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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Пасічної Анастасії Романівни
(ПІБ)

академічної групи 123-20ск-1
(шифр)

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

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

на тему «Інтелектуальна комп'ютерна система паркінгу ЖК «Маршал» з детальним опрацюванням побудови та налаштування корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Каштан В.Ю.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент	доц. Сафаров О.О.			

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » 2023 року

ЗАВДАННЯ

на кваліфікаційну роботу ступеня бакалавр

студента Пасічної А.Р. **академічної групи** 123-20ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему: «Інтелектуальна комп'ютерна система паркінгу ЖК «Маршал» з детальним опрацюванням побудови та налаштування корпоративної мережі» затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-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 постанова завдання	02.06.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	16.06.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	23.06.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	30.06.2023

Завдання видано _____ доц.Каштан В.Ю.
(підпис керівника) (прізвище, ініціали)
Дата видачі 19.04.2023
Дата подання до екзаменаційної комісії 13.07.2023
Прийнято до виконання _____ Пасічна А.Р.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 92 с., 31 рис., 11 табл., 1 додаток, 10 джерел.

Об’єкт розробки: інтелектуальна комп’ютерна система паркінгу ЖК «Маршал» з детальним опрацюванням побудови та налаштування корпоративної мережі

Мета: розробити інтелектуальну комп’ютерну систему паркінгу ЖК «Маршал»

Система розробки інтелектуального паркінгу спрямована на збереження, передачу даних та взаємодію з користувачами паркінгових послуг з метою забезпечення ефективного управління паркінгом. Вона використовує передові технології Інтернету речей для оптимального функціонування. Система включає в себе різноманітні компоненти, такі як сенсори руху, датчики світла, відеокамери та інші пристрої IoT, що збирають дані про стан паркінгу. Ці дані передаються на центральний сервер, де проводиться їх обробка та аналіз.

Відповідно до вимог кваліфікаційної роботи бакалавра була виконана розробка комп'ютерної мережі.

Схема цієї мережі була реалізована у вигляді логічної топології за допомогою середи проектування Cisco Packet Tracer.

Виконана перевірка спроектованої мережі, результати якої були задокументовані у вигляді таблиць та графіків, які детально описані і наведені у пояснювальній записці або додатках.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ ТА ТЕРМІНІВ

КС – комп’ютерна система

КМ – корпоративна мережа

ЖК – житловий комплекс

БФК – багатофункціональний комплекс

КБ – клубний будинок

IoT – Internet of Things

ПК – персональний комп’ютер

ПЗ – програмне забезпечення

NAT – Network Address Translation

PAgP – Port Aggregation Protocol

LACP – Link Aggregation Control

VLAN – Virtual Local Area Network, віртуальна локальна мережа

VLSM – Variable Length Subnet Masking

ISAKMP – Internet Security Association and Key Management Protocol

AAA – Authentication, Authorization, and Accounting

ПЛК – програмований логічний контролер

ВСТУП

Сьогодні, зі швидким розвитком технологій, все більше і більше багатоповерхових комплексів приймають рішення про встановлення розумних паркінгів. Це має ряд переваг як для мешканців, так і для власників багатоповерхових будинків.

Зокрема, розумний паркінг дозволяє ефективно використовувати простір, завдяки системі автоматичного паркування. Дозволяючи розмістити автомобілі на території житлового комплексу з максимальною компактністю, що зберігає більше місця для зелених насаджень, альтернативних маршрутів руху та інших потреб мешканців.

Розумні паркінги також підвищують безпеку на території житлового комплексу. Автоматична система контролю зменшує ризик крадіжок автомобілів та інших небажаних подій.

Третя перевага розумних паркінгів полягає у тому, що вони дозволяють економити час та зберігати зручність для мешканців. Автоматизована система паркування дозволяє мешканцям заощадити час, який витрачається на пошук місця для паркування, а також забезпечує зручність, оскільки автомобілі можуть бути відправлені на паркінг з допомогою мобільного додатку або іншого пристрою з підключенням до Інтернету.

Нарешті, використання розумних паркінгів в житлових комплексах може підвищити ціну нерухомості та зробити її більш привабливою для потенційних покупців та орендарів.

Узагальнюючи, використання розумних паркінгів у житлових комплексах дозволяє забезпечити ефективне використання простору, підвищити безпеку та зручність для мешканців, а також зробити нерухомість більш привабливою на ринку.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування КС

Житловий комплекс «Маршал» – це один із проектів забудовника Daytona Development Company, який на ринку нерухомості з 2010 року.

ЖК «Маршал» складається з двох будинків, які сполучені спільною територією. Зовнішній вигляд будівель відповідає сучасним тенденціям: вони мають панорамне скління, фасади з темної клінкерної цегли і стильні прості лінії. Територія ЖК розділена на функціональні зони та втілена за всіма правилами ландшафтного дизайну. У проекті використано концепцію «двір без авто», що забезпечує комфорт та безпеку мешканців під час прогулянок по території. Для зберігання автомобілів передбачені багаторівневі наземний та підземний паркінги, а окрема стоянка спроектована для гостей[3].

Загалом, ЖК «Маршал» від Daytona Development Company є вдалою інвестицією в нерухомість, яка пропонує комфортне та безпечне життя в сучасному житловому комплексі.

1.2 Характеристика і структура об’єкта впровадження

ЖК «Маршал» розташований у м. Дніпро за адресою – вулиця Набережна Перемоги, 128, Дніпро, Дніпропетровська область (рисунок 1.1).

Головний офіс забудовника Daytona Development Company у м. Дніпро знаходиться за наступною адресою: проспект Дмитра Яворницького, 22, офіс 705, Дніпро, Дніпропетровська область (рисунок 1.2).

Офіс забудовника розташувався за 5,6 км від ЖК «Маршал». Розташування ЖК «Маршал» та головного офісу відносно одне одного можна побачити на рисунку 1.3.

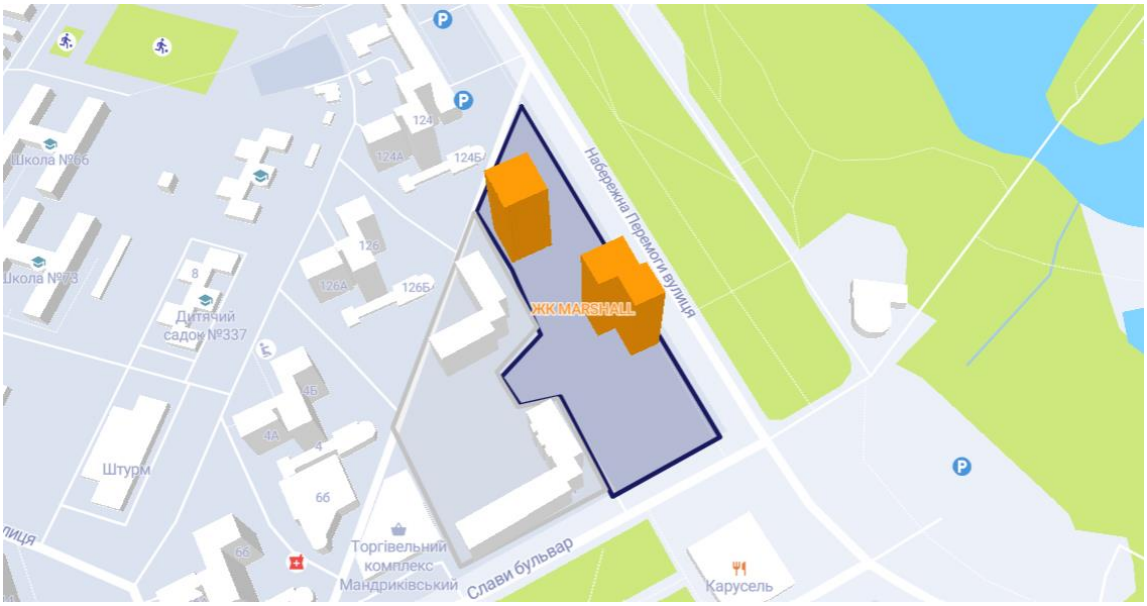

Рисунок 1.1 – Місцезнаходження ЖК «Маршал» на мапі наданою ріелтором

Рисунок 1.2 – Розташування головного офісу на мапі Google maps

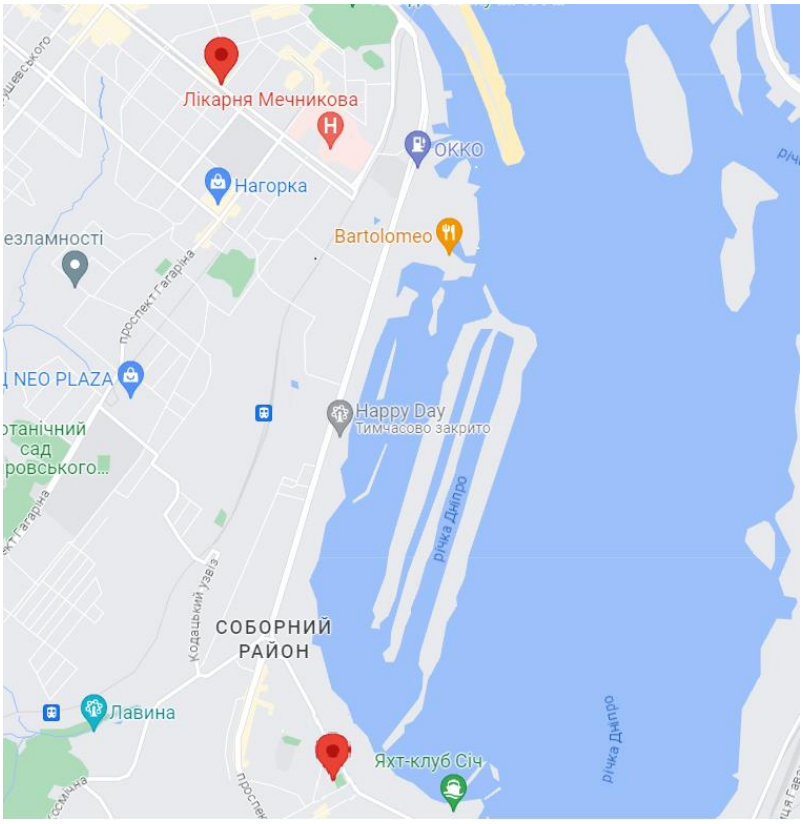

Рисунок 1.3 – Відстань між ЖК «Маршал» та головним офісом на мапі Google maps

Забудовник Daytona Development Company реалізує свої проекти в м. Дніпро та в м. Київ, головним напрямком діяльності Daytona Development Company є проектування та реалізація ЖК та багатофункціональних комплексів, бізнес-комплексів, а також це надання якісних послуг своїм клієнтам.

Серед реалізованих та проектів в процесі будівництва можна назвати такі: ЖК Tourbillion, БФК MAYAK, КБ K12, ЖК MAISON, ЖК GENEVE, ЖК «Маршал».

Серед послуг, які надає забудовник для обслуговування своїх проектів можна виділити:

– продаж. Відділ продажу відповідає за продаж нерухомості в ЖК;

– реклама. Рекламний відділ відповідальний за просування та рекламування нових проектів забудовника;

– обслуговування житлових та бізнес-комплексів. Головною метою

відділу обслуговування є збір і аналіз інформації про потреби клієнтів та забезпечення їх задоволеності якісними послугами. До обов'язків відділу також входить планування і координація робіт з технічного обслуговування, ремонту та обслуговування систем безпеки, а також забезпечення чистоти та порядку на території обслуговування. Компетентний та ефективний відділ обслуговування допомагає забезпечити максимальний комфорт для жителів та бізнес-клієнтів, що користуються послугами комплексу.

Більш детальну структуру управління Daytona Development Company, зокрема детально наведено обслуговування та управління ЖК «Маршал» на рисунку 1.4.

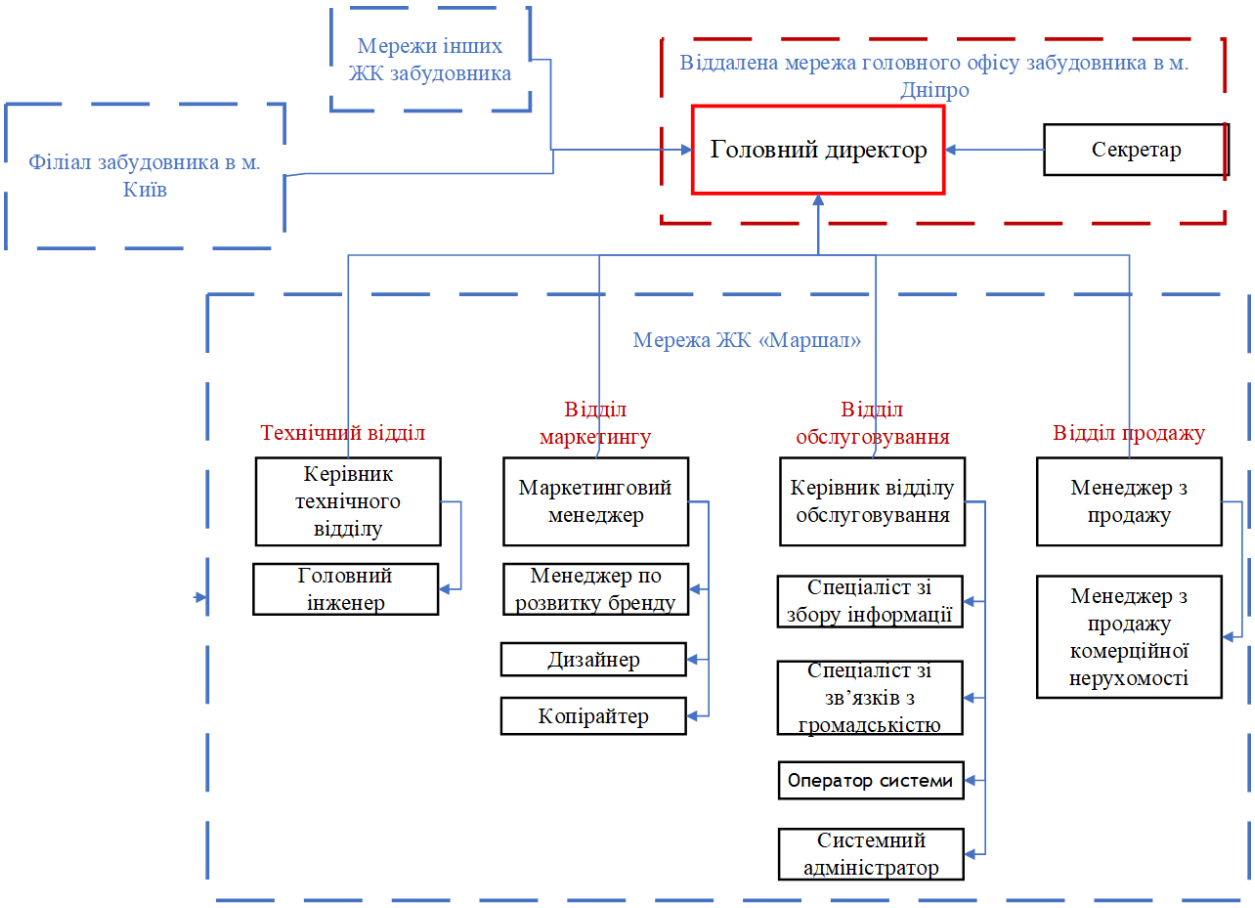

Рисунок 1.4 – Структура управління Daytona Development Company

Нижче наведено план приміщень головного офісу забудовника та приміщень ЖК «Маршал».

На рисунку 1.5 зображено приміщення офісу забудовника в ТЦ

Рисунок 1.5 – Приміщення офісу забудовника на плані будівлі ТЦ Atrium

Площа головного офісу 60м^2, в офісі розташовано робоче місце головного директора та його секретаря.

План першого та другого поверху ЖК «Маршал», де розташувались технічний відділ та відділи продажу, маркетингу та обслуговування, а також паркінг з приміщенням для оренди магазинів наведено на планах взятих з офіційного сайту ЖК (рисунок 1.6-1.7).

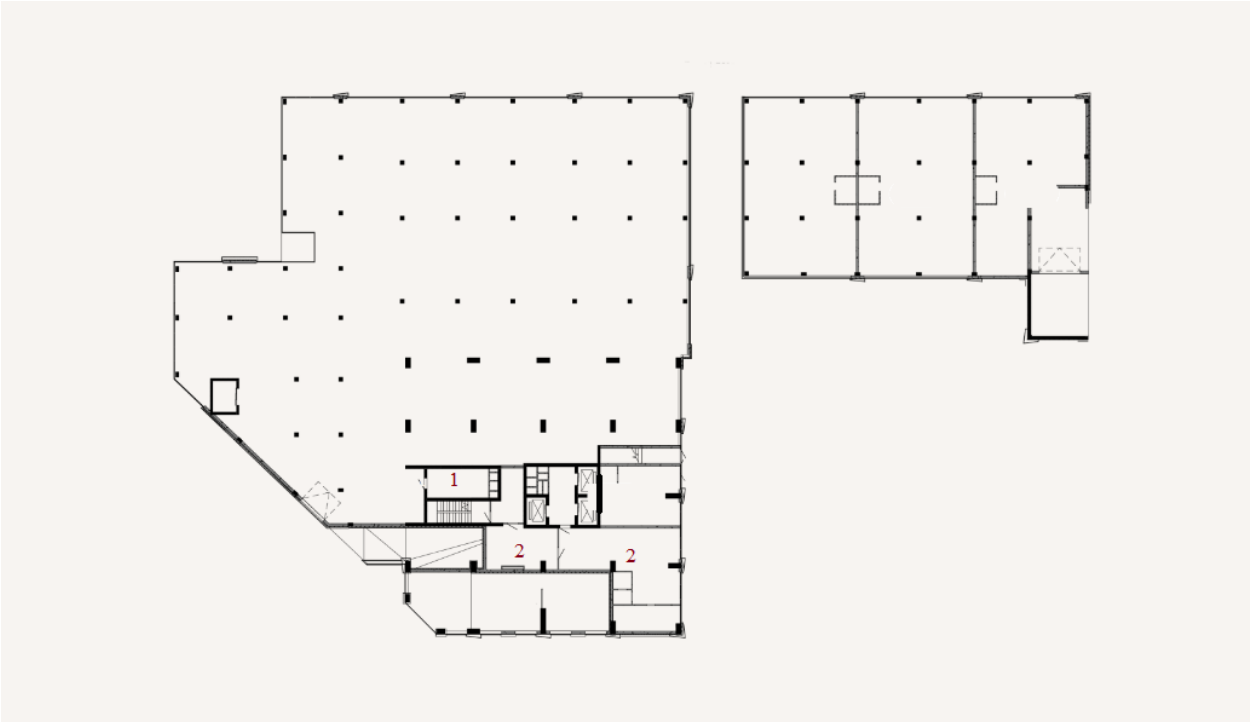

Рисунок 1.6 – План першого поверху ЖК: 1 – серверна; 2 – відділ продажу

Площа серверної кімнати складає 24,3м^2.

Відділ продажу розташувався в 2 приміщеннях, згідно плану їх площа складає 33,6 та 78,7 м^2.

Рисунок 1.7 – План другого поверху ЖК

На другому поверсі ЖК розташувались офіси наступних підрозділів:

– офіс відділу маркетингу. Відділ знаходиться в приміщенні 2-2, згідно плану забудовника, площа приміщення складає 153,79 м^2;

– офіс відділу обслуговування. Розташовано відділ в приміщенні 2-7, площа приміщення складає 66,94 м^2;

– офіс технічного відділу. Відділ знаходиться в приміщенні 2-1, за планом, площа даного приміщення 122,19 м^2.

Кількість персональних комп'ютерів, що забезпечує роботу підприємства наведена у таблиці 1.1.

Таблиця 1.1 – Кількість ПК на підприємстві

Назва підрозділу	Кількість персоналу	Кількість ПК
Головний офіс	2	2
Технічний відділ	10	10
Відділ продажу	9	9
Відділ обслуговування	10	6
Відділ маркетингу	8	8
	29	25

Опираючись на таблицю 1.1, можна зробити висновок, що 25 з 29 співробітників забезпечені ПК, а отже підприємство має великий рівень діджиталізації свого персоналу.

1.3 Огляд існуючих інженерних рішень КС в галузі

Один з прикладів успішного впровадження розумного паркінгу в світі може стати SmartGuide, що було встановлено на рівні 5 паркінгу SAP Tower в Окленді.

SAP Tower є однією з найбільш відомих будівель класу А в цьому місті та розташована в елітному районі на головній бізнес-адресі Нової Зеландії – Квін-стріт. Загальна площа приміщень становить 17,648 м2, а якість офісних та роздрібних приміщень є неперевершеною. У зв'язку з таким престижним

місцем, було встановлено технологію розумного паркування SmartGuide на рівні 5 паркінгу з 313 місцями за допомогою датчиків виявлення транспортних засобів SmartEye. Ця технологія дозволяє визначати наявні місця та направляти водіїв до них за допомогою світлових вказівок зеленого та червоного кольорів, а сині світла показують доступні місця для інвалідів. Знак на вході рівня 5 показує кількість вільних місць.

Застосування цієї технології дозволяє водіям легко виявляти доступні місця, що економить їхній час та зменшує викиди транспортних засобів. Крім того, це збільшує зайнятість паркінгу, оскільки місця, які мало використовувались, тепер стали більш помітними. Дані про зайнятість паркінгу передаються в реальному часі до системи управління паркінгом SmartRep, що дозволяє Wilson Parking краще розуміти поведінку водіїв та використовувати цю інформацію в майбутніх політиках паркування [4].

1.4 Завдання і мета роботи

Основним завданням роботи є розробка та налаштування комп’ютерної мережі ЖК Маршал, а також впровадження розумного паркінгу.

Для досягнення поставленої мети важливо враховувати багато дрібних деталей та аспектів.

Серед цих аспектів можна виділити наступні:

– вибір мережевої архітектури;

– вибір кабельної системи для КМ;

– аналіз мережного трафіку;

– вибір способу управління мережею;

– конфігурація мережного обладнання;

– забезпечення безпеки мережі.

Отже, для успішної реалізації проекту необхідно розробити гнучку та оптимальну схему мережі, яка буде забезпечувати надійний захист від зловмисників та легко піддається подальшій конфігурації.

1.5 Основні особливості та проблематика впровадження розумного паркінгу

Впровадження розумного паркінгу в житловому комплексі відкриває широкі перспективи для поліпшення управління місцями паркінгу, забезпечення комфорту мешканців та ефективного використання доступних ресурсів. Однак, цей процес також вносить свої особливості та стикається з певними проблемами.

Одна з основних особливостей впровадження розумного паркінгу в ЖК полягає в створенні інфраструктури, яка підтримує збір і обробку даних з місцями паркінгу. Це включає встановлення датчиків або інших технологій, які можуть виявляти наявність та вільність місцями паркінгу, а також здатність передавати цю інформацію до централізованої системи керування.

Проблематика впровадження розумного паркінгу в ЖК включає такі аспекти:

– інфраструктура та апаратне забезпечення. ЖК повинен бути обладнаний необхідною мережевою інфраструктурою для збору даних та передачі інформації. Це може включати встановлення датчиків, камер спостереження, систем збору даних та централізованої системи управління. Проблеми можуть виникати при встановленні та налаштуванні цих компонентів, а також забезпеченні їх надійності та взаємодії;

– інтеграція з існуючими системами. У багатьох ЖК вже існують системи управління безпекою, доступом та іншими інфраструктурними рішеннями. Впровадження розумного паркінгу потребує інтеграції з цими системами, щоб забезпечити повну функціональність та взаємодію;

– управління та організація. Впровадження розумного паркінгу в ЖК вимагає налагодження ефективних процесів управління та організації. Це включає встановлення правил користування місцями паркінгу, розробку системи бронювання та розподілу місць, а також забезпечення безперервної підтримки та обслуговування системи. Проблеми можуть виникати при встановленні ефективного механізму контролю доступу, розробці зручного

інтерфейсу для користувачів та забезпеченні швидкого реагування на проблеми або аварійні ситуації;

– кібербезпека та конфіденційність даних. Розумний паркінг вимагає збору, передачі та обробки великої кількості даних, включаючи персональну інформацію про користувачів. Забезпечення кібербезпеки та конфіденційності даних є критичним аспектом впровадження розумного паркінгу. Проблеми можуть виникати при захисті системи від хакерських атак, зломів та несанкціонованого доступу до даних. Застосування сучасних шифрувальних технологій, механізмів автентифікації та захисту даних можуть допомогти уникнути цих проблем;

– фінансові аспекти. Впровадження розумного паркінгу може вимагати значних фінансових вкладень. Вартість обладнання, налаштування системи, навчання персоналу та підтримка можуть становити значну частину бюджету. Крім того, варто враховувати економічну вигідність і повернення інвестицій у довгостроковій перспективі. Проблеми можуть виникати при оцінці фінансової доцільності впровадження розумного паркінгу, ураховуючи витрати на обладнання, інтеграцію, підтримку та обслуговування системи. Додатково, можуть виникати складнощі при визначенні оптимальної цінової моделі для користувачів паркінгу, забезпеченні прозорості та справедливості у розподілі місць, а також установленні механізмів оплати та контролю;

– взаємодія з міськими структурами. Впровадження розумного паркінгу в ЖК може потребувати співпраці з міськими органами та структурами, особливо якщо система паркінгу має інтегруватись з загальноміською інфраструктурою. Узгодження правил, нормативних актів та вимог щодо паркування може становити виклик, а також виникнення проблем з організацією спільної роботи та обміном даними між різними системами;

– прийняття та звички користувачів. Впровадження розумного паркінгу в ЖК вимагає зміни в поведінці та звичках користувачів паркування. Важливо провести ефективну інформаційну кампанію, навчання та підтримку користувачів, щоб вони могли зручно користуватись новою системою,

бронювати місця та дотримуватись встановлених правил;

– загальна проблематика впровадження розумного паркінгу в ЖК полягає у збалансованому поєднанні технологічних, організаційних, фінансових та соціальних аспектів. Подолання цих викликів вимагає ретельного планування, співпраці між різними зацікавленими сторонами та ефективного управління проектом. Важливо провести детальний аналіз і обговорення всіх особливостей і проблематики, враховуючи потреби мешканців, вимоги до інфраструктури та можливості впровадження нових технологій;

– загалом, впровадження розумного паркінгу в ЖК може покращити якість життя мешканців, забезпечити оптимальне використання місць паркінгу та знизити витрати на управління паркінгом. Але варто пам'ятати, що успішне впровадження цієї технології вимагає комплексного підходу, ретельного планування та врахування всіх вищезгаданих аспектів. Тільки шляхом ретельного аналізу, розробки ефективної стратегії та співпраці з усіма зацікавленими сторонами можна досягти успіху в впровадженні розумного паркінгу в ЖК та створити зручне та інноваційне середовище для мешканців.

1.6 Потенційні шляхи вирішення поставлених завдань

У контексті використання розумного паркінгу в ЖК «Маршал», з урахуванням його інноваційного характеру, ми маємо можливість обрати найоптимальніший курс дій для досягнення запланованих цілей.

На даному етапі, топологія мережі в житловому комплексі відображається таким чином (рисунок 1.8).

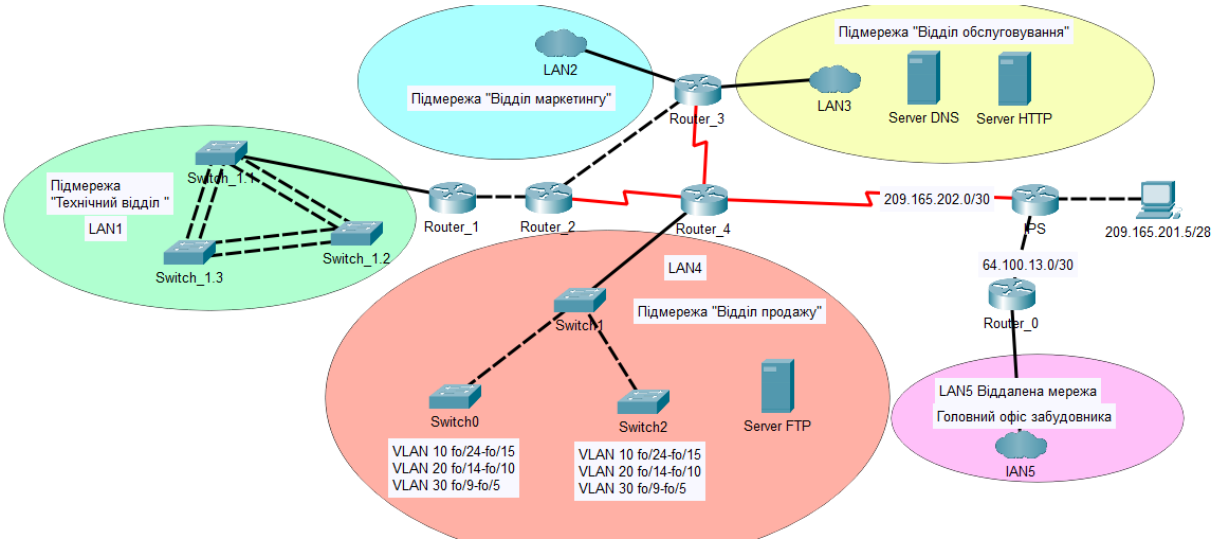

Рисунок 1.8 – Топологія мережі підприємства

Топологія мережі ЖК «Маршал» складається з 4 підмереж: «Технічний відділ», «Відділ маркетингу», «Відділ обслуговування», «Відділ продажу». А також до загальної структури входить віддалена мережа головного офісу забудовника.

Потенційним шляхом вирішення поставлених завдання є впровадження додаткової підмережі, LAN6, для розгортання системи розумного паркінгу в загальній мережі житлового комплексу. Також з підмережі будуть збиратись данні та відправлятись на IoT-сервер.

Житловий комплекс «Маршал» дбає про своїх мешканців і тому вся КС організована на мережевому обладнанні від Cisco. Такий вибір пов’язаний з тим, що Cisco відома своєю надійністю та видатною репутацією на ринку. Використання цієї технології гарантує надійність і безпеку мережі, особливо важливу роль грає забезпечення захисту від потенційних зловмисників. Завдяки такому обладнанню, мешканці ЖК «Маршал» можуть бути впевнені, що їхні дані та особиста інформація зберігаються в надійних руках, забезпечуючи їм спокій та комфорт.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до структури і функціонуванню системи

Кіберфізична система паркінгу ЖК «Маршал», призначена для моніторингу і оптимізації паркінгової інфраструктури з метою забезпечення ефективного управління транспортними потоками та підвищення зручності для користувачів. Система має забезпечувати автоматизоване керування процесами, такими як розподіл доступних паркомісць, надання інформації про вільні місця, контроль за в'їздом і виїздом автомобілів, а також моніторинг стану паркінгової зони.

Кіберфізична система паркінгу має забезпечити синхронізацію різних елементів розумного паркінгу, таких як камери спостереження, датчики температури та вологості, датчики CO_2. Вона має контролювати температуру та вентиляцію в паркінговій зоні, забезпечуючи належні умови для збереження автомобілів та запобігаючи утворенню конденсату. Також вона має здійснювати відеонагляд за всією зоною, що є одним із головних аспектів системи. Для цього передбачені польові підсистеми, а також підсистеми архівації, обробки та відображення інформації.

Комп'ютерна система має складатись з наступних підсистем:

– LAN 1 «Технічний відділ»;

– LAN 2 «Відділ маркетингу»;

– LAN 3 «Відділ обслуговування»;

– LAN 4 «Відділ продажу»;

– LAN 5 віддалена мережа «Головний офіс»;

– LAN P1 «Паркінг, перший корпус»;

– LAN P2 «Паркінг, другий корпус».

2.1.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему інтелектуального паркінгу, їх режим роботи

Кількість необхідного персоналу, яка необхідна для забезпечення ефективного функціонування системи інтелектуального паркінгу наведена у таблиці 2.1.

Таблиця 2.1 – Необхідна кількість персоналу та режими роботи

Посада	Кількість персоналу	Кваліфікація	Режими роботи
Оператор системи	3	Середня технічна освіта	3 зміни
Системний адміністратор	1	Вища технічна освіта	1 зміна

Також враховується, що при екстрених ситуаціях інженери мають бути завжди на зв’язку і при цьому режим роботи може змінюватись.

2.1.3 Вимоги до надійності системи інтелектуального паркінгу

Система повинна забезпечувати безперебійну роботу, навіть у разі виникнення помилок, збоїв або аварійних ситуацій. Недоступність чи втрата одного компоненту не повинна призводити до повного зупину системи. Максимальний час відновлення системи після збою має складати 30 секунд, максимальний час перерви у обслуговуванні користувачів під час відновлення – 5 секунд.

Система повинна мати механізми автоматичного відновлення після збоїв. Це означає, що після виявлення проблеми система здатна відновити свою працездатність, відновити з'єднання та продовжити свою роботу без значних перерв у обслуговуванні користувачів. Час для відновлення системи після збою, немає перевищувати 10 секунд.

Всі дані, що зберігаються в системі, повинні регулярно резервуватися для забезпечення їх збереження у випадку втрати або пошкодження. Резервні копії повинні зберігатись в безпечному місці і відновлюватися за потреби.

Резервне копіювання даних має відбуватись щогодини, а резервні копію мають зберігатись на сервері протягом 30 днів.

Система повинна мати резервні джерела енергії, які забезпечують продовження роботи в разі виникнення перебоїв у електропостачанні. Це дозволить уникнути втрати даних і забезпечити безперебійне функціонування системи. Час автономної роботи системи в разі перебоїв у електропостачанні має бути не менше 6 годин.

Однією з вимог надійності системи також є ліцензійне програмне забезпечення. Також в системі має здійснюватися регулярне оновлення ПЗ.

Система має бути масштабованою і здатною до розширення, щоб задовольняти зростаючі потреби паркінгової інфраструктури. Вона повинна бути гнучкою і забезпечувати можливість додавання нових компонентів, паркомісць без значних змін в архітектурі системи.

2.1.4 Вимоги до захисту інформації від несанкціонованого доступу

Система має бути забезпечена ефективними заходами захисту для запобігання несанкціонованому доступу до системи або даних. Має відповідати вимогам стандартів безпеки, що застосовуються до паркінгових систем. Це включає використання паролів, шифрування даних та контроль доступу до системи, а також фізичну безпеку обладнання, захист від вторгнень та інших потенційних загроз безпеці користувачів і даних:

– мінімальна довжина паролів 8 символів;

– пароль повинен складатись з різноманітної комбінації великих і малих літер, цифр і спеціальних символів;

– час автоматичного вимкнення сесії бездіяльності має бути не більше 15 хвилин;

– при шифруванні даних використовувати алгоритми шифрування AES-256;

– забезпечити двофакторну аутентифікацію;

– забезпечення фізичного захисту обладнання, тобто система має бути

розміщена в захищеному приміщенні з обмеженим доступом.

– використання виявлення вторгнень (IDS) і системи запобігання вторгнень (IPS).

– моніторинг безпеки, система має бути обладнана механізмами моніторингу подій і логування для виявлення можливих загроз і атак.

Ці заходи захисту повинні відповідати стандартам безпеки, що застосовуються до паркінгових систем, таким як ISO/IEC 27001:2013 та інші відповідні нормативні документи.

2.1.5 Вимоги до ергономіки системи

Система повинна мати інтуїтивно зрозумілий та легкий у використанні інтерфейс для користувачів. Елементи керування та взаємодії повинні бути зрозумілими та легко доступними, забезпечуючи зручну навігацію та виконання операцій.

Також система має мінімізувати використання фізичного простору та забезпечувати ефективне розташування паркінгових місць.

2.1.6 Вимоги до патентної чистоти інтелектуального паркінгу

Система розумного паркінгу повинна бути розроблена та функціонувати з урахуванням патентної чистоти. Це означає, що вся технологія, алгоритми, інноваційні рішення та інтелектуальна власність, використані в системі, повинні бути належним чином захищені патентами або мати легальні права використовуватися. Також система повинна відповідати всім вимогам та обмеженням, передбаченим українським законодавством щодо патентної чистоти та права на інтелектуальну власність. Вона не повинна порушувати патентні права третіх осіб або використовувати нелегальні або неохайні патентні практики.

2.1.7 Вимоги до уніфікації та стандартизації обладнання в системі інтелектуального паркінгу

Система розумного паркінгу повинна відповідати міжнародним стандартам і нормам, що стосуються автоматизованих систем паркування. Це забезпечить її сумісність з іншими системами, легкість обміну даними та інтеграцію з різними технологічними платформами. Деякі з основних міжнародних норм і стандартів, які можуть бути застосовані до системи розумного паркінгу, включають:

– ISO 21448:2019 (SOTIF - Safety of the Intended Functionality). Цей стандарт визначає вимоги до безпеки систем, враховуючи непередбачувані функції та небезпеки, пов'язані з автоматизованими системами;

– ISO 17361:2020 (Parking facilities - Data exchange between parking information provider and parking facility). Цей стандарт встановлює протоколи і формати обміну даними між постачальниками інформації про паркування та системами паркування;

– ISO 15638:2018 (Intelligent transport systems - Framework for cooperative ITS). Цей стандарт визначає загальний фреймворк для розумних транспортних систем, який включає системи паркування, і сприяє їх взаємодії та інтеграції з іншими розумними системами.

Застосування цих міжнародних норм і стандартів допоможе забезпечити сумісність, інтеграцію та стандартизацію компонентів системи розумного паркінгу, полегшуючи обмін даними та заміну окремих компонентів.

2.2 Вимоги до видів забезпечення

2.2.1 Вимоги до інформаційного забезпечення

Інформаційна система повинна забезпечувати швидкий доступ до даних та ефективну обробку інформації включаючи:

– максимальний час відповіді на запити користувача повинен бути менше 1 секунди;

– система повинна мати достатню пропускну здатність для обробки

одночасних запитів великої кількості користувачів, забезпечуючи швидку обробку та відображення даних;

– забезпечення реал-тайм моніторингу, тобто система повинна надавати актуальну інформацію з відеокамер, яка буде оновлюватись в режимі реального часу. Це дозволить операторам системи слідкувати за станом паркінгу і приймати швидкі рішення на основі актуальних даних;

– система повинна швидко обробляти дані про інтенсивність задимленості, вологості та температури в приміщенні паркінгу. Це дозволить вчасно виявляти та реагувати на можливі проблеми або аварійні ситуації;

– система повинна бути оптимізована для швидкого виконання складних запитів та аналізу даних;

Забезпечення швидкого доступу до даних та ефективної обробки інформації є ключовими вимогами до інформаційної системи розумного паркінгу, що дозволить забезпечити швидке реагування на запити користувачів та ефективно спостерігати за станом паркінгу.

2.2.2 Вимоги до технічного забезпечення системи

Мережеве обладнання повинно бути від виробника Cisco, яке задовольняє наступні вимоги:

– маршрутизатори повинні підтримувати віртуальні локальні мережі, та протокол маршрутизації OSPF. Вони також мають мати можливість розширення за допомогою модулів для додавання серійних портів. Шлюзові маршрутизатори мають підтримувати віртуальні приватні мережі (VPN);

– комутатори повинні підтримувати віртуальні локальні мережі і мати не менше 24 портів Fast Ethernet. Комутатори в підмережі паркінгу повинні мати порти Fast Ethernet з підтримкою технології передачі енергії через Ethernet (PoE).

Датчики які використовуються в системі повинні відповідати наступним конкретним вимогам:

– високий ступінь захисту від вологості, IP65 або вище. Це забезпечить

їх захист від бризок, конденсації та інших вологих умов, які можуть бути присутні у паркінговому середовищі;

– широкий діапазон робочих температур, від -20°C до +60°C. Це дозволить їм надійно працювати як в холодних зимових умовах, так і в спекотному літньому кліматі;

– висока точність та швидкість вимірювання, забезпечуючи достовірну інформацію про вологість, температуру та задимленість. Точність вимірювання має бути в межах ±1% для вологості та ±0,5°C для температури.

– зручний та швидкий монтаж, щоб забезпечити простоту установки у паркінговому середовищі.

– конструкція датчиків повинна бути міцною, щоб вони могли витримувати умови паркінгового середовища, таких як вібрації, удари та потенційні пошкодження.

Для керування системою треба використовувати програмований логічний контролер від Овен.

2.3 Розробка апаратної частини комп’ютерної системи

2.3.1 Розробка загальної структури компютерної системи ЖК «Маршал»

Основними елементами структури комп'ютерної системи ЖК «Маршал» є:

– сервери, вони є центральними обчислювальними вузлами, які надають ресурси та послуги іншим комп'ютерам у мережі. Вони забезпечують централізоване зберігання даних, обробку і передачу інформації, а також виконання спеціалізованих завдань;

– клієнтські комп'ютери, або робочі станції, вони є терміналами, з яких користувачі отримують доступ до ресурсів та послуг, що надаються серверами;

– мережеве обладнання. До мережевого обладнання належать комутатори, маршрутизатори та мережеві контролери, які забезпечують

з'єднання та комунікацію між різними компонентами мережі.

У ЖК «Маршал» розглядається структурна схема комплексу технічних засобів комп'ютерної системи, рівень ядра та розподілу мережі будуть поєднуватися через маршрутизатори КС.

Рівень ядра має складатись з шести маршрутизаторів, що забезпечують маршрутизацію трафіка та підключені мережами WAN. Згідно підрозділу 2.1.2.2, для забезпечення доступу до віддаленої мережі головного офісу забудовника, використовується технологія VPN. За допомогою шлюзового маршрутизатора рівня ядра здійснюється підключення проектованої мережі до Інтернету.

Рівень доступу включає тринадцять комутаторів, які розгорнуті для формування LAN та VLAN підмереж. Цей підхід до розподілу даних дозволяє безпосередньо передавати дані від кожного комутатора до отримувача, покращуючи продуктивність та забезпечуючи безпеку мережі. Крім того, така архітектура гарантує, що дані не обробляються на інших сегментах мережі, які не є їхніми призначеними отримувачами.

У підмережі «Відділ продажу» використовуються два комутатори, до яких підключаються всі користувачі цього підрозділу шляхом використання технології VLAN. Це забезпечує ізольований доступ до мережевих ресурсів для цього відділу. А в підмережі «Технічний відділ» використовуються три комутатори, до яких також підключаються всі користувачі цього підрозділу, але з використанням технологій PAgP та LACP на комутаторах. Ці технології дозволяють збільшити пропускну здатність та надійність каналу передачі даних.

Структурна схема системи ЖК «Маршал» зображена на рисунку 2.1.

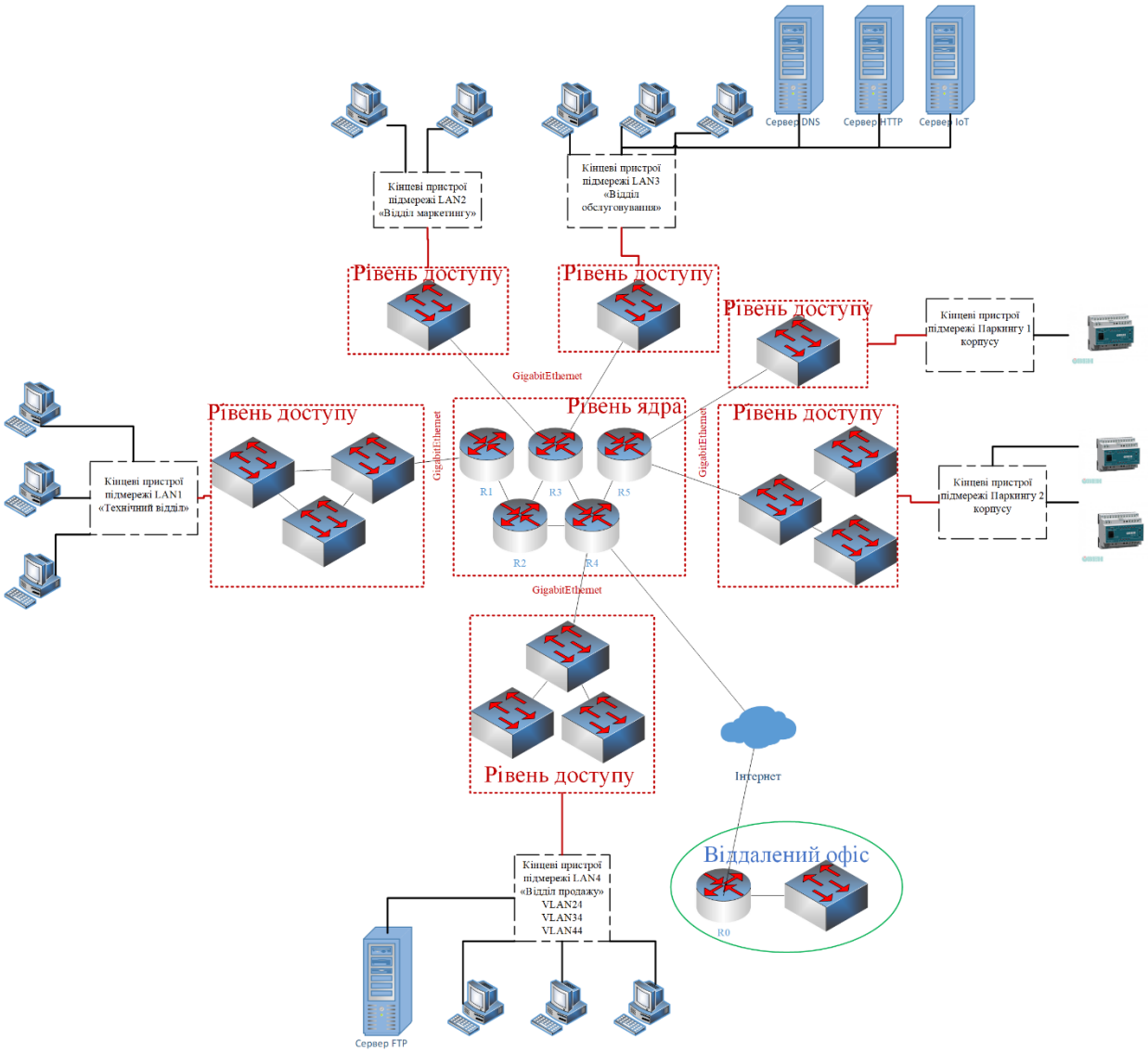

Рисунок 2.1 – Структурна схема комп’ютерної системи ЖК «Маршал»

2.3.2 Вибір і обґрунтування комплексу технічних засобів комп’ютерної системи

Для маршрутизації трафіку в середині мережі було використано маршрутизатори Cisco 2911 (CISCO2911/K9). Ці роутери мають наступні характеристики: вбудований одноядерний процесор з тактовою частотою 1.2 ГГц, 512 МБ оперативної пам'яті DDR2 і вбудовану флеш-пам'ять об'ємом 256 МБ. У них також є два порти 10/100/1000Base-T Ethernet (RJ-45), один порт консолі RJ-45 для локального підключення і один порт адміністрування RJ-45 для віддаленого керування. Додатково присутні два роз'єми USB типу A для підключення зовнішніх пристроїв. Ці маршрутизатори підтримують різні

протоколи маршрутизації, включаючи BGP, OSPF, EIGRP, RIP, IS-IS, PIM, HSRP, VRRP та інші. Вони також мають вбудовану підтримку механізмів безпеки, таких як функція захисту від атак, вбудований брандмауер, підтримка VPN (IPsec, SSL) і шифрування даних. Крім того, за допомогою модулів розширення, можна додати серійні порти для розширення можливостей роутера.

В якості кордоних маршрутизаторів, підключених до Інтернету, було використано маршрутизатори Cisco ISR 4331 (ISR4331/K9). Ці роутери мають наступні характеристики: вони оснащені одноядерним процесором з тактовою частотою 1.8 ГГц, 4 ГБ оперативної пам'яті DDR4 і вбудовану флеш-пам'ять об'ємом 4 ГБ. Вони мають два порти 10/100/1000Base-T Ethernet (RJ-45), один порт консолі RJ-45 для локального підключення та один порт адміністрування RJ-45 для віддаленого керування. Також присутні два роз'єми USB типу A для підключення зовнішніх пристроїв. Ці маршрутизатори підтримують різні протоколи маршрутизації, включаючи BGP, OSPF, EIGRP, RIP, IS-IS, PIM, HSRP, VRRP та інші. Вони також забезпечують різноманітні механізми безпеки, включаючи функцію захисту від атак, вбудований брандмауер, підтримку VPN (IPsec, SSL) і шифрування даних. Ці маршрутизатори є надійними рішеннями для забезпечення з'єднання з Інтернетом та забезпечення безпеки мережі.

У мережі були використані комутатори Cisco Catalyst 2960 Plus 24 10/100 +2T/SFP LAN Base (WS-C2960+24TC-L). Ці комутатори мають наступні характеристики: вони оснащені 24 портами 10/100 для підключення пристроїв зі швидкістю 10 або 100 Мбіт/с. Крім того, вони також мають 2 порти SFP (Small Form-Factor Pluggable) для підключення пристроїв з використанням оптичного зв'язку. Ці комутатори підтримують LAN Base-функціонал, що надає ряд функцій для управління мережею, включаючи керування VLAN, QoS (Quality of Service), безпеку мережі та багато іншого.

В підмережі інтелектуального паркінгу було використано комутатори Cisco Catalyst 2960 Plus 48 10/100 PoE + 2 1000BT + 2 SFP LAN Base (WS-

C2960+48PST-L). Ці комутатори мають наступні характеристики: вони оснащені 48 портами 10/100 з підтримкою технології PoE (Power over Ethernet), що дозволяє живити підключені до них пристрої, такі як IP-камери або точки доступу, за допомогою одного кабелю Ethernet. Крім того, вони мають 2 порти 1000BT і 2 порти SFP для підключення пристроїв з використанням оптичного зв'язку. Ці комутатори використовують LAN Base-функціонал, що забезпечує управління VLAN, QoS та безпекою мережі.

Функція PoE є особливо важливою для управління пристроями в мережі інтелектуального паркінгу. Вона дозволяє живити пристрої безпосередньо через Ethernet-кабель, елімінуючи потребу в окремих джерелах живлення для кожного пристрою. Це спрощує процес установки та забезпечує більшу гнучкість розміщення пристроїв. Крім того, функція PoE дозволяє централізовано керувати живленням пристроїв, що полегшує їх управління та забезпечує більш ефективну роботу мережі. Таким чином, комутатори Cisco Catalyst 2960 Plus з функцією PoE є необхідними для успішної інтеграції та оптимального функціонування пристроїв у мережі інтелектуального паркінгу.

В таблиці 2.2 наведена специфікація мережевого обладнання комп’ютерної системи ЖК Маршал.

Таблиця 2.2 – Специфікація обладнання

Позиція	Найменування	Марка	Одиниця вимірювання	Кількість
1	Маршрутизатор 2911w3 GE4 EHWIC2 DSP1SM256MB CF512MBDRAM,IPB	Cisco	шт.	4
2	Маршрутизатор ISR 4331 (3GE,2NIM,1SM,4G FLASH,4G DRAM,IPB)	Cisco	шт.	2
3	Комутатор Catalyst 2960 Plus 24 10/100 +2T/SFP LAN Base (WS-C2960+24TC-L)	Cisco	шт.	9
4	Комутатор Catalyst 2960 Plus 48 10/100 PoE + 2 1000BT + 2 SFP LAN Base (WS-C2960+48PST-L)	Cisco	шт.	3

Щодо кабельної системи, вона використовує різні технології передачі даних залежно від рівня доступу та ядра мережі. На рівні доступу використовується технологія Fast Ethernet, зі швидкістю передачі даних 100 Мбіт/с. На рівні ядра використовується технологія Gigabit Ethernet, яка забезпечує швидкість передачі даних 1 Гбіт/с, а також технологія Serial для сполучення між різними вузлами мережі.

Для оптимальної продуктивності серверів було обрано апаратне забезпечення з наступними характеристиками: використано процесор з потужністю 4,0 GHz і 12 ядрами. Для ефективного кешування і обробки великого обсягу запитів було встановлено 64 ГБ оперативної пам'яті. Для швидкого обміну даними з клієнтами та іншими серверами були використані високошвидкісні мережеві інтерфейси 10 Гбіт/с Ethernet. Щодо зберігання кешованих записів був використаний SSD-накопичувач з швидкістю читання/запису 1 ГБ/с і об'ємом 2 ТБ. Для надійності роботи сервера в разі відключення електроенергії використовується безперебійне живлення (UPS), яке забезпечує безперебійну роботу сервера протягом 30-60 хвилин.

2.3.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Найбільшою мережею підприємства є підмережа «Відділ продажу», тобто LAN_4. Щоб розрахувати інтенсивність вхідного трафіку дано:

– кількість вузлів в підмережі 85;

– середня інтенсивність трафіку складає μ=134 (кадрів/с);

− середня довжина повідомлення становить l=650 байт;

– затримка передачі пакету ≤ 6 мс;

– кількість портів комутатора – 24 шт.

Нижче наведено рішення наданої задачі.

Для визначення пропускної здатності мережі на рівні доступу застосовується формула (2.1).

$$Pp.p = \mu * l * n, \quad (2.1)$$

де Pp.p – пропускна здатність, біт/с;

μ – інтенсивність обслуговування, кадрів/с;

l – середня довжина повідомлення, байт;

n – кількість портів комутатора.

Підставляємо відомі значення:

μ = 134 кадри/с;

l = 650 байт;

n = 24;

Pp.p = 134 * 650 * 24 = 2 597 200 ≈ 2.6 (Мбіт/с)

Для розрахунку значення інтенсивності виходу використовуємо формулу (2.2). При розрахунках враховується, що навантаження на комутаторі розраховується через лінію 1000 Мбіт/с.

$$\mu вих = C/ (8 * l), \quad (2.2)$$

де C – пропускна здатність лінії, біт/с;

l – середня довжина повідомлення байт.

Підставляємо відомі значення:

C = 1 000 000 000 біт/с;

l = 650 байт.

μвих = 1 000 000 000 біт/с / (8 * 650) байт = 192 307 (пакетів/с)

Розрахунок максимальної кількості вузлів, яку можна приєднати до комутатора рівня розподілу на основі заданої середньої інтенсивності трафіку, робимо за допомогою формули (2.3).

$$N = \mu вих / \mu, \quad (2.3)$$

де N – кількість вузлів, яку можна приєднати;

μвих – інтенсивність виходу, пакетів/с;

μ – середня інтенсивність трафіку, пакетів/с.

За наданими значеннями, інтенсивність виходу становить 192 307 пакетів/с, а середня інтенсивність трафіку дорівнює 134 пакетів/с.

Виходячи з цього отримуємо:

N = 192 307/ 134 ≈ 1436.42 (вузлів)

Отже, за наданими значеннями, кількість вузлів, яку можна приєднати до комутатора рівня розподілу, становить приблизно 1436.42. Оскільки кількість вузлів зазвичай є цілим числом, можна округлити результат до найближчого цілого значення. Тому максимальна кількість вузлів, яку можна приєднати, складатиме 1436.

Для розрахунку загальної інтенсивності трафіку від всіх користувачів застосовуємо формулу (2.4).

$$\lambda = x * \mu, \quad (2.4)$$

де λ – загальна інтенсивність трафіку, пакети/с;

x – коефіцієнт, який представляє кількість користувачів або вузлів в мережі;

μ - середня інтенсивність трафіку, пакети/с.

Підставляємо відомі значення:

x = 85;

μ = 134.

λ = 85*134 = 11 390 (пакетів/с)

Для розрахунку коефіцієнту затримки на рівні розподілу, використовується формула (2.5):

$$\rho = \lambda / \mu вих, \quad (2.5)$$

де ρ – коефіцієнт затримки на рівні розподілу;

λ – загальна інтенсивність трафіку від всіх користувачів;

μвих – інтенсивність виходу, яка вказує на кількість пакетів, що виходять з комутатора за одиницю часу.

Підставляємо відомі значення:

λ = 11 390 пакетів/с;

μвих = 192 307 пакетів/с.

ρ = 11 390 / 192 307 ≈ 0.0592

Щоб розрахувати коефіцієнт зайнятості комутатора на рівні розподілу, використовується формула (2.6).

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

де r – коефіцієнт зайнятості комутатора;

ρ – коефіцієнт затримки на рівні розподілу.

Задано значення коефіцієнта затримки на рівні розподілу ρ ≈ 0.0592.

Підставимо ці значення в формулу:

r = 0.0592 / (1 - 0.0592) ≈ 0.063

Для розрахунку середньої затримки кадру, використовується формула (2.7).

$$T = 1 / (\mu вих - \lambda), \quad (2.7)$$

де T – середня затримка кадру;

λ – загальна інтенсивність трафіку від всіх користувачів;

μвих – інтенсивність виходу, яка вказує на кількість пакетів, що виходять з комутатора за одиницю часу.

Підставляємо відомі значення:

λ = 11 390 пакетів/с;

μвих = 192 307 пакетів/с.

T = 1 / (192 307 – 11 390) ≈ 0.0052 (секунд) = 52 * 10^{-6}(секунд)

Для розрахунку середньої довжини черги використовується формула (2.8).

$$Lчерги = \rho^2 / (1 - \rho), \quad (2.8)$$

де Lчерги – середня довжина черги;

ρ – коефіцієнт затримки на рівні розподілу.

Отримане значення коефіцієнта затримки на рівні розподілу $\rho \approx 0.0592$, підставимо це значення в формулу:

Lчерги = $(0.0592)^2$ / (1 - 0.0592) ≈ 0.00361 / 0.9408 ≈ 0.0038

Отже, отримали середню довжину черги приблизно рівною 0.0038.

Для розрахунку середнього часу перебування пакета в черзі використовується формула (2.9).

$$Точік = Lчерги / \lambda, \quad (2.9)$$

де Точік – середній час перебування пакета в черзі;

Lчерги – середня довжина черги;

λ – загальна інтенсивність трафіку від всіх користувачів.

Задане значення середньої довжини черги Lчерги ≈ 0.0038 і загальна інтенсивність трафіку λ = 11 390 пакетів/с.

Підставимо ці значення в формулу:

Точік = 0.0038 / 11 390 = 0.334 (мс)

Значення Точік менше ніж у наданих вимогах (6 мс), а отже вимоги виконані.

Розрахунок пропускної здатності каналу можна виконати за формулою (2.10).

$$b = \lambda * l, \qquad (2.10)$$

де b - пропускна здатність каналу, біт/с;

λ - інтенсивність трафіку, пакетів/с;

l - середня довжина пакету, байт.

Замінивши значення у формулу, отримаємо:

λ = 11 390 пакетів/с;

l = 650 байт.

b = 11 390 * 650 = 7 403 500 біт/с.

Отже, результат розрахунку пропускної здатності каналу 7.4035 Мбіт/с співпадає з вихідною пропускною здатністю каналу 1000 Мбіт/с.

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

3.1 Розрахунок схеми адресації корпоративної мережі

Для побудови мережі ЖК «Маршал» був використаний адресний простір 172.23.152.0/21. Це означає, що у нас доступно 11 біт для розподілу підмереж та пристроїв у цій мережі.

Для розрахунку підмереж можна використовувати VLSM, щоб ефективно використовувати доступні IP-адреси та мінімізувати втрату адресного простору. VLSM – це технологія, яка дозволяє ефективно використовувати IP-адреси, розподіляючи їх на підмережі з різними розмірами масок. У стандартних мережевих конфігураціях, усі підмережі використовують однакові маски підмереж (як правило, класові маски), незалежно від розміру мережі або кількості пристроїв. Це може приводити до неефективного використання IP-адрес. VLSM дозволяє розподіляти IP-адреси більш гнучко, надаючи можливість використовувати маски підмереж різної довжини в мережі. Це дозволяє точніше визначити розмір кожної підмережі відповідно до потреб мережі, забезпечуючи економію IP-адрес і краще використання доступних ресурсів.

Зауважимо, що адреси з діапазону 10.0.11.0/24 використовуються лише для послідовних каналів між маршрутизаторами. Вони не входять у загальний адресний простір 172.23.152.0/21.

Розглянемо детальний опис розбиття мережі на прикладі найбільшої підмережі, яка в даному випадку є LAN4 (Відділ продажу) з 85 пристроями.

Для визначення необхідної маски підмережі для найбільшої наданої мережі, спочатку потрібно визначити кількість необхідних вузлів (пристроїв) для цієї підмережі.

Застосовуючи формулу $2^n - 2 \geq$ кількість необхідних вузлів, ми шукаємо найменше значення «n», для якого $2^n - 2$ буде більше або рівне 85.

Знайдемо таке значення «n»:

$2^n - 2 \geq 85$

$2^n \geq 87$

Найменше значення «n», яке задовольняє це нерівність, є 7, оскільки $2^7 = 128$, що більше за 87. Отже, нам потрібно 7 бітів для ідентифікації хостів у найбільшій підмережі.

Тепер можна побудувати маску підмережі, розмістивши 7 «1» у масці, а решту бітів (25 бітів) заповнивши «0». У двійковому форматі маска підмережі буде мати вигляд: 11111111.11111111.11111111.10000000.

Потім, з використанням цієї маски підмережі, можна встановити початкову IP-адресу для найбільшої підмережі, яка надається як 172.23.152.0, а також мережеву адресу, яка буде такою ж, як початкова IP-адреса, і широкомовну адресу, яка буде останньою адресою в доступному діапазоні, тобто 172.23.152.127.

Отже, для найбільшої наданої мережі, маска підмережі буде 255.255.255.128 або /25, а доступний діапазон IP-адрес буде від 172.23.152.1 до 172.23.152.126, з мережевою адресою 172.23.152.0 та широкомовною адресою 172.23.152.127.

Усі підмережі розраховуються аналогічним принципом, всі результати розрахунків наведено в таблиці 3.1.

Таблиця 3.1 – Схема адресації корпоративної мережі ЖК «Маршал»

Назва підмережі	Необхідна кількість вузлів	Номер мережі	Маска мережі	Діапазон доступних адрес
LAN1 (технічний відділ)	61	172.23.152.128	255.255.255.192	172.23.152.129 – 172.23.152.190
LAN2 (відділ маркетингу)	32	172.23.152.192	255.255.255.192	172.23.152.193 – 172.23.152.254

Продовження таблиці 3.1

Назва підмережі	Необхідна кількість вузлів	Номер мережі	Маска мережі	Діапазон доступних адрес
LAN3 (відділ обслуговування)	10	172.23.153.32	255.255.255.240	172.23.153.33 – 172.23.153.46
LAN4 (відділ продажу)	85	172.23.152.0	255.255.255.128	172.23.152.1 – 172.23.152.126
VLAN24 (маркетологи)	27	172.23.152.0	255.255.255.224	172.23.152.1 – 172.23.152.30
VLAN34 (дизайнери)	27	172.23.152.32	255.255.255.224	172.23.152.33 – 172.23.152.62
VLAN44 (копірайтери)	27	172.23.152.64	255.255.255.224	172.23.152.65 – 172.23.152.94
VLAN99	4	172.23.152.96	255.255.255.248	172.23.152.97 – 172.23.152.102
LAN5 (віддалена мережа головного офісу)	19	172.23.153.0	255.255.255.224	172.23.153.1 – 172.23.153.30
WAN1	2	10.0.14.0	255.255.255.252	10.0.14.1 – 10.0.14.2
WAN2	2	10.0.14.4	255.255.255.252	10.0.14.5 – 10.0.14.6
WAN3	2	10.0.14.8	255.255.255.252	10.0.14.9 – 10.0.14.10
WAN4	2	10.0.14.12	255.255.255.252	10.0.14.13 – 10.0.14.14
WAN5	2	10.0.14.16	255.255.255.252	10.0.14.17 – 10.0.14.18
WAN_IPS	2	209.165.202.0	255.255.255.224	209.165.202.1 – 209.165.202.30

Результуючі розрахунок підмереж, можна зробити висновки, що з 2046

доступних адрес використано 294, при необхідній кількості 207. Тобто 15% доступного адресного простору використовуються на 70%.

3.2 Розрахунок схеми адресації пристроїв

Для розрахунку схеми адресації пристроїв, потрібно визначити IP-адреси для кожного пристрою в мережі, враховуючи вимоги проектування, таких як:

– інтерфейсам і підінтерфейсам маршрутизаторів у LAN призначаються перші можливі для використання IP-адреси;

– комутаторам призначаються другі з можливих IP-адрес для кожної LAN;

– вузлам призначаються останні з використовуваних IP-адрес;

– в мережах VLAN використовується адресація кінцевих пристроїв за допомогою протоколу DHCP.

На основі розрахованих даних, наведених у таблиці 3.1, була складена схема адресації пристроїв, яка представлена у таблиці 3.2.

Таблиця 3.2 – Схема адресації пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Pasichna_ Router_1	Gig0/0	10.0.14.14	/30	-	-	Gig0/0
	Gig0/1	172.23.152.129	/26	-	-	Fa0/1
Pasichna_ Router_2	Se0/1/1	10.0.14.9	/30	-	-	Se0/0/1
	Gig0/0	10.0.14.13	/30	-	-	Gig0/0
	Gig0/1	10.0.14.5	/30	-	-	Gig0/1
Pasichna_ Router_3	Se0/2/0	10.0.14.2	/30	-	-	Se0/1/0
	Gig0/0	172.23.153.33	/28	-	-	Gig0/1
	Gig0/1	10.0.14.6	/30	-	-	Gig0/1
	Gig0/2	172.23.152.193	/26	-	-	Gig0/2
Pasichna_ Router_4	Se0/1/0	209.165.202.2	/27	-	-	Se0/0/0
	Se0/1/1	10.0.14.10	/30	-	-	Se0/0/1

Продовження таблиці 3.2

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Pasichna_ Router_4	Se0/2/0	10.0.14.1	/30	-	-	Se0/1/0
	Gig0/1	-	-	-	-	Gig0/1
	Gig0/1.24	172.23.152.1	/27	-	24	Gig0/1
	Gig0/1.34	172.23.152.33	/27	-	34	Gig0/1
	Gig0/1.44	172.23.152.65	/27	-	44	Gig0/1
	Gig0/1.99	172.23.152.97	/29	-	99	Gig0/1
Pasichna_ Router_0	Gig0/0/1	172.23.153. 0	/27	-	-	Gig0/1
	Gig0/0/0	64.100.13.2	/30	-	-	Gig0/2
Pasichna_ Router_ IPS	Se0/0/0	209.165.202.1	/30	-	-	Se0/1/0
	Gig0/0	209.165.201.1	/28	-	-	NIC
	Gig0/2	64.100.13.1	/27	-	-	Gig0/0/1
Pasichna_ Switch_1. 1	VLAN1	172.23.152.130	/26	172.23.152.129	-	Gig0/1
						F0/2
						F0/3
						F0/6
						F0/7
Pasichna_ Switch_1. 2	VLAN1	172.23.152.131	/26	172.23.152.129	-	F0/2
						F0/3
						F0/4
						F0/5
Pasichna_ Switch_1. 3	VLAN1	172.23.152.132	/26	172.23.152.129	-	F0/4
						F0/5
						F0/6
						F0/7
Pasichna_ Switch_2	VLAN1	172.23.152.194	/26	172.23.152.193	-	Gig0/2
Pasichna_ Switch_3	VLAN1	172.23.153.34	/28	172.23.153.33	-	Gig0/0
Pasichna_ Switch_4. 1	VLAN99	172.23.152.98	/29	172.23.152.97	-	Gig0/1
						F0/1
						F0/2
Pasichna_ Switch_4. 2	VLAN99	172.23.152.99	/29	172.23.152.97	-	F0/1

Кінець таблиці 3.2

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Pasichna_Switch_4.3	VLAN99	172.23.152.100	/29	172.23.152.97	-	F0/2
Pasichna_Switch_5	VLAN1	172.23.153.2	/27	172.23.153.1	-	Gig0/0

3.3 Розробка топологічної схеми корпоративної мережі

На основі топології та таблиць 3.1-3.2, була побудована модель комп'ютерної мережі в Cisco Packet Tracer, яку можна побачити на рисунку 3.1.

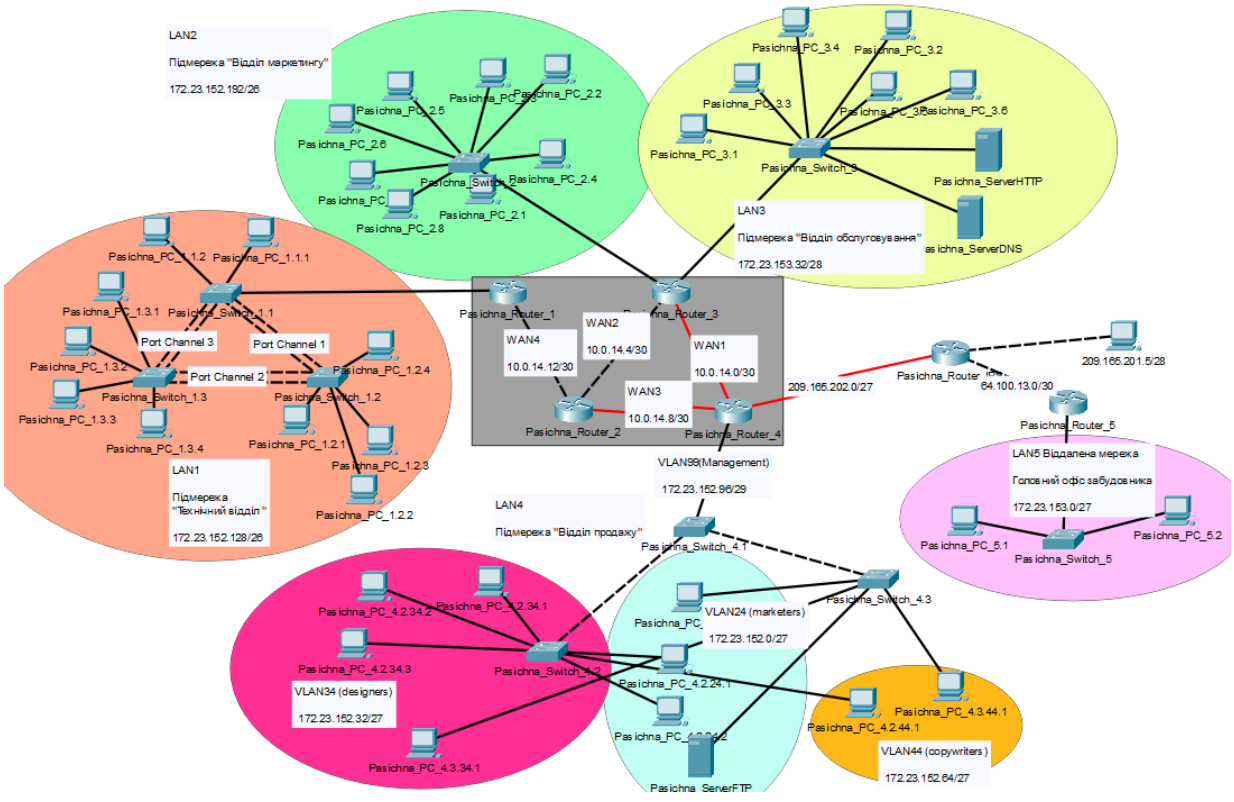

Рисунок 3.1 – Модель мережі, розроблена в Cisco Packet Tracer

3.4 Налаштування роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв КС

Для початкового налаштування параметрів пристроїв потрібно виконати базову конфігурацію. Для цього було виконано наступні дії:

– надано унікальні ім’я пристроям;

– налаштовано пароль cisco на консолі та лінії vty;

– застосовано пароль class для привілейованого режиму;

– забезпечено шифрування усіх паролів;

− виконано налаштування банеру MOTD;

− налаштовано на лініях vty застосування протоколу ssh;

– назначено користувача 12320sk1_Pasichna з паролем admincisco;

– використовуючи ім’я пристрою налаштовано ім’я домену та згенеровано ключ RSA завдовжки 1024 біт;

– встановлено значення тактової частоти 128000 на DCE-інтерфейсах маршрутизаторів

− з використанням локальної бази було налаштовано аудит і відправку повідомлень про початок і завершення процесу exec.

Далі розглядаються приклади налаштування пристроїв.

Надання пристрою унікального ім’я, використовуючи команду *hostname*:

Router(config)#hostname Pasichna_Router_1

Налаштування паролів cisco на консолі та лінії vty 0 15:

Pasichna_Router_1(config)#line console 0

Pasichna_Router_1(config-line)#password cisco

Pasichna_Router_1(config-line)#login

Pasichna_Router_1(config-line)#exit

Pasichna_Router_1(config)#line vty 0 15

Pasichna_Router_1(config-line)#password cisco

Pasichna_Router_1(config-line)#login

Pasichna_Router_1(config-line)#exit

Застосування паролю class для входу у привілейований режим:

Pasichna_Router_1(config)#enable secret class

Використання сервісу шифрування усіх паролів, які у відкритому доступі:

Pasichna_Router_1(config)#service password-encryption

Налаштування банеру MOTD:

Pasichna_Router_1(config)#banner motd #Pasichna_Router_1. This is a secure system. Authorized Access Only!#

Налаштування протоколу SSH:

– створення домену:

Pasichna_Router_1(config)#ip domain name Pasichna_Router_1

– налаштування версії протоколу SSH:

Pasichna_Router_1(config)#ip ssh version 2

– генерація ключа RSA довжиною 1024 bit:

Pasichna_Router_1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

– створення користувача 12320sk1_Pasichna з паролем admincisco:

Pasichna_Router_1(config)#username 12320sk1_Pasichna privilege 15 password admincisco

– налаштування протоколу SSH лініях VTY 0 15:

Pasichna_Router_1(config)#line vty 0 15

Pasichna_Router_1(config-line)#transport input ssh

Pasichna_Router_1(config-line)#login local

Pasichna_Router_1(config-line)#exec-time 60 0

Встановлення IP-адрес на інтерфейсах, відповідно до таблиці 3.2, в якості прикладу наведено налаштування інтерфейсу GigabitEthernet0/0 на маршрутизаторі Pasichna_Router_1:

Pasichna_Router_1(config)#int g0/0

Pasichna_Router_1(config-if)#no sh duwn

Pasichna_Router_1(config-if)#ip addr 10.0.14.14 255.255.255.252

Pasichna_Router_1(config-if)#exit

На DCE-інтерфейсах налаштування тактової частоти 128000:

Pasichna_Router_2(config-if)#clock rate 128000

3.4.2 Налаштування маршрутизаторів в КС ЖК «Маршал»

Для забезпечення динамічної маршрутизації в системі ЖК «Маршал» використовується протокол OSPF. Цей протокол має ряд переваг, які сприяють ефективній та надійній роботі мережі ЖК.

Однією з переваг OSPF є його здатність пристосовуватися до змін у мережі. Він автоматично оновлює маршрути, коли відбуваються зміни в топології мережі, такі як додавання або вилучення маршрутизаторів або зміна стану з'єднань. Це робить OSPF ідеальним протоколом для житлових комплексів, де можуть виникати зміни у конфігурації мережі, наприклад, через підключення нових користувачів або відключення обладнання.

Один зі способів, яким OSPF забезпечує динамічну маршрутизацію, - це використання алгоритму Дейкстри для визначення найкоротшого шляху до кожного вузла в мережі. Це дозволяє OSPF знаходити оптимальні маршрути, що сприяє ефективному використанню ресурсів мережі ЖК. Наприклад, OSPF може визначити найкоротший шлях до сервера медіа-контенту або до іншого важливого вузла в мережі.

Одна з інших переваг OSPF полягає в його масштабованості. OSPF може працювати у великих мережах з багатьма маршрутизаторами, розділеними на різні області. Це робить його ідеальним протоколом для великих житлових комплексів, де мережева інфраструктура може бути розподілена на різні сегменти або підмережі.

Крім того, OSPF підтримує безпеку мережі ЖК. Він використовує різні механізми, такі як аутентифікація та шифрування, для захисту від несанкціонованого доступу та перехоплення даних. Це дозволяє забезпечити конфіденційність та цілісність даних, що передаються по мережі ЖК.

Загалом, протокол OSPF є потужним і надійним інструментом для

забезпечення динамічної маршрутизації в системі житлового комплексу. Він забезпечує ефективну передачу даних, швидке відновлення після відмов, підтримку QoS та безпеку мережі. Використання OSPF допомагає забезпечити стабільну та високоякісну мережеву інфраструктуру, що задовольняє потреби мешканців житлового комплексу.

Нижче, на прикладі маршрутизатора Pasichna_Router_1, наведено налаштування маршрутизації, безпосередньо з реалізацією протоколу OSPF:

– активація протоколу маршрутизації OSPF з вказанням номеру процесу OSPF, який буде використовуватися:

Pasichna_Router_1(config)#router ospf 9

– додавання мереж до області маршрутизації 0:

Pasichna_Router_1(config-router)#network 172.23.152.128 0.0.0.63 area 0

Pasichna_Router_1(config-router)#network 10.0.14.12 0.0.0.3 area 0

Налаштування статичного маршруту на маршрутизаторі, який має пряме підключення до маршрутизатора провайдера:

Pasichna_Router_4(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1

На serial-інтерфейсах виконується налаштування пропускної спроможності та значення метрики OSPF:

– перехід до налаштування інтерфейсу Serial 0/0/1:

Pasichna_Router_2(config)#int se0/0/1

– встановлення значення пропускної здатності 128Кбіт/с:

Pasichna_Router_2(config-if)#bandwidth 128

– встановлення значення метрики на 7500:

Pasichna_Router_2(config-if)#ip ospf cost 7500

3.4.3 Налаштування служби AAA на маршрутизаторах

Служба AAA – це механізм аутентифікації, авторизації та обліку, що використовується для керування доступом до мережевих ресурсів. Вона надає рівень безпеки і контролю над користувачами, які намагаються отримати доступ до мережевих пристроїв.

Основні функції служби AAA:

– аутентифікація, перевірка ідентифікації користувача, який намагається отримати доступ до мережевого пристрою;

– авторизація, визначення прав доступу після успішної аутентифікації;

– облік, збір і реєстрація інформації про використання мережевих ресурсів користувачами.

Служба AAA дозволяє організаціям централізовано керувати доступом до мережевих ресурсів, надає зручність управління користувачами, спрощує процеси аутентифікації та авторизації, а також надає засоби для виконання аудиту і контролю за використанням мережі.

Відповідно до вимог, на маршрутизаторах налаштовано підтримку служби AAA та налаштовано RADIUS-сервер з ключовим словом «radius123». Для облікових записів користувачів використовується ім'я пристрою з паролем «admin123».

Нижче наведено процес налаштування аутентифікації AAA з використанням RADIUS-сервера для доступу до консольної лінії та ліній VTY на маршрутизаторі Pasichna_Router_3 в якості прикладу.

Увімкнення використання моделі AAA та налаштування аутентифікацію для входу:

Pasichna_Router_3(config)#aaa new-model

Pasichna_Router_3(config)#aaa authentication login default group radius local

Налаштування RADIUS-сервера:

Pasichna_Router_3(config)#radius server serverRadius

Pasichna_Router_3(config-radius-server)#addr ipv4 172.23.153.46

Pasichna_Router_3(config-radius-server)#key radius123

Pasichna_Router_3(config-radius-server)#exit

Налаштування аутентифікації для консольної лінії та VTY:

Pasichna_Router_3(config)#line console 0

Pasichna_Router_3(config-line)#login authentication default

Pasichna_Router_3(config-line)#line vty 0 15

Pasichna_Router_3(config-line)#login authentication default

На рисунку 3.2 зображено успішний вхід до маршрутизатора Pasichna_Router_3 через аутентифікацію сервера RADIUS

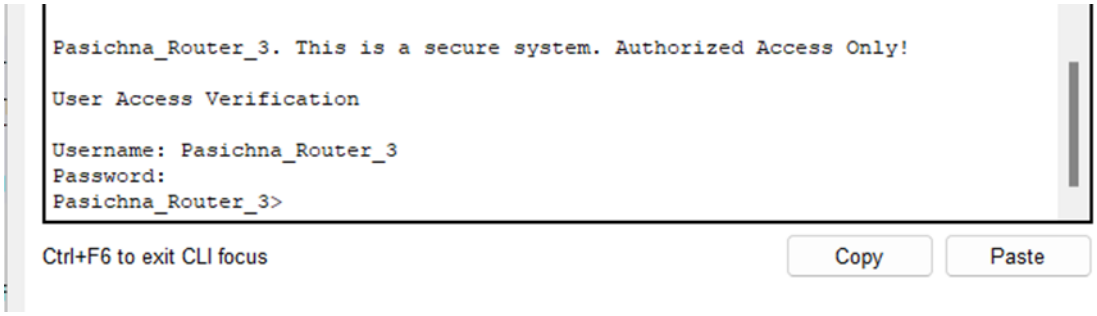

Рисунок 3.2 – Аутентифікація через RADIUS сервер

3.4.4 Налаштування роботи Інтернету в КС ЖК «Маршал»

За вимогами для розгортання корпоративної мережі, заданий блок адрес з приватних адрес з використанням діапазону. Щоб забезпечити доступ робочих станцій організації до Інтернету, на прикордонному маршрутизаторі потрібно використовувати технологію NAT.

NAT – це технологія, яка використовується для перетворення IP-адрес між різними мережевими доменами. Основна функція NAT – забезпечити доступ до Інтернету для приватних IP-адрес, які не можуть маршрутизувати через Інтернет.

У процесі NAT, приватні IP-адреси заміняються на публічні IP-адреси, що можуть маршрутизувати через Інтернет. Це забезпечує масштабованість мережі, оскільки можна використовувати обмежений блок публічних IP-адрес для багатьох приватних IP-адрес.

На прикордонному маршрутизаторі було налаштовано NAT відповідно до вимог, що включають наступні параметри:

– ім'я пулу Internet;

– пул IP-адрес від 209.165.202.5 до 209.165.202.30;

– адреса серверу HTTP 209.165.200.4;

– номер списку доступу 14.

Це означає, що при здійсненні NAT, IP-адреси з пулу 209.165.202.5-209.165.202.30 будуть використовуватися для перетворення приватних адрес. Цей процес дозволить приватній мережі отримати доступ до Інтернету, використовуючи публічні IP-адреси з заданого пулу. Додатково, номер списку доступу 14 може використовуватися для налаштування правил контролю доступу до мережі.

Нижче наведено процес налаштування маршрутизатора Pasichna_Router_4:

– створення список доступу з номером 14, який дозволяє трафіку з мережі 172.23.152.0/21 (від 172.23.152.0 до 172.23.159.255) проходити через NAT:

Pasichna_Router_4(config)#access-list 14 permit 172.23.152.0 0.0.7.255

– створення пулу IP-адрес з назвою «Internet» від 209.165.202.5 до 209.165.202.30 з маскою підмережі 255.255.255.224. Цей пул буде використовуватися для перетворення приватних адрес в публічні:

Pasichna_Router_4(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224

– налаштування використання пулу «Internet» для перетворення IP-адрес, що відповідають списку доступу 14:

Pasichna_Router_4(config)#ip nat inside source list 14 pool Internet

– задання статичного NAT, де локальна IP-адреса 172.23.153.45 буде перетворена на публічну IP-адресу 209.165.202.4:

Pasichna_Router_4(config)#ip nat inside source static 172.23.153.45 209.165.202.4

– налаштування інтерфейсу маршрутизатора, як зовнішній інтерфейс для NAT. Цей інтерфейс з'єднується з Інтернетом:

Pasichna_Router_4(config)#int se0/1/0

Pasichna_Router_4(config-if)#ip nat outside

– встановлення інтерфейсів, як внутрішні інтерфейси для NAT, на

прикладі інтерфейсу se0/2/0:

Pasichna_Router_4(config-subif)#in se0/2/0

Pasichna_Router_4(config-if)#ip nat inside

На рисунку 3.3 зображено таблицю перетворень NAT на маршрутизаторі Pasichna_Router_4.

NAT Table for Pasichna_Router_4

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.7:5	172.23.153.35:5	209.165.201.5:5	209.165.201.5:5
icmp	209.165.202.7:6	172.23.153.35:6	64.100.13.2:6	64.100.13.2:6
icmp	209.165.202.5:8	172.23.153.38:8	64.100.13.2:8	64.100.13.2:8
icmp	209.165.202.6:24	172.23.153.39:24	64.100.13.2:24	64.100.13.2:24
icmp	209.165.202.4:7	172.23.153.45:7	64.100.13.2:7	64.100.13.2:7
icmp	209.165.202.4:8	172.23.153.45:8	64.100.13.2:8	64.100.13.2:8
icmp	209.165.202.4:9	172.23.153.45:9	209.165.202.1:9	209.165.202.1:9

0

Рисунок 3.3 – NAT Table for Pasichna_Router_4

3.4.5 Впровадження VPN

Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec забезпечує безпеку та захищений обмін даними між різними мережами організації. Цей процес передбачає встановлення правил фільтрації, шифрування, аутентифікації та інших параметрів, що забезпечують конфіденційність та цілісність даних під час передачі через публічну мережу.

IPsec використовує шифрування для захисту інформації від несанкціонованого доступу та перехоплення. IPsec також забезпечує цілісність даних, що передаються між мережами. Це означає, що інформація не може бути змінена або порушена під час передачі через мережу. Це важливо для запобігання можливим атакам на дані та забезпечення їх непошкодженості.

IPsec дозволяє проводити процес аутентифікації та авторизації між

мережами. Це дозволяє перевіряти, що сторони, що спілкуються, є дійсними та мають право на доступ до ресурсів мережі. Це допомагає уникнути несанкціонованого доступу та забезпечує контроль над використанням мережевих ресурсів.

Віртуальна приватна мережа site-to-site VPN дозволяє інтегруватися з існуючою мережевою інфраструктурою організації. Це дозволяє забезпечити безпечний обмін даними між різними підрозділами підприємства, навіть якщо вони знаходяться на віддалених місцях.

Нижче розглядається приклад налаштування на маршрутизаторі Pasichna_Router_4.

Перш за все, виконується налаштування списку контролю доступу 100. Цей список використовується для визначення правил фільтрації трафіку, які дозволяють або забороняють певні типи IP-пакетів:

Pasichna_Router_4(config)ip access-list extended 100

Pasichna_Router_4(config-ext-nacl)#permit ip any 209.165.200.0 0.0.0.31

Pasichna_Router_4(config-ext-nacl)#permit ip 172.23.152.0 0.0.7.255 209.165.202.0 0.0.0.31

Pasichna_Router_4(config-ext-nacl)#permit ospf any any

Перше правило дозволяє IP-пакетам будь-якого джерела йти до мережі 172.23.152.0/21. Друге правило дозволяє IP-пакетам з підмережі 172.23.152.0/21 надсилатись до мережі 209.165.202.0/27. Третє правило дозволяє IP-пакетам протоколу OSPF проходити в будь-якому напрямку.

Після цього налаштовується прив'язка списку контролю доступу 100 до інтерфейсу s0/1/0, де відбувається вхідний трафік.

Далі налаштовується список контролю доступу VPN, який визначає правила для трафіку, що пройде через VPN-з'єднання:

Pasichna_Router_4(config)#ip access-list extended VPN

Pasichna_Router_4(config-ext-nacl)#permit ip 172.23.152.0 0.0.7.255 172.23.153.0 0.0.0.31

Це правило дозволяє IP-пакетам з діапазону 172.23.152.0/21 йти до

діапазону 172.23.153.0/27.

Потім налаштовується політика ISAKMP, яка визначає параметри шифрування та аутентифікації:

Pasichna_Router_4(config)#crypto isakmp policy 1

Pasichna_Router_4(config-isakmp)#encryption aes 256

Pasichna_Router_4(config-isakmp)#authentication pre-share

Pasichna_Router_4(config-isakmp)#group 1

Політика ISAKMP використовує шифрування AES з довжиною ключа 256 біт, аутентифікацію за допомогою попередньо обмінюваних ключів та групу 1 для обміну ключами.

Далі налаштовується ключ ISAKMP з адресою 64.100.13.2

Pasichna_Router_4(config)#crypto isakmp key cisco address 64.100.13.2

Цей ключ використовується для аутентифікації та обміну ключами між мережами.

Потім налаштовується набір трансформацій IPsec, який визначає методи шифрування та хешування для IPsec-з'єднання:

Pasichna_Router_4(config)#crypto ipsec transform-set VPN-IPSEC-SET esp-aes esp-sha-hmac

Цей набір трансформацій використовує шифрування AES та хешування SHA для захисту даних, що передаються через VPN.

Далі створюється криптографічна карта. Проте, ця карта залишається вимкненою до налаштування піра (віддаленої мережі) та дійсного списку контролю доступу.

На наступному етапі встановлюється адреса піра, з яким буде встановлено з'єднання VPN:

Pasichna_Router_4(config-crypto-map)#set peer 64.100.13.2

Встановлюється набір трансформацій для шифрування та хешування даних. Вказується, що до трафіку, що проходить через криптографічну карту, будуть застосовуватися правила зі списку контролю доступу «VPN».

Далі встановлюється криптографічна карта інтерфейсу se0/1/0.

Також налаштовується правило перетворення адреси NAT для трафіку, що проходить через VPN.

На рисунку 3.4 зображено результат виконання команди, яка допомагає адміністраторам мережі контролювати та діагностувати безпекові асоціації IPsec, перевіряти стан трафіку та виявляти можливі проблеми з налаштуванням або з'єднанням.

Рисунок 3.4 – Демонстрація стану IPsec

3.4.6 Налаштування агрегування каналів в підмережі «Технічний відділ»

PAgP та LACP – це протоколи, що використовуються для агрегації портів в мережевих комутаторах з метою створення логічних груп з'єднаньабо транкових каналів. Обидва протоколи дозволяють об'єднати кілька фізичних портів в одне віртуальне з'єднання, що забезпечує більшу пропускну здатність та надійність мережі.

PAgP є Cisco-специфічним протоколом і працює тільки на комутаторах Cisco. Він дозволяє автоматично створювати та управляти агрегованими з'єднаннями портів між комутаторами. PAgP має різні режими роботи, такі як «auto», «desirable» та «on», які контролюють спосіб утворення та підтримки агрегованих з'єднань між комутаторами.

LACP є стандартом IEEE 802.3ad і може використовуватись на різних виробниках комутаторів. Він забезпечує створення та керування агрегованими з'єднаннями портів. LACP також має режими роботи, такі як «active» та «passive», які визначають, яка сторона ініціює утворення та підтримку агрегованого з'єднання.

За допомогою технології EtherChannel, було створено агреговані з'єднання фізичних портів на комутаторах в мережі LAN_1 з метою збільшення пропускної здатності та надійності каналів. Це дозволяє об'єднати кілька фізичних портів в один логічний канал, що має головну перевагу у вигляді підвищеної швидкості передачі даних. Таке об'єднання створює здатність до передачі даних через паралельне використання кількох портів одночасно, забезпечуючи велику пропускну здатність і балансування навантаження. При цьому, в разі відмови одного порту, інші порти продовжують працювати безперебійно, що покращує надійність каналу.

Налаштування комутаторів наведено нижче.

Встановлення діапазону портів на комутаторах у режим trunk, на прикладі комутатора Pasichna_Switch_1.1:

Pasichna_Switch_1.1(config)#int range fa0/2-3, fa0/6-7

Pasichna_Switch_1.1(config-if-range)#switchport mode trunk

Налаштування EtherChannel за допомогою протоколу Cisco PAgP на прикладі команд на комутаторі Pasichna_Switch_1.1:

Pasichna_Switch_1.1(config)#int range fa0/6-7

Pasichna_Switch_1.1(config-if-range)#sh

Pasichna_Switch_1.1(config-if-range)#channel-group 3 mode desirable

Pasichna_Switch_1.1(config-if-range)#

Creating a port-channel interface Port-channel 3

Pasichna_Switch_1.1(config-if-range)#no sh

Pasichna_Switch_1.1(config-if-range)#exit

Pasichna_Switch_1.1(config)#int port-channel 3

Pasichna_Switch_1.1(config-if)#switchport mode trunk

Налаштування EtherChannel LACP 802.3ad за приклад взято дії виконанні на комутаторі Pasichna_Switch_1.2:

Pasichna_Switch_1.2(config-if)#int range fa0/4-5

Pasichna_Switch_1.2(config-if-range)#sh

Pasichna_Switch_1.2(config-if-range)#channel-group 2 mode passive

Pasichna_Switch_1.2(config-if-range)#

Creating a port-channel interface Port-channel 2

Pasichna_Switch_1.2(config-if-range)#no sh

Pasichna_Switch_1.2(config-if-range)#exit

Pasichna_Switch_1.2(config)#int port-channel 2

Pasichna_Switch_1.2(config-if)#switchport mode trunk

Щоб переконатись в роботі протоколів PAgP та LACP на комутаторах, було виконано команду *show etherchennal summary* (рисунок 3.5-3.7).

```
Pasichna_Switch_1.1(config)#do sh eth sum
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)           LACP   Fa0/2(P) Fa0/3(P)
3      Po3(SU)           PAgP   Fa0/6(P) Fa0/7(P)
Pasichna_Switch_1.1(config)#
```

Рисунок 3.5 – Перевірка стану та конфігурації порт-каналів на комутаторі Pasichna_Switch_1.1

```
Pasichna_Switch_1.2(config)#do sh eth sum
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)           LACP   Fa0/2(P) Fa0/3(P)
2      Po2(SU)           LACP   Fa0/4(P) Fa0/5(P)
Pasichna_Switch_1.2(config)#
```

Рисунок 3.6 – Перевірка стану та конфігурації порт-каналів на комутаторі Pasichna_Switch_1.2

```
Pasichna_Switch_1.3(config)#do sh eth sum
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
------+-------------+-----------
+----------------------------------------------

2      Po2(SU)           LACP   Fa0/4(P) Fa0/5(P)
3      Po3(SU)           PAgP   Fa0/6(P) Fa0/7(P)
Pasichna_Switch_1.3(config)#
```

Рисунок 3.7 – Перевірка стану та конфігурації порт-каналів на комутаторі Pasichna_Switch_1.3

3.5 Захист інформації в КС ЖК «Маршал» від несанкціонованого доступу

3.5.1 Налаштування VLAN в підмережі «Відділ продажу»

У відділі продажу працює значна кількість спеціалістів, тому для організації мережі було розбито її на окремі логічні підмережі, або VLAN. Однією з ключових переваг такого підходу є можливість зекономити на додатковому обладнанні.

Цей підхід до розподілу мережі на VLAN дозволяє використовувати один фізичний інфраструктурний шар для розмежування трафіку між різними

групами співробітників. Використання VLAN дозволяє зменшити потребу у додаткових комутаторах та маршрутизаторах, оскільки різні групи користувачів можуть бути обслуговані на різних VLAN, використовуючи той самий комутатор або мережевий з'єднувач. Це призводить до економії на додатковому обладнанні, зниження вартості впровадження та обслуговування мережі.

Крім економії на обладнанні, використання VLAN також дозволяє покращити безпеку мережі шляхом логічного відокремлення різних груп користувачів. Кожен VLAN може мати свої правила доступу і обмеження, що дозволяє забезпечити контроль над трафіком і знизити ризик несанкціонованого доступу до ресурсів мережі.

В таблиці 3.3 представлено розподілення підмережі «Відділ продажу» на VLAN.

Таблиця 3.3 – Список мереж VLAN

Номер VLAN	Назва VLAN	Примітка
1	default	Не використовується
24	Marketers	Для маркетологів
34	Designers	Для дизайнерів
44	Copywriters	Для копірайтерів
99	Management	Для управління пристроями
100	Native	Власна мережа

Налаштування пристрої для виконання розподілення мережі на VLAN наведено нижче

Налаштування інтерфейсу GigabitEthernet0/1, який підключений до маршрутизатора на комутаторі Pasichna_Switch_4.1:

– перехід до налаштувань інтерфейсу GigabitEthernet0/1:

Pasichna_Switch_4.1 (config)#int g0/1

– встановлення інтерфейсу в режим роботи "trunk:

Pasichna_Switch_4.1 (config-if)#switchport mode trunk

– встановлення VLAN 100 , як власний VLAN для непомаркованого трафіку на транк-порту:

Pasichna_Switch_4.1 (config-if)#switchport trunk native vlan 100

– визначення спуску дозволених VLAN на транк-порту:

Pasichna_Switch_4.1 (config-if)#switchport trunk allowed vlan 24,34,44,99-100

– ввімкнення інтерфейсу GigabitEthernet0/1:

Pasichna_Switch_4.1 (config-if)#no sh

Створення VLAN 24, 34, 44, 99, 100 та надання ім’я кожному VLAN:

Pasichna_Switch_4.1 (config)#vlan 24

Pasichna_Switch_4.1 (config-vlan)#name Marketers

Pasichna_Switch_4.1 (config-vlan)#vlan 34

Pasichna_Switch_4.1 (config-vlan)#name Designers

Pasichna_Switch_4.1 (config-vlan)#vlan 44

Pasichna_Switch_4.1 (config-vlan)#name Copywriters

Pasichna_Switch_4.1 (config-vlan)#vlan 99

Pasichna_Switch_4.1 (config-vlan)#name Management

Pasichna_Switch_4.1 (config-vlan)#vlan 100

Pasichna_Switch_4.1 (config-vlan)#name Native

Налаштування VLAN 99, а саме надання опису призначення інтерфейсу, надання IP-адреси для інтерфейсу VLAN 99, встановлення шлюзу за замовчуванням та ввімкнення інтерфейсу VLAN 99, в якості прикладу наведено налаштування комутатора Pasichna_Switch_4.1:

Pasichna_Switch_4.1 (config)#int vlan 99

Pasichna_Switch_4.1 (config-if)#description LAN vlan_99_Sw4.1

Pasichna_Switch_4.1 (config-if)#ip add 172.23.152.98 255.255.255.248

Pasichna_Switch_4.1 (config-if)#no shut

Pasichna_Switch_4.1 (config-if)#ip default-gateway 172.23.152.97

Налаштування інтерфейсів на комутаторах, встановлення діапазону інтерфейсів для наданих VLAN, за приклад наведено виконані дії на

комутаторі Pasichna_Switch_4.2:

– діапазон інтерфейсів FastEthernet0/15-24 переведено в режим access та призначено VLAN 24 до діапазону інтерфейсів, увімкнено порти:

Pasichna_Switch_4.2(config-if-range)#int range fa0/15-24

Pasichna_Switch_4.2(config-if-range)#switchport mode access

Pasichna_Switch_4.2(config-if-range)#switchport access vlan 24

Pasichna_Switch_4.2(config-if-range)#no sh

– діапазон інтерфейсів FastEthernet0/10-14 переведено в режим access та призначено VLAN 34 до діапазону інтерфейсів, увімкнено порти:

Pasichna_Switch_4.2(config-if-range)#int range fa0/10-14

Pasichna_Switch_4.2(config-if-range)#switchport mode access

Pasichna_Switch_4.2(config-if-range)#switchport access vlan 34

Pasichna_Switch_4.2(config-if-range)#no sh

– діапазон інтерфейсів FastEthernet0/5-9 переведено в режим access та призначено VLAN 44 до діапазону інтерфейсів, увімкнено порти:

Pasichna_Switch_4.2(config-if-range)#int range fa0/5-9

Pasichna_Switch_4.2(config-if-range)#switchport mode access

Pasichna_Switch_4.2(config-if-range)#switchport access vlan 44

Pasichna_Switch_4.2(config-if-range)#no sh

– діапазон інтерфейсів FastEthernet0/1, FastEthernet0/3-4, GigabitEthernet0/1-2 переведено в режим access та призначено VLAN 44 до діапазону інтерфейсів, увімкнено порти:

Pasichna_Switch_4.2(config-vlan)#int range fa0/1, fa0/3-4, g0/1-2

Pasichna_Switch_4.2(config-if-range)#switchport mode access

Pasichna_Switch_4.2(config-if-range)#switchport access vlan 100

Pasichna_Switch_4.2(config-if-range)#do wr

Далі наведено фрагмент конфігурації маршрутизатора, а саме налаштування підінтерфейсів. Subinterface є способом розділити фізичний інтерфейс на кілька віртуальних логічних інтерфейсів. Кожен Subinterface має свій власний ідентифікатор VLAN і може мати окремі налаштування

мережевих параметрів.

Виконується створення Subinterface, кожен з яких використовує протокол 802.1Q (dot1Q) для маркування пакетів з відповідним ідентифікатором VLAN. Усі Subinterface вмикаються, тобто активуються, для того щоб отримати здатність до передачі трафіку:

Pasichna_Router_4(config)#int g0/0/0

Pasichna_Router_4(config-if)#no sh

Pasichna_Router_4(config-if)#int g0/0/0.24

Pasichna_Router_4(config-subif)#encapsulation dot1Q 24

Pasichna_Router_4(config-subif)#ip addr 172.23.152.1 255.255.255.224

Pasichna_Router_4(config-subif)#no sh

Pasichna_Router_4(config-subif)#int g0/0/0.34

Pasichna_Router_4(config-subif)#encapsulation dot1Q 34

Pasichna_Router_4(config-subif)#ip addr 172.23.152.33 255.255.255.224

Pasichna_Router_4(config-subif)#no sh

Pasichna_Router_4(config-subif)#int g0/0/0.44

Pasichna_Router_4(config-subif)#encapsulation dot1Q 44

Pasichna_Router_4(config-subif)#ip addr 172.23.152.65 255.255.255.224

Pasichna_Router_4(config-subif)#no sh

Pasichna_Router_4(config-subif)#int g0/0/0.99

Pasichna_Router_4(config-subif)#encapsulation dot1Q 99

Pasichna_Router_4(config-subif)#ip addr 172.23.152.97 255.255.255.248

Pasichna_Router_4(config-subif)#no sh

Нижче наведено налаштування DHCP pool, на прикладі маршрутизатора Pasichna_Router_4 та діапазону адрес для мережі 172.23.152.0 255.255.255.224:

Pasichna_Router_4(config)#ip dhcp pool Vlan24pool

Pasichna_Router_4(dhcp-config)#network 172.23.152.0 255.255.255.224

Pasichna_Router_4(dhcp-config)#default-router 172.23.152.1

Pasichna_Router_4(dhcp-config)#dns-server 172.23.153.46

Pasichna_Router_4(dhcp-config)#exit

Pasichna_Router_4(config)#ip dhcp excluded-address 172.23.152.1 172.23.152.10

3.5.2 Налаштування безпеки портів на комутаторах

Впровадження безпеки портів є важливою складовою забезпечення безпеки мережі. Це дозволяє обмежити доступ до портів комутатора та контролювати підключення пристроїв до мережі. Налаштування безпеки порту включає такі параметри, як обмеження максимальної кількості підключених пристроїв, використання статичних або автоматично збережених MAC-адрес, а також реакцію на порушення безпеки, наприклад, блокування порту.

Це допомагає захистити мережу від несанкціонованого доступу, атак типу «MAC flooding» та забезпечити відповідність вимогам безпеки. Налаштування безпеки порту також може допомогти виявити та ізолювати несправні пристрої, а також зменшити ризик витоку конфіденційної інформації.

Враховуючи важливість безпеки мережі, розгляд налаштування безпеки портів є необхідним кроком для забезпечення безпеки мережі та захисту важливих даних.

Відповідно до вимог функцію безпеки портів було налаштовано на портах комутаторів, який підключені до серверів. В якості прикладу, нижче наведено налаштування інтерфейсу FastEthernet0/15 на комутаторі Pasichna_Switch_4.3, а саме налаштування максимальної кількості пристроїв, які можуть підключатись до порту та налаштовано вимкнення порту у разі порушення правил безпеки:

Pasichna_Switch_4.3(config)#int Fat0/15

Pasichna_Switch_4.3(config-if)#switchport port-security maximum 2

Pasichna_Switch_4.3(config-if)#switchport port-security mac-address sticky

Pasichna_Switch_4.3(config-if)#switchport port-security violation shutdown

3.6 Перевірка роботи комп'ютерної системи

Для перевірки роботи внутрішньої мережі використано команду ping, з мережі LAN2 відправлено ехо-запит в мережу LAN1 (рисунок 3.4).

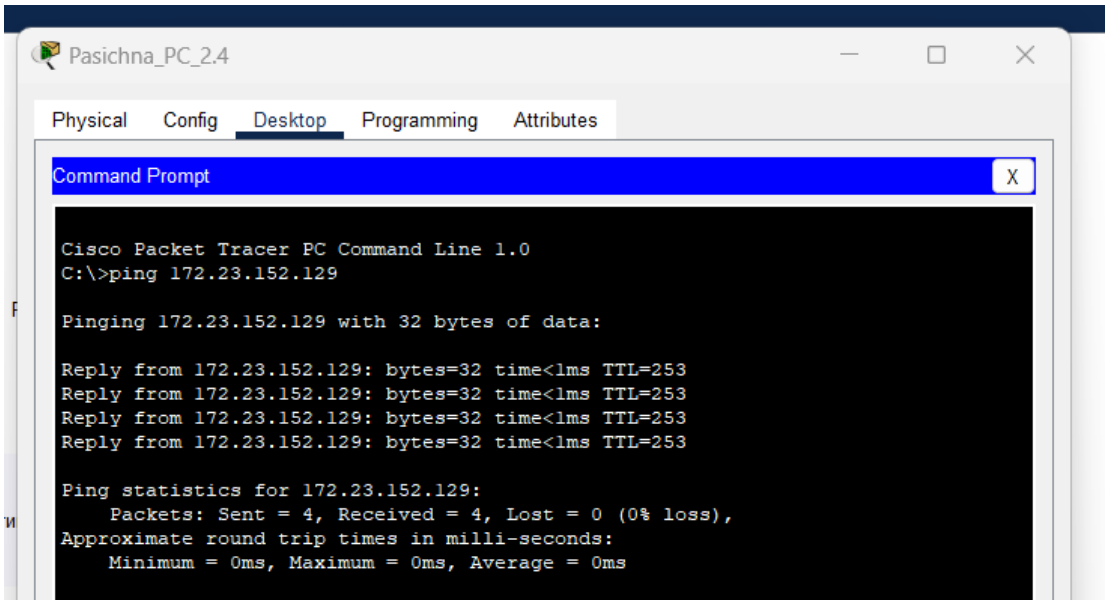

Рисунок 3.4 – Ехо-запит від ПК в мережі LAN2 на маршрутизатор в мережі LAN1

Також ехо-запит було виконано з віддаленої мережі LAN5 на сервер HTTP (рисунок 3.5).

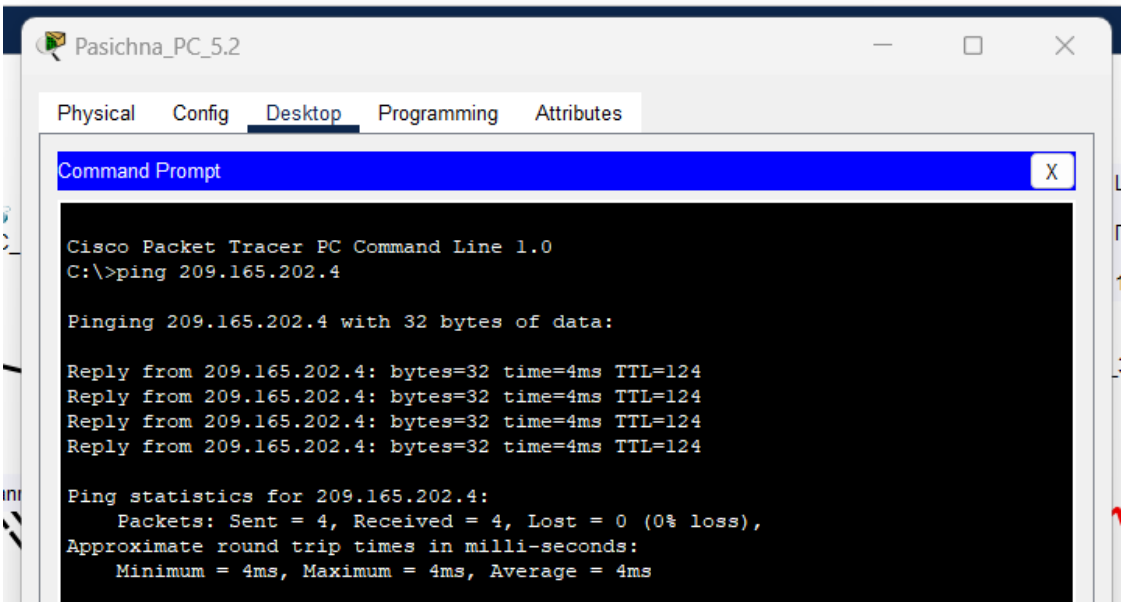

Рисунок 3.5 – Ехо-запит з віддаленої мережі на сервер HTTP

Перевірено роботу HTTP серверу, відкрито веб-сторінку з відомостями про кваліфікаційну роботу (рисунок 3.6).

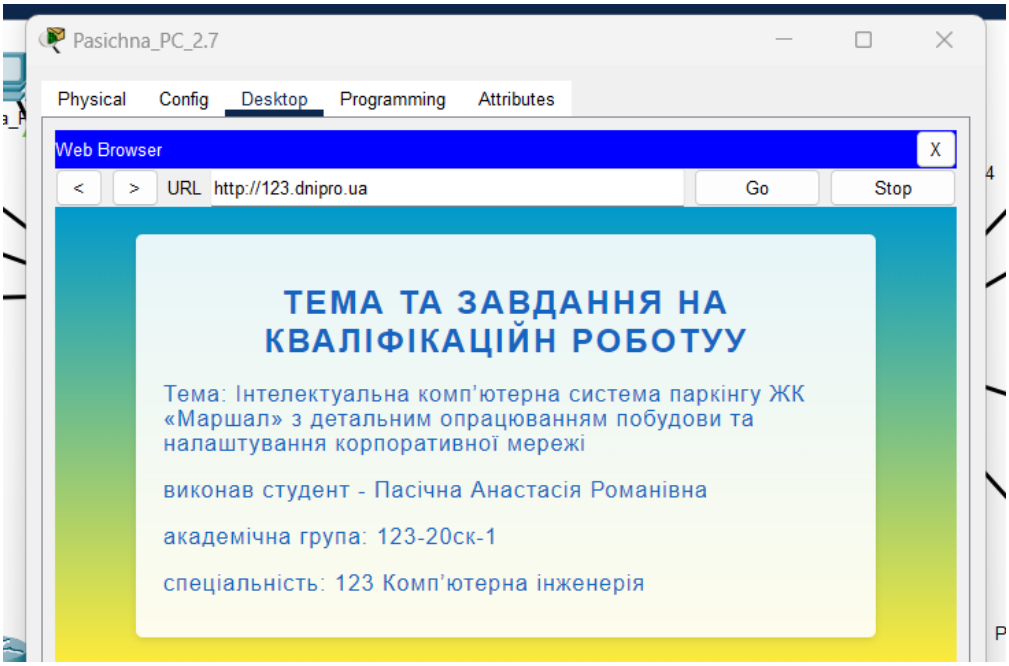

Рисунок 3.6 – Веб-сторінка в браузері на ПК Pasichna_PC_2.7

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Розробка системи інтелектуального паркінгу ЖК «Маршал»

4.1.1 Загальна функціональна схеми роботи інтелектуального паркінгу

Інтелектуальний паркінг ЖК «Маршал» працює відповідно до наступної схеми. При в'їзді на паркінг автомобілів, система перевіряє доступ за допомогою RFID-мітки та ключа. Якщо дані відповідають, шлагбаум автоматично піднімається, дозволяючи автомобілю в'їхати на територію паркінгу.

Після в'їзду на паркінг система автоматично вмикає світло, використовуючи датчики руху. Якщо датчик виявляє рухи, світильники активуються, забезпечуючи належне освітлення на паркінгу.

Вся ця система контролюється та оброблюється за допомогою IoT-сервера. Він отримує дані від різних датчиків і пристроїв, таких як RFID-читачі, датчики руху та даних з мікроконтролера, який керує системою вентиляції. Сервер обробляє ці дані та забезпечує відповідні керуючі сигнали для елементів паркінгу, забезпечуючи безперебійну та ефективну роботу системи.

Загальна функціональна схема роботи інтелектуального паркінгу складається з різних компонентів, включаючи RFID-читачі, шлагбаум, датчики руху, світлові прилади та IoT-сервер.

4.1.2 Вибір і обґрунтування комплексу технічних засобів системи інтелектуального паркінгу

При виборі та обґрунтуванні комплексу технічних засобів для системи інтелектуального паркінгу було враховано кілька факторів. Основними критеріями були ефективність, надійність та забезпечення необхідного рівня безпеки для користувачів паркінгу. На основі цих вимог було обрано наступні технічні засоби:

– система проїзду ZkTeco UHF є RFID-системою для контролю проїзду транспортних засобів. Вона використовує технологію RFID, включаючи RFID-читачі та метки (теги), для автоматичної ідентифікації транспортних засобів. Система дозволяє керувати шлагбаумами та контролювати доступ у двох напрямках;

– датчики руху, використовуються модель датчика руху AXIS T8341 PIR Motion Sensor. Цей датчик руху працює за технологією Power over Ethernet (PoE), що дозволяє передавати живлення та передавати дані через один Ethernet-кабель. Він підтримує стандарт PoE IEEE 802.3af/at, що дозволяє підключати його до PoE -комутаторів або PoE -інжекторів Датчик фіксує рухи автомобілів та осіб на паркінгу, що дозволяє автоматично увімкнути світлові прилади для належного освітлення;

– світильники, використовуються світильники моделі BY235P G2 LED HB 200W/NW PSU WB RU від компанії Philips. Ці світильники забезпечують яскраве та ефективне освітлення на паркінгу, використовуючи технологію LED і забезпечуючи низьке споживання енергії;

– датчики вологості, температури та CO2. Датчик вологості SHT11 від Sensirion, який працює в діапазоні від 0% до 100% вологості з точністю ±3%, SHT11 має аналоговий вихід, де напруга змінюється пропорційно зміні вологості. Аналоговий датчик температури LM35 від компанії Texas Instruments. Він працює в діапазоні від -55°C до +150°C і має лінійну характеристику виходу, де 10 мВ відповідають 1°C зміни температури. Датчик вимірювання CO2 CO2Detect-300 від ABC Technologies, цей датчик працює в діапазоні від 0 до 5000 часток на мільйон (ppm) з точністю ±50 ppm або ±5% від змірюваного значення. CO2Detect-300 використовує аналоговий вихідний сигнал, де напруга змінюється пропорційно зміні концентрації CO2 в повітрі. Ці сенсори забезпечують моніторинг та збір даних про рівень вологості, температури та рівень CO2 в середовищі паркінгу, що дозволяє регулювати систему вентиляції та забезпечити комфортні умови;

– система вентиляції на ПЛК150 Овен, використання програмованого

логічного контролера для керування системою вентиляції дозволяє ефективно контролювати рівень вологості, температуру та інші параметри повітря на паркінгу. Це забезпечує комфортні умови для автомобілів та їх власників. Використання цього ПЛК обумовлено вимогами в підрозділі 2.1.2.2;

– модуль виведення аналогових сигналів MB110-8A, який використовується для розширення кількості аналогових портів на (ПЛК) 150. Використання цього модуля дозволяє розширити функціональні можливості ПЛК і забезпечити більш гнучкий контроль над аналоговими сигналами у системі;

– камера спостереження AXIS P1347-E від компанії Axis Communications є високоякісним зовнішнім пристроєм, який працює на технології PoE. Вона пропонує роздільну здатність зображення 1920 x 1080 пікселів, що дозволяє отримувати деталізовані зображення для точного спостереження. Крім того, вона має великий динамічний діапазон від 0,04 до 142000 люкс, що дозволяє збалансувати яскраві та темні області на зображенні..

Нижче наведено специфікацію обладнання (таблиця 4.1)

Таблиця 4.1 – Специфікація обладнання

Позиція	Найменування	Марка	Одиниця вимірювання	Кількість
1	Система проїзду ZkTeco UHF	Gant	шт.	2
2	Датчик руху AXIS T8341 PIR Motion Sensor	Axis	шт.	6
3	Світильник BY235P G2 LED HB 200W/NW PSU WB RU	Philips	шт.	24
4	Датчик вологості SHT11	Sensirion	шт.	6
5	Аналоговий датчик температури LM35	Texas Instruments	шт.	9
6	Датчик вимірювання CO2 CO2Detect-300	ABC Technologies	шт.	9
7	ПЛК150	Овен	шт.	3

Продовження таблиці 4.1

Позиція	Найменування	Марка	Одиниця вимірювання	Кількість
8	Модуль введення аналогових сигналів МВ110-8А	Овен	шт.	3
9	Камера спостереження AXIS P1347-E	Axis Communications	шт.	40

Обрані технічні засоби враховують потреби і вимоги інтелектуального паркінгу, забезпечують безпроблемний доступ, контроль руху автомобілів, належне освітлення, комфортні умови та ефективне керування системою вентиляції. Кожен засіб має свою функціональність та сприяє створенню безпечного та зручного середовища для користувачів паркінгу.

4.1.3 Розробка функціональної схеми роботи вентиляційної системи інтелектуального паркінгу

Система вентиляції паркінгу ЖК «Маршал» використовує інноваційний підхід для забезпечення комфортних та безпечних умов в приміщенні. Ця система дозволяє автоматично регулювати рівень вентиляції, враховуючи показники температури, вологості та рівня CO_2 в паркінгу.

Основою системи є датчики, розташовані у різних частинах паркінгу. Ці датчики постійно слідкують за температурою повітря, вологістю та рівнем CO_2, що генерується від автомобілів. Зібрана інформація передається до спеціального мікроконтролера, який відповідає за керування системою вентиляції.

Мікроконтролер програмується таким чином, щоб при досягненні певних показників датчиків (наприклад, високої температури чи забрудненості повітря), система вентиляції автоматично ввімкнулася. Це забезпечує ефективне видалення забрудненого повітря та підтримку оптимальної температури в паркінгу.

Крім того, мікроконтролер також відображає поточні показники

датчиків на моніторах. Це дозволяє операторам та персоналу локально відслідковувати стан повітря в режимі реального часу і при необхідності вживати відповідних заходів.

Зібрані дані з датчиків також передаються на віддалений сервер. Цей сервер збирає, аналізує та зберігає інформацію про стан роботи системи вентиляції в паркінгу.

Нижче наведено функціональну схему (рисунок 4.1).

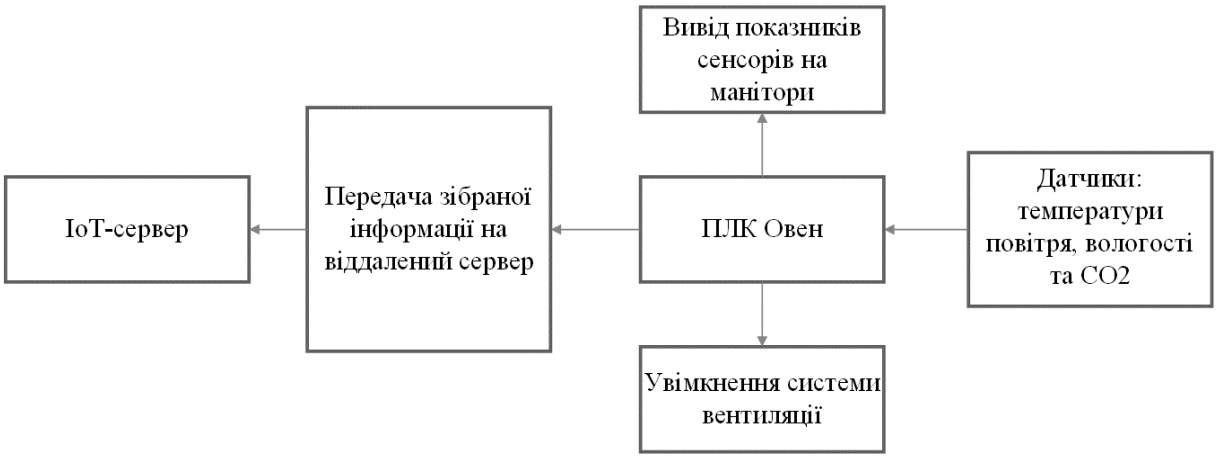

Рисунок 4.1 – Функціональна схема

4.1.4 Розробка переліку вхідних та вихідних сигналів і даних для системи вентиляції

Для визначення входів і виходів необхідно ретельно проаналізувати та поділити на категорії вхідні та вихідні сигнали, які надходять від датчиків.

Аналіз сигналі записано в таблицю 4.2

Таблиця 4.2 – Аналіз вхідних і вихідних сигналів

№	Найменування інформації(сигнали данні)	Іден-тифі-катор	Напр. вх./вих.	Функція	Вид	Джерело/ отримувач	Форма подання		Період вв./вив., сек.
1	Температура	TEMP	Вхід	Вимірювання температури	Аналог. сигнал	Датчик температури	4/20 мА	4 байта	1
2	Дим	SMOKE	Вхід	Вимірювання рівня диму	Аналог. сигнал	Датчик диму	4/20 мА	4 байта	1

Продовження таблиці 4.2

№	Найменування інформації(сигнали данні)	Іден-тифі-катор	Напр. вх./вих.	Функція	Вид	Джерело/ отримувач	Форма подання		Період вв./вив., сек.
3	Вологість	HUM	Вхід	Вимірювання рівня вологості	Аналог. сигнал	Датчик вологості	4/20 мА	4 байта	1
4	Стан системи	SYSTEM_STATE	Вихід	Керування режимами системи	Лог. сигнал	Контролер	Лог. значення (Імп)	Змінний	4
5	Поточна інформація	INFO	Вихід	Передача поточних даних	Циф. сигнал	Монітор инговий блок	4 байти	Змінний	5

4.1.5 Вибір пристрою керування системи вентиляції

В якості пристрою керування системи було обрано ПЛК150 Овен, відповідно до вимог.

ПЛК150 має достатню кількість входів та виходів для підключення системи. З його аналогових входів буде зчитуватись значення з датчиків температури, вологості, рівня CO2. Ці дані дозволять контролеру виконувати відповідні дії, наприклад, активувати систему вентиляції при певних значеннях датчиків.

За допомогою 4 цифрових виходів ПЛК150, дані з датчиків будуть виводиться на монітори та ПЛК буде керувати системою вентиляції

Крім того за допомогою інтерфейсу Ethernet буде здійснюватися підключення до загальної мережі, це відкриває можливості для збору та обміну даними з IoT-сервером. Інтерфейс RS-485 у ПЛК150 дозволяє підключити до нього блок розширення для збільшення кількості аналогових портів для підключення більшої кількості датчиків.

Загалом, ПЛК150 забезпечує достатні можливості для керування системою вентиляції, підключення датчиків та виведення інформації на LCD-монітори. Його програмована логіка дозволяє налаштувати роботу системи згідно з потребами та вимогами проекту.

4.1.6 Розробка принципової схеми системи вентиляції

Після проведеного детального аналізу було розроблено принципову схему системи вентиляції для інтелектуального паркінгу. На рисунку 4.2 представлена принципова схема системи вентиляції інтелектуального паркінгу. Схема включає в себе компоненти, такі як система вентиляції, ПЛК та сенсори вологості, температури та рівня CO2.

У цій схемі система вентиляції, підключена до виходів ПЛК, контролюються залежно від зчитаних даних з сенсорів.

Ця принципова схема є основою для подальшого проектування та реалізації системи вентиляції. Вона надає загальний огляд зв'язку між компонентами та їх функціональним призначенням. Завдяки цій схемі розробники та інженери можуть краще розуміти взаємодію компонентів та виконувати подальші кроки в процесі реалізації системи вентиляції для інтелектуального паркінгу.

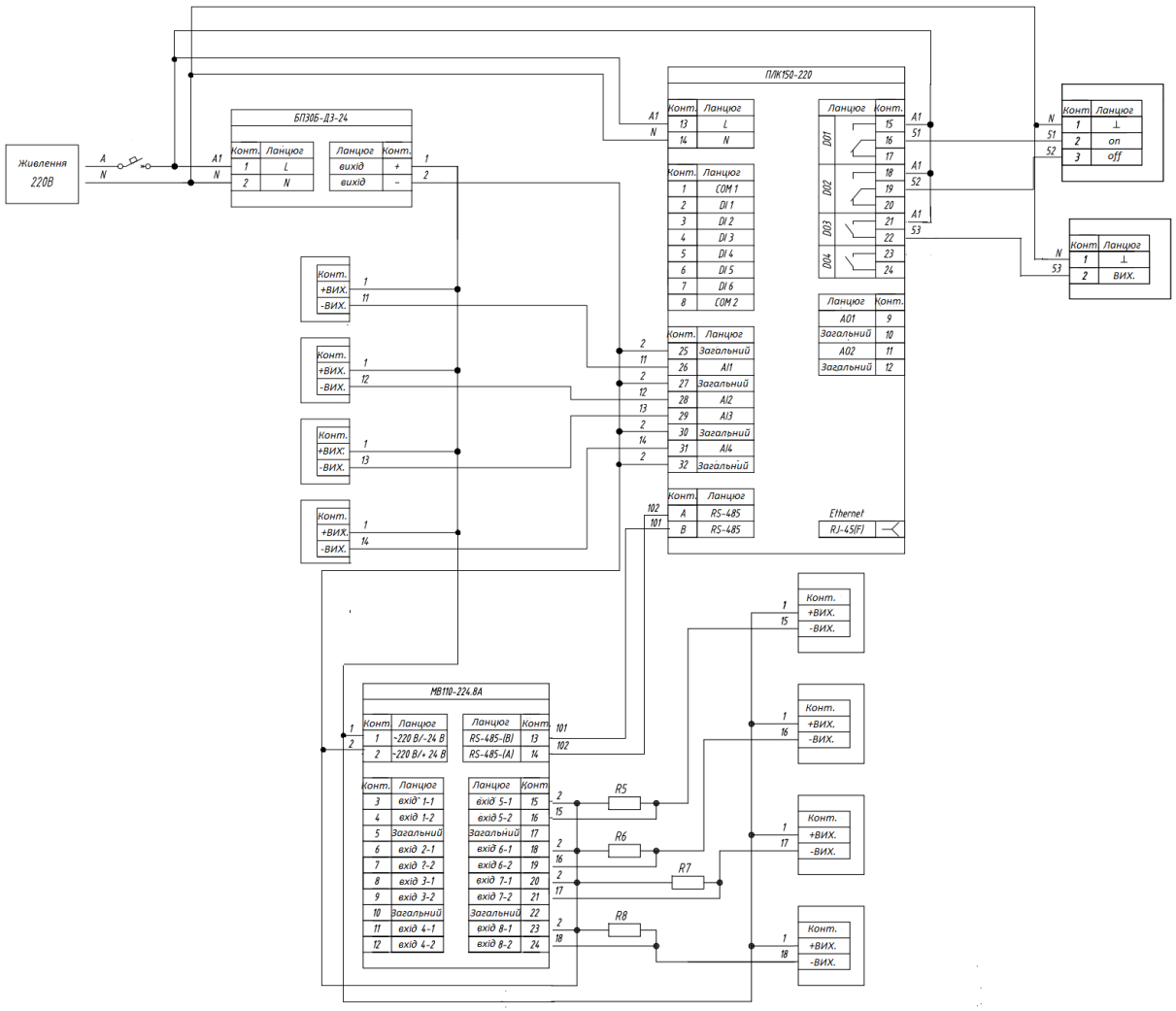

Рисунок 4.2 – Принципова схема

4.2 Проектування моделі системи розумного паркінгу

До моделі мережі, яка була наведена у розділі 3, будуть додані дві додаткові підмережі для обслуговування двох паркінгів.

В таблиці 4.3 наведена схема адресації для підмереж паркінгу.

Таблиця 4.3 – Схема адресації підмереж паркінгу

Назва підмережі	Номер мережі	Маска мережі	Діапазон доступних адрес
LAN_P1 (Паркінг перший корпус)	172.23.154.0	255.255.255.0	172.23.154.1 – 172.23.154.254
LAN_P2 (Паркінг другий корпус)	172.23.155.0	255.255.255.0	172.23.155.1 – 172.23.155.254
WAN5	10.0.14.16	255.255.255.252	10.0.14.17 – 10.0.14.18

Нижче, в таблиці 4.4, наведено схему адресації пристроїв.

Таблиця 4.4 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	Інтерфейс підключеного пристрою
Pasichna_Router_5	Gig0/0/0	172.23.154.1	/24	-	Gig0/2
	Gig0/0/1	172.23.155.1	/24	-	Fa0/2
	Se0/1/1	10.0.14.18	/30	-	Se0/2/1
Pasichna_Switch_P1.1	VLAN1	172.23.154.2	/24	172.23.154.1	Gig0/0/0
Pasichna_Switch_P2.1	VLAN1	172.23.155.2	/24	172.23.155.1	Gig0/0/1
					Gig0/1
					Gig0/2
Pasichna_Switch_P2.2	VLAN1	172.23.155.3	/24	172.23.155.1	Gig0/1
Pasichna_Switch_P2.3	VLAN1	172.23.155.4	/24	172.23.155.1	Gig0/2

Також опираючись на схему адресації мережі та пристроїв з урахуванням підпункту 4.1.1, було розроблено модель підмереж паркінгу в середовищі проектування Cisco Packet Tracer. На рисунках 4.3-4.5 зображено моделі підмереж.

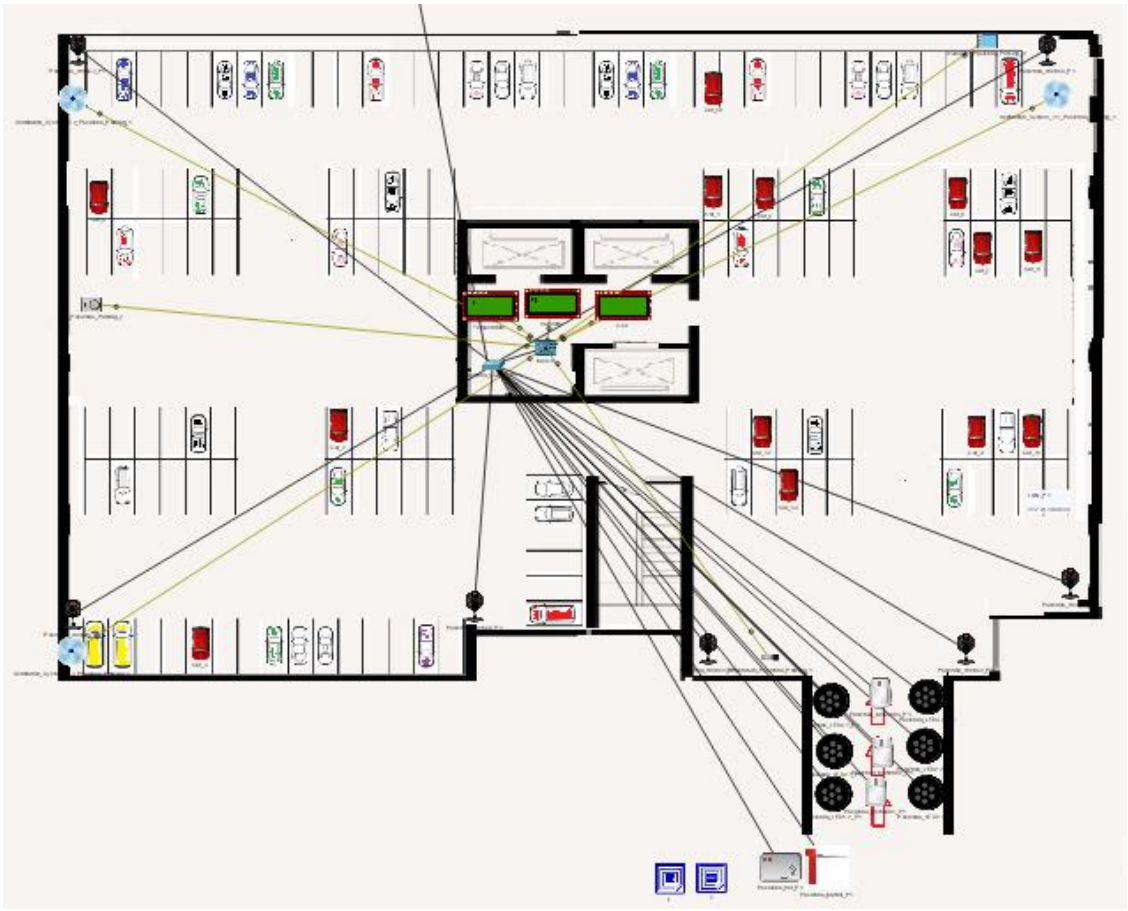

Рисунок 4.3 – Модель підмережі паркінгу першого корпусу

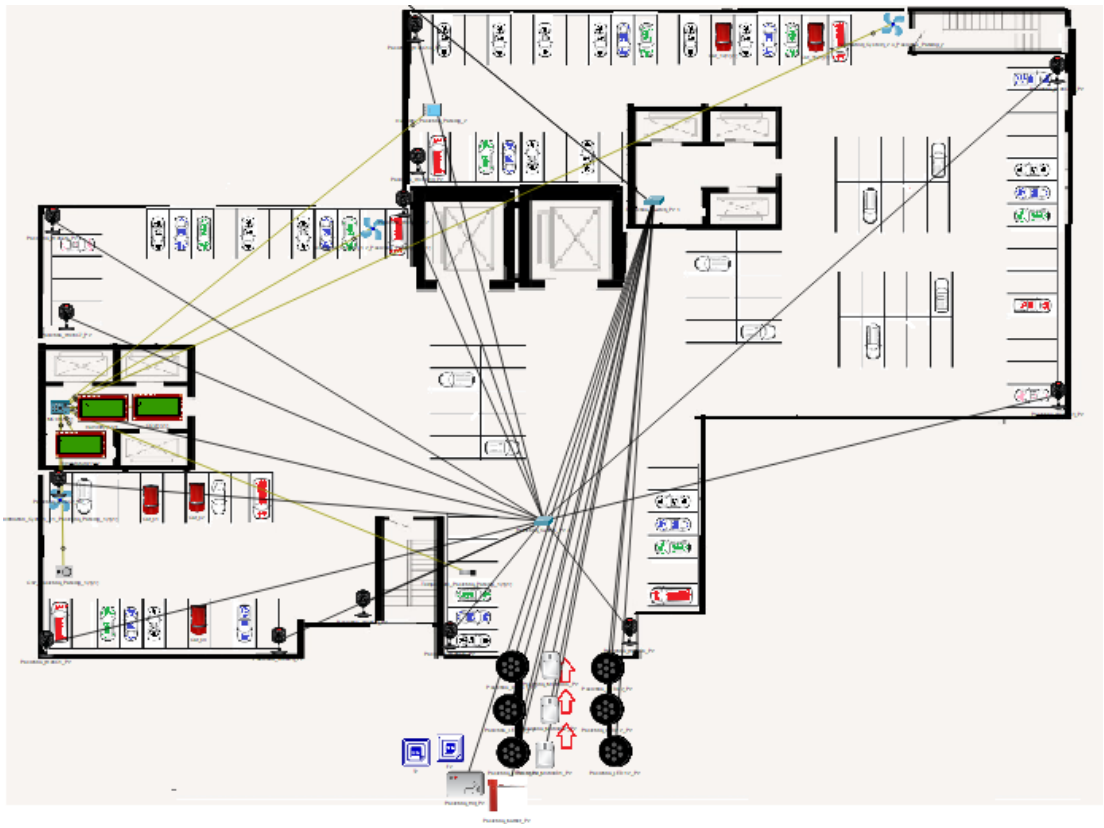

Рисунок 4.4 – Модель підмережі паркінгу другого корпусу перший поверх

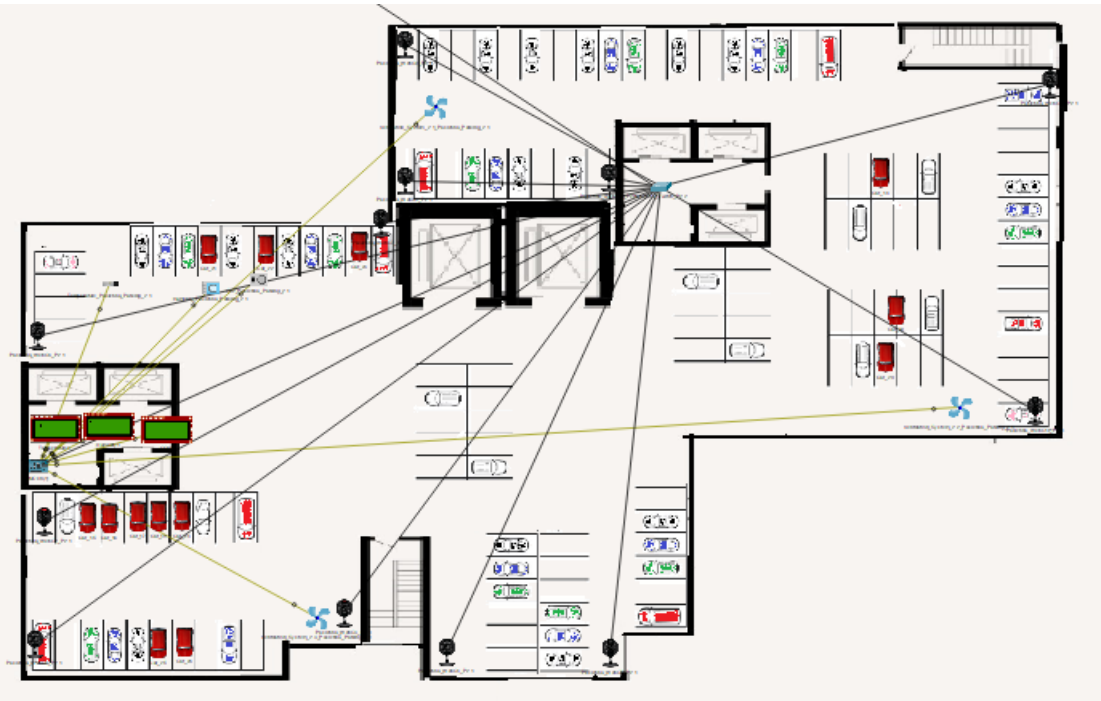

Рисунок 4.4 – Модель підмережі паркінгу другого корпусу другий поверх

4.2.1 Розробка блок-схем функціонування елементів інтелектуального паркінгу

Систему інтелектуального паркінгу умовно можна поділити на 4 частини: система вентиляції на основі мікроконтролера, систему контролю за в’їздом, система відеонагляду та систему увімкнення світла.

Блок-схема функціонування системи вентиляції наведена на рисунку 4.5.

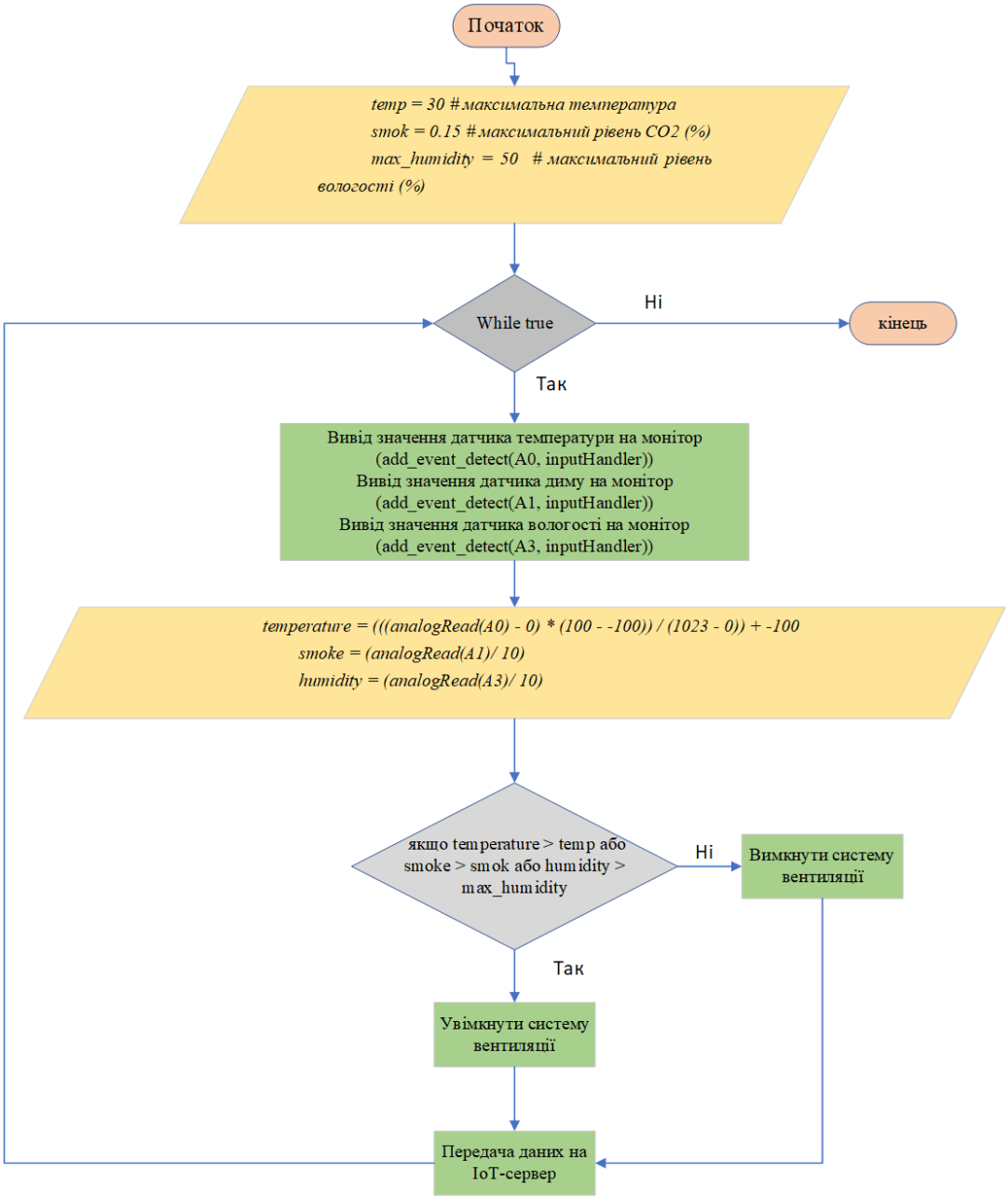

Рисунок 4.5 – Блок-схема системи вентиляції

Система контролю за в’їздом працює за наступним принципом: зчитується RFID-мітка читачем, якщо мітка дійсна підіймається шлагбаум. Блок-схема функціонування наведена на рисунку 4.6.

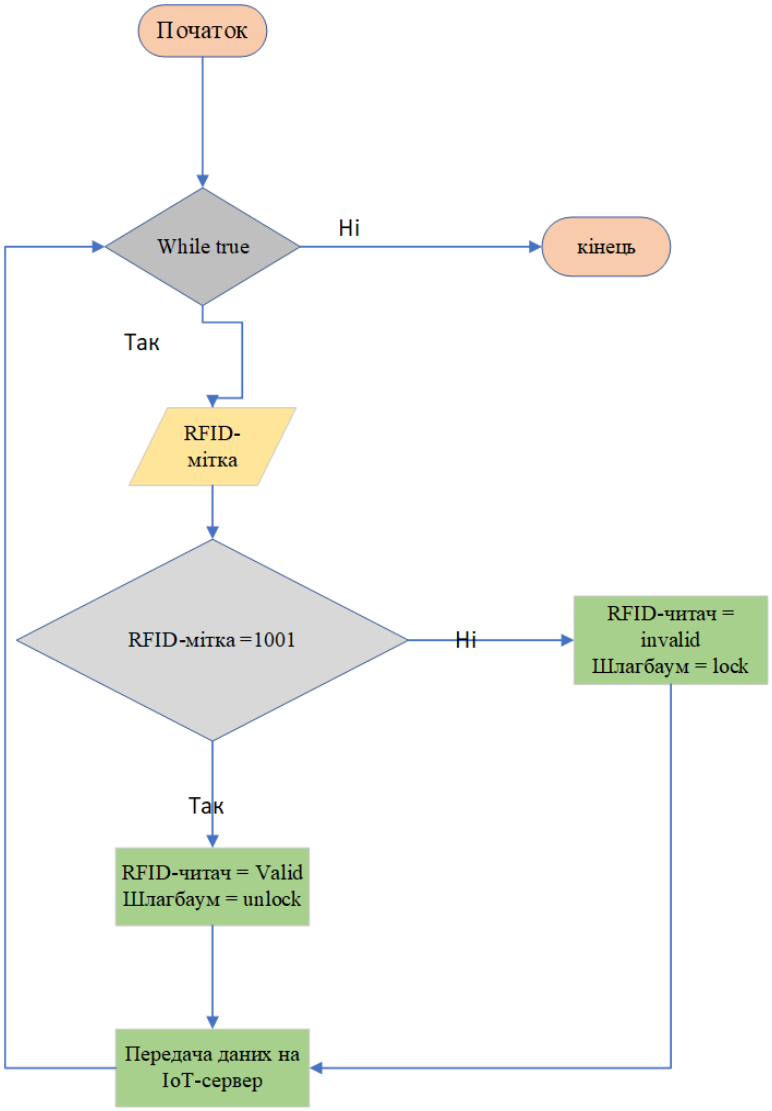

Рисунок 4.6 – Блок-схема системи контролю за в’їздом

Система увімкнення освітлення функціонує за такою схемою: при спрацюванні датчиків руху активуються відповідні освітлювачі (рисунок 4.7).

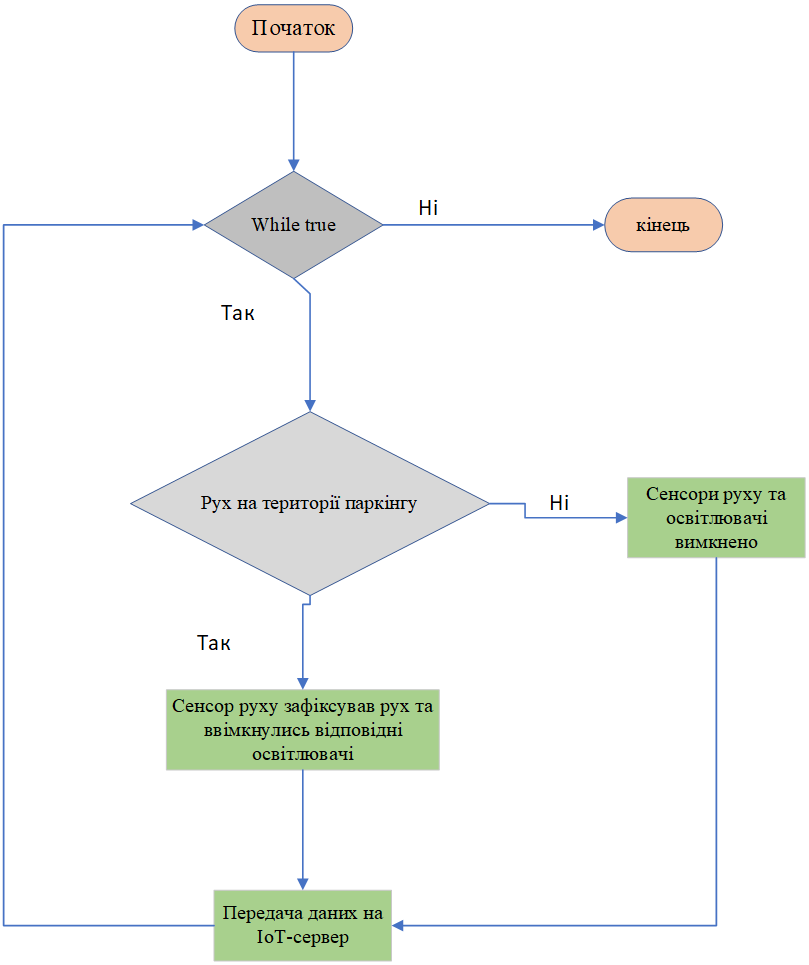

Рисунок 4.7 – Блок-схема системи управління

Система відеоспостереження функціонує безперервно з метою забезпечення безпеки мешканців та їх автомобілів (рисунок 4.8).

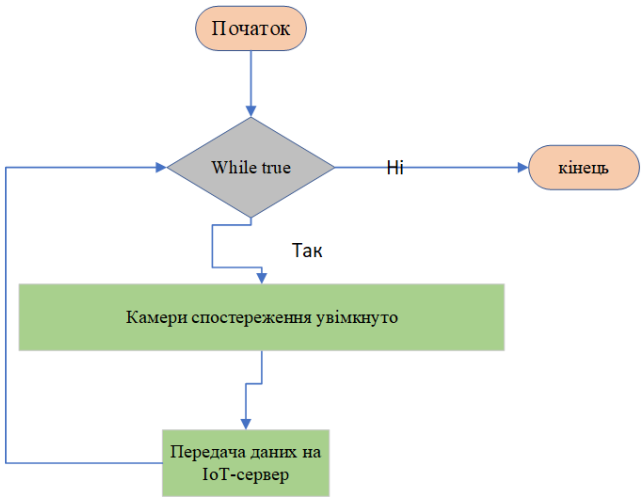

Рисунок 4.8 – Блок-схема функціонування системи спостереження

4.2.2 Налаштування функціонування системи вентиляції в моделі

Для демонстрації роботи системи вентиляції було розроблено модель системи, що базується на мікроконтролері та датчиках, які використовуються у середовищі моделювання. Додатково, для MCU була розроблена програма на мові Python, що дозволяє збирати дані з датчиків, аналізувати їх на мікроконтролері та передавати на IoT-сервер. Крім цього, при досягненні заданих значень датчиків, мікроконтролер активує систему вентиляції.

Нижче наведено фрагмент програми на мові Python.

Встановлення максимальних значень:

```
temp = 30  # максимальна температура
smok = 0.15  # максимальний рівень CO2 (%)
max_humidity = 50  # максимальний рівень вологості (%)
```

Вивід значень на монітори:

```
add_event_detect(A0, inputHandler)  # вивід значення датчика температури на монітор
add_event_detect(A1, inputHandler)  # вивід значення датчика диму на монітор
add_event_detect(A3, inputHandler)  # вивід значення датчика вологості на монітор
```

Управління роботою системи вентиляції

```
while True:
    temperature = (((analogRead(A0) - 0) * (100 - -100)) / (1023 - 0)) + -100
    smoke = (analogRead(A1)/ 10)
    humidity = (analogRead(A3)/ 10)
    if temperature > temp or smoke > smok or humidity > max_humidity:
      customWrite(2, 2)  # увімкнути Ventilation_System
      customWrite(4, 2)  # увімкнути Ventilation_System
      customWrite(5, 2)  # увімкнути Ventilation_System
    else:
```

```
        customWrite(2, 0)  # вимкнути Ventilation_System
        customWrite(4, 0)  # вимкнути Ventilation_System
        customWrite(5, 0)  # вимкнути Ventilation_System
```

Передача даних з датчиків на IoT-сервер:

```
  IoEClient.setup({
    "type": "Ventilation_System",
    "states": [{
      "name": "Smoke",
      "type": "number",
    },
    {
      "name": "Temperature",
      "type": "number"
    },
    {
      "name": "Humidity",
      "type": "number"
    }]
  })
while True:
    IoEClient.reportStates([smoke, temperature, humidity])
    delay(100)
```

4.2.3 Налаштування IoT-серверу

Управління та моніторинг системи паркінгу здійснюється за допомогою IoT-сервера, який відіграє ключову роль у забезпеченні ефективної роботи всієї системи. IoT-сервер забезпечує зв'язок та обмін даними між різними компонентами паркінгової системи, включаючи шлагбауми, відеокамери, датчики руху, освітлення та мікроконтролери.

Завдяки використанню IoT-сервера, можна отримувати актуальну

інформацію про стан шлагбаумів, відеодані, дані з датчиків руху, стан освітлення та інші важливі показники у режимі реального часу. Крім того, IoT-сервер надає можливість виконувати додаткові функції, такі як віддалене керування системою. На сервері встановлюються правила та сценарії взаємодії між RFID-читачем та шлагбаумом, датчиками руху та освітленням, що дозволяє гнучко налаштовувати роботу системи залежно від потреб та вимог (таблиця 4.5).

Таблиця 4.5 – Частина сценаріїв на IoT-сервері

Назва сценарію	Умова	Дії
barrier_1 unlock	Pasichna_rfid_P1 Status is Valid	Set Pasichna_barrier_P1 On to true
barrier_1 lock	Pasichna_rfid_P1 Status is Invalid	Set Pasichna_barrier_P1 On to false
rfid_1 valid	Pasichna_rfid_P1 Card ID = 1001	Set Pasichna_rfid_P1 Status to Valid
rfid_1 invalid	Pasichna_rfid_P1 Card ID != 1001	Set Pasichna_rfid_P1 Status to Invalid
motion1.2 true	Pasichna_MotionD1_P2 On is true	Set Pasichna_LED1.2_P2 On to true Set Pasichna_LED1.1_P2 On to true
motion1.2 false	Pasichna_MotionD1_P2 On is false	Set Pasichna_LED1.2_P2 On to false Set Pasichna_LED1.1_P2 On to false

4.2.4 Демонстрація роботи моделі системи паркінгу

На рисунку 4.9 представлено функціонування вентиляційної системи, яка була активована внаслідок високого рівня CO_2 в повітрі.

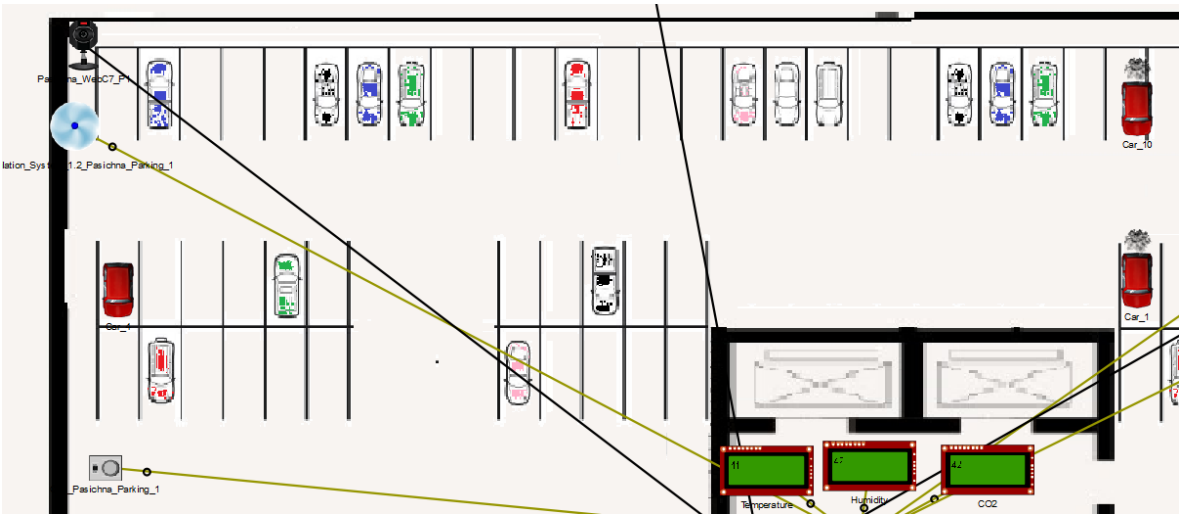

Рисунок 4.9 – Робота вентиляційної системи

Рисунок 4.10 демонструє взаємодію між RFID-читачем та шлагбаумом в їх спільній роботі.

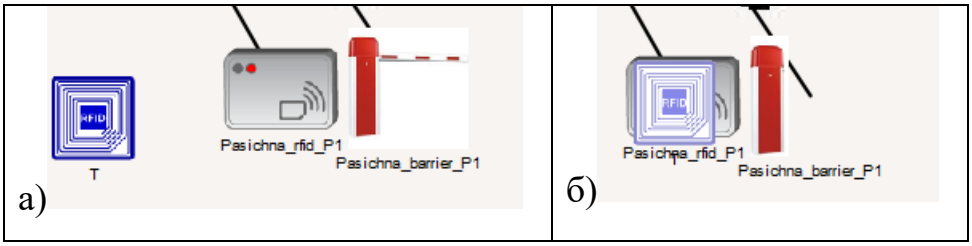

Рисунок 4.10 – Функціонування системи проїзду: а) до RFID-читача не прикладено ключ, шлагбаум опущено; б) до RFID-читача прикладено ключ, шлагбаум піднято

Система включення освітлення працює таким чином, що при спрацюванні датчика руху вмикаються певні освітлювачі, які пов'язані з цим датчиком, як показано на рисунку 4.11.

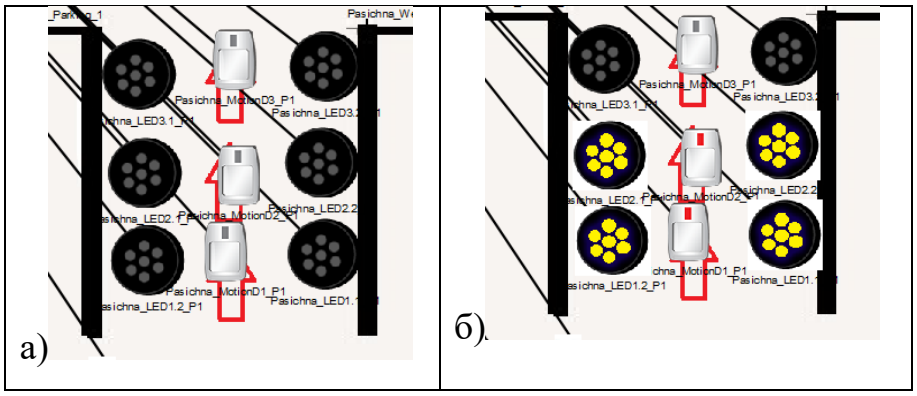

Рисунок 4.11 – Функціонування системи освітлення: а) датчики руху не фіксують рухів, світло вимкнено; б) певні датчики руху фіксують рухи, взаємопов’язані з ними світильники увімкнено

ВИСНОВКИ

Роблячи висновки, можна сказати, що впровадження розумних паркінгів є дуже актуальним та перспективним напрямком у розвитку сучасних міст. Зараз зростає кількість автомобілів на дорогах, що призводить до дефіциту паркомісць в багатоповерхових комплексах, оскільки традиційні паркінги не можуть задовольнити потреби мешканців. Розумні паркінги можуть вирішити цю проблему, дозволяючи ефективно використовувати простір та забезпечуючи зручність та безпеку для мешканців. Крім того, використання розумних паркінгів може підвищити ціну нерухомості та зробити її більш привабливою для потенційних покупців та орендарів. У світлі цих переваг, впровадження розумних паркінгів є необхідним кроком у покращенні якості життя мешканців та розвитку міст.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «Дніпровська політехніка», 2022.

2. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

3. ЖК MARSHALL, Дніпро – Квартири в новобудовах – ЛУН [Електронний ресурс] – Режим доступу до ресурсу: https://lun.ua/uk/%D0%B6%D0%BA-marshall-%D0%B4%D0%BD%D1%96%D0%BF%D1%80%D0%BE

4. Smart Parking – Wilson Parking Case Study – Smart Parking [Електронний ресурс] – Режим доступу до ресурсу: https://www.smartparking.com/latest/case-studies/wilson-parking

5. ISO - International Organization for Standardization [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/home.html

6. What is Open Shortest Path First (OSPF)? [Електронний ресурс] – Режим доступу до ресурсу: https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf

7. What is AAA? | FreeRADIUS Documentation – NetworkRADIUS)? [Електронний ресурс] – Режим доступу до ресурсу: https://networkradius.com/doc/current/concepts/introduction/AAA.html

8. Wat is NAT en hoe werkt het? – VOIPZeker [Електронний ресурс] – Режим доступу до ресурсу: https://voipzeker.nl/alles-over-bellen-met-voip/nat

9. LACP vs PAGP: What's the Difference? – GeeksforGeeks [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/lacp-vs-

pagp-whats-the-difference/#:~:text=LACP%20is%20an%20Open%20standard%2C%20i.e.%2C%20supported%20by%20most%20vendors,be%20used%20between%20Cisco%20devices.&text=LACP%20has%20two%20modes%2C%20i.e.,ports%20by%20exchanging%20LACP%20packets.)

10. ОВЕН [Електронний ресурс] – Режим доступу до ресурсу: https://owen.ua/

ДОДАТОК А

Конфігураційний файл шлюзового маршрутизатора Pasichna_Router_4

```
Building configuration...

Current configuration : 4099 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Pasichna_Router_4
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.23.152.1 172.23.152.10
ip dhcp excluded-address 172.23.152.24
ip dhcp excluded-address 172.23.152.33 172.23.152.43
ip dhcp excluded-address 172.23.152.65 172.23.152.75
!
ip dhcp pool Vlan24pool
network 172.23.152.0 255.255.255.224
default-router 172.23.152.1
dns-server 172.23.153.46
ip dhcp pool Vlan34pool
network 172.23.152.32 255.255.255.224
```

default-router 172.23.152.33

dns-server 172.23.153.46

ip dhcp pool Vlan44pool

network 172.23.152.64 255.255.255.224

default-router 172.23.152.65

dns-server 172.23.153.46

!

!

aaa new-model

!

aaa authentication login default group radius local

!

!

!

!

!

!

!

no ip cef

no ipv6 cef

!

!

!

username 12320sk1_Pasichna privilege 15 password 7 082048430017061E010803

!

!

crypto isakmp policy 1

encr aes 256

authentication pre-share

```
!
crypto isakmp key cisco address 64.100.13.2
crypto isakmp key cisco address 209.165.202.2
!
!
!
crypto ipsec transform-set VPN-IPSEC-SET esp-aes esp-sha-hmac
!
crypto map MAP 14 ipsec-isakmp
set peer 64.100.13.2
set transform-set VPN-IPSEC-SET
match address VPN
!
!
!
!
ip ssh version 2
ip domain-name Pasichna_Router_4
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
```

```
speed auto
!
interface GigabitEthernet0/0/0.24
encapsulation dot1Q 24
ip address 172.23.152.1 255.255.255.224
ip nat inside
!
interface GigabitEthernet0/0/0.34
encapsulation dot1Q 34
ip address 172.23.152.33 255.255.255.224
ip nat inside
!
interface GigabitEthernet0/0/0.44
encapsulation dot1Q 44
ip address 172.23.152.65 255.255.255.224
ip nat inside
!
interface GigabitEthernet0/0/0.99
encapsulation dot1Q 99
ip address 172.23.152.97 255.255.255.248
ip nat inside
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
```

```
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 209.165.202.2 255.255.255.224
ip ospf cost 7500
ip access-group 100 in
ip nat outside
crypto map MAP
!
interface Serial0/1/1
ip address 10.0.14.10 255.255.255.252
ip ospf cost 7500
ip nat inside
clock rate 128000
!
interface Serial0/2/0
ip address 10.0.14.1 255.255.255.252
ip ospf cost 7500
ip nat inside
clock rate 128000
!
interface Serial0/2/1
ip address 10.0.14.17 255.255.255.252
ip ospf cost 7500
!
interface Vlan1
no ip address
shutdown
```

```
!
router ospf 9
log-adjacency-changes
network 10.0.14.8 0.0.0.3 area 0
network 10.0.14.0 0.0.0.3 area 0
network 172.23.152.0 0.0.0.31 area 0
network 172.23.152.32 0.0.0.31 area 0
network 172.23.152.64 0.0.0.31 area 0
network 172.23.152.96 0.0.0.7 area 0
network 209.165.202.0 0.0.0.31 area 0
network 10.0.14.16 0.0.0.3 area 0
!
ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224
ip nat inside source list 114 pool Internet
ip nat inside source static 172.23.153.45 209.165.202.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
!
ip access-list extended VPN
permit ip 172.23.152.0 0.0.7.255 172.23.153.0 0.0.0.31
access-list 14 permit 172.23.152.0 0.0.7.255
access-list 114 deny ip 172.23.152.0 0.0.7.255 172.23.153.0 0.0.0.31
access-list 114 permit ip 172.23.152.0 0.0.7.255 any
access-list 100 permit ip any 209.165.202.0 0.0.0.31
access-list 100 permit ospf any any
!
banner motd ^CPasichna_Router_4. This is a secure system. Authorized
```

```
Access Only!^C
!
!
radius server serverRadius
address ipv4 172.23.153.46 auth-port 1645
key radius123
radius server 172.23.153.46
address ipv4 172.23.153.46 auth-port 1645
key radius123
!
!
!
line con 0
password 7 0822455D0A16
login authentication default
!
line aux 0
!
line vty 0 4
exec-timeout 60 0
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
exec-timeout 60 0
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
```