані без затримок і втрат. Для підключення окремих офісів, терміналів, камер використовують кабелі категорії «6» або «6а», які надають можливість досягати стабільної швидкості при мінімальному рівні перешкод. Зображення одномодового волокна та кабелів категорії «6» та «6а» зображено нижче на рисунках 1.1-1.2.

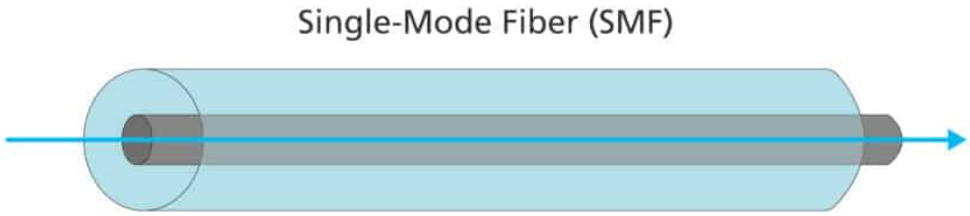

Рисунок 1.1 – Напрям передачі світла у одномодовому волокні

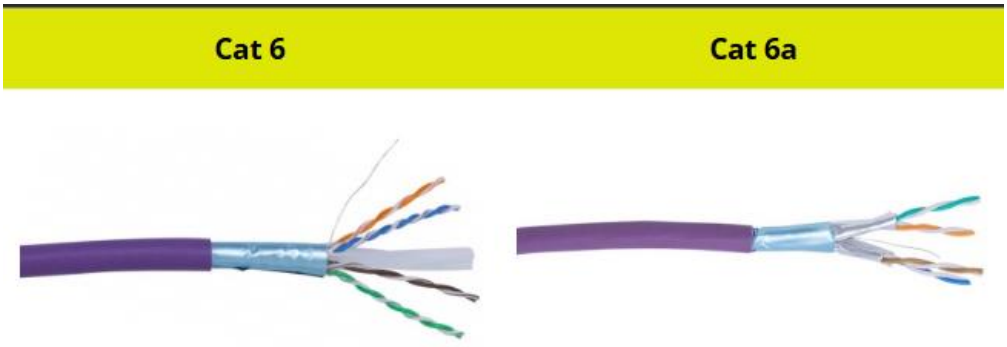

Рисунок 1.2 – Зовнішній вигляд кабелів категорії «6» та «6а»

Все більш часто ТРЦ впроваджують рішення із централізованою серверною кімнатою, в якій знаходяться як інфраструктура для локальної мережі, так і сервери контролю доступу, систем управління приміщеннями, відеоспостереження та CRM-системи для управління орендарями. Наприклад, ТРЦ Gulliver побудував серверну, на базі віртуалізованих середовищ Hyper-V та VMWare, що дає можливість розподіляти ресурси між підсистемами, мінімізувати простої та швидко масштабуватись.

Wi-Fi у більшості ТРЦ реалізований, як гостьові Wi-Fi зони на базі стандарту Wi-Fi 6, котрі можуть забезпечити підключення сотні користувачів одночасно без вагомої просадки швидкості. Використовують точки доступу «Ubiquiti UniFi», «Aruba», або «Cisco Meraki», вони підтримують функції пріоритету трафіка,

формування променя для направленої передачі сигналу та балансування навантаження. Для забезпечення якісного сигналу використовуються мережі з високою щільністю точок доступу, для забезпечення стабільного та швидкого інтернету в усіх зонах ТРЦ, особливо у місцях з великою кількістю людей. Для якісного покриття точки доступу встановлюють зважаючи увагу на перекриття зон, для уникання мертвих зон та збереження швидкості. Зображення точки доступу Cisco Meraki розміщено нижче на рисунку 1.3

Рисунок 1.3 – Точка доступу Cisco Meraki

Безпека даних є критично важливою складовою надійного функціонування всієї інфраструктури ТРЦ, насамперед це стосується обробки та зберігання персональної інформації відвідувачів, платіжних даних та даних відеоспостереження. Основним є захист інформації, який отримується шляхом шифрування передачі даних. Всі дані, які передаються мережею проходять через захищені канали з використанням протоколів HTTPS.

Ще однією важливою частиною є аутентифікація користувачів і чітке розмежування доступу до різних частин мережі. До критичних елементів інфраструктури, таких як сервери, бази даних та системи відеоспостереження, доступ повинен надаватися тільки довіреним особам. Застосовується багатофакторна аутентифікація та складні паролі, що досить сильно ускладнює можливість несанкціонованого доступу.

У системі безпеки не можна обійтись без фаєрволів та антивірусного захисту. Ці рішення забезпечують фільтр даних, які потрапляють у систему, та блокують ймовірно шкідливі запити. Також доречно до використання є наявність зовнішніх

дата-центрів для резервного копіювання даних, для зменшення ризику втрати інформації.

У роботі КС важливу роль відіграє те, як передаються дані між пристроями, серверами, камерами спостереження. Від швидкості обміну інформацією та надійності роботи залежить не лише зручність відвідувачів, а й безпека, ефективність управління та стабільність роботи закладу. Самим поширеним протоколом є TCP/IP, він забезпечує послідовну і стабільну передачу даних, особливо важливо, коли йдеться про фінансові операції, дистанційне керування пристроями, адміністрування баз даних. TCP забезпечує надійність, він контролює, щоб всі пакети даних досягали адресата у правильному порядку.

Також у багатьох підсистемах ТРЦ доволі часто використовують UDP у системах відеоспостереження. Протокол не дає гарантії доставки кожного пакету, замість того дозволяє передавати відео швидко з мінімальною затримкою. Незначні втрати кадрів непомітні для людини, зате здійснюється плавне відтворення відео без зависань.

Важливими є протоколи HTTP/HTTPS, вони використовуються для передачі інформації через веб-інтерфейси, від перегляду звітів про роботу підприємства до моніторингу систем або адміністрування Wi-Fi. HTTPS здійснює шифрування трафіку для забезпечення безпеки.

Не менш значними є протокол DHCP, який автоматично видає IP-адреси пристроям у мережі та DNS, який працює з доменними іменами, замість IP-адрес, що сильно спрощує адміністрування.

Всі ці протоколи, вони хоч і виконують різні функції, але разом забезпечують ефективну роботу всієї системи ТРЦ, від безперебійної роботи мережі, до миттєвого доступу до інтернету для відвідувачів.

1.3 Аналіз внутрішньої структури та підрозділів ТРЦ

Організаційна структура торгово-розважального центру розроблена таким чином, щоб всі підрозділи ефективно співпрацювали один з одним, щоб задовольнити потреби клієнтів і гарантувати безперебійну роботу об’єкта в цілому.

У центрі структури знаходиться директор ТРЦ, який займається керуванням роботи всіх відділів, приймає важливі рішення в управлінні та несе відповідальність за роботу ТРЦ.

Відділ безпеки відіграє важливу роль в системі функціонування ТРЦ. У його складі працюють начальник служби безпеки, охоронці, оператори відеоспостереження та фахівець з контролю доступу. Вони відповідають за фізичну охорону приміщень, контроль входу, виходу, а також за функціонування систем відеонагляду та сигналізації. Безпека персоналу та відвідувачів є одним з пріоритетів, тож цей відділ функціонує у постійному режимі.

Адміністративний відділ виконує функції, які пов’язані з організацією внутрішніх процесів, ведення кадрового обліку, займається документообігом та комунікацією між підрозділами. У його складі працюють керівник відділу, HR-менеджер, офіс менеджер і секретар. Якраз адміністрація забезпечує оперативність прийняття внутрішніх рішень, займається веденням особистих справ працівників, а також проведенням нарад і зборів.

Фінансово-економічний відділ є важливим у стратегічному плануванні й управлінні ресурсами ТРЦ. В його склад входять фінансовий директор, головний бухгалтер, фінансовий аналітик і економіст. Вони займаються формуванням бюджету, здійснюють контроль над витратами, аналізом прибутковості та фінансовим звітуванням. Завдяки цьому підрозділу, ТРЦ зможе бути економічно стабільним.

Юридичний відділ гарантує правову підтримку діяльності ТРЦ. До нього входять юрисконсульт і помічник юриста. Вони займаються підготовкою та аналізом договорів, супроводжують угоди з орендарями, представляють інтереси ТРЦ у разі судових справ, а також займаються консультацією інших підрозділів з правових питань. Цей відділ гарантує, що рішення прийняті керівництвом є законними та правовими.

Відділ оренди та взаємодії з орендарями несе відповідальність за пошук, обслуговування орендарів та залучення, які формують комерційну діяльність ТРЦ. Менеджер з оренди, координатор орендарів та фахівець з комерційної нерухомості

ведуть переговори з потенційними орендарями, укладають договори, контролюють дотримання умов оренди та підтримують зв’язок з торговими об’єктами.

Маркетинговий відділ займається просуванням ТРЦ, та його репутацією, організовує заходи. У цьому відділі працюють SMM-менеджер, Event-менеджер, дизайнер і PR-менеджер. Команда займається розробкою рекламних компаній, веде соціальні мережі та забезпечують комунікацію з аудиторією.

ІТ-відділ займається підтримкою комп’ютерної інфраструктури, налаштуванням мережі, захистом даних та стабільністю внутрішніх цифрових мереж. Серед його співробітників керівник відділу, мережевий інженер, системний адміністратор та спеціаліст з кібербезпеки. Їхня задача здійснити стабільну роботу комп’ютерної системи, мережі Wi-Fi, систем відеоспостереження, серверів, а також захистити дані від зовнішніх загроз. ІТ-відділ активно співпрацює з іншими структурами, вводячи нові технології в управління ТРЦ.

Технічний відділ забезпечує справність інженерних систем, та здійснює технічну підтримку всього комплексу ТРЦ. У відділі працюють головний інженер, інженер з вентиляції та кондиціювання, електрик і сантехнік-слюсар. Вони слідкують за освітленням, водопостачанням, вентиляцією, опаленням та електропостачанням, усувають технічні несправності, які впливають на безпеку і комфорт відвідувачів та персоналу.

Аналітичний відділ, до складу якого входять керівник, бізнес-аналітик і маркетинговий аналітик. Вони аналізують поведінку клієнтів, фінансові показники, ефективність рекламних компаній і роботу орендарів. Їх аналіз дозволяє швидко змінити стратегію розвитку, щоб вона адаптувалась до змін на ринку. Схема організації роботи ТРЦ знаходиться нижче на рисунку 1.4

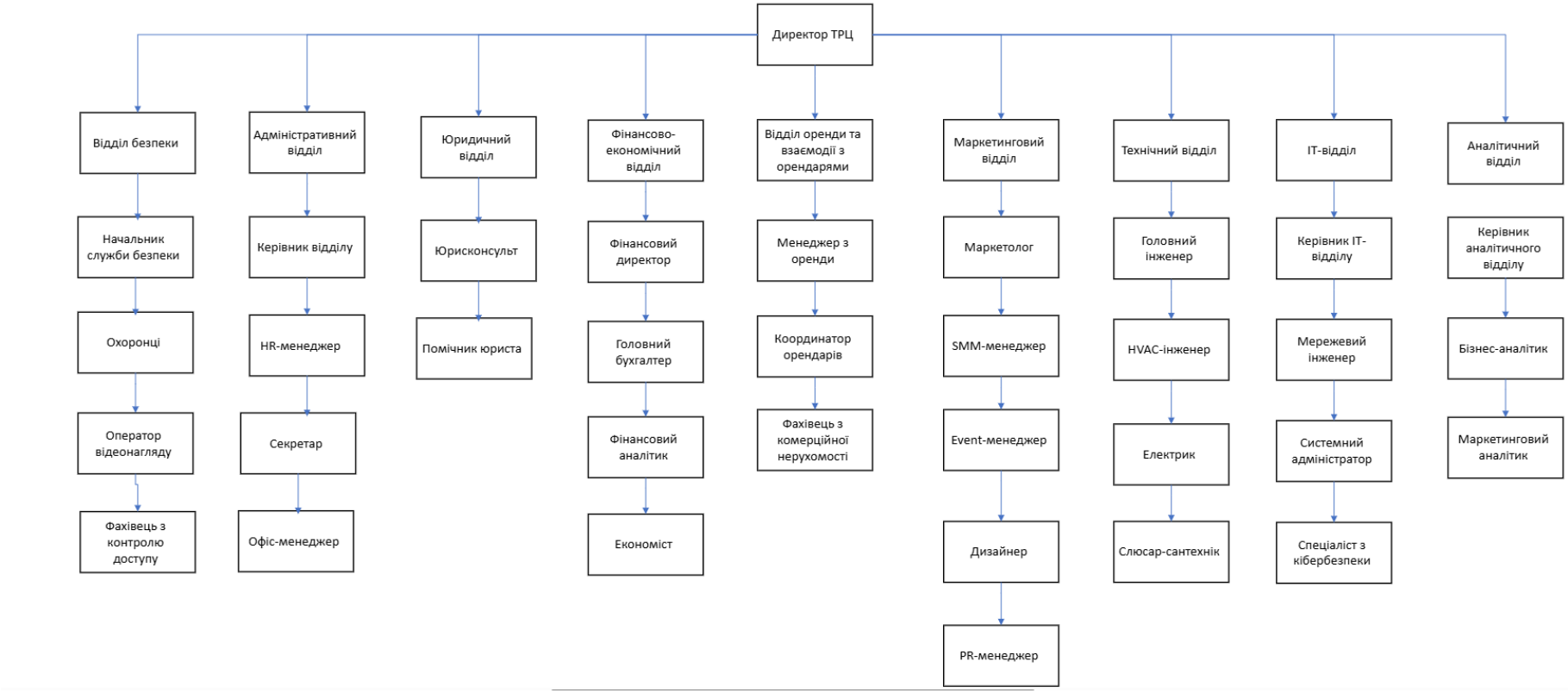

Рисунок 1.4 – Організаційна структура ТРЦ

1.4 Топологія внутрішньої структури ТРЦ і методи інформаційної взаємодії

ТРЦ розташовується у регіоні, з розвиненою інфраструктурою та активним торговим життям, що робить його ідеальним місцем для створення сучасного торгово-розважального комплексу. ТРЦ об’єднує в собі магазини, супермаркети, офісні приміщення та зони відпочинку, забезпечуючи комфортне середовище для відвідувачів різного віку.

Внутрішня структура ТРЦ побудована з урахуванням логічних зв’язків і фізичного розміщення підрозділів у будівлі. Ми маємо триповерхову будівлю, кожен поверх якої займає 2800 квадратних метрів. Простора структура дозволяє забезпечити якісне покриття мережевими приладами, а також дозволяє раціонально розподілити функціональні зони та підрозділи. Висота одного поверху становить близько 4,5 метрів, що забезпечує достатній простір для вентиляційних систем, освітлення, внутрішніх комунікацій, а також для комфортного перебування відвідувачів. Товщина перекриття між поверхами 30 сантиметрів, що забезпечує необхідну міцність конструкції та дає змогу безпечно проводити кабелі, труби та інші інженерні елементи між рівнями.

На першому поверсі розміщуються підрозділи, що тісно пов’язані з щоденним функціонуванням об’єкта. Розміщуються такі відділи:

- відділ безпеки;
- відділ оренди та взаємодії з орендарями.

Також на поверсі розміщуються торгові зали з магазинами різного типу, та великий супермаркет. Цей рівень являє собою «обличчя» ТРЦ, оскільки перше враження відвідувач отримує саме тут, а значить, що поверх повинен бути максимально зручним, технологічно оснащеним і безпечним. З метою забезпечення якісного інформаційного обслуговування, слід впровадити сучасні зони Wi-Fi, розгорнуті на базі точок доступу. Вони встановлюються в зонах з високою щільністю відвідувачів, а саме біля входу до супермаркету, у центральних коридорах, торгових приміщеннях і дозволяють забезпечити стабільний і швидкий зв’язок без мертвих зон. Для підтримання безпеки та своєчасного реагування на

інциденти доцільно впровадити систему відеоспостереження з IP-камерами, які інтегруються з IoT-сервером. Це дає змогу в реальному часі відслідковувати ситуацію на поверхах, оперативно реагувати на підозрілі дії. Розміщення камер доцільно здійснювати на входах і виходах, у зонах високої прохідності. План першого поверху розміщено нижче на рисунку 1.6.

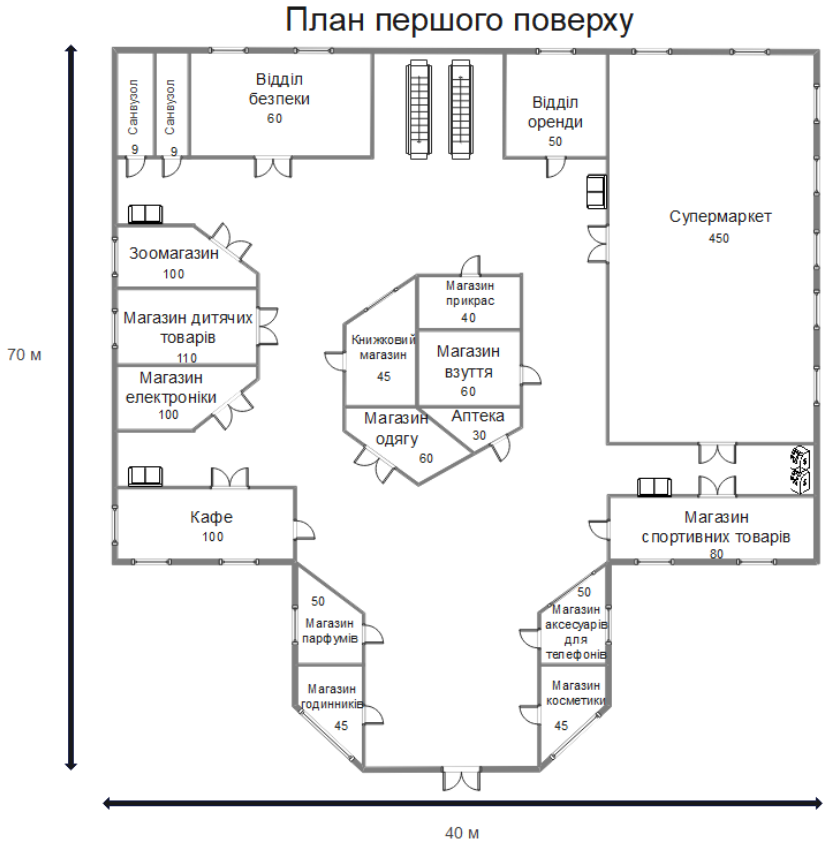

Рисунок 1.6 – План першого поверху ТРЦ

На другому поверсі зосереджена адміністративна діяльність. Тут розміщені наступні відділи:

- кабінет директора;
- адміністративний відділ;
- фінансово-економічний відділ;
- юридичний відділ.

Офісна частина поверху вимагає високого рівня захищеності даних, особливо для передачі документів, юридичних даних, бухгалтерських операцій та внутрішньої комунікації між підрозділами. Це досягається за допомогою сегментованої мережевої інфраструктури, яка використовує керовані комутатори і підтримує

VLAN. Це дозволяє розділяти трафік працівників відділів, крім того сервісні системи і кіберзахист мають свої канали. Для відвідувачів на поверсі містяться ігрові зони, зона для харчування, кінотеатр та різні магазини. Поверх слід забезпечити точками доступу Wi-Fi. Зображення плану другого поверху наведено нижче на рисунку 1.7.

Рисунок 1.7 – План другого поверху ТРЦ

Третій поверх містить найбільш технічно складних підрозділів. Тут розміщені наступні відділи:

- технічний відділ;
- ІТ-відділ;
- маркетинговий відділ;
- аналітичний відділ.

Також заплановано організувати серверну кімнату, оскільки саме на цьому рівні передбачено розташування основних вузлів інфраструктури: серверів, маршрутизаторів, комутаторів рівня ядра. Для забезпечення захищеності інформаційних ресурсів планується впровадити кілька рівнів безпеки, зокрема:

фізичний контроль доступу, багатофакторну автентифікацію та відеоспостереженні у серверній.

Протоколи передачі даних, такі як Ethernet для дротового з'єднання та 802.11ax для бездротового доступу, використовуватимуться для забезпечення надійності та швидкості взаємодії між усіма відділами.

Передбачається, створення центрального вузла комутації поверху на основі трьох взаємопов'язаних комутаторів, з'єднаних між собою у вигляді замкненого трикутника. Така конфігурація забезпечить надійність мережі та її безперервну роботу навіть у разі відмови одного з каналу зв'язку.

На поверсі також є розважальні зони, включаючи боулінг, зону віртуальної реальності та різні магазини. План поверху наведено на рисунку 1.8.

Рисунок 1.8 – План третього поверху ТРЦ

На території торгово-розважального центру є відкритий загальнодоступний паркінг, його наявність забезпечує зручність для відвідувачів і працівників, сприяючи комфортному доступу до ТРЦ.

1.5 Постановка завдання

У межах цієї роботи ставиться завдання розробки повної моделі апаратної частини комп’ютерної системи, а також налаштування моделі корпоративної мережі, яка відповідатиме сучасним вимогам швидкості, безпеки передавання даних та надійності. Мережа має одночасно забезпечувати безперебійну роботу всіх підрозділів ТРЦ, обслуговування магазинів та території та створювати зручні умови для відвідувачів. Щоб досягти цього, потрібно чітко організувати мережеві ресурси, налаштувати доступ, захистити дані та мати надійне технічне забезпечення.

Мета проєкту полягає в розробці комп’ютерної системи, яка охопить два основні напрямки:

- інфраструктура підприємства ТРЦ, яка складається з внутрішніх відділів. Кожному з яких необхідно створити стабільну локальну мережу, гарантувати захищений обмін даними, отримати доступ до внутрішніх послуг, таких як документообіг, аналітичні платформи і створити систему резервного зберігання даних;
- система для відвідувачів та магазинів ТРЦ, до якої входять публічні Wi-Fi зони, інформаційні табло, системи навігації по ТРЦ. Також враховуються потреби магазинів, розміщених на території, для них передбачається підключення до мережі ТРЦ із базовим мережевим доступом. Для обох категорій, як для відвідувачів, так і для магазинів передбачається окремий шлюз виходу до мережі інтернет. Доступ до внутрішньої критичної інфраструктури ТРЦ буде жорстко обмежений з метою забезпечення безпеки. Усі ці елементи мають бути інтегровані в загальну систему, але фізично та логічно ізольовані від внутрішніх службових підсистем.

Окрім мережевої інфраструктури, проєкт передбачає впровадження ключових IoT-систем:

- відеоспостереження;
- пожежної безпеки;
- контролю доступу на базі RFID;

- клімат-контроль.

Вся інформація з цих систем буде централізовано зберігатися на IoT-сервері, що забезпечить оперативний моніторинг та керування об’єктом.

У результаті виконання поставленого завдання, передбачається створення комплексної моделі комп’ютерної системи для ТРЦ, що забезпечить ефективне управління підприємством і зручне цифрове середовище для відвідувачів.

1.6 Визначення можливих напрямків рішення поставлених завдань

Оскільки ТРЦ є єдиною будівлею, мережа має бути побудована за ієрархічною структурою з чітким поділом на рівень доступу, рівень розподілу та ядро. Такий підхід дозволяє забезпечити гнучке управління трафіком, спростити адміністрування й підвищити масштабованість системи в разі подальшого розширення інфраструктури.

Треба здійснити вибір обладнання, яке відповідатиме потребам ТРЦ за критеріями продуктивності, масштабованості, енергоефективності та вартості. Для цього буде проведено аналіз вимог до кількості користувачів, обсягів трафіку та зон обслуговування. Планується використання керованих комутаторів рівня 2/3, маршрутизаторів з підтримкою сучасних протоколів безпеки, серверів із можливістю віртуалізації, а також точок доступу для забезпечення високої якості бездротового зв’язку.

Фізична інфраструктура мережі передбачає використання структурованої кабельної системи. В межах поверху та приміщень застосовуватиметься вита пара категорії 6, що забезпечить надійну та швидку передачу даних. Для з’єднання між поверхами, а також з серверною кімнатою, доцільним є використання оптоволоконних каналів, які забезпечують високошвидкісну та стійку передачу інформації.

Щодо технологій і протоколів, пріоритет буде надаватися сучасним, стабільним і гнучким рішенням. Використання протоколу динамічної маршрутизації OSPF забезпечить оптимальну побудову маршрутів у мережі з великою кількістю сегментів. Запровадження агрегації каналів через EthernetChannel дозволить

об’єднати декілька фізичних ліній у логічний канал із підвищеною пропускною здатністю. Також планується реалізація NAT для захисту внутрішніх IP-адрес.

Розмежування функціональних зон у мережі буде досягнуто шляхом впровадження VLAN, це дозволить ізолювати трафік, що значно підвищить рівень безпеки та оптимізує навантаження на мережеву інфраструктуру.

У межах реалізації заходів із безпеки буде передбачено налаштування мережевих екранів, ACL списків контролю доступу, шифрування даних, політик авторизації й автентифікації користувачів.

Серверна інфраструктура передбачає розгортання базових служб, зокрема DNS, Web, FTP, IOT. Передбачається створення розподіленої IoT-мережі в межах приміщень ТРЦ, яка забезпечуватиме автоматизований збір і передавання даних із підключених пристроїв до центрального сервера. Такий підхід дозволить здійснювати моніторинг важливих параметрів об’єкта в реальному часі, своєчасно реагувати на зміни стану середовища та підвищити ефективність керування інфраструктурою.

Для забезпечення стабільної та безперервної роботи мережі, слід розробити комплекс заходів із резервуванням критичних каналів зв’язку та компонентів інфраструктури, зокрема організацію додаткових каналів зв’язку. Це дозволить мінімізувати ризики простою та швидко відновлювати працездатність у разі виникнення несправностей.

2. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ

2.1 Технічні вимоги комп’ютерної системи ТРЦ

2.1.1 Найменування і призначення системи

Повна назва Системи: “Комп’ютерна система торгово-розважального центру з детальним налаштуванням мережі організації”. Система призначена для забезпечення стабільної та захищеної передачі даних між усіма відділами ТРЦ, підтримки роботи адміністративних і технічних служб, автоматизації бізнес-процесів, а також інтеграції з інженерними системами, системами безпеки, контролю доступу й відеоспостереження.

2.1.2 Вимоги до структури та функціонування системи

2.1.2.1 Структура підсистем: призначення, характеристика та вимоги до організації ієрархії системи

Організація комп’ютерної системи ТРЦ вимагає логічного поділу інфраструктури на окремі підсистеми з чітко визначеним функціональним призначенням. Кожна з підсистем повинна відповідати організаційній структурі відділів і забезпечувати стабільне функціонування окремих сфер діяльності ТРЦ без втрати цілісності мережі. Основною вимогою є створення взаємопов’язаної, але розмежованої системи, в якій підсистеми працюють автономно, але централізована ієрархія контролюватиме їх.

Відділи на першому поверсі ТРЦ, належать до LAN_1. Відділи безпеки та оренди входять до її складу. Ця підмережа має забезпечувати взаємодію персоналу, відповідного за управління орендними площами, передачу службової інформації, моніторинг відеоспостереження. Основна вимога до LAN_1 стабільне з’єднання з мінімальними затримками, так як в роботі служби безпеки критичне значення має безперебійний доступ до перегляду камер та взаємодією з базою даних.

Гостьова мережа LAN_2 призначена для відвідувачів ТРЦ та для магазинів. Вона повинна мати повну логічну ізоляцію від інших LAN і мати підключення до мережі інтернет через окремий шлюз. Це дозволить забезпечити безпечний доступ клієнтам до Wi-Fi послуг, не ризикуючи внутрішньою інфраструктурою ТРЦ і мереж

магазинів. Окремо необхідно забезпечити ізоляцію трафіку магазинів від трафіку відвідувачів для запобігання можливих загроз і витоків інформації.

До складу LAN_3 мають входити IT-відділ та технічний відділ, а також окрема серверна кімната, що має розташовуватися в межах IT-відділу. IT-відділ повинен забезпечувати обслуговування, налаштування та адміністрування внутрішніх мереж, систем безпеки, серверів і робочих станцій. Технічний відділ має відповідати за функціонування інженерних систем, таких як освітлення, вентиляція та клімат-контроль. LAN_3 повинна характеризуватися підвищеною надійністю, високою пропускною здатністю та постійним доступом до систем моніторингу стану обладнання. У серверній кімнаті необхідно розмістити ключові сервери: DNS, AAA, IOT та HTTP.

LAN_4 поєднує в собі відділи маркетингу та аналітики, що працюють над збором, обробкою та аналізом даних. Крім того, вони працюють над розробкою стратегій залучення клієнтів. Також важливою є висока продуктивність і стабільність передачі даних.

LAN_5 повинна обслуговувати адміністративні служби ТРЦ, серед яких юридичний, фінансово-економічний, адміністративний відділи, а також кабінет директора. Для цієї підмережі необхідно забезпечити високий рівень захисту, адже тут здійснюється обробка конфіденційних даних, бухгалтерської звітності, юридичних документів та персональної інформації працівників і партнерів. Використання окремих VLAN для кожного підрозділу є обов’язковим, це дозволить реалізувати чіткий розподіл доступу, захист від несанкціонованого втручання та ефективний документообіг. Мережа має функціонувати стабільно й безперебійно, відповідаючи підвищеним вимогам до інформаційної безпеки та надійності.

Ієрархія системи має включати три рівня:

- нижній рівень: робочі станції співробітників, користувацькі пристрої та IoT-обладнання, що взаємодіє з інфраструктурою;
- середній рівень: комутаційне та мережеве обладнання, точки доступу;
- верхній рівень: серверна частина, сховище даних, системи управління мережею.

Централізація ресурсів має здійснюватися ІТ-відділом, який відповідає за керування ключовими компонентами. При цьому кожна підсистема повинна мати обмежену автономію, щоб зберігати працездатність навіть у разі збою сусідніх сегментів або втрати зв’язку з головним сервером. Такий метод дозволить забезпечити стабільну роботу всієї системи ТРЦ, зберігаючи цілісність даних, що є важливим для безперебійного функціонування ТРЦ.

2.1.2.2 Вимоги до способів і засобів зв’язку для інформаційного обміну між компонентами системи

Фізичне з’єднання кінцевих пристроїв із мережею має реалізовуватись через Ethernet-порти типу RJ-45, що вбудовані у комутатори. Треба використовувати екрановану виту пару категорії 6, так як вона забезпечує стабільну передачу даних на швидкості до 1 Гбіт/с, що дуже важливо для роботи із великими обсягами даних.

Підключення комутаторів до маршрутизаторів необхідно виконувати через порти GigabitEthernet, що дозволяє реалізувати VLAN-транкінг. Такий підхід забезпечує логічне розділення підмереж і підвищує ефективність маршрутизації трафіку між відділами та поверхами.

Зв’язок між маршрутизаторами потрібно здійснювати через послідовні інтерфейси типу Serial, що дозволяє досягти точного контролю маршрутів, стабільності передавання та підвищеної надійності при об’єднанні окремих LAN у єдину корпоративну мережу. Водночас слід забезпечити також з’єднання між маршрутизаторами через порти GigabitEthernet для збільшення пропускної здатності та підвищення швидкості обміну даними.

Гостьовий доступ до Wi-Fi має бути реалізований як окрема автономна мережа, з виділеним маршрутизатором та ізольованими точками доступу. Така організація дозволяє відвідувачам безпечно користуватись інтернетом без ризику для критично важливої внутрішньої інфраструктури.

Крім того, треба передбачити використання резервного каналу зв’язку, між ключовими мережевими вузлами, щоб уникнути збоїв у випадку пошкодження основної лінії.

2.1.2.3 Вимоги до характеристик взаємозв'язків створюваної Системи із суміжними системами

Інформаційна система ТРЦ повинна підтримувати сумісність із суміжними системами за допомогою протоколів TCP/IP та технологій Ethernet на фізичних і логічних рівнях. Обов'язковим є підтримка протоколів HTTPS, DNS, SFTP, IEEE 802.11 для забезпечення обміну з внутрішніми сервісами, а також IoT-пристроями.

Формати передавання даних мають бути уніфіковані для взаєморозуміння між усіма компонентами. Найпоширенішими форматами є JSON і XML.

2.1.2.4 Вимоги до режимів функціонування Системи

Система повинна працювати у цілодобовому режимі, з можливістю безперервного обслуговування критичних підсистем, таких як відеоспостереження, системи контролю доступу, серверні ресурси, мережеве обладнання та IoT-пристрої.

У разі аварійного відключення живлення, система повинна автоматично переходити до режиму аварійного живлення через UPS та забезпечувати збереження критичних даних із подальшим автоматичним відновленням роботи після відновлення електропостачання. Система повинна мати режим планового технічного обслуговування. Резервне копіювання даних має виконуватись автоматично щодня, архіви мають зберігатися щонайменше 30 днів у захищеному сегменті мережі з обмеженим доступом.

2.1.2.5 Перспективи розвитку, модернізації Системи

Мережеве обладнання має оновлюватися відповідно до зростаючих вимог навантаження, зокрема замінюватися застарілі моделі мережних пристроїв на сучасні пристрої з підтримкою актуальних стандартів і розширених засобів захисту. Система повинна забезпечувати можливість масштабування, передбачаючи наявність резервних портів, IP-адрес та мережевих ресурсів для швидкого підключення нових відділів, підрозділів або сервісів. Архітектура мережі має бути гнучкою й відкритою для інтеграції сучасних технологічних рішень без потреби в повній перебудові інфраструктури, що забезпечить легке розширення та модернізацію системи.

2.1.3 Показники призначення

Система повинна забезпечувати ефективну роботу з високим рівнем доступності та продуктивності. Пропускна здатність мережі має відповідати навантаженню з боку відділів, а також забезпечувати одночасне обслуговування відвідувачів, систем відеонагляду, контролю доступу, IoT-пристроїв.

Затримка передачі даних між вузлами мережі не повинна перевищувати 50 мс для локального сегмента та 100 мс для зовнішніх з'єднань, щоб забезпечити швидке реагування на внутрішні запити та ефективну роботу служб інформаційних сервісів.

Рівень доступності повинен становити не менше 99,9% у місяць, а середній час відновлення після збою не повинен перевищувати 15 хвилин для критичних сервісів. Система має бути розрахована на цілодобову експлуатацію з урахуванням пікового навантаження у години максимальної відвідуваності ТРЦ.

Умови експлуатації обладнання повинні відповідати температурному режиму від +10°C до +35°C та при вологості не вище 80% при наявності вентиляції та стабільного живлення. Також система має відповідати вимогам щодо інформаційної безпеки, зокрема щодо фільтрації доступу, логічного розділення трафіку та використання сучасних протоколів шифрування для захисту даних у процесі передавання.

2.1.4 Додаткові вимоги

2.1.4.1 Вимоги до серверного приміщення

Серверне приміщення необхідно забезпечити оптимальними кліматичними умовами, підтримкою температури в межах 18-24 °C та відносної вологості 40-60%, що є необхідним для стабільної та надійної роботи обладнання. Серверне приміщення має бути оснащене системами кондиціювання та вентиляції з резервним живленням для запобігання перегріву і забезпечення безперервного функціонування. Пил, волога та сторонні предмети не повинні потрапляти до приміщення, оскільки це може призвести до пошкодження техніки. Доступ до серверної кімнати повинен бути обмежений лише для авторизованого персоналу з

використанням систем контролю доступу та відеоспостереження. Обладнання необхідно розміщувати на спеціальних стійках, що забезпечують належну циркуляцію повітря. Планове технічне обслуговування має проводитись регулярно, при цьому слід гарантувати безперервність роботи критичних сервісів завдяки використанню резервних рішень.

2.1.4.2 Вимоги до технічного обслуговування та ремонту

Обслуговування повинно включати регулярну перевірку фізичного стану обладнання, очищення від пилу, оновлення ПЗ, контроль стабільності живлення та виконання резервного копіювання даних. Пристрої, що виконують критично важливі функції – сервери, комутатори, маршрутизатори, мають проходити обслуговування не рідше одного разу на місяць. Офісне обладнання та персональні комп’ютери необхідно перевіряти мінімум раз на квартал, за умови відсутності ознак несправностей. У разі виходу з ладу окремих компонентів системи потрібно оперативно проводити ремонт на місці, або за необхідності замінювати їх на запасні пристрої, які мають бути наявні в спеціально відведеному сховищі. Ведення обліку всіх ремонтних та сервісних робіт є обов’язковим для оцінки технічного стану обладнання та ефективності використання ресурсів системи.

2.1.4.3 Потреба в персоналі для підтримки функціонування системи

Враховуючи обсяг мережі та кількість підрозділів, обслуговування системи має передбачати участь як технічного, так і аналітичного персоналу. Для забезпечення якісної підтримки необхідна участь кількох ключових фахівців. Системний адміністратор має відповідати за стабільну роботу серверного обладнання, своєчасне оновлення програмного забезпечення, контроль функціонування мережі та оперативне усунення збоїв. Мережевий інженер повинен здійснювати налаштування, оптимізацію та захист мережевих з’єднань, включаючи VLAN, комутатори та маршрутизатори. Технічний інженер забезпечує фізичне обслуговування обладнання, усуває несправності на місцях встановлення та відповідає за підключення нових пристроїв. Фахівець з кібербезпеки має розробляти політики безпеки, здійснювати моніторинг підозрілої активності та забезпечувати

захист інформації від внутрішніх і зовнішніх загроз.

Крім IT-фахівців, у підтримці стабільної та ефективної роботи системи важливою є роль спеціаліста з аналізу даних, який займається збором і обробкою інформації, підготовкою звітів, а також розробкою рішень для оптимізації функціонування інфраструктури. Також доцільно передбачити регулярне навчання персоналу або підвищення кваліфікації, що сприятиме зростанню продуктивності та забезпечить належний рівень технічного обслуговування.

2.1.4.4 Вимоги до кабель-каналів, інформаційних та електричних розеток

Кабель-канали мають бути з негорючих матеріалів, що відповідають вимогам пожежної безпеки відповідно до ДСТУ 4809:2007. Їхній переріз повинен мати запас від 20% до 30% для майбутньої модернізації або розширення мережі. Кабель-канали повинні мати можливість відкривання для доступу до кабелів у разі обслуговування чи заміни кабелів. В офісних приміщеннях кріплення кабель-каналів здійснюється вздовж стін або під стелею. У коридорах кріплення здійснюється за підвісною стелею або в загальних перфорованих лотках.

Інформаційні розетки повинні встановлюватись на робочих місцях користувачів. Для кожного робочого місця має бути щонайменше одна подвійна розетка RJ-45 категорії не нижче 6-ої. Розетки мають бути промарковані відповідно до схеми кабельної системи. Їх треба розмістити на висоті 25-30 см від підлоги або ж в спеціальних місцях на робочих столах. Електричні розетки повинні бути на кожному робочому місці, не менше двох на кожного співробітника. Потужність електромережі повинна забезпечувати одночасне під’єднання офісної техніки. Всі електричні точки мають бути заземлені відповідно до стандартів електробезпеки.

2.2 Розробка інженерних рішень для реалізації системи

2.2.1 Розробка структурної схеми технічних засобів

Для забезпечення ефективної роботи структурних підрозділів торгово-розважального центру комп'ютерна система поділяється на кілька локальних підмереж (LAN) відповідно до функціональних особливостей відділів. Понад 540 вузлів потрібно забезпечити, включаючи персональні комп'ютери, серверне обладнання, пристрої IoT та клієнтські точки доступу. Розподіл підмереж:

- LAN_1 – для відділу безпеки та оренди. Потребує забезпечення 63 мережевих вузлів;
- LAN_2 – призначений для відвідувачі і магазинів. Вимагає підтримки 206 вузлів, розподілених між VLAN90 – підмережа для відвідувачів, яка включає гостьові точки для підключення по Wi-Fi, VLAN100 – забезпечує підмережу для магазинів і торгових точок;
- LAN_3 – призначений для IT-відділу, серверної та технічного відділу, забезпечується 113 вузлів;
- LAN_4 – призначений для відділів маркетингу та аналітики. Передбачено 86 вузлів, які розподілені між VLAN70 – відділ маркетингу, VLAN80 – аналітичний відділ;
- LAN_5 – призначений для юридичного відділу VLAN40, фінансово-економічного відділу VLAN50, та адміністративного відділу. Потребує забезпечення 79 вузлів.

На канальному рівні застосовується технологія Ethernet як основа побудови локальної мережі. Для з'єднання між маршрутизаторами застосовується підключення Serial кабелями. Комутатори та маршрутизатори між собою спілкуються один з одним через прямі Ethernet-кабелі. Для об'єднання комутаторів між собою використовуються крос-кабель, для забезпечення ефективної взаємодії.

Інтеграція IoT-інфраструктури відбувається через окремі підмережі: LAN_1, що обслуговує відділ безпеки та оренди, та LAN_3, яка призначена для технічного обслуговування та IT-відділу. Усі компоненти відеоспостереження, пристрої кліматконтролю входять до середовища управління. Кожен поверх торгово-розважального

центра оснащується локальними системами клімат-контролю, датчиками температури та вологості, а також керованими кондиціонерами та зволожувачами повітря. Для забезпечення стабільного покриття Wi-Fi по всі території ТРЦ застосовуються точки доступу, які підключаються до мережі через Ethernet.

Комплексна система безпеки включає систему контролю доступу до приміщень відділень. RFID-зчитувачі та мітки, веб-камери та автоматизовані двері . Для забезпечення пожежної сигналізації встановлюються датчики диму, у разі виникнення загрози вони активують сигналізацію.

На структурній схемі, яка зображена на рисунку 2.1 наведено такі основні пристрої:

- маршрутизатори рівня ядра, які здійснюють маршрутизацію між сегментами мережі;
- маршрутизатор ISP для підключення до мережі інтернет;
- комутатори рівня доступу, що з’єднують ПК, сервери та точки доступу;
- AAA сервер для автентифікації та авторизації користувачів;
- HTTP, DNS сервер, який виконує запити на домен;
- IOT-сервер для керування розумними пристроями;
- точки доступу, які підключені через комутатори, для покриття бездротового доступу.

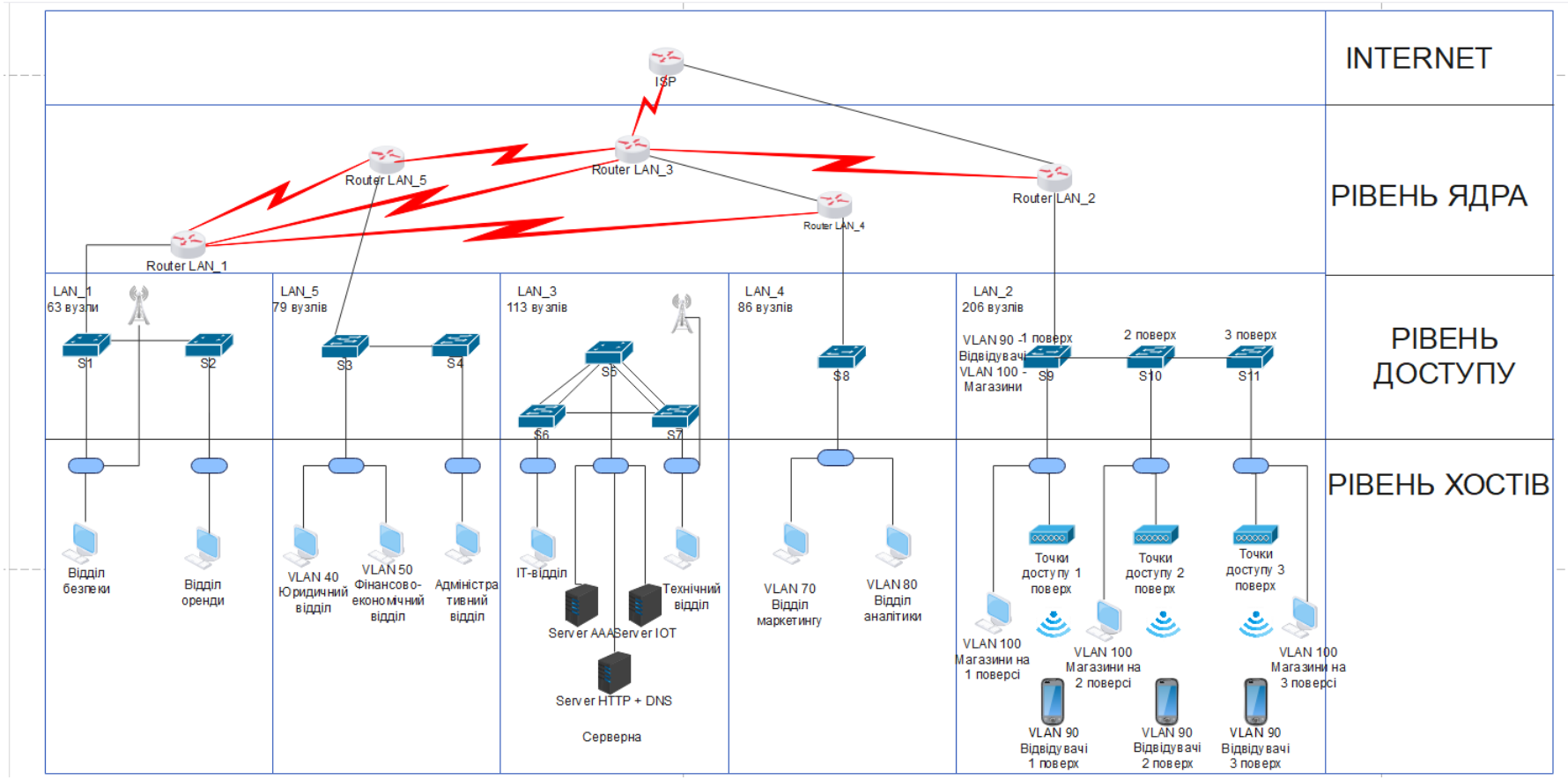

Рисунок 2.1 - Структурна схема засобів комп’ютерної системи

2.2.2 Розробка специфікації апаратних засобів комп'ютерної системи

Для побудови надійної комп'ютерної системи у ТРЦ виконується підбір обладнання, що відповідає вимогам масштабованості, продуктивності, безпеки та сумісності з іншими компонентами системи.

На етапі вибору маршрутизаторів розглядаються моделі Cisco 1941, Cisco 2911 та MikroTik CCR1009. Cisco 1941 забезпечує базовий рівень безпеки та підтримує VPN, але має обмежену масштабованість, меншу кількість портів GigabitEthernet, та має обмежену підтримку додаткових модулів, що ускладнює його використання у великій корпоративній мережі. MikroTik CCR1009 вирізняється високою продуктивністю, багатоядерний процесором та доступною ціною, однак складний інтерфейс налаштування та менш стабільна підтримка у корпоративному середовищі знижують доцільність його використання у проєкті.

Маршрутизатор Cisco 2911 демонструє оптимальний баланс між функціональністю, гнучкістю розширення за рахунок модулів і високим рівнем безпеки (VPN, фаєрвол, шифрування, IDS). Він має два інтегровані Gigabit Ethernet порти, три слоти для HWIC/SM-модулів, підтримку до 2 ГБ оперативної пам’яті, а також вбудовані засоби безпеки, включно з VPN, фаєрволом, шифруванням, механізмами виявлення атак (IDS/IPS) та підтримкою протоколів високої доступності. Завдяки можливості гнучкого розширення, централізованого керування та повної сумісності з іншим мережевим обладнанням Cisco, маршрутизатор Cisco 2911 обирається як основний елемент для реалізації міжмережевого зв’язку та організації доступу до інтернету в рамках комп’ютерної системи торгово-розважального центру.

Для організації дротового з’єднання між різними зонами та поверхами торгово-розважального центру розглядаються декілька моделей комутаторів: Cisco Catalyst 2960, Cisco Catalyst 3560 та TP-Link T2600G-28TS. Cisco Catalyst 2960 забезпечує підтримку важливих мережевих функцій, таких як VLAN, STP (Spanning Tree Protocol) і QoS (Quality of Service), а також має 24 порти, що дозволяє ефективно керувати мережевим трафіком у корпоративному середовищі. Cisco Catalyst 3560, крім цих можливостей, також підтримує маршрутизацію на рівні 3-го шару, однак

така функція є надмірною для завдань рівня доступу і значно підвищує вартість обладнання. Модель TP-Link T2600G-28TS пропонує бюджетний варіант з необхідними базовими функціями, але поступається у надійності, інтеграції з іншими компонентами мережі Cisco та рівні сервісної підтримки. З огляду на технічні вимоги, стабільність роботи та повну сумісність із наявними мережевими елементами, вибір зупиняється на комутаторі Cisco Catalyst 2960 як найбільш збалансованому та оптимальному рішенні для організації дротового з'єднання на рівні доступу.

Для покриття бездротової мережі в зонах загального користування розглядаються моделі Cisco Catalyst 9105AX, Ubiquiti UniFi 6 Lite та TP-Link EAP660 HD. Ubiquiti та TP-Link підтримують сучасний стандарт Wi-Fi 6 (802.11ax) і здатні обслуговувати велику кількість клієнтів одночасно, проте мають обмежену інтеграцію із системою управління Cisco та не забезпечують корпоративний рівень контролю доступу і безпеки. Cisco Catalyst 9105AX повністю сумісна з іншими компонентами мережі Cisco, підтримує 802.11ax, має розвинені функції безпеки, фільтрації трафіку та контролю доступу, що робить її ідеальним вибором для корпоративного середовища. Через це вибір робиться на користь точки доступу Cisco Catalyst 9105AX, яка гарантує стабільне, безпечне та кероване бездротове покриття.

Для організації обробки даних, зберігання інформації та підтримки ключових сервісів (HTTP, DNS, AAA, IoT) розглядаються сервери Cisco UCS C220 M4, Cisco UCS C240 M4 та HPE ProLiant DL380 Gen10. Модель Cisco UCS C220 M4 підходить для базових задач, однак має обмежені можливості масштабування, що може стати вузьким місцем у разі зростання навантаження. Сервер HPE ProLiant DL380 Gen10 демонструє високу потужність та надійність, але менш інтегрований у Cisco-інфраструктуру, що ускладнює централізоване управління і сумісність. Cisco UCS C240 M4 поєднує високу продуктивність, масштабованість, підтримку віртуалізації та централізоване управління через Cisco UCS Manager, що спрощує адміністрування та забезпечує гнучкість для майбутнього розвитку системи. Саме тому для розгортання серверних функцій обирається Cisco UCS C240 M4.

Таблиця 2.1 - Специфікація обладнання

№	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1.	Комутатор Cisco Catalyst 2960. 24 порти Ethernet 10/100 Мбіт/с, 2 порти Gigabit Ethernet (10/100/1000 Мбіт/с), Продуктивність до 6,5 млн пакетів/с, Пропускна здатність 16 Гбіт/с, Оперативна пам’ять (DRAM) 16 МБ	Cisco WS-C2960-24TT	од.	14	Специфікація пристрою: [10]
2.	Маршрутизатор Cisco 2911. 3 порти Fast Ethernet, 2 порти Gigabit Ethernet, Підтримка VPN, IPS, QoS, модульна архітектура, 512 MB DRAM, 256 MB Flash	Cisco 2911/K9	од.	5	Специфікація пристрою: [11]
3.	Бездротові точки доступу Cisco Catalyst 9105AX Series . підтримка стандарту 802.11n Wi-Fi 6, швидкість до 1/5 Гбіт/с, діапазони 2.4 GHz (2x2:2), 5 GHz (2x2:2)	Cisco C9105AXI-E	од.	45	Специфікація пристрою: [12]
4.	Сервер для мережевих сервісів. 2× Intel Xeon E5-2630 v 3, 32 GB DDR4 RAM, 2× SSD по 480 GB, RAID-контролер, 1× Gigabit Ethernet	Cisco UCS C240 M4	од.	3	Специфікація пристрою: [13]

Закінчення таблиці 2.1

5.	IoT-шлюз DLC-100. 2 × Ethernet (RJ-45, 10/100 Mbps), Підтримка Wi-Fi (802.11b/g/n), підтримка 3G/4G LTE через зовнішній USB-модем, Modbus TCP/RTU, MQTT— протоколи зв'язку	Cisco DLC-100	од.	2	Специфікація пристрою: [14]

Для проєктування структурованої кабельної системи (СКМ) розглянемо третій поверх. На основі цього створюється схема розміщення вузлів комп'ютерної мережі для відділів і магазинів, та проєктуємо топологію кабельних ліній, яка представлена на рисунку 2.2

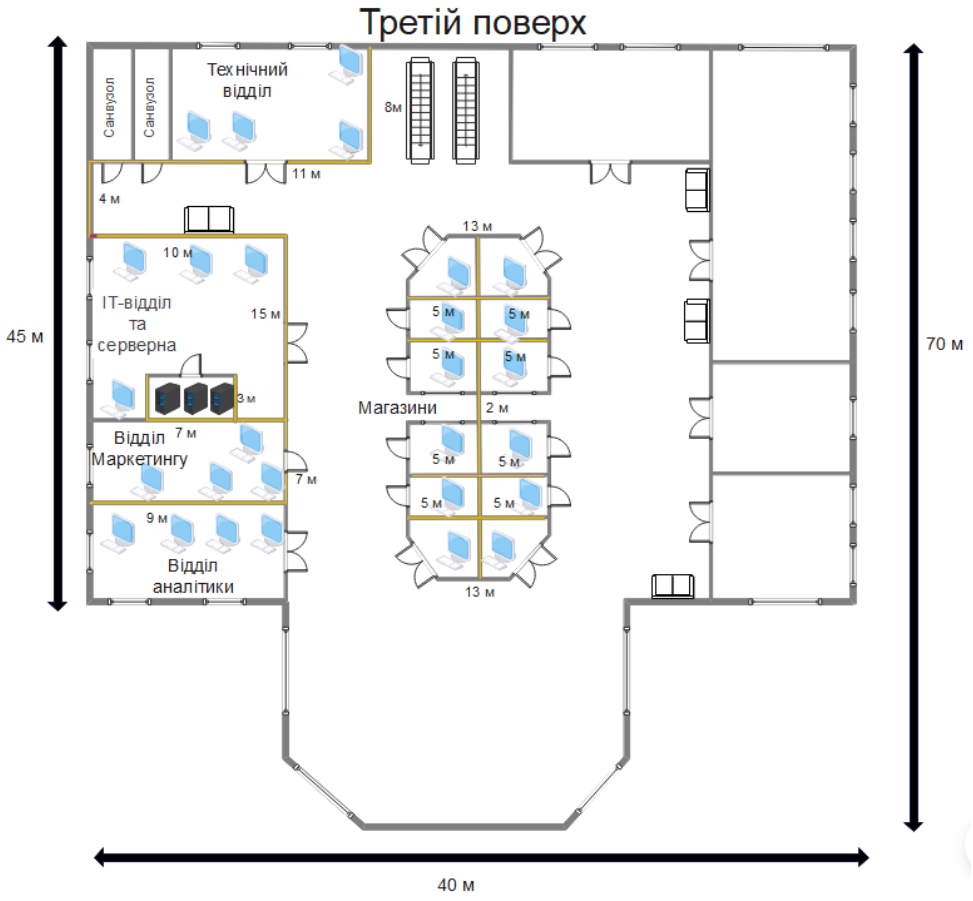

Рисунок 2.2 – Розміщення кабельних мереж на третьому поверсі ТРЦ

Для побудови структурованої кабельної системи на третьому поверсі

торгово-розважального центру ми аналізуємо декілька варіантів обладнання з урахуванням технічних характеристик, сумісності, надійності та відповідності сучасним стандартам.

Для підключення комп'ютерного обладнання розглядаються розетки категорії 6A від різних виробників, зокрема Legrand, Schneider Electric та Digitus. Зрештою, ми обираємо розетку Schneider Electric Actassi S-One Cat.6A, оскільки вона забезпечує високошвидкісну передачу даних (до 10 Гбіт/с), має зручну конструкцію для монтажу, сумісна з обраним кабелем і гарантує стабільну роботу в умовах інтенсивної експлуатації у відділах і магазинах ТРЦ.

Для прокладання сигнальних ліній ми розглядаємо кабель-канали від DKC, Legrand та Kopos. Після порівняння вартості, якості пластику та зручності монтажу, обираємо DKC 01140D (40×16 мм) для мережевого сегменту. Він достатньо місткий, міцний, має надійну фіксацію кришки та забезпечує охайний вигляд прокладки кабелів. Для силового сегменту, де не потрібна така ширина, вибираємо DKC 01125D (25×16 мм) — цього розміру достатньо для прокладки кабелів живлення.

Для організації електроживлення офісного та мережевого обладнання ми порівнюємо розетки Schneider Asfora, Legrand Valena та Viko. Вибір зупиняється на Schneider Asfora EPH2900321 — вона має якісну конструкцію, заземлення, відповідає європейським стандартам безпеки та естетично виглядає в інтер'єрі.

Живлення до розеток подається через кабель. Ми порівнюємо кілька варіантів від виробників «Одескабель», «Південкабель» та Nexans. Перевагу надаємо мідному кабелю ПВС 2×2.5 мм² від Одескабель, який демонструє хорошу гнучкість, стійкість до зовнішніх впливів і повністю відповідає нормам для внутрішніх електромереж.

Щодо мережевого кабелю, ми аналізуємо продукцію від Draka, Nexans та Hyperline. Для забезпечення надійної роботи гігабітного з'єднання в умовах підвищених електромагнітних завад обираємо Draka UC400 Cat.6A F/UTP з LSZH-оболонкою. Він гарантує високі швидкості передачі даних, екранування від завад і безпечне використання у публічних приміщеннях.

Для з'єднання комп'ютерів із розетками потрібні короткі надійні патч-корди.

Ми порівнюємо рішення від Digitus, LogiLink та Belkin. Найкращим варіантом є Digitus DK-1617-A-010/BL, оскільки він має високу якість конекторів, гнучкий кабель і повністю сумісний з обраними розетками. Вибір та обсяг СКС для третього поверху наведено в таблиці 2.2

Таблиця 2.2 – Специфікація СКС

№	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1.	Розетка комп'ютерна RJ45 кат.6A	Schneider Electric Actassi S-One	од.	27	Для відділів, магазинів
2.	Кабельний канал пластиковий 40x16	DKC 01140D	м	283	Для прокладання витої пари
3.	Розетка електрична з заземленням 16A, 250B	Schneider Asfora EPH2900321	од.	27	Для живлення офісного, торгового та мережевого обладнання
4.	Кабель живлення ПВС 2x25 мм, мідний	Одескабель	м	135	Для розеток живлення
5.	Кабельний канал 25x16 мм	DKC 01125D	м	135	Для прокладання електроживлення
6.	Кабель витої пари F/UTP	Draka UC400 Cat.6A LSZH Cca Euroclass	м	405	Для високошвидкісної передачі даних
7.	Мережевий патч-корд RJ45 Cat.6A, 1м	Digitus DK-1617-A-010/BL	од.	27	Підключення ПК до розеток

3. РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Для повного функціонування корпоративної комп'ютерної мережі необхідно правильно розподілити IP-адреси між різними локальними сегментами. Це дозволяє не лише забезпечити унікальність адрес для кожного пристрою, а й спростити адміністрування, підвищити безпеку й оптимізувати використання доступного адресного простору.

Надано блок адрес 172.25.76.0/22, який охоплює 1024 IP-адреси, починаючи від 172.25.76.0 і закінчуючи 172.25.79.255. З цього діапазону доступні 1022 адреси. З них дві мережеві та широкомовні адреси, які не використовуються у кожній підмережі. Цього цілком достатньо для задоволення потреб кожної локальної мережі.

Таблиця 3.1 – Кількість вузлів в підмережах ТРЦ

LAN_1	LAN_2	LAN_3	LAN_4	LAN_5
63	206	113	86	79

Щоб забезпечити оптимальний розподіл адрес, застосуємо VLSM (Variable Length Subnet Masking) – це метод, що дозволяє створювати підмережі з різною маскою, залежно від кількості вузлів, щоб забезпечити найкращий розподіл адрес. Під час цього процесу, адреси виділяються в порядку спадання, починаючи з підмережі з найбільшою кількістю пристроїв. Таблиця 3.2 містить розраховану схему адресації мережі ТРЦ.

Таблиця 3.2 Схема адресації

Назва підмережі	Розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
1	**2**	**3**	**4**	**5**	**6**
LAN_2	254	172.25.76.0	255.255.255.0	172.25.76.1 – 172.25.76.254	172.25.76.255
LAN_3	126	172.25.77.0	255.255.255.128	172.25.77.1 – 172.25.77.126	172.25.77.127

Закінчення таблиці 3.2

1	2	3	4	5	6
LAN_4	126	172.25.77.128	255.255.255.128	172.25.77.129 – 172.25.77.254	172.25.77.255
LAN_5	126	172.25.78.0	255.255.255.128	172.25.78.1 – 172.25.76.126	172.25.78.127
LAN_1	126	172.25.78.128	255.255.255.128	172.25.78.129 – 172.25.78.254	172.25.78.255
WAN_1	2	10.0.0.0	255.255.255.252	10.0.0.1 – 10.0.0.2	10.0.0.3
WAN_2	2	10.0.0.4	255.255.255.252	10.0.0.5 – 10.0.0.6	10.0.0.7
WAN_3	2	10.0.0.8	255.255.255.252	10.0.0.9 – 10.0.0.10	10.0.0.11
WAN_4	2	10.0.0.12	255.255.255.252	10.0.0.13 – 10.0.0.14	10.0.0.15
WAN_5	2	10.0.0.16	255.255.255.252	10.0.0.17 – 10.0.0.18	10.0.0.19
WAN_6	2	10.0.0.20	255.255.255.252	10.0.0.21 – 10.0.0.22	10.0.0.23
WAN_ISP	2	209.165.201.0	255.255.255.252	209.165.201.1 – 209.165.201.2	209.265.201.3
WAN_IPS_2	2	209.165.202.0	255.255.255.252	209.165.202.1 – 209.165.202.2	209.265.202.3

Поділ на дві логічні підмережі відбувається у LAN_2. Перша з них – це VLAN 90, яка відповідає за підключення відвідувачів, і займає адресу 172.25.76.0/25. Вона охоплює діапазон IP-адрес від 172.25.76.1 до 172.25.76.126, що забезпечує до 126 активних підключень. VLAN 100 є другою підмережею в межах LAN_2, яка призначена для підключення магазинів ТРЦ. Вона має адресу 172.25.76.128/26 з діапазоном 172.25.76.129 – 172.25.76.190, що забезпечує 62 доступні IP-адреси для пристроїв, які працюють у торгових точках.

У LAN_4 також реалізується логічне розділення на два окремих відділи. Для відділу маркетингу виділяється VLAN 70 з адресою 172.25.77.128/26. Це дозволяє підключити до 62 пристроїв у діапазоні від 172.25.77.129 до 172.25.77.190. Друга підмережа – VLAN 80, що обслуговує аналітичний відділ. Її адреса 172.25.77.192/26, з діапазоном 172.25.77.193 – 172.25.77.254.

В LAN_5 виконується поділ на три VLAN-підмережі. Для юридичного відділу створено VLAN_40, який має адресу 172.25.78.0/27, забезпечуючи 30 IP-адрес у діапазоні від 172.25.78.1 до 172.25.78.30. VLAN 50, що обслуговує фінансово-економічний відділ, займає наступний блок – 172.25.78.32/27, з діапазоном 172.25.78.33 – 172.25.78.62. Адміністративний відділ отримує адресу 172.25.78.64/26, яка дозволяє підключити до 62 пристроїв, використовуючи діапазон 172.25.78.65-172.25.78.126.

Наступним кроком є детальне адресування пристроїв мережі, таких як ПК, сервери, маршрутизатори, комутатори, точки доступу. Нижче представлено таблицю 3.3, яка відображає призначення IP-адрес для всіх основних пристроїв, які входять до складу мережевої інфраструктури.

Таблиця 3.3 Адресація пристроїв мережі

Ім’я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
1	**2**	**3**	**4**	**5**	**6**	**7**
LAN_1						
Ryndin_R_LAN_1	G0/0	172.25.78.129	255.255.255.128	-	-	Fa0/1
	Se0/0/0	10.0.0.1	255.255.255.252	-	-	Se0/0/0
	Se0/0/1	10.0.0.13	255.255.255.252	-	-	Se0/0/0
	Se0/1/0	10.0.0.9	255.255.255.252	-	-	Se0/0/1
PC1-PC5	NIC	172.25.78.130 – 172.25.78.134	255.255.25.128	172.25.78.129	-	Fa0/3 – Fa0/7
DLC100	Internet	172.25.78.138	255.255.255.128	172.25.78.129	-	Fa0/8
IoT1 – IoT10	Wireless	192.168.25.100	255.255.255.0	192.168.25.1	-	Wireless
LAN_5						
Ryndin_R_LAN_5	G0/0.1	172.25.78.65	255.255.255.192	-	1	Fa0/1
	G0/0.40	172.25.78.1	255.255.255.224	-	40	Fa0/1
	G0/0.50	172.25.78.33	255.255.255.224	-	50	Fa0/1
	Se0/0/0	10.0.0.2	255.255.255.252	-	-	Se0/0/0

Закінчення таблиці 3.3

1	2	3	4	5	6	7
	Se0/0/1	10.0.0.5	255.255.255.252	-	-	Se0/0/0
Ryndin_Switch3	Vlan 40	172.25.78.0	255.255.255.128	172.25.78.1	40	Fa0/3 – Fa0/12
Ryndin_Switch4	Vlan 1	172.25.78.64	255.255.255.192	172.25.78.65	1	Fa0/2 - Fa0/24
PC9–PC11	NIC	172.25.78.6 – 172.25.78.8	255.255.255.224	172.25.78.1	40	Fa0/5 – Fa0/7
PC12-PC14	NIC	172.25.78.38 – 172.25.78.40	255.255.255.224	172.25.78.33	50	Fa0/13 – Fa0/15
PC15-PC18	NIC	172.25.78.70 – 172.25.78.73	255.255.255.192	172.25.78.65	1	Fa0/2 – Fa0/5
LAN_3						
Ryndin_R_LAN_3	G0/0	172.25.77.1	255.255.255.128	-	-	Fa0/3
	G0/2	10.0.0.18	255.255.255.252	-	-	G0/2
	Se0/0/0	10.0.0.6	255.255.255.252	-	-	Se0/0/0
	Se0/0/1	10.0.0.10	255.255.255.252	-	-	Se0/1/0
	Se0/1/0	209.165.201.2	255.255.255.240	-	-	Se0/0/0
	Se0/1/1	10.0.0.21	255.255.255.252	-	-	Se0/0/0
PC19-PC26	NIC	172.25.77.6 – 172.77.13	255.255.255.128	172.25.77.1	-	Fa0/5 – Fa0/8
Server DNS + HTTP	NIC	172.25.77.2	255.255.255.128	172.25.77.1	-	Fa0/8
Server IoT	NIC	172.25.77.3	255.255.255.128	172.25.77.1	-	Fa0/6
Server AAA	NIC	172.25.77.4	255.255.255.128	172.25.77.1	-	Fa0/7
DLC 100	Internet	172.25.77.7	255.255.255.128	172.25.77.1	-	Fa0/9
IoT11 – IoT20	Wireless	192.168.25.100	255.255.255.0	192.168.25.1	-	Wireless
LAN_4						
Ryndin_R_LAN_4	G0/0.70	172.25.77.129	255.255.255.192	-	70	Fa0/1
	G0/0.80	172.25.77.193	255.255.255.192	-	80	Fa0/1
	G0/2	10.0.0.17	255.255.255.252	-	80	G0/2
	Se0/0/0	10.0.0.14	255.255.255.252	-	-	Se0/0/1

Закінчення таблиці 3.3

1	2	3	4	5	6	7
Ryndin_Switch8	Vlan 70	172.25.77.128	255.255.255.192	172.25.77.129	70	Fa0/2 – Fa0/10
	Vlan 80	172.25.77.192	255.255.255.192	172.25.77.193	80	Fa0/11 – Fa0/20
PC27-PC30	NIC	172.25.77.13 – 172.25.77.133	255.255.255.192	172.25.77.129	70	Fa0/2 – Fa0/5
PC31-PC34	NIC	172.25.77.194 - 172.25.77.197	255.255.255.192	172.25.77.193	80	Fa0/11 – Fa0/14
LAN_2						
Ryndin_R_LAN_2	G0/0	209.165.202.2	255.255.255.240	-	-	Fa0/1
	G0/1.90	172.25.76.1	255.255.255.128	-	90	Fa0/1
	G0/1.100	172.25.76.129	255.255.255.192	-	100	Fa0/1
	Se0/0/0	10.0.0.22	255.255.255.252	-	-	Se0/1/1
Ryndin_Switch9,10,11	Vlan 90	172.25.76.1	255.255.255.128	172.25.76.1	90	Fa0/1, Fa0/2, Fa0/6
	Vlan 100	172.25.76.128	255.255.255.192	172.25.76.129	100	Fa0/1, Fa0/2, Fa0/6
PC35-PC37	NIC	172.25.76.130 - 172.25.76.132	255.255.255.192	172.25.76.129	100	Fa0/13 – Fa0/15
Access-Point x9	Port 1	-	-	172.25.76.1	90	Fa0/2 - Fa0/4
Smartphone	Wireless	172.25.76.3 - 172.25.76.8	255.255.255.128	172.25.76.1	90	Wireless
Laptop x3	Wireless	172.25.76.11 - 172.25.76.13	255.255.255.128	172.25.76.1	90	Wireless
ISP	G0/1	209.165.202.1	255.255.255.240	-	-	G0/0
	Se0/0/0	209.165.201.1	255.255.255.240	-	-	Se0/1/0

3.2 Розробка топологічної схеми корпоративної мережі

Наступний крок – побудова топологічної схеми, яка візуально відображає з’єднання між маршрутизаторами, комутаторами, серверами кінцевими пристроями. Така схема не тільки дозволяє зрозуміти логіку з’єднань, а й дозволяє оцінити розміщення обладнання, структуру доступу до мережі та забезпечення зв’язку

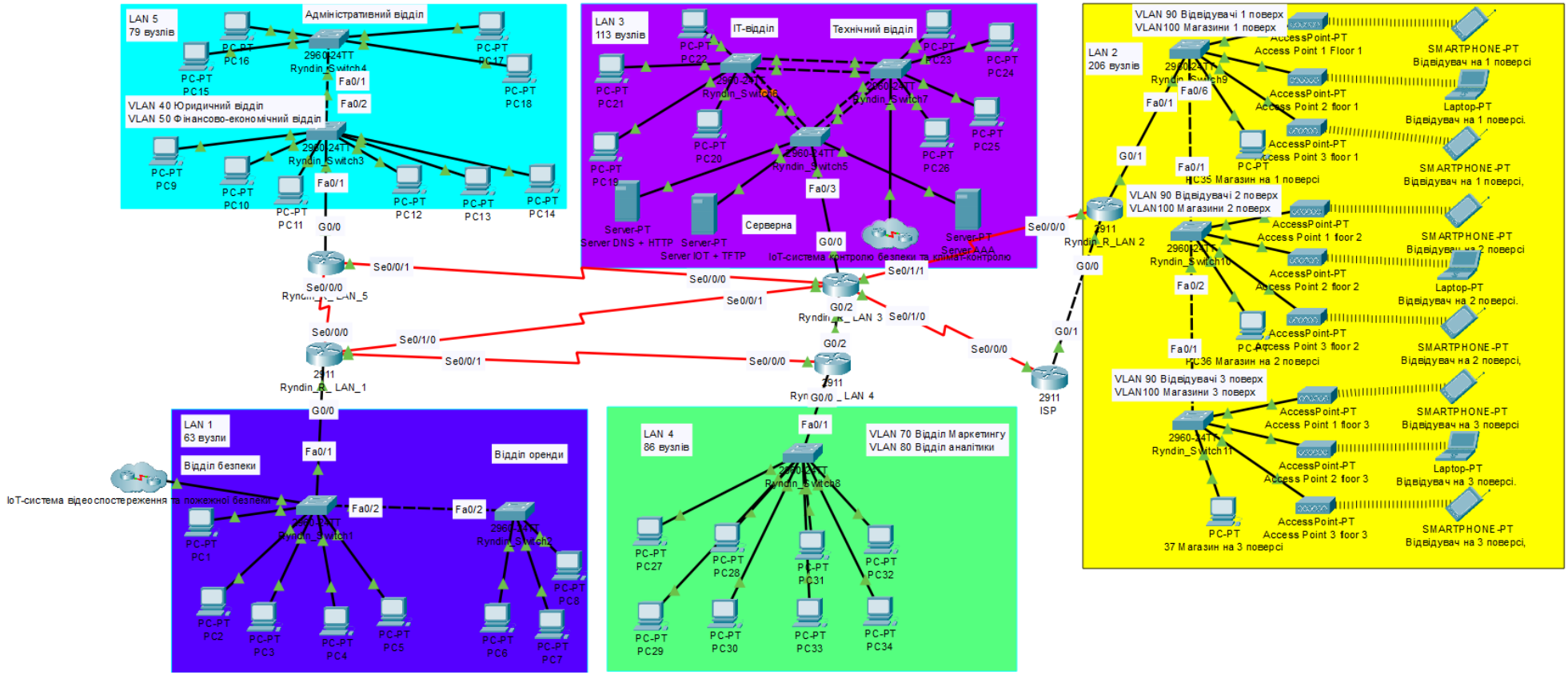

Рисунок 3.1 – Архітектура комп’ютерної системи ТРЦ

3.3 Впровадження та перевірка працездатності комп’ютерної системи

На початковому етапі було виконано фізичне підключення мережевого обладнання для забезпечення надійного зв’язку між усіма елементами системи. Для забезпечення безпеки та розподілу мережевого трафіку було введено сегментацію мережі за допомогою VLAN, які відповідають окремим службам та відділам. Це дозволяє ізолювати інформаційні потоки та контролювати доступ до ресурсів, які є критично важливими.

Маршрутизатори не тільки забезпечують міжмережеву взаємодію, але й розподіляють IP-адреси, що дозволяє оптимізувати роботу мережі без використання окремих серверів DHCP. Динамічний протокол OSPF використовується для міжмережевої маршрутизації, щоб забезпечити взаємодію між різними LAN та VLAN підмережами, це дозволяє автоматично оновлювати маршрути, оптимізуючи передачу даних у разі зміни мережевої інфраструктури або відмови окремих вузлів.

З метою виходу локальної мережі ТРЦ в Інтернет та захисту внутрішніх IP-адрес застосовано протокол NAT, який дозволяє перетворювати приватні адреси у публічні, приховуючи внутрішню структуру мережі та унеможливлюючи прямий доступ ззовні.

Значна увага приділяється налаштуванню основних серверів, серед яких AAA-сервер для управління доступом і автентифікацією користувачів, HTTP та DNS сервери, які обробляють запити та надають доступ до веб-ресурсів, а також IoT-сервер, що відповідає за збір , обробку та керування пристроями Інтернету речей у мережі ТРЦ. Відділ безпеки керує системою відеоспостереження, яка складається з IP-камер та вся інформація зберігається на IoT-сервері. Технічний відділ контролює інтелектуальні системи обігріву, вентиляції, освітлення, кондиціювання та контролю доступу.

3.3.1 Базова конфігурація мережевих пристроїв

Початкове налаштування мережевих пристроїв є важливим кроком для подальшої безпечної та стабільної роботи мережі. На цьому етапі необхідно створити захищені умови доступу до пристроїв, активувати шифрування даних і

запровадити звичайні методи контролю.

Базова конфігурація охоплює такі дії:

- надання унікального імені кожному пристрою для зручності ідентифікації;
- встановлення надійного паролю до привілейованого режиму;
- увімкнення сервісу шифрування паролів;
- обмеження доступу до консольного порту та ліній VTY;
- створення банера попередження MOTD, який інформує про правила доступу;

Фрагмент базових налаштувань на роутері Ryndin_R_LAN_1:

Router>en

Перехід у привілейований режим

Router#conf t

Перехід у режим глобальної конфігурації

Router(config)#hostname Ryndin_R_LAN_1

Зміна імені пристрою

Ryndin_R_LAN_1(config)#service password-encryption

Увімкнення шифрування паролів

Ryndin_R_LAN_1(config)#enable secret RyndinCisco123

Встановлення захищеного паролю для доступу до привілейованого режиму

Ryndin_R_LAN_1(config)#line console 0

Перехід до налаштування консольного порту

Ryndin_R_LAN_1(config-line)#password Ryndin123

Встановлення паролю для входу через консоль

Ryndin_R_LAN_1(config-line)#login

Увімкнення авторизації по паролю на консольному порті

Ryndin_R_LAN_1(config-line)#exit

Вихід з режиму налаштування лінії

Ryndin_R_LAN_1(config)#line vty 0 4

Перехід до налаштування віртуальних термінальних ліній

Ryndin_R_LAN_1(config-line)#password Ryndin123Cisco

Встановлення паролю для Telnet/SSH доступу

Ryndin_R_LAN_1(config-line)#login

Увімкнення запиту пароля при підключенні по VTY

Ryndin_R_LAN_1(config-line)#exit

Ryndin_R_LAN_1(config)#banner motd # 123-21-2 Ryndin. Access only for authorized personnel. #

Налаштування банера повідомлення

3.3.2 Налаштування динамічної маршрутизації за допомогою OSPF

Налаштування протоколу OSPF дозволяє маршрутизаторам автоматично обмінюватись маршрутною інформацією у межах мережі, що значно спрощує адміністрування у разі зміни топології. Цей протокол типу link-state, створює карту мережі з даними про кожне з’єднання, а потім обчислює найкоротші шляхи передачі даних. У конфігурації вказуються мережі, які маршрутизатор бачить, і область, в яку вони входять. Приклад налаштування OSPF на маршрутизаторі:

Ryndin_R_LAN_3> enable

Ryndin_R_LAN_3#conf t

Ryndin_R_LAN_3(config)#router ospf 1

Ініціація процесу OSPF з номером 1

Ryndin_R_LAN_3(config-router)#log-adjacency-changes

Увімкнення логування змін у сусідських зв’язках OSPF

Ryndin_R_LAN_3(config-router)#network 172.25.77.0 0.0.0.127 area 0

Додавання внутрішньої мережі

Ryndin_R_LAN_3(config-router)#network 10.0.0.4 0.0.0.3 area 0

Додавання мережі між маршрутизаторами

Ryndin_R_LAN_3(config-router)#network 10.0.0.8 0.0.0.3 area 0

Додавання мережі між маршрутизаторами

Ryndin_R_LAN_3(config-router)#network 10.0.0.16 0.0.0.3 area 0

Додавання мережі між маршрутизаторами

Ryndin_R_LAN_3(config-router)#network 10.0.0.20 0.0.0.3 area 0

Додавання мережі між маршрутизаторами

Ryndin_R_LAN_3(config-router)#network 209.165.201.0 0.0.0.15 area 0

Додавання мережі ISP

```
Ryndin_R_LAN_3(config)#do show 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 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O       10.0.0.0/30 [110/128] via 10.0.0.5, 04:49:02, Serial0/0/0
                    [110/128] via 10.0.0.9, 04:49:02, Serial0/0/1
C       10.0.0.4/30 is directly connected, Serial0/0/0
L       10.0.0.6/32 is directly connected, Serial0/0/0
C       10.0.0.8/30 is directly connected, Serial0/0/1
L       10.0.0.10/32 is directly connected, Serial0/0/1
O       10.0.0.12/30 [110/65] via 10.0.0.17, 04:48:32, GigabitEthernet0/2
C       10.0.0.16/30 is directly connected, GigabitEthernet0/2
L       10.0.0.18/32 is directly connected, GigabitEthernet0/2
C       10.0.0.20/30 is directly connected, Serial0/1/1
L       10.0.0.21/32 is directly connected, Serial0/1/1
     172.25.0.0/16 is variably subnetted, 10 subnets, 4 masks
O       172.25.76.0/25 [110/65] via 10.0.0.22, 04:49:02, Serial0/1/1
O       172.25.76.128/26 [110/65] via 10.0.0.22, 04:49:02, Serial0/1/1
C       172.25.77.0/25 is directly connected, GigabitEthernet0/0
L       172.25.77.1/32 is directly connected, GigabitEthernet0/0
O       172.25.77.128/26 [110/2] via 10.0.0.17, 04:48:32, GigabitEthernet0/2
O       172.25.77.192/26 [110/2] via 10.0.0.17, 04:48:32, GigabitEthernet0/2
O       172.25.78.0/27 [110/65] via 10.0.0.5, 04:49:02, Serial0/0/0
O       172.25.78.32/27 [110/65] via 10.0.0.5, 04:49:02, Serial0/0/0
O       172.25.78.64/26 [110/65] via 10.0.0.5, 04:49:02, Serial0/0/0
O       172.25.78.128/25 [110/65] via 10.0.0.9, 04:49:02, Serial0/0/1
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/28 is directly connected, Serial0/1/0
L       209.165.201.2/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0

Ryndin_R_LAN_3(config)#
```

Рисунок 3.2 – Таблиця маршрутизації OSPF Ryndin_R_LAN_3

```
Ryndin_R_LAN_1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C       10.0.0.0/30 is directly connected, Serial0/0/0
L       10.0.0.1/32 is directly connected, Serial0/0/0
O       10.0.0.4/30 [110/128] via 10.0.0.2, 04:47:59, Serial0/0/0
                    [110/128] via 10.0.0.10, 04:47:59, Serial0/1/0
C       10.0.0.8/30 is directly connected, Serial0/1/0
L       10.0.0.9/32 is directly connected, Serial0/1/0
C       10.0.0.12/30 is directly connected, Serial0/0/1
L       10.0.0.13/32 is directly connected, Serial0/0/1
O       10.0.0.16/30 [110/65] via 10.0.0.14, 04:47:44, Serial0/0/1
                     [110/65] via 10.0.0.10, 04:47:44, Serial0/1/0
O       10.0.0.20/30 [110/128] via 10.0.0.10, 04:48:09, Serial0/1/0
     172.25.0.0/16 is variably subnetted, 10 subnets, 4 masks
O       172.25.76.0/25 [110/129] via 10.0.0.10, 04:48:09, Serial0/1/0
O       172.25.76.128/26 [110/129] via 10.0.0.10, 04:48:09, Serial0/1/0
O       172.25.77.0/25 [110/65] via 10.0.0.10, 04:48:09, Serial0/1/0
O       172.25.77.128/26 [110/65] via 10.0.0.14, 04:48:09, Serial0/0/1
O       172.25.77.192/26 [110/65] via 10.0.0.14, 04:48:09, Serial0/0/1
O       172.25.78.0/27 [110/65] via 10.0.0.2, 04:47:59, Serial0/0/0
O       172.25.78.32/27 [110/65] via 10.0.0.2, 04:47:59, Serial0/0/0
O       172.25.78.64/26 [110/65] via 10.0.0.2, 04:47:59, Serial0/0/0
C       172.25.78.128/25 is directly connected, GigabitEthernet0/0
L       172.25.78.129/32 is directly connected, GigabitEthernet0/0
     209.165.201.0/28 is subnetted, 1 subnets
O       209.165.201.0/28 [110/128] via 10.0.0.10, 04:48:09, Serial0/1/0

Ryndin_R_LAN_1#
```

Рисунок 3.3 – Таблиця маршрутизації OSPF Ryndin_R_LAN_1

```
Ryndin_R_LAN_2(config)#do show 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, 7 subnets, 2 masks
O       10.0.0.0/30 [110/192] via 10.0.0.21, 05:48:38, Serial0/0/0
O       10.0.0.4/30 [110/128] via 10.0.0.21, 05:48:38, Serial0/0/0
O       10.0.0.8/30 [110/128] via 10.0.0.21, 05:48:38, Serial0/0/0
O       10.0.0.12/30 [110/129] via 10.0.0.21, 05:48:13, Serial0/0/0
O       10.0.0.16/30 [110/65] via 10.0.0.21, 05:48:13, Serial0/0/0
C       10.0.0.20/30 is directly connected, Serial0/0/0
L       10.0.0.22/32 is directly connected, Serial0/0/0
     172.25.0.0/16 is variably subnetted, 11 subnets, 4 masks
C       172.25.76.0/25 is directly connected, GigabitEthernet0/1.90
L       172.25.76.1/32 is directly connected, GigabitEthernet0/1.90
C       172.25.76.128/26 is directly connected, GigabitEthernet0/1.100
L       172.25.76.129/32 is directly connected, GigabitEthernet0/1.100
O       172.25.77.0/25 [110/65] via 10.0.0.21, 05:48:38, Serial0/0/0
O       172.25.77.128/26 [110/66] via 10.0.0.21, 05:48:13, Serial0/0/0
O       172.25.77.192/26 [110/66] via 10.0.0.21, 05:48:13, Serial0/0/0
O       172.25.78.0/27 [110/129] via 10.0.0.21, 05:48:38, Serial0/0/0
O       172.25.78.32/27 [110/129] via 10.0.0.21, 05:48:38, Serial0/0/0
O       172.25.78.64/26 [110/129] via 10.0.0.21, 05:48:38, Serial0/0/0
O       172.25.78.128/25 [110/129] via 10.0.0.21, 05:48:38, Serial0/0/0
     209.165.201.0/28 is subnetted, 1 subnets
O       209.165.201.0/28 [110/128] via 10.0.0.21, 05:48:38, Serial0/0/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/28 is directly connected, GigabitEthernet0/0
L       209.165.202.2/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1

Ryndin R LAN 2(config)#
```

Рисунок 3.5 - Таблиця маршрутизації OSPF Ryndin_R_LAN_2

```
Ryndin_R_LAN_4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.0.0.0/30 [110/128] via 10.0.0.13, 05:49:36, Serial0/0/0
O       10.0.0.4/30 [110/65] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
O       10.0.0.8/30 [110/65] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
C       10.0.0.12/30 is directly connected, Serial0/0/0
L       10.0.0.14/32 is directly connected, Serial0/0/0
C       10.0.0.16/30 is directly connected, GigabitEthernet0/2
L       10.0.0.17/32 is directly connected, GigabitEthernet0/2
O       10.0.0.20/30 [110/65] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
     172.25.0.0/16 is variably subnetted, 11 subnets, 4 masks
O       172.25.76.0/25 [110/66] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
O       172.25.76.128/26 [110/66] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
O       172.25.77.0/25 [110/2] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
C       172.25.77.128/26 is directly connected, GigabitEthernet0/0.70
L       172.25.77.129/32 is directly connected, GigabitEthernet0/0.70
C       172.25.77.192/26 is directly connected, GigabitEthernet0/0.80
L       172.25.77.193/32 is directly connected, GigabitEthernet0/0.80
O       172.25.78.0/27 [110/66] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
O       172.25.78.32/27 [110/66] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
O       172.25.78.64/26 [110/66] via 10.0.0.18, 05:49:06, GigabitEthernet0/2
O       172.25.78.128/25 [110/65] via 10.0.0.13, 05:49:36, Serial0/0/0
     209.165.201.0/28 is subnetted, 1 subnets
O       209.165.201.0/28 [110/65] via 10.0.0.18, 05:49:06, GigabitEthernet0/2

Ryndin_R_LAN_4#
```

Рисунок 3.5 - Таблиця маршрутизації OSPF Ryndin_R_LAN_4

```
Ryndin_R_LAN_5#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.0.0.0/30 is directly connected, Serial0/0/0
L       10.0.0.2/32 is directly connected, Serial0/0/0
C       10.0.0.4/30 is directly connected, Serial0/0/1
L       10.0.0.5/32 is directly connected, Serial0/0/1
O       10.0.0.8/30 [110/128] via 10.0.0.6, 05:54:32, Serial0/0/1
                    [110/128] via 10.0.0.1, 05:54:32, Serial0/0/0
O       10.0.0.12/30 [110/128] via 10.0.0.1, 05:54:32, Serial0/0/0
O       10.0.0.16/30 [110/65] via 10.0.0.6, 05:54:12, Serial0/0/1
O       10.0.0.20/30 [110/128] via 10.0.0.6, 05:54:32, Serial0/0/1
     172.25.0.0/16 is variably subnetted, 12 subnets, 4 masks
O       172.25.76.0/25 [110/129] via 10.0.0.6, 05:54:32, Serial0/0/1
O       172.25.76.128/26 [110/129] via 10.0.0.6, 05:54:32, Serial0/0/1
O       172.25.77.0/25 [110/65] via 10.0.0.6, 05:54:32, Serial0/0/1
O       172.25.77.128/26 [110/66] via 10.0.0.6, 05:54:12, Serial0/0/1
O       172.25.77.192/26 [110/66] via 10.0.0.6, 05:54:12, Serial0/0/1
C       172.25.78.0/27 is directly connected, GigabitEthernet0/0.40
L       172.25.78.1/32 is directly connected, GigabitEthernet0/0.40
C       172.25.78.32/27 is directly connected, GigabitEthernet0/0.50
L       172.25.78.33/32 is directly connected, GigabitEthernet0/0.50
C       172.25.78.64/26 is directly connected, GigabitEthernet0/0.1
L       172.25.78.65/32 is directly connected, GigabitEthernet0/0.1
O       172.25.78.128/25 [110/65] via 10.0.0.1, 05:54:32, Serial0/0/0
     209.165.201.0/28 is subnetted, 1 subnets
O       209.165.201.0/28 [110/128] via 10.0.0.6, 05:54:32, Serial0/0/1

Ryndin_R_LAN_5#
```

Рисунок 3.6 - Таблиця маршрутизації OSPF Ryndin_R_LAN_5

3.3.3 Налаштування маршрутизаторів для Інтернет-доступу через NAT

Для забезпечення виходу в інтернет з локальної мережі ТРЦ, були налаштовані два маршрутизатори з підтримкою NAT. Перший це граничний маршрутизатор Ryndin_R_LAN_3, на ньому налаштовано NAT, що дозволяє транслювати приватні IP-адреси в публічну для доступу до зовнішніх ресурсів. Другий маршрутизатор розміщений у сегменті LAN_2, який призначений для відвідувачів і магазинів. Він має свій власний канал, який дозволяє йому виходити в Інтернет, незалежно від внутрішньої мережі. Це забезпечує ізоляцію трафіку, що є важливим з міркувань безпеки. Налаштування NAT на граничному маршрутизаторі Ryndin_R_LAN_3 наведено нижче:

Ryndin_R_LAN_3(config)# int se0/1/0

Налаштування зовнішнього інтерфейсу, який підключений до провайдера

Ryndin_R_LAN_3(config-if)# ip address 209.165.201.2 255.255.255.240

Призначення публічної IP-адреси інтерфейсу

Ryndin_R_LAN_3(config-if)# ip nat outside

Призначення інтерфейсу як зовнішнього для NAT

Ryndin_R_LAN_3(config-if)#exit

Ryndin_R_LAN_3(config) ip access-list standard NAT_ACL

Створення ACL списку контролю доступу для NAT

Ryndin_R_LAN_3(config std-nacl)# permit 172.25.77.0 0.0.0.127

Дозвіл на трансляцію адрес

Ryndin_R_LAN_3(config std-nacl)# permit 172.25.78.0 0.0.0.127

Дозвіл на трансляцію адрес

Ryndin_R_LAN_3(config std-nacl)# permit 172.25.78.128 0.0.0.127

Дозвіл на трансляцію адрес

Ryndin_R_LAN_3(config std-nacl)# permit 172.25.77.128 0.0.0.127

Дозвіл на трансляцію адрес

Ryndin_R_LAN_3(config std-nacl)# permit 172.25.78.64 0.0.0.63

Дозвіл на трансляцію адрес

Ryndin_R_LAN_3(config std-nacl)# permit 172.25.77.192 0.0.0.63

Дозвіл на трансляцію адрес

Ryndin_R_LAN_3(config std-nacl)#exit

Ryndin_R_LAN_3(config)# int g0/1

Налаштування внутрішнього інтерфейсу

Ryndin_R_LAN_3(config-if)#ip nat inside

Позначення інтерфейсу як внутрішнього

Ryndin_R_LAN_3(config)# int g0/2

Налаштування внутрішнього інтерфейсу

Ryndin_R_LAN_3(config-if)#ip nat inside

Позначення інтерфейсу як внутрішнього

Ryndin_R_LAN_3(config-if)#int se0/0/0

Налаштування внутрішнього інтерфейсу

Ryndin_R_LAN_3(config-if)#ip nat inside

Позначення інтерфейсу як внутрішнього

Ryndin_R_LAN_3(config-if)#int se0/0/1

Налаштування внутрішнього інтерфейсу

Ryndin_R_LAN_3(config-if)#ip nat inside

Позначення інтерфейсу як внутрішнього

Ryndin_R_LAN_3(config-if)#exit

Ryndin_R_LAN_3(config)# ip nat inside source list NAT_ACL interface Serial0/1/0 overload

Увімкнення PAT, приватні адреси з ACL транслюються через IP зовнішнього інтерфейсу

Ryndin_R_LAN_3(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0

Додавання статичного маршруту за замовчуванням

Конфігурація ISP

ISP(config)# int se0/0/0

Інтерфейс з'єднання ISP з граничним маршрутизатором Ryndin_R_LAN_3

ISP(config-if)# ip address 209.165.201.1 255.255.255.240

Призначення IP-адреси

ISP(config-if)# ip nat outside

Позначення зовнішнього інтерфейсу

ISP(config-if)#exit

ISP(config)#ip route 0.0.0.0 0.0.0.0 Se0/0/0

Маршрут за замовчуванням

NAT Table for Ryndin_R_ LAN 3

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.201.2:5	172.25.77.10:5	209.165.202.1:5	209.165.202.1:5
icmp	209.165.201.2:11	172.25.77.197:11	209.165.202.1:11	209.165.202.1:11
icmp	209.165.201.2...	172.25.77.8:1	209.165.202.1:1	209.165.202.1...
icmp	209.165.201.2...	172.25.78.131:1	209.165.202.1:1	209.165.202.1...
icmp	209.165.201.2:8	172.25.78.138:8	209.165.202.1:8	209.165.202.1:8
icmp	209.165.201.2:1	172.25.78.8:1	209.165.202.1:1	209.165.202.1:1

Рисунок 3.7 – Таблиця NAT перетворювань на Ryndin_R_LAN_3

Налаштування маршрутизатора Ryndin_R_LAN_2 з гостьової мережі LAN_2 наведено нижче:

Ryndin_R_LAN_2(config)# int g0/0

Вхід в інтерфейс

Ryndin_R_LAN_2(config-if)# ip address 209.165.202.2 255.255.255.240

Призначення IP-адреси

Ryndin_R_LAN_3(config-if)#ip nat outside

Визначення інтерфейсу як зовнішнього для NAT

Ryndin_R_LAN_2(config)# int g0/1.90

Вхід в підінтерфейс

Ryndin_R_LAN_2(config-if)#ip nat inside

Визначення підінтерфейсу як внутрішнього для NAT

Ryndin_R_LAN_2(config)# int g0/1.100

Вхід в підінтерфейс

Ryndin_R_LAN_2(config-if)#ip nat inside

Визначення підінтерфейсу як внутрішнього для NAT

Ryndin_R_LAN_2(config) ip access-list standard LAN_2_POOL

Створення списку доступу

Ryndin_R_LAN_2(config std-nacl)# permit 172.25.76.0 0.0.0.127

Дозвіл на трансляцію адрес

Ryndin_R_LAN_2(config std-nacl)# permit 172.25.76.128 0.0.0.63

Дозвіл на трансляцію адрес

Ryndin_R_LAN_2(config)#ip nat pool LAN2_POOL 209.165.202.3 209.165.202.5 netmask 255.255.255.240

Заміна адреси внутрішньої мережі на інтернет адреси

Ryndin_R_LAN_2(config)# ip nat inside source list LAN_2_POOL interface G0/0 overload

Увімкнення PAT, приватні адреси з ACL транслюються через IP зовнішнього інтерфейсу

Конфігурація ISP

ISP(config)# Int g0/1

Вхід в інтерфейс

ISP(config-if)# 209.165.202.1 255.255.255.240

Призначення IP-адреси

ISP(config-if)#ip nat outside

Визначення інтерфейсу як зовнішнього для NAT

NAT Table for Ryndin_R_LAN 2

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.3:1027	172.25.76.10:1	209.165.202.1:1	209.165.202.1:1027
icmp	209.165.202.3:11	172.25.76.3:11	209.165.202.1:11	209.165.202.1:11
icmp	209.165.202.3:1026	172.25.76.5:1	209.165.202.1:1	209.165.202.1:1026
icmp	209.165.202.3:1025	172.25.76.6:1	209.165.202.1:1	209.165.202.1:1025
icmp	209.165.202.3:1024	172.25.76.7:1	209.165.202.1:1	209.165.202.1:1024

Рисунок 3.8 - Таблиця NAT перетворювань на Ryndin_R_LAN_2

3.3.4 Обмеження доступу для гостьового сегмента мережі

З метою забезпечення безпеки внутрішніх ресурсів ТРЦ, було реалізовано обмеження трафіку з гостьового сегмента мережі, який призначений для відвідувачів і магазинів. Цей сегмент не повинен мати доступу до локальних мереж відділів ТРЦ, щоб запобігти несанкціонованому доступу до службових даних і підвищити рівень мережевої ізоляції. Для впровадження цього обмеження використовуються списки контролю доступу ACL, які блокують трафік з гостьової мережі до інших корпоративних мереж. У той же час дозволено трафік у зворотному напрямку з внутрішніх мереж до гостьової, що дозволяє підтримувати адміністрування та спостереження. Реалізація наведена нижче:

Ryndin_R_LAN_2(config)#ip access-list extended LAN_2

Створення розширеного списку контролю доступу

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.0 0.0.0.127 172.25.77.0 0.0.0.127 echo

Заборона доступу з підмережі відвідувачів до LAN_3

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.0 0.0.0.127 172.25.78.0 0.0.0.127 echo

Заборона доступу з підмережі відвідувачів до LAN_5

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.128 0.0.0.63 172.25.77.0 0.0.0.127 echo

Заборона доступу з підмережі магазинів до LAN_3

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.128 0.0.0.63 172.25.78.0 0.0.0.127 echo

Заборона доступу з підмережі магазинів до LAN_5

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.0 0.0.0.127 172.25.77.128 0.0.0.63 echo

Заборона доступу з підмережі відвідувачів до LAN_4

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.128 0.0.0.63 172.25.77.128 0.0.0.63 echo

Заборона доступу з підмережі магазинів до LAN_4

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.0 0.0.0.127 172.25.77.192 0.0.0.63 echo

Заборона з підмережі відвідувачів до LAN_4

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.128 0.0.0.63 172.25.77.192 0.0.0.63 echo

Заборона доступу з підмережі магазинів до LAN_1

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.0 0.0.0.127 172.25.78.128 0.0.0.127 echo

Заборона з підмережі відвідувачів до LAN_1

Ryndin_R_LAN_2(config-ext-nacl)#deny icmp 172.25.76.128 0.0.0.63 172.25.78.128 0.0.0.127 echo

Заборона з підмережі магазинів до LAN_1

Ryndin_R_LAN_2(config-ext-nacl)#permit ip any any

Дозвіл на весь інший трафік

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Відвід...	PC25.	ICMP		0.000	N	0	(edit)	
	Failed	PC35 ...	PC32.	ICMP		0.000	N	1	(edit)	
	Failed	Відвід...	PC14.	ICMP		0.000	N	2	(edit)	
	Failed	Відвід...	PC8.	ICMP		0.000	N	3	(edit)	
	Failed	PC36 ...	PC18.	ICMP		0.000	N	4	(edit)	
	Failed	Відвід...	PC34.	ICMP		0.000	N	5	(edit)	

Рисунок 3.9 – Перевірка досяжності з мережі LAN_2 до інших мереж

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC14.	Відвідувач на ...	ICMP		0.000	N	0	(edit)	
	Successful	PC18.	PC35 Магазин...	ICMP		0.000	N	1	(edit)	
	Successful	PC20.	PC35 Магазин...	ICMP		0.000	N	2	(edit)	
	Successful	PC32.	Відвідувач на ...	ICMP		0.000	N	3	(edit)	
	Successful	PC3	37 Магазин на...	ICMP		0.000	N	4	(edit)	

Рисунок 3.10 – Перевірка досяжності з мереж LAN_1,3,4,5 до LAN_2

3.3.5 Призначення адрес у мережі за допомогою DHCP

У мережі торгово-розважального центру для автоматичної видачі IP-адрес використовується протокол DHCP, це спрощує підключення пристроїв і зменшує навантаження на адміністратора при обслуговуванні великої кількості клієнтів. Приклад налаштування DHCP на Ryndin_R_LAN_3

Ryndin_R_LAN_3(config)#int g0/0

Перехід до налаштування інтерфейсу

Ryndin_R_LAN_3(config-if)#ip address 172.25.77.1 255.255.255.128

Призначення IP-адреси та маски

Ryndin_R_LAN_3(config-if)#no shut

Увімкнення інтерфейсу

Ryndin_R_LAN_3(config)#ip dhcp excluded-address 172.25.77.1 172.25.77.5

Виключення перших п’яти адрес з пулу видачі

Ryndin_R_LAN_3(config)#ip dhcp pool LAN3

Створення пулу DHCP

Ryndin_R_LAN_3(dhcp-config)#network 172.25.77.0 255.255.255.128

Визначення підмережі для видачі IP-адрес

Ryndin_R_LAN_3(dhcp-config)#default-router 172.25.77.1

Вказання шлюзу за замовчуванням

Ryndin_R_LAN_3(dhcp-config)#dns-server 172.25.77.2

Призначення DNS-сервера

Ryndin_R_LAN_3(dhcp-config)#exit

```
Ryndin_R_LAN_3(config)#do show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.25.77.6      0030.F221.2B01           --                     Automatic
172.25.77.8      000D.BDCB.8E44           --                     Automatic
172.25.77.12     000B.BE2C.079E           --                     Automatic
172.25.77.7      0002.1614.4172           --                     Automatic
172.25.77.13     000A.41D6.6E32           --                     Automatic
172.25.77.14     00D0.BC3D.76A6           --                     Automatic
Ryndin_R_LAN_3(config)#
```

Рисунок 3.11 – Перевірка динамічної видачі IP-адрес

3.4 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.4.1 Інтеграція служби AAA на маршрутизаторах

Важливо, щоб у мережі ТРЦ доступ до маршрутизаторів був обмежений для авторизованих користувачів. Для цього було впроваджено систему AAA, яка дозволяє перевіряти ім’я користувача та пароль, визначати його права доступу, а також вести облік підключень.

Ryndin_R_LAN_3 (config)# aaa new-model

Увімкнення системи AAA на маршрутизаторі

Ryndin_R_LAN_3 (config)# radius-server host 172.25.77.4 key Ryndin123

Додавання Radius-сервера з IP-адресою

Ryndin_R_LAN_3 (config)# aaa authentication login AAA group radius

Створення методу автентифікації

Ryndin_R_LAN_3 (config)#line vty 0 4

Перехід до налаштування віртуальних термінальних ліній

Ryndin_R_LAN_3 (config)#login authentication AAA

Застосування методу автентифікації

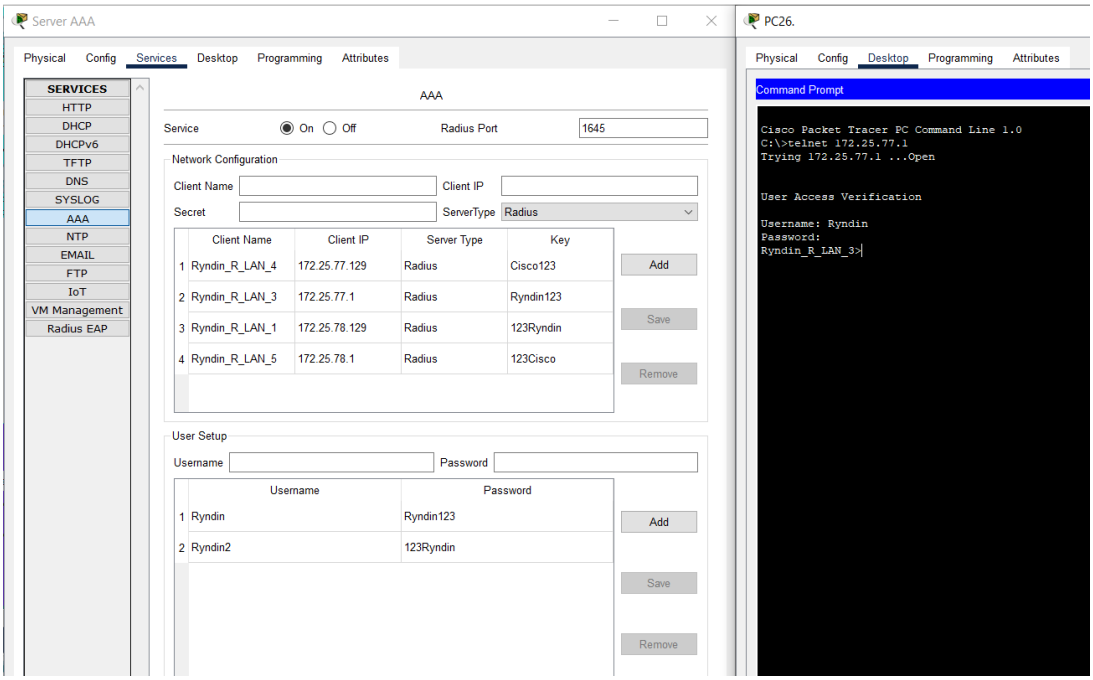

Рисунок 3.12 – Налаштування служби AAA на сервері та перевірка підключення

3.4.2 Налаштування мереж VLAN

Щоб розмежувати трафік між різними відділами та забезпечити уращу безпеку в мережі, були створені окремі VLAN. Вони дозволяють поділити мережу на логічні сегменти, якщо всі пристрої фізично з’єднані через одне обладнання.

Таблиця 3.4 – Назви VLAN

№	VLAN ID	Назва VLAN	Призначення
1	**2**	**3**	**4**
1	40	Legal	Юридичний відділ
2	50	Finance	Фінансово-економічний відділ
3	70	Marketing	Відділ маркетингу
4	80	Analytics	Аналітичний відділ
5	90	Guest	Для відвідувачів ТРЦ
6	100	Shop	Для магазинів ТРЦ

```
Ryndin_Switch3(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
40   Legal                            active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
50   Finance                          active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Ryndin_Switch3(config)#
```

Рисунок 3.13 – Налаштування VLAN на Ryndin_Switch3

```
Ryndin_Switch8(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
70   Marketing                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
80   Analytics                        active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Ryndin_Switch8(config)#
```

Рисунок 3.14 – Налаштування VLAN на Ryndin_Switch8

```
Ryndin_Switch9(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
90   Guest                            active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
100  Shop                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Ryndin_Switch9(config)#
```

Рисунок 3.15 - Налаштування VLAN на Ryndin_Switch9

Щоб забезпечити передачу трафіку між VLAN, треба налаштувати інтерфейс GigabitEthernet0/0 на маршрутизаторі Ryndin_R_LAN_4 з інкапсуляцією 802.1Q

Ryndin_R_LAN_4(config)#int g0/0.70

Створення підінтерфейсу для VLAN 70

Ryndin_R_LAN_4(config-subif)#encapsulation dot1Q 70

Встановлення інкапсуляції 802.1Q для VLAN 70 на підінтерфейсі

Ryndin_R_LAN_4(config-subif)#ip address 172.25.77.129 255.255.255.192

Призначення IP-адреси і маски для підінтерфейсу

Ryndin_R_LAN_4(config-subif)#exit

Ryndin_R_LAN_4(config)# int g0/0.80

Створення підінтерфейсу для VLAN 80

Ryndin_R_LAN_4(config-subif)#encapsulation dot1Q 80

Встановлення інкапсуляції 802.1Q для VLAN 80 на підінтерфейсі

Ryndin_R_LAN_4(config-subif)#ip address 172.25.77.193 255.255.255.192

Призначення IP-адреси і маски для підінтерфейсу

Ryndin_R_LAN_4(config-subif)#exit

Ryndin_R_LAN_4(config)# int g0/0

Ryndin_R_LAN_4(config-if)# no shut

Port Status Summary Table for Ryndin_R_ LAN 4

Device Name: Ryndin_R_ LAN 4
Device Model: 2911
Hostname: Ryndin_R_LAN_4

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	<not set>	<not set>	0000.0C4E.A1CD
GigabitEthernet0/0.70	Up	--	172.25.77.129/26	<not set>	0000.0C4E.A1CD
GigabitEthernet0/0.80	Up	--	172.25.77.193/26	<not set>	0000.0C4E.A1CD
GigabitEthernet0/1	Up	--	<not set>	<not set>	000A.F37B.919C
GigabitEthernet0/2	Up	--	10.0.0.17/30	<not set>	00D0.BA24.83BD
Serial0/0/0	Up	--	10.0.0.14/30	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Serial0/1/0	Down	--	<not set>	<not set>	<not set>
Serial0/1/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	000D.BD7E.5C8D

Рисунок 3.16 – Перегляд налаштувань на Ryndin_R_LAN_4

3.4.3 Налаштування порт-каналів PAgP

Використання порт-каналів з протоколом PAgP у системі допомагає об’єднати кілька фізичних з’єднань між комутатором в один логічний канал. Якщо один із фізичних портів вийде з ладу, трафік автоматично перенаправляється через інший канал, щоб мережа продовжувала працювати без перебоїв.

Ryndin_Switch6(config)#int range fa0/2-3

Вибір інтерфейсів для одночасного налаштування

Ryndin_Switch6(config-if-range)#switchport mode trunk

Встановлення режиму транк для передачі трафіку

Ryndin_Switch6(config-if-range)#channel-group 1 mode desirable

Об’єднання портів у порт-канал 1 з протоколом PAgP

Ryndin_Switch6(config)#int fa0/1

Вибір інтерфейсу

Ryndin_Switch6(config-if)#channel-group 2 mode desirable

Додавання порту до порт-каналу 2

Ryndin_Switch6(config-if)#int fa0/4

Вибір інтерфейсу

Ryndin_Switch6(config-if)# channel-group 2 mode desirable

Додавання порту до порт-каналу 2

```
Ryndin_Switch6(config)#do show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

1      Po1(SU)           PAgP   Fa0/2(P) Fa0/3(I)
2      Po2(SU)           PAgP   Fa0/1(P) Fa0/4(P)
Ryndin_Switch6(config)#
```

Рисунок 3.17 – Наявність PAgP

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Опис компонентів системи

З метою впровадження сучасних технологій, розробляється ряд важливих компонентів системи, щоб забезпечити безпеку та комфорт для відвідувачів і співробітників. Основна ідея полягає в інтеграції різних технологій, що дозволяють автоматизувати контроль доступу, регулювати мікроклімат у приміщеннях та вести постійний моніторинг об’єктів за допомогою відеоспостереження.

Система контролю доступу на основі RFID-технології є першим компонентом. Вона дозволяє ідентифікувати користувачів за допомогою RFID-міток, що значно спрощує вхід у зони з обмеженим доступом. Такий метод не тільки зручний, але й надзвичайно безпечний, оскільки доступ отримують лише співробітники.

Другий компонент – це комплексна система відеоспостереження та безпеки, яка включає забезпечення пожежної безпеки та моніторинг за допомогою відеокамер. У системі є можливість постійного відео контролю в важливих місцях ТРЦ, щоб виявити будь-які підозрілі дії та швидко реагувати на надзвичайні ситуації. До системи входять пожежні датчики та системи оповіщення, які автоматично повідомляють персонал про загрозу та дозволяють швидко евакуювати людей у разі небезпеки.

Третій компонент – система клімат-контролю, яка автоматично підтримує оптимальні умови у приміщеннях. Вона контролює температуру, вологість і вентиляцію, адаптуючись до змін навколишнього середовища.

4.1.1 Огляд і специфікація IoT-пристроїв

4.1.1.1 Розробка специфікації пристроїв для системи контролю доступу

У процесі створення сучасної системи контролю доступу ми обираємо IoT-пристрої, що відповідають високим вимогам надійності, сумісності, простоти інтеграції та функціональності. Усі елементи системи взаємодіють між собою для забезпечення безперебійного й безпечного доступу до приміщень, а також фіксації подій у реальному часі.

Для ідентифікації користувачів для доступу до приміщень відділів та серверної кімнати ми використовуємо RFID-картки HID iCLASS Seos 5006, що працюють на частоті 13.56 MHz за стандартом ISO/IEC 14443A. Ці мітки вирізняються високим рівнем криптографічного захисту (AES-128), стійкістю до підробки та забезпечують надійну ідентифікацію користувача. Це критично важливо для об’єктів, де необхідно запобігти несанкціонованому доступу.

У парі з картками застосовується зчитувач HID R10 iCLASS SE (модель 6100) компактний настінний пристрій, що підтримує багато популярних RFID-форматів, зокрема iCLASS, MIFARE, DESFire. Завдяки обмеженому радіусу зчитування (до 5 см) забезпечується точність і безпека авторизації, виключаючи можливість випадкового чи віддаленого зчитування.

Для візуального контролю за подіями на вході до серверної кімнати встановлюється мережева відеокамера Hikvision DS-2CD2046G2-I, яка має 4 Мп роздільну здатність, підтримує аналітичні функції (виявлення облич, перетин охоронної зони, виявлення вторгнення), і працює через ONVIF-протокол. Це забезпечує просту інтеграцію з іншими системами спостереження або контролю доступу. Для об'єднання всіх елементів системи (RFID-зчитувача, камери, розумних дверей) використовується IoT-шлюз Cisco IR1101. Цей пристрій дозволяє централізовано збирати, обробляти та передавати дані на локальний сервер або в хмару. Він підтримує численні протоколи зв’язку, забезпечує високу надійність та придатний для роботи в критичних умовах. Усі пристрої підключені до IoT-шлюзу Cisco IR1101 по захищеному бездротовому зв’язку. Шлюз виконує роль центрального вузла, через який відбувається взаємодія між компонентами системи, RFID-зчитувачами, відеокамерою. Дані з пристроїв надходять на шлюз, обробляються та передаються на сервер. Специфікацію наведено у таблиці 4.1.

Таблиця 4.1 – Специфікація IoT-пристроїв

Компонент	Модель/Тип	Призначення	Кількість	Примітка
1	**2**	**3**	**4**	**5**
RFID-мітка	HID iCLASS Seos 5006	Ідентифікатор співробітників	25	Специфікація компонента: [15]

Закінчення таблиці 4.1

RFID-зчитувач	HID R10 iCLASS SE 6100	Зчитувач міток	5	Специфікація компонента: [16]
Відеокамера	Hikvision DS-2CD2046G2-I	Спостереження за серверною кімнатою	1	Специфікація компонента: [17]
IoT-шлюз	Cisco IR1101	Збір і передача даних	1	Специфікація компонента: [18]
Блок живлення	Mean Well HDR-15-24	Живлення RFID-зчитувачів, IoT-шлюзу, камери	8	Специфікація компонента: [24]

4.1.1.2 Розробка специфікації пристроїв для системи відеоспостереження та протипожежної безпеки

Для відеоспостереження використовуються бездротові IP-камери, які спрощують монтаж і мінімізують кількість кабельних підключень. Зокрема, камера Hikvision DS-2CV1041G0-IDW1 підтримує Wi-Fi, має роздільну здатність 2 Мп, інфрачервоне підсвічування для нічного бачення до 30 метрів та функції виявлення руху, що дозволяє забезпечити надійний відеоконтроль у будь-який час доби.

Керування підсистемою пожежної безпеки здійснюється за допомогою одноплатного комп’ютера Raspberry Pi 4 Model B із 4 ГБ оперативної пам’яті, який виконує функції центрального контролера. До нього підключено провідний оптичний датчик диму Bosch FAP-420, що забезпечує надійне та своєчасне виявлення диму. Крім того, до системи інтегрована тривожна сигналізація, яка активує звукові й світлові оповіщення при виникненні пожежі. Для автоматичного гасіння пожежі застосовуються пожежні спринклери Rain Bird PESB, оснащені електромагнітними клапанами, що відкриваються за сигналом від контролера. Така система дозволяє швидко виявляти пожежу, оперативно інформувати персонал і локалізувати загрозу, мінімізуючи ризики для майна та безпеки людей.

Усі відеокамери бездротово під’єднуються до IoT-шлюзу Cisco IR1101, який виконує функцію мережевого вузла. Решта пристроїв: датчики диму та тривожна сигналізація, електромагнітні клапани підключені до центрального контролера. Контролер, у свою чергу, передає дані на IoT-шлюз, який здійснює централізовану обробку та надсилання інформації на сервер або в хмару. Таким чином,

забезпечується взаємодія між усіма елементами системи та оперативне реагування в разі надзвичайної ситуації. Специфікацію наведено нижче у таблиці 4.2.

Таблиця 4.2 – Специфікація пристроїв

Компонент	Модель/Тип	Призначення	Кількість	Примітка
1	**2**	**3**	**4**	**5**
Бездротова IP-камера	Hikvision DS-2CV1041G0-IDW1	Відеоспостереження	10	Специфікація компонента: [19]
Центральний контролер	Raspberry Pi 4 Model B (4 ГБ)	Керування пожежною безпекою	1	Специфікація компонента: [20]
Датчик диму та тривожна сигналізація	Bosch FAP-420	Виявлення диму, підключення до плати керування	2	Специфікація компонента: [21]
Пожежні спринклери	Tyco TY3251	Автоматичне гасіння пожежі	40	Специфікація компонента: [22]
Електромагнітний клапан	Rain Bird PESB	Керує подачею води в спринклер	3	Специфікація компонента: [23]
IoT-шлюз	Cisco IR1101	Збір і передача даних	1	Специфікація компонента: [25]
Блок живлення для відеокамер	Hikvision 12V DC Power Adapter	Живлення IP-камер	10	12V, сумісний із моделлю відеокамери DS-2CV1041G0-IDW1
Блок живлення для центрального контролера	Raspberry Pi Power Supply 5.1V 3A	Живлення одноплатного комп’ютера	1	Специфікація компонента: [26]
Блок живлення для клапанів	Блок живлення 220/24V AC, 0,6 A,	Для електромагнітних клапанів 24В систем поливу і водопостачання	3	Специфікація компонента: [27]

4.1.1.3 Розробка специфікації пристроїв для системи клімат-контролю

Для автоматичного регулювання температурного режиму в системі клімат-контролю торговельно-розважального центру використовується сучасне IoT-обладнання з підтримкою стандартних протоколів (MQTT, HTTP, Modbus TCP), що дозволяє інтегруватися з IoT шлюзом Cisco IR1101. Кондиціонери Daikin Stylish FTXA-AW оснащені вбудованим Wi-Fi інтерфейсом (модуль BRP15A81), який забезпечує бездротове підключення до шлюзу Cisco IR1101. Через цей модуль кондиціонери отримують команди на увімкнення/вимкнення, регулювання

температури та режимів роботи, а також передають телеметричні дані (поточна температура, стан пристрою, енергоспоживання) на центральний сервер для моніторингу та аналітики.

Обігрівачі Heatzy Pilote Wi-Fi мають вбудований Wi-Fi модуль керування, що дозволяє віддалено включати або вимикати обігрівачі через IoT-шлюз. Управління здійснюється на основі даних із сенсорів температури та сценаріїв роботи, налаштованих у центральній системі.

Сенсори температури і вологості Shelly H&T передають виміри за допомогою Wi-Fi безпосередньо на шлюз, використовуючи MQTT протокол. Ці дані використовуються для оперативного коригування режимів клімат-контролю.

Датчики руху Aqara Motion Sensor P1 працюють по протоколу Zigbee і підключаються до Zigbee-шлюзу, який інтегрується з Cisco IR1101. Виявлення присутності людей дозволяє автоматично регулювати освітлення та клімат у зоні їх перебування, підвищуючи енергоефективність.

Вентиляційні установки Systemair SAVE VSR 300 оснащені Ethernet-модулем з підтримкою TCP, що забезпечує дротове підключення до IoT-шлюзу. Вентиляція працює під централізованим управлінням, реагуючи на дані сенсорів вологості та температури для підтримки оптимального мікроклімату.

Розумні LED лампи Signify (Philips) Interact Ready LED Panel 600x600 40W мають Ethernet PoE модулі, що забезпечують стабільне підключення та живлення через кабель. Управління освітленням відбувається в реальному часі, з можливістю автоматичного регулювання яскравості і увімкнення/вимкнення залежно від часу доби, сценаріїв або наявності людей у зоні.

Живлення всіх пристроїв забезпечується за допомогою стандартної електромережі 220 В (для кондиціонерів, обігрівачів і вентиляції), батарейок (для бездротових сенсорів і датчиків руху) або PoE (для розумного освітлення), що забезпечує надійну роботу й інтеграцію в IoT-екосистему через шлюз Cisco IR1101. Специфікацію наведено нижче в таблиці 4.3.

Таблиця 4.3 – Специфікація пристроїв

Виконуваний пристрій	IoT-компонент/модуль	Тип підключення	Кількість	Примітка
1	**2**	**3**	**4**	**5**
Кондиціонер Daikin Stylish FTXA-AW	Daikin Wi-Fi Interface Module (BRP15A81)	Wireless	2	Вбудований модуль BRP15A81 для підключення по Wi-Fi та керування через IoT-шлюз
Обігрівач Heatzy Pilote Wi-Fi	Heatzy Wi-Fi Control Module	Wireless	2	Wi-Fi модуль для керування через шлюз
Сенсор температури та вологості Shelly H&T	Shelly H&T Wi-Fi Module	Wireless	4	Wi-Fi модуль для передачі даних температури та вологості
Датчик руху Aqara Motion Sensor P1	Aqara Zigbee Motion Sensor Module	Wireless	6	Zigbee модуль, дані передаються через Zigbee-шлюз, який підключається до шлюзу
Вентиляційна установка Systemair SAVE VSR 300	Systemair Modbus TCP Communication Module	Wired	3	Ethernet модуль для підключення по Modbus TCP до шлюзу
Розумна LED лампа Signify Interact LED Panel	Signify Interact Ethernet PoE Module	Wired	15	Ethernet PoE модуль для живлення та керування освітленням через шлюз

4.2 Налаштування моделі IoT у системі

4.2.1 Реалізація системи контролю доступу

Система контролю доступу реалізована на третьому поверсі ТРЦ, використовується п’ять дверей, обладнаних по одному RFID-зчитувачу. Кожен зчитувач відповідає за відкриття дверей лише при наявності коректної RFID-мітки, що гарантує, що доступ отримують лише уповноважені особи. Всі події доступу контролюються центральним сервером, який фіксує стан та інформацію про кожен підключений IoT пристрій. Особливу увагу приділено серверній кімнаті, при

відкриванні дверей автоматично запускається відеозапис, це дозволяє не лише контролювати вхід, а й дозволяє вести запис будь-яких дій, що підвищуж рівень безпеки.

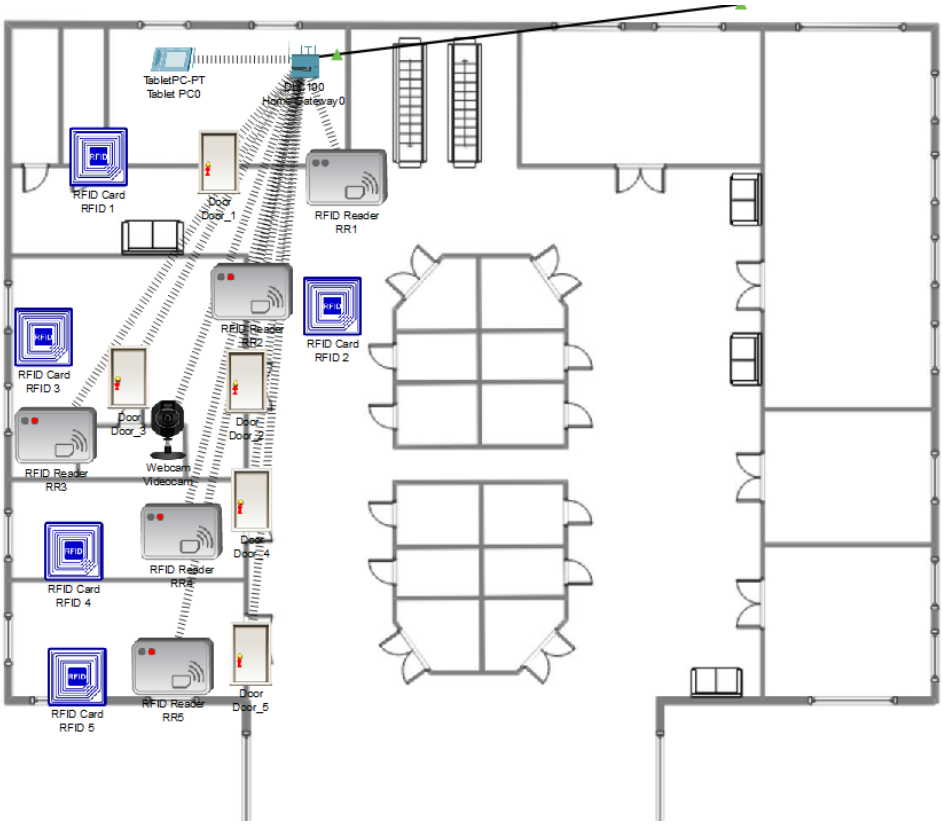

Рисунок 4.1 – Структурна схема системи контролю доступу

Маршрутизатор типу HomeGateway DLC100 підтримує технологію Wi-Fi, яка дозволяє IoT-пристроям взаємодіяти один з одним. Цей маршрутизатор гарантує стабільне бездротове підключення, керуючи зв’язком усіх компонентів системи.

Таблиця 4.4 – Параметри HomeGateway

Параметр	Значення
1	**2**
IP-адреса LAN	192.168.25.1
Маска	255.255.255.0
SSID	Tech
Спосіб автентифікації	WPA-2-PSK AES
Пароль	Ryndin123

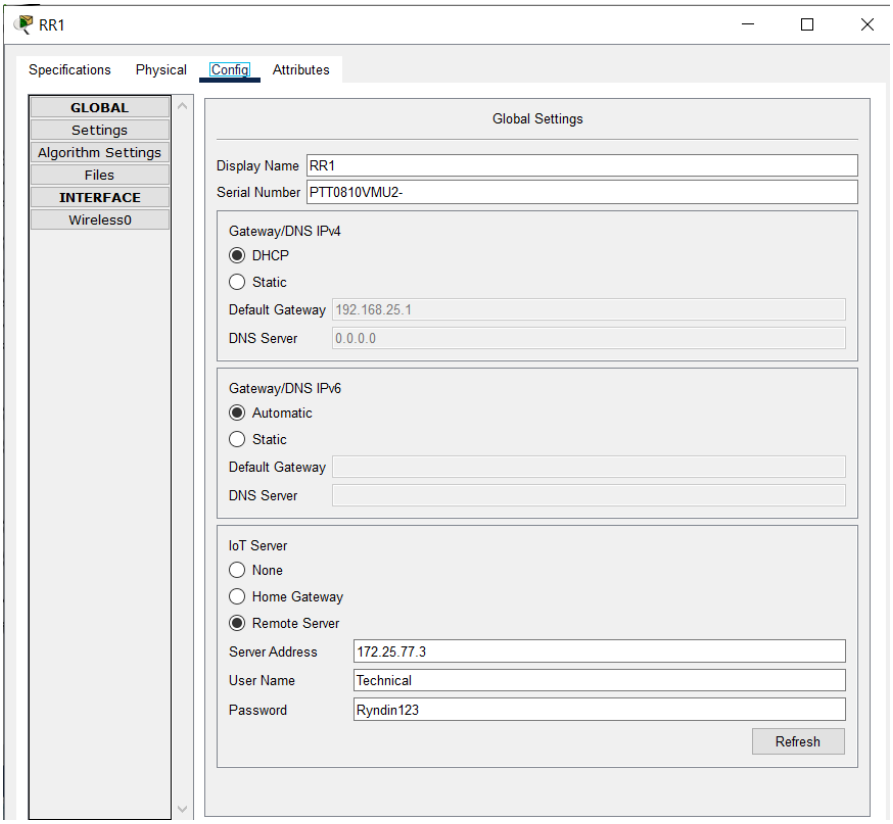

Рисунок 4.2 – Під’єднання RFID зчитувача до HomeGateway та до віддаленого сервера

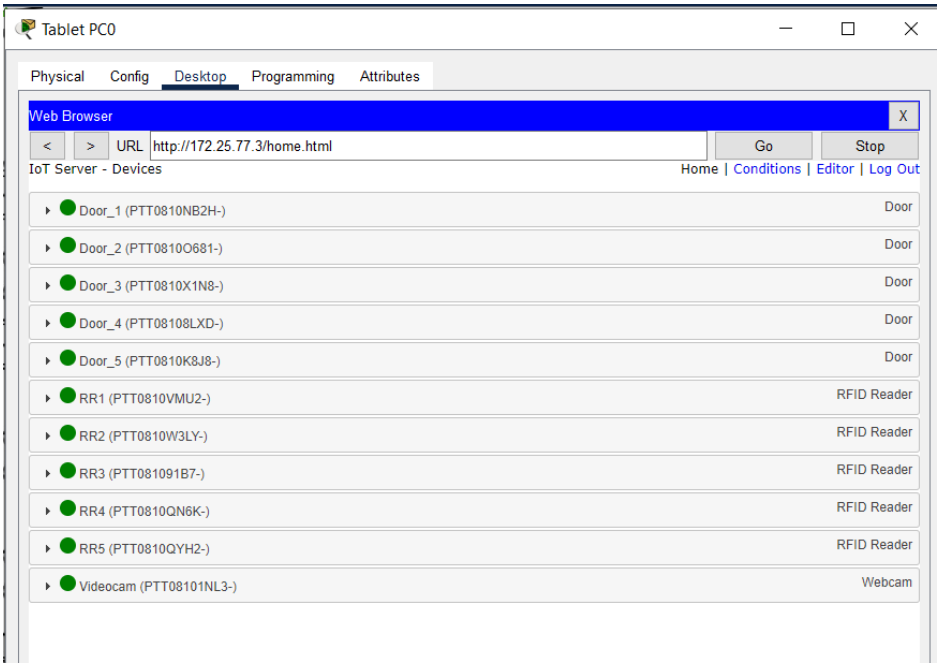

Рисунок 4.3 – Відображення всіх підключених IoT-пристроїв на віддаленому сервері

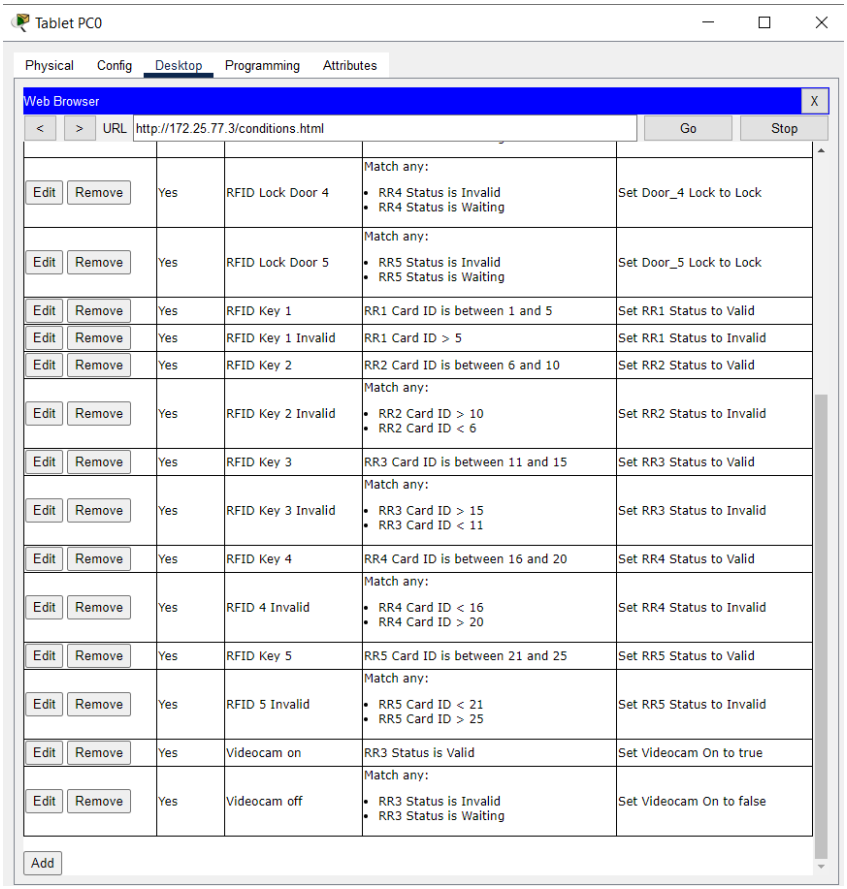

Рисунок 4.4 – Реалізація сценарію для доступу

При піднесенні коректної RFID-мітки до RFID зчитувача у серверній кімнаті, в нас повинні відчинитись двері та починатись відеозапис.

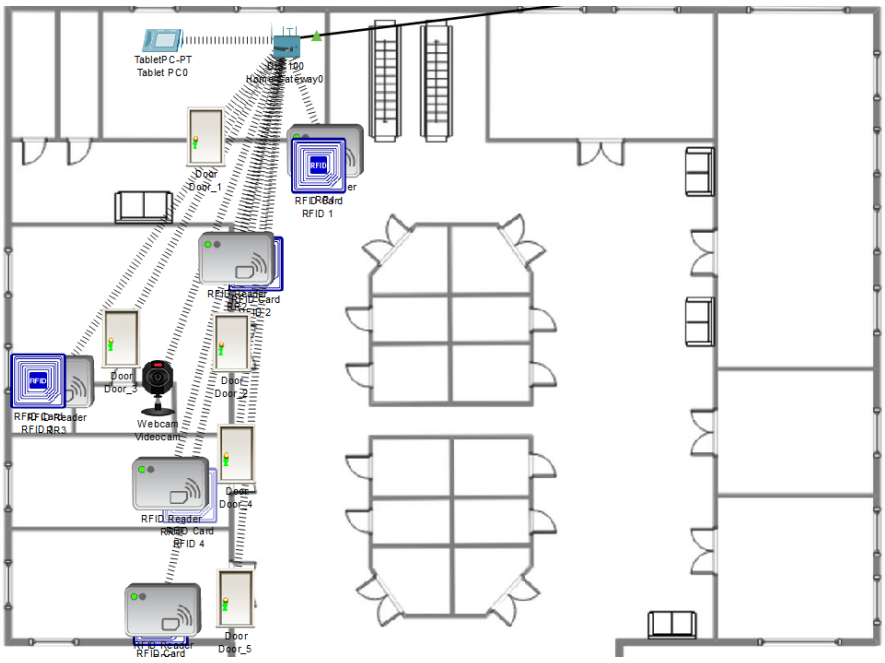

Рисунок 4.5 – Перевірка роботи правил, все спрацювало правильно

4.2.2 Налаштування системи відеоспостереження та пожежної безпеки

Для забезпечення високого рівня безпеки в приміщеннях ТРЦ, було впроваджено дві критично важливі системи: відеоспостереження та пожежної безпеки. Їх інтеграція дозволяє здійснювати цілодобовий контроль за станом об’єкта та оперативно реагувати на надзвичайні події.

Система відеоспостереження побудована на основі IP-камер, які розташовані по всьому першому поверху. Відеокамери працюють у постійному режимі, забезпечуючи безперервну трансляцію зображення до сервера зберігання. Для забезпечення пожежної безпеки використовуються розпилювачі на стелі, які рівномірно найбільш вразливі ділянки поверху. Для сповіщення персоналу й відвідувачів встановлено дві сирени, що активуються одночасно. Управління підсистемою здійснюється через мережу за допомогою IoT-обладнання, підключеного до IoT-сервера.

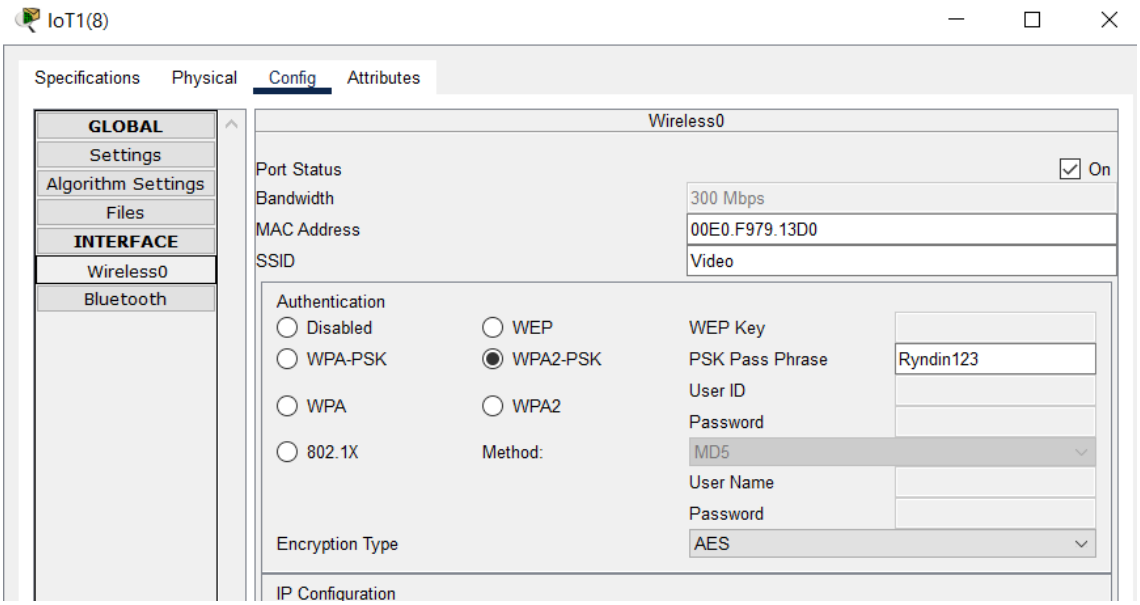

Рисунок 4.6 – Приклад підключення відеокамери

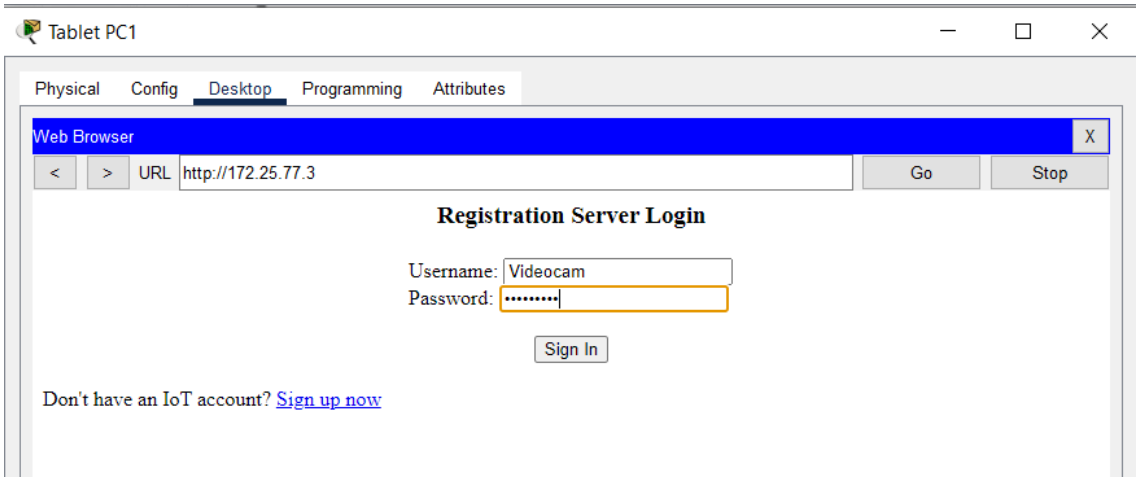

Рисунок 4.7 – Вхід до сервера, на якому містяться пристрої

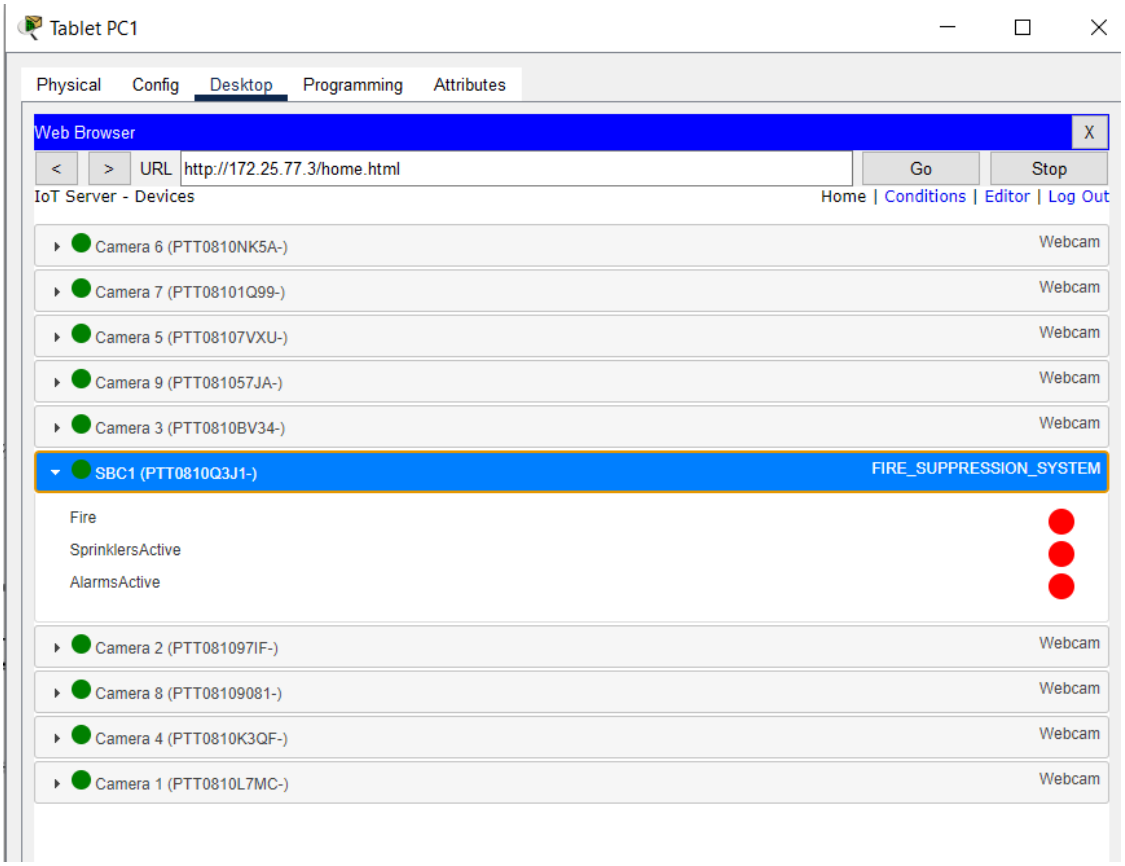

Рисунок 4.8 – Повний перелік пристрої підсистеми

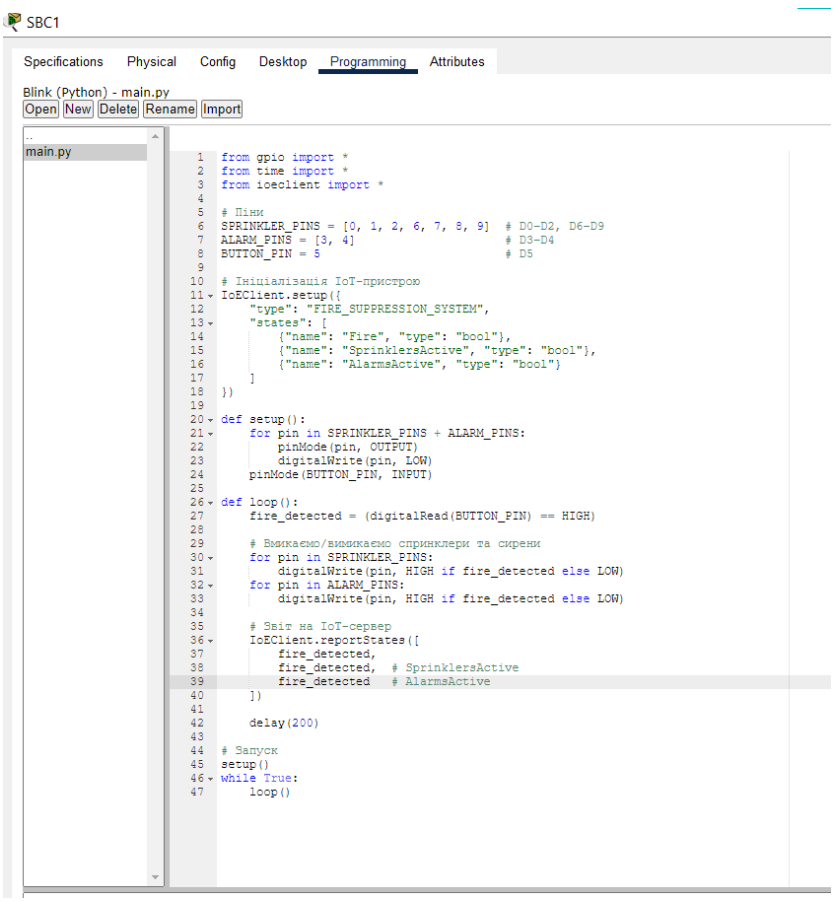

Рисунок 4.9 – Код контролера, в якому реалізується увімкнення розпилювачів та сирени при пожежі

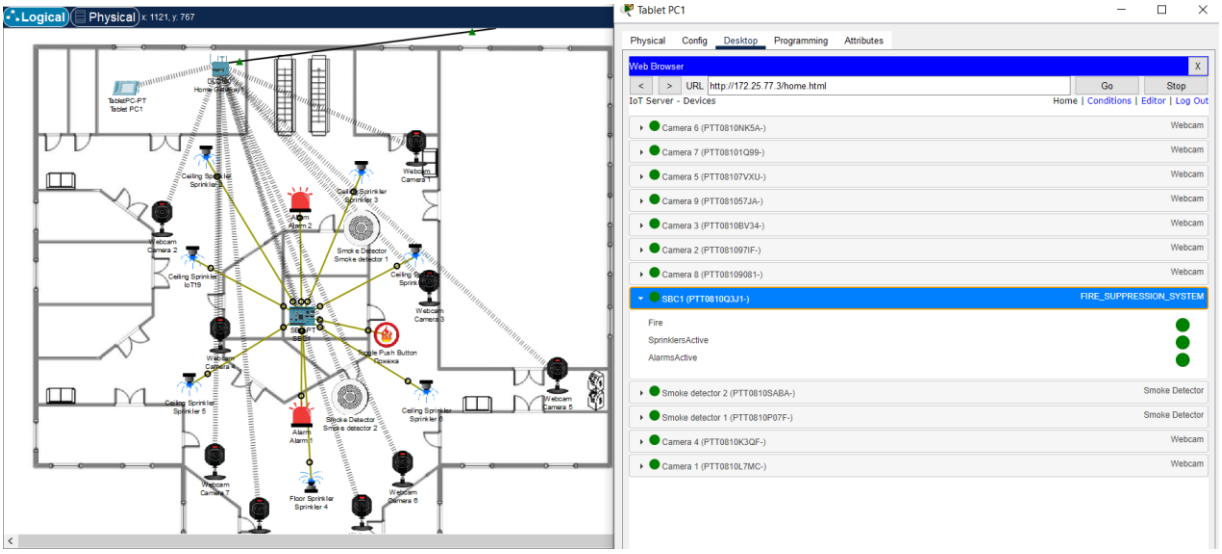

Рисунок 4.10 – Перевірка працездатності при пожежі

4.2.3 Налаштування Системи клімат-контролю

Підсистема працює за допомогою налаштованих сценаріїв, які реагують на показники з датчиків температури, вологості та руху. Ці сценарії активують

опалення при зниженні температури нижче встановленого рівня, і запускають кондиціонери, коли температура підвищується понад встановлений рівень. Вентиляція налаштовується від рівня вологості, щоб створити ідеальний мікроклімат на поверсі.

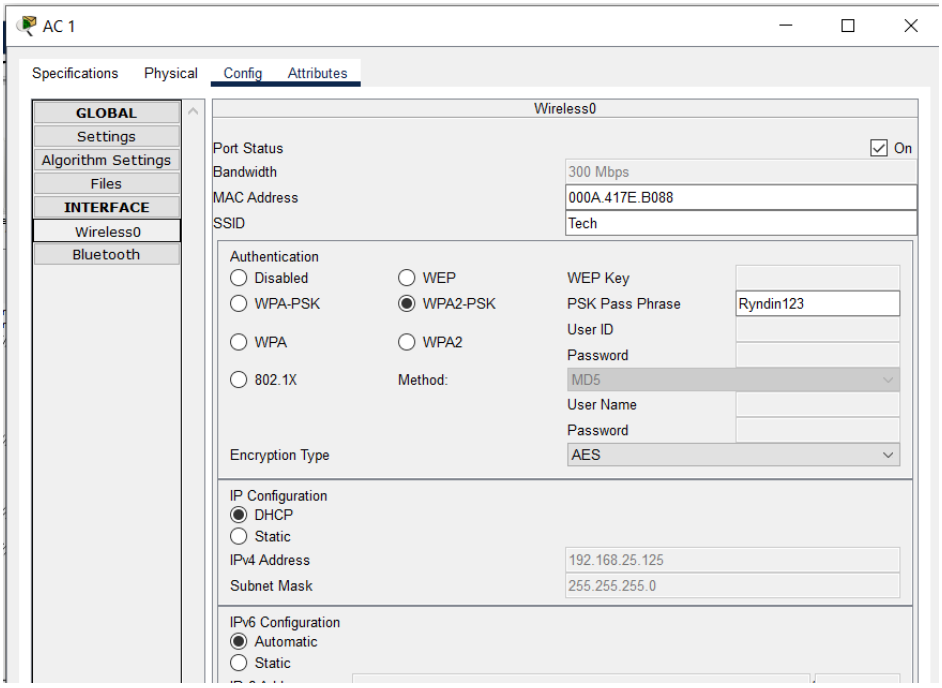

Рисунок 4.11 – Налаштування IoT-пристроїв на прикладі кондиціонера

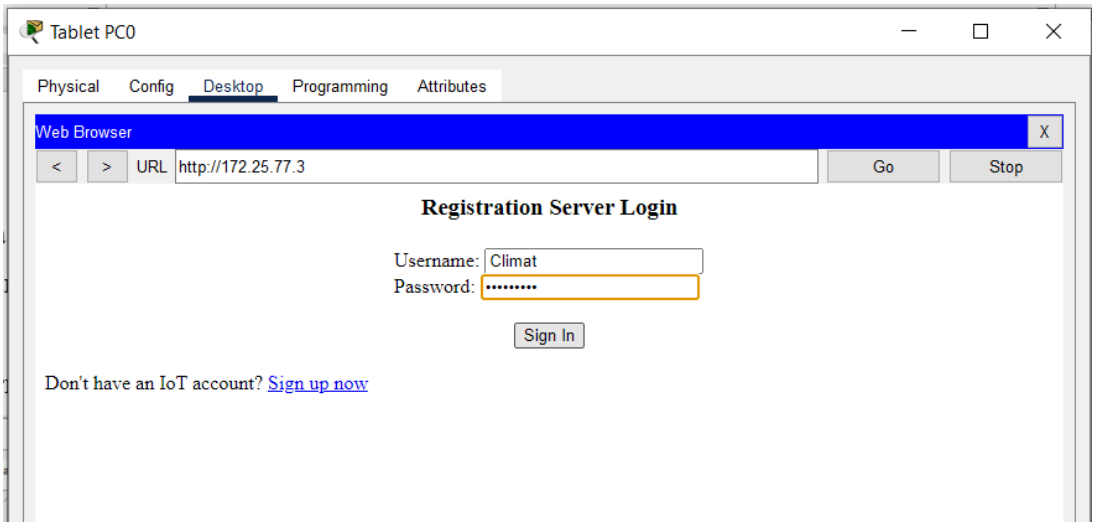

Рисунок 4.12 – Перехід до акаунту клімат-контролю

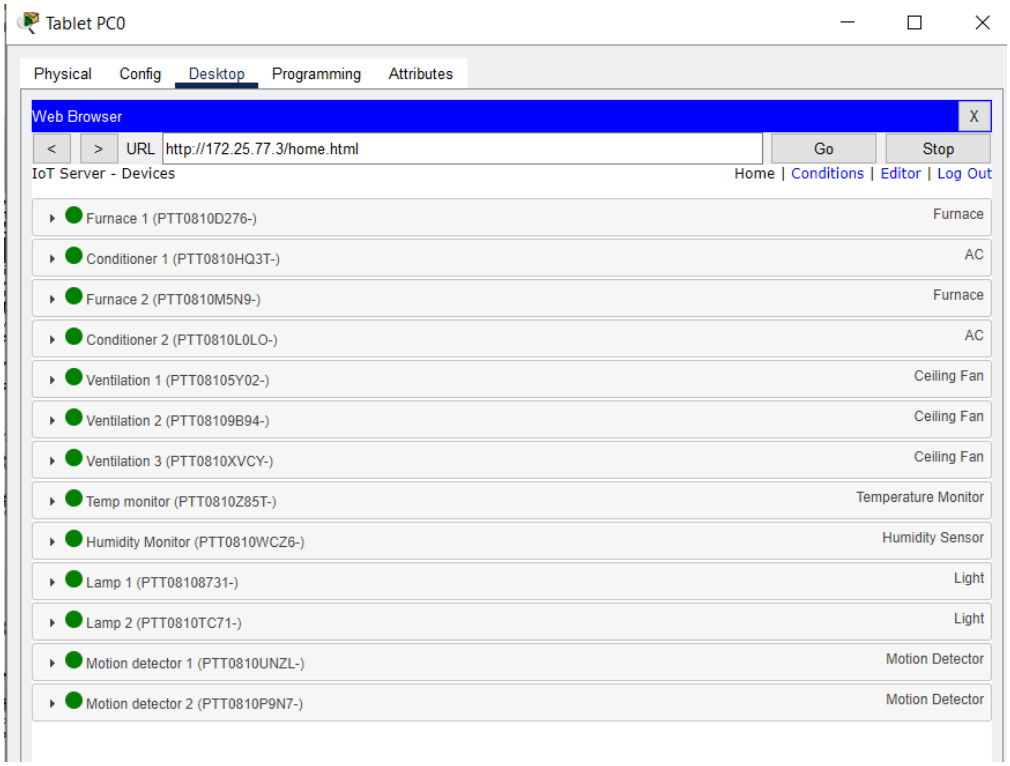

Рисунок 4.13 – Перелік всіх пристроїв підсистеми

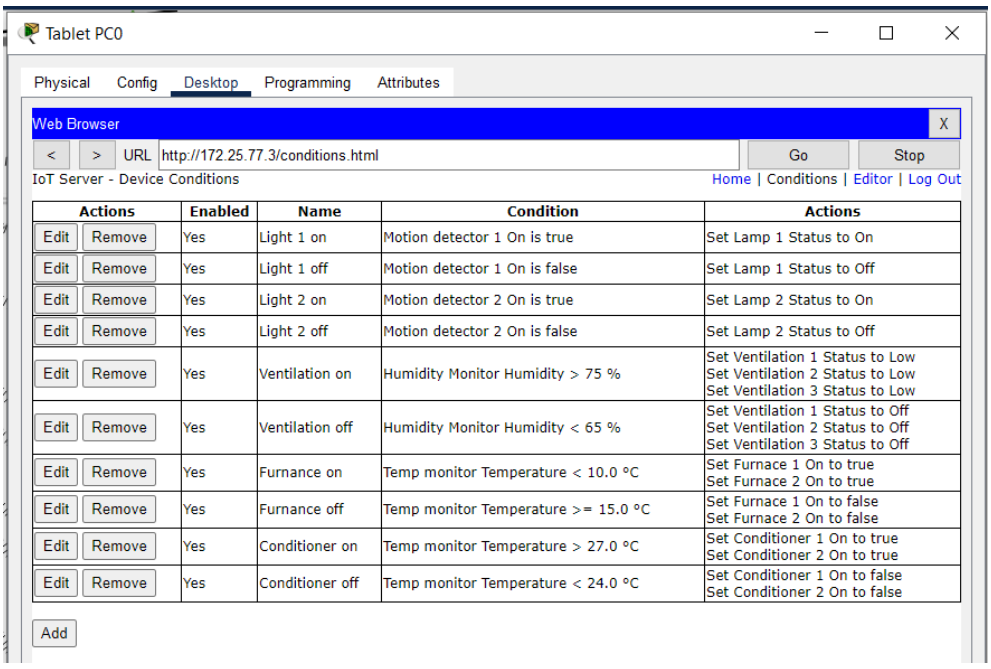

Рисунок 4.14 – Налаштовані сценарії

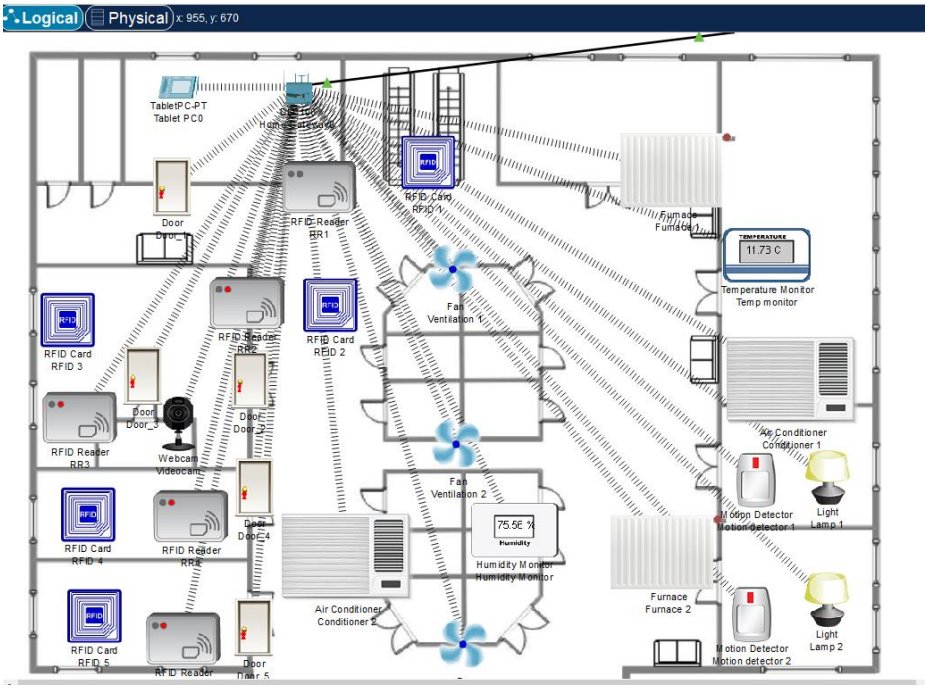

Рисунок 4.15 – Перевірка працездатності підсистеми клімат-контролю

Налаштований сценарій у системі клімат-контролю працює коректно. Після активації датчика руху автоматично вмикається світло у відповідному приміщенні. Коли рух припиняється, світло вимикається. Вентиляція починає працювати, якщо рівень вологості в кімнаті перевищує 75%, і вимикається, коли вологість знижується нижче 65%. Обігрівач вмикається автоматично, якщо температура опускається нижче 10°C, і вимикається, коли температура піднімається вище 15°C. Кондиціонер вмикається, коли температура перевищує 27°C, і вимикається, якщо температура знижується нижче 24°C. Таким чином, система забезпечує автоматичне керування освітленням та мікрокліматом у приміщенні, що сприяє комфортному перебуванню та енергоефективності.

ВИСНОВКИ

У рамках цієї кваліфікаційної роботи було розроблено та налаштовано сучасну комп'ютерну систему для торгово-розважального центру, яка включає повноцінну локальну мережу з усіма необхідними компонентами для стабільної та безпечної роботи організації. Розробка охоплює створення структурованої мережі з логічним поділом на VLAN, відповідно до функціональних відділів, що дало змогу оптимізувати розподіл ресурсів і підвищити рівень захисту даних.

Конфігурація маршрутизаторів із підтримкою NAT і динамічної маршрутизації за протоколом OSPF стала важливою складовою побудови мережі. Сервери IoT, HTTP, DNS, AAA були налаштовані для забезпечення стабільної роботи системи. Мережа передбачає окремий вихід до інтернету для відвідувачів та магазинів, це рішення дозволяє розділяти зовнішній трафік і зменшувати ризики порушення безпеки. Було впроваджено політики безпеки, зокрема контролю доступу до ресурсів, авторизації користувачів і захисту внутрішнього трафіку. Було реалізовано фільтрацію небажаних запитів і обмеження доступу до критично важливих сегментів мережі.

Реалізована інфраструктура дозволяє масштабуватися, додаючи нові підрозділи або збільшуючи кількість клієнтських пристроїв, не порушуючи стабільність і цілісність мережі. Це рішення дозволяє підтримувати як поточні потреби ТРЦ, так і потенційне зростання навантаження в майбутньому.

Для покращення безпеки та автоматизації торгово-розважального центру також було впроваджено кілька IoT-підсистем. Зокрема, реалізовано систему відеоспостереження, камери передають дані до сервера з подальшим збереженням архіву та можливістю перегляду у реальному часі. З метою захисту від пожежі введено систему виявлення диму із автоматичним увімкненням спринклерів та сирени. Внутрішні процеси були оптимізовані за допомогою системи автоматичного керування мікрокліматом, система автоматично керує роботою кондиціонерів, вентиляції, обігріву та освітленням. RFID-контроль у зонах з обмеженим доступом забезпечує авторизований вхід працівників.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cisco Packet Tracer – офіційний інструмент моделювання мереж [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://www.netacad.com (дата звернення 29.05.2025)

2. Мережеве обладнання Cisco [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.lu/rmmtnb (дата звернення 29.05.2025)

3. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра здобувачам галузі знань 12 Інформаційні технології спеціальності 124 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта – Д.: НТУ «ДП», 2025. – 65 с.

4. Бездротові мережі: стандарти, безпека, покриття [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://support.linksys.com/home/ (дата заернення 29.05.2025)

5. Основи відеоспостереження в торгових центрах [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу https://www.hikvision.com/en/ (дата звернення 29.05.2025)

6. ТРЦ «Nikolsky» - проєктування та впровадження систем електропостачання та автоматизації. [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://surl.li/zhfmzx (дата звернення 29.05.2025)

7. Бренд Ruijie – мережеве обладнання для ТРЦ. [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://bezpeka.club/ruijie (дата звернення 29.05.2025)

8. Cisco. «Cisco Networking Products and Solutions». [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.lu/unxlaw (дата звернення: 29.05.2025)

9. Hikvision. «Shopping Malls - Solutions by Scenario». [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.li/fpfwnb (дата звернення: 29.05.2025)

10. Комутатор Cisco Catalyst 2960 [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surli.cc/zkopoc (дата звернення 29.05.2025)

11. Маршрутизатор Cisco 2911 [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surli.cc/ruyfvg (дата звернення 29.05.2025)

12. Бездротова точка доступу Cisco Catalyst 9105AX Series [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.li/bjleci (дата звернення 29.05.2025)

13. Сервер для мережевих сервісів [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.lu/nagdfy (дата звернення 29.05.2025)

14. IoT-шлюз DLC-100 [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.li/ncnrog (дата звернення 29.05.2025)

15. RFID-мітка [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surli.cc/teyahg (дата звернення 29.05.2025)

16. RFID-зчитувач [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.li/qxyihx (дата звернення 29.05.2025)

17. Відеокамера [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.lu/hhomow (дата звернення 29.05.2025)

18. IoT-шлюз [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.li/qqmmjl (дата звернення 29.05.2025)

19. Бездротова IP-камера [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surli.cc/ydglgr (дата звернення 29.05.2025)

20. Центральний контролер [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surli.cc/csapgw (дата звернення 29.05.2025)

21. Датчик диму та тривожна сигналізація [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.li/shocab (дата звернення 29.05.2025)

22. Пожежні спринклери [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.gd/daohlv (дата звернення 29.05.2025)

23. Електромагнітний клапан [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://surl.li/yhnyva (дата звернення 29.05.2025)

24. Блок живлення Mean Well HDR-15-24 [Електронний ресурс] : surli.cc. – Режим доступу: https://surli.cc/ktbwuw (дата звернення 29.05.2025)

25. IoT-шлюз Cisco IR1101 [Електронний ресурс] : surl.lu. – Режим доступу: https://surl.lu/trmliz (дата звернення 29.05.2025)

26. Блок живлення центрального контролера Raspberry Pi Power Supply 5.1V

3А [Електронний ресурс] : surl.li. – Режим доступу: https://surl.li/dgpnsi (дата звернення 29.05.2025)

27. Блок живлення для клапанів [Електронний ресурс] : surl.lu. – Режим доступу: https://surl.lu/alwpvc (дата звернення 29.05.2025)

ДОДАТОК А

Текст програми налаштування компонентів мережі комп’ютерної системи

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ КОМПОНЕНТІВ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.2203-01 12 01
Листів 10

2025

АНОТАЦІЯ

Ця програма включає частину конфігураційного коду, який використовується для налаштування компонентів мережі. Основна мета - забезпечення стабільної та безпечної роботи всієї інфраструктури центру, з урахуванням специфіки функціонування різних підрозділів. Конфігурація охоплює налаштування таких служб, як DHCP для автоматичної видачі IP-адрес, AAA для автентифікації доступу до ресурсів, NAT для організації безпечного виходу в Інтернет, а також впровадження динамічної маршрутизації за допомогою протоколу OSPF.

ЗМІСТ

Налаштування маршрутизатора Ryndin_R_LAN_3

```
Building configuration...

Current configuration : 2236 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Ryndin_R_LAN_3
!
enable secret 5
$1$mERr$Dm906WSm15/D/HJgeKgUb/
!
ip dhcp excluded-address 172.25.77.1
172.25.77.5
!
ip dhcp pool LAN3
network 172.25.77.0 255.255.255.128
default-router 172.25.77.1
dns-server 172.25.77.2
!
aaa new-model
!
aaa authentication login AAA group radius
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn
FTX152413EH-
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 172.25.77.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
ip address 10.0.0.18 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.0.0.6 255.255.255.252
ip nat inside
clock rate 2000000
!
interface Serial0/0/1
ip address 10.0.0.10 255.255.255.252
ip nat inside
clock rate 2000000
!
interface Serial0/1/0
ip address 209.165.201.2 255.255.255.240
ip nat outside
clock rate 2000000
!
interface Serial0/1/1
ip address 10.0.0.21 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 172.25.77.0 0.0.0.127 area 0
network 10.0.0.4 0.0.0.3 area 0
network 10.0.0.8 0.0.0.3 area 0
network 10.0.0.16 0.0.0.3 area 0
network 10.0.0.20 0.0.0.3 area 0
network 209.165.201.0 0.0.0.15 area 0
default-information originate
!
ip nat inside source list NAT_ACL interface
Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
!
ip flow-export version 9
!
ip access-list standard NAT_ACL
permit 172.25.77.0 0.0.0.127
permit 172.25.78.0 0.0.0.127
permit 172.25.78.128 0.0.0.127
permit 172.25.77.128 0.0.0.127
permit 172.25.78.64 0.0.0.63
permit 172.25.77.192 0.0.0.63
```

```
!
banner motd ^C 123-21-2 Ryndin. Access only
for authorized personnel.^C
!
radius server 172.25.77.4
address ipv4 172.25.77.4 auth-port 1645
key Ryndin123
!
line con 0
password 7 081355400D100B464058
Building configuration...

Current configuration : 2482 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Ryndin_Switch3
!
enable secret 5 $1$mERr$Dm906WSm15/D/HJgeKgUb/
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 40
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 40
switchport mode access
!
line aux 0
!
line vty 0 4
password 7
081355400D100B4640582F0D39282B
login authentication AAA
!
End
```

Налаштування комутатора Ryndin_Switch3

```
interface FastEthernet0/8
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C 123-21-2 Ryndin. Access only
for authorized personnel.^C
!
!
!
line con 0
password 7 081355400D100B464058
login
!
line vty 0 4
password 7
081355400D100B4640582F0D39282B
login
line vty 5 15
login
!
end
```