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 Моісеєнка Михайла Олеговича
(П.І.Б.)
академічної групи 123-21-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)
на тему «Комп'ютерна система компанії з монтажу та обслуговування ліфтів з детальним опрацюванням побудови та налаштування мережі організації»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Бешта Д.О.			
загального розділу	доц. Бешта Д.О.			
спеціальних розділів	доц. Бешта Д.О.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

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

"___" _____ 2025 року.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента ___Моісеєнко М.О.___**академічної групи**___123-21-1____
(прізвище, ініціали)(шифр)

спеціальності _____123 Комп'ютерна інженерія_____
(код і назва спеціальності)

за освітньо-професійною програмою_____Комп'ютерна інженерія_____
(офіційна назва)

на тему __«Комп'ютерна система компанії з монтажу та обслуговування ліфтів з детальним опрацюванням побудови та налаштування мережі організації»_____

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

Розділ	Зміст завдання	Термін виконання
Стан питання і постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел показати актуальність завдання, сформулювати мету та задачі виконання кваліфікаційної роботи	10.02.2025
Технічні вимоги до об'єкту вивчення	Сформулювати найменування й призначення комп'ютерної системи, висунути технічні вимоги до неї	15.03.2025
Розробка апаратної частини	Виконати технічне проєктування апаратної частини комп'ютерної системи з необхідними інженерними розрахунками	20.04.2025
Розробка мережі організації	Розрахувати й розподілити адреси вузлів комп'ютерної системи, розробити заходи з обмеження доступу до даних системи	07.05.2025
Програмування компонента системи	Обґрунтувати технічні характеристики програми й розробити програму для компонента системи	31.05.2025

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

Дата видачі _25.01.2025 р._

Дата подання до атестаційної комісії __16.06.2025 р.__

Прийнято до виконання _____ Моісеєнко М.О.

РЕФЕРАТ

Пояснювальна записка: 78 с., 43 рис., 12 табл., 1 додаток, 7 джерел.

КОМП'ЮТЕРНА СИСТЕМА, ЛОКАЛЬНА МЕРЕЖА, АДРЕСАЦІЯ ВУЗЛІВ, СЕРВЕРНЕ ОБЛАДНАННЯ, МЕРЕЖЕВА ІНФРАСТРУКТУРА, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Об'єкт розробки − комп'ютерна система підприємства, що спеціалізується на монтажі та технічному обслуговуванні ліфтів.

Мета − розробити та обґрунтувати побудову комп'ютерної системи з локальною мережею для підприємства з монтажу та обслуговування ліфтів, яка забезпечить ефективний обмін інформацією між структурними підрозділами та підвищить рівень інформаційної безпеки.

У кваліфікаційній роботі розглянуто питання створення комп'ютерної системи для підприємства з надання послуг монтажу та обслуговування ліфтового обладнання. Здійснено аналіз вимог до системи, сформульовано її основні функції та технічні характеристики. Розроблено структурну схему мережі організації, виконано проєктування апаратної частини системи з урахуванням обчислювального навантаження та оптимального розміщення обладнання.

Розподілено IP-адреси вузлів мережі, реалізовано заходи з обмеження доступу до внутрішніх ресурсів. Також обґрунтовано вибір програмного забезпечення для роботи системи та розроблено апаратно-програмний модуль, що забезпечує дистанційний контроль за ліфтовими приміщеннями.

Результатом виконаної роботи є комплексне технічне рішення, яке може бути впроваджене на підприємстві з подальшою можливістю масштабування.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

СКС	–	Структурована кабельна система, яка є ієрархічною кабельною мережею для передачі інформації
КС	–	Комп’ютерна система, комплекс апаратного та програмного забезпечення, що забезпечує обробку, збереження та передачу даних
SVI	–	(Switched Virtual Interface) використовується для забезпечення рівня 3 (мережевого) доступу на комутаторах, дозволяючи їм взаємодіяти з іншими пристроями у VLAN
VLAN	–	(Virtual Local Area Network) технологія, що дозволяє логічно розділяти мережу на окремі сегменти без фізичного розмежування
LAN	–	(Local Area Network) локальна мережа, що об'єднує комп'ютери та інші пристрої в межах обмеженої території, наприклад офісу, будинку або підприємства
LACP	–	(Link Aggregation Control Protocol) мережевий протокол, що використовується для об'єднання кількох фізичних з'єднань у один логічний канал
NAT	–	(Network Address Translation) технологія, що використовується для зміни IP-адрес у мережевих пакетах під час їх проходження через маршрутизатор або брандмауер
WAN	–	(Wide Area Network) комп'ютерна мережа, що охоплює великі географічні території, такі як міста, країни або навіть континенти.
AAA	–	(Authentication, Authorization, and Accounting) мережевий протокол, що використовується для управління доступом до ресурсів, перевірки прав користувачів та ведення обліку їхніх дій
RADIUS	–	(Remote Authentication Dial-In User Service) мережевий протокол, що використовується для аутентифікації, авторизації та обліку (AAA) користувачів у корпоративних та провайдерських мережах

ВСТУП

У сучасних умовах функціонування підприємств усе більшої важливості набуває ефективне використання комп’ютерних систем та мережевих технологій. Особливо це стосується компаній, які займаються монтажем і технічним обслуговуванням складного обладнання, зокрема ліфтів. Така діяльність передбачає оперативну взаємодію між підрозділами, ведення технічної документації, облік звернень клієнтів і контроль виконання заявок, що вимагає надійної інформаційної інфраструктури.

Забезпечення внутрішніх процесів за допомогою сучасної комп’ютерної системи дозволяє не лише підвищити продуктивність праці персоналу, а й значно покращити якість обслуговування клієнтів. Організація локальної мережі, яка забезпечує швидкий доступ до даних, централізоване зберігання інформації та захист від несанкціонованого доступу, є невід’ємною складовою таких систем.

Актуальність теми кваліфікаційної роботи полягає у необхідності розробки ефективної комп’ютерної системи для підприємства з монтажу та обслуговування ліфтів, яка дозволить оптимізувати інформаційні потоки, забезпечити злагоджену роботу між підрозділами компанії та створити надійну основу для подальшого розвитку інформаційної інфраструктури.

Метою даної роботи є розробка комп’ютерної системи для компанії з монтажу та обслуговування ліфтів, що включає побудову локальної мережі організації та розробку апаратно-програмного комплексу – IoT-підсистеми для контролю за ліфтовими приміщеннями. Робота також передбачає реалізацію заходів із захисту інформації, розрахунок адресного простору мережі та обґрунтування вибору технічних і програмних засобів.

1. СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Роль і значення комп’ютерних систем у сфері застосування

Сучасна інженерна та сервісна діяльність у сфері монтажу й технічного обслуговування ліфтового обладнання неможлива без застосування комп’ютерних систем. Зростаючі вимоги до оперативності, безпеки та точності виконання робіт вимагають цифровізації процесів на всіх етапах – від обробки клієнтських заявок до контролю технічного стану об’єктів. У цьому контексті комп’ютерні системи відіграють ключову роль як інструмент управління, моніторингу та забезпечення зв’язку між усіма структурними елементами підприємства.

Комп’ютерні системи забезпечують злагоджену роботу локальної мережі організації, дають змогу організувати централізоване зберігання та обробку інформації, а також реалізувати доступ до даних за допомогою внутрішніх серверів або хмарних технологій. Важливою перевагою є можливість швидкої комунікації між підрозділами, що дозволяє оперативно реагувати на зміну ситуації, координувати виїзні бригади, вести електронний облік технічного обслуговування, а також планувати профілактичні заходи.

Також одним із найважливіших напрямів розвитку є інтеграція комп’ютерних систем з технологіями Інтернету речей (IoT), що дозволяє здійснювати безперервний контроль за станом об’єктів у режимі реального часу. У випадку компанії, яка обслуговує ліфти, це відкриває можливості для віддаленого моніторингу ліфтових приміщень, зокрема параметрів освітлення, температури, вологості, стану дверей, наявності руху тощо. Таким чином, апаратно-програмні комплекси на основі IoT стають невід’ємною частиною комп’ютерної системи підприємства, підвищуючи її функціональність, безпеку та ефективність.

Завдяки використанню комп’ютерних систем із відповідним програмним забезпеченням досягається вища точність у роботі, зменшується вплив людського фактору, підвищується продуктивність і якість обслуговування. Усі ці чинники вказують на важливість інтеграції сучасних комп’ютерних рішень у виробничу

діяльність підприємств, пов’язаних з технічно складними об’єктами, такими як ліфти.

1.2 Характеристика, структура, особливості, умови роботи об’єкту впровадження

1.2.1 Характеристика об’єкту впровадження

Об’єктом впровадження є підприємство, яке здійснює діяльність у сфері монтажу та технічного обслуговування ліфтового обладнання в житлових і громадських будівлях. Основними напрямами роботи підприємства є встановлення нових ліфтів, модернізація існуючих підйомних механізмів, а також забезпечення їхнього стабільного та безпечного функціонування шляхом періодичного технічного огляду й усунення несправностей.

Підприємство має структурну організацію, що включає адміністративний відділ, інженерно-технічну службу, диспетчерську службу, виїзні сервісні бригади та складське господарство. Ефективна координація між цими підрозділами вимагає надійної комп’ютерної системи, яка б забезпечувала обмін інформацією, облік заявок, моніторинг технічного стану обладнання та організацію виїздів спеціалістів.

На сьогоднішній день підприємство використовує застарілі або ізольовані засоби зв’язку, що не дозволяють в повному обсязі автоматизувати та контролювати ключові процеси. Зокрема, відсутній єдиний центр збору інформації про стан ліфтових приміщень, не реалізовано централізовану обробку заявок, що надходять до диспетчерської служби, та не впроваджено сучасні механізми контролю доступу до критичної інформації.

У зв’язку з цим виникає потреба у впровадженні сучасної комп’ютерної системи з локальною мережею, серверною інфраструктурою та IoT-підсистемою для моніторингу стану ліфтових приміщень. Передбачається встановлення апаратно-програмного комплексу, який забезпечуватиме безперервний збір і передачу інформації з датчиків (температури, руху, вологості, відкриття дверей тощо) на центральний сервер або хмарне середовище.

Реалізація запропонованої системи дозволить значно підвищити рівень обробки процесів, покращити якість технічного обслуговування, знизити витрати часу на реагування, а також забезпечити надійне збереження та захист інформації.

1.2.2 Організаційна структура компанії

Організаційна структура компанії, що здійснює монтаж та технічне обслуговування ліфтів, побудована за функціональним принципом і забезпечує ефективний розподіл обов'язків між підрозділами. Така структура дозволяє оперативно реагувати на звернення клієнтів, виконувати технічні завдання, вести документацію та координувати дії виїзних сервісних бригад.

Компанія включає такі основні структурні підрозділи.

Адміністрація. Здійснює загальне керівництво підприємством, розподіл ресурсів, організацію взаємодії між відділами та прийняття управлінських рішень.

Відділ технічного обслуговування. Відповідає за планування й виконання робіт з обслуговування, ремонту та модернізації ліфтового обладнання. Взаємодіє з виїзними бригадами та веде технічну документацію.

Виїзні сервісні бригади. Складаються з кваліфікованих інженерів і техніків, які виконують безпосереднє обслуговування ліфтів на об'єктах замовників. Оснащені мобільними пристроями для отримання й оновлення завдань у реальному часі.

Диспетчерська служба. Приймає виклики від користувачів ліфтів, реєструє звернення, передає їх відповідним службам. Також здійснює контроль виконання заявок і надає звіти керівництву.

Служба інформаційних технологій (IT-відділ). Забезпечує належне функціонування комп'ютерної системи, підтримку мережевої інфраструктури, зберігання даних та обслуговування IoT-підсистеми моніторингу ліфтових приміщень.

Складське господарство. Відповідає за облік, зберігання й видачу запасних частин, інструментів та матеріалів для сервісних бригад.

У межах реалізації комп’ютерної системи всі підрозділи будуть об’єднані єдиною інформаційною мережею, що забезпечить централізований облік, оперативну комунікацію та моніторинг технічного стану ліфтових приміщень. Ключову роль у цьому процесі відіграватиме ІТ-відділ, який координуватиме інтеграцію апаратно-програмного комплексу в існуючу організаційну структуру.

Впровадження комп’ютерної системи з IoT-підсистемою дозволить підвищити ефективність управління ресурсами, скоротити час реагування на несправності та забезпечити належний рівень інформаційної безпеки у межах організації.

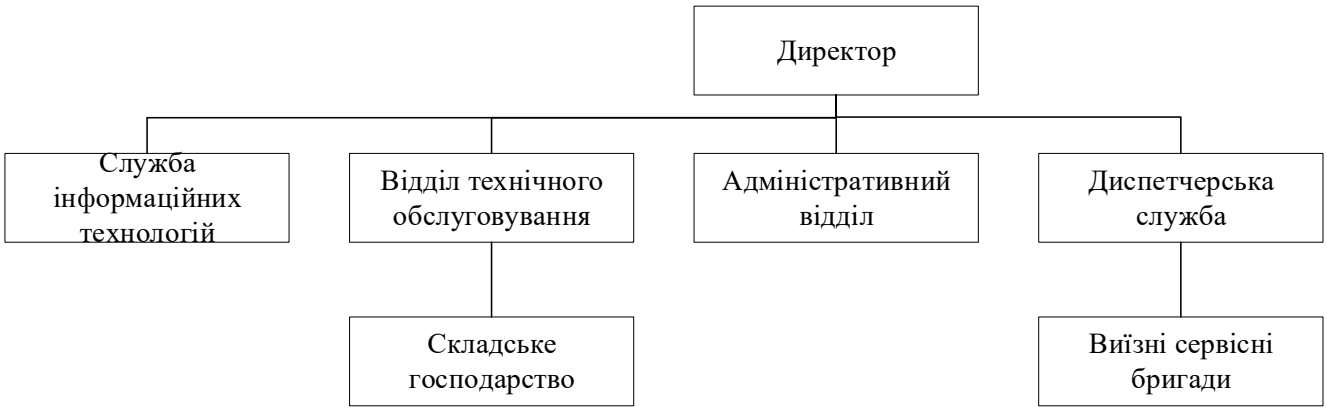

Рисунок 1.1 – Схема організаційної структури компанії

1.2.3 Особливості об’єкту впровадження

Об’єкт впровадження має низку особливостей, які слід враховувати під час розробки та реалізації комп’ютерної системи. Ці особливості обумовлюють як технічні вимоги до системи, так і організаційні підходи до її впровадження.

1) Територіальна розподіленість об’єктів обслуговування. Ліфтові установки, які обслуговує компанія, розташовані на значній території, часто у віддалених житлових масивах, адміністративних будівлях або комерційних об’єктах. Це створює потребу в системі моніторингу на базі IoT, яка забезпечує дистанційний збір даних із ліфтових приміщень без постійної присутності персоналу.

2) Критичність оперативного реагування. Несправність ліфтів може призвести до серйозних незручностей або навіть загрози життю і здоров'ю користувачів. Тому важливо забезпечити цілодобове отримання інформації про аварійні ситуації та миттєву передачу повідомлень до диспетчерської служби або виїзної бригади.

3) Високі вимоги до надійності та безперервності роботи. Оскільки від роботи комп'ютерної системи залежить оперативність обслуговування та безпека користувачів, вона повинна бути відмовостійкою, стабільною та безпечною. Передбачено використання резервних джерел живлення, безпечного з'єднання та захисту даних.

4) Необхідність інтеграції апаратних та програмних засобів. Є потреба у встановленні апаратно-програмного комплексу, до складу якого входять контролери, датчики (температури, вологості, руху, відкриття дверей тощо), комунікаційне обладнання та серверна частина з відповідним програмним забезпеченням.

5) Вимога централізації обробки інформації. Для ефективної роботи всіх підрозділів необхідна єдина база даних, в якій зберігається інформація про стан обладнання, заявки, історію обслуговування та дії персоналу. Це забезпечує прозорість, аналітику та можливість керівництва приймати обґрунтовані рішення.

6) Потреба в багаторівневому контролі доступу. Різні категорії працівників мають різні права доступу до інформації. Наприклад, диспетчер може переглядати та створювати заявки, а ІТ-відділ – змінювати конфігурацію системи. Система повинна реалізовувати автентифікацію, авторизацію та аудит дій користувачів.

З огляду на ці особливості комп'ютерна система має бути гнучкою, масштабованою, зручною в адмініструванні та адаптованою до специфіки обслуговування ліфтового обладнання.

1.2.4 Умови роботи та проблематика об'єкту впровадження

Підприємство, функціонує в умовах підвищеної відповідальності перед споживачами та має справу з інфраструктурними об'єктами, критичними для

щоденного користування мешканцями багатоповерхових будівель. Це формує специфічні умови роботи та виклики, які необхідно врахувати під час впровадження комп’ютерної системи.

Режим роботи 24/7. Оскільки зупинка чи несправність ліфта може статися в будь-який момент, підприємство зобов’язане забезпечувати цілодобовий моніторинг та швидке реагування. У зв’язку з цим необхідно впровадити постійну технічну підтримку та автоматизований збір сигналів від IoT-пристроїв, що контролюють стан ліфтових приміщень.

Велика кількість об'єктів обслуговування. Компанія обслуговує десятки, а іноді й сотні ліфтових установок у різних районах міста чи області. Це вимагає масштабованої інформаційної системи, здатної обробляти великі обсяги даних із багатьох джерел одночасно.

Відсутність єдиної інформаційної бази. На момент початку впровадження відсутня централізована база даних про ліфтові установки, графіки обслуговування, аварійні виклики та виконані роботи. Така ситуація ускладнює контроль і звітність, що негативно впливає на якість послуг.

Низький рівень автоматизації обліку і звітності. Більшість операцій, пов’язаних з прийомом заявок, передачею завдань виїзним бригадам, формуванням технічної документації, виконується вручну або із застосуванням застарілих програмних рішень. Це призводить до затримок, помилок і дублювання інформації.

Слабкий контроль за технічним станом ліфтових приміщень. Через відсутність сучасної IoT-підсистеми облік змін параметрів мікроклімату (температури, вологості), стану дверей, руху або задимлення в машинному відділенні ведеться нерегулярно або не ведеться зовсім. Це підвищує ризики аварійних ситуацій та зменшує ресурс обладнання.

Обмежений контроль доступу до інформації. Інформація про технічний стан об’єктів або про виконання заявок доступна багатьом працівникам без належного розмежування прав. Відсутність системи авторизації створює ризики витоку або несанкціонованої зміни даних.

Нерозвинена мережна інфраструктура. У багатьох віддалених точках об’єкта (наприклад, у машинних відділеннях ліфтів) відсутнє якісне підключення до мережі або електроживлення, що ускладнює встановлення і роботу IoT-пристроїв без відповідних автономних рішень (наприклад, живлення від батарей чи використання мобільного інтернету).

1.2.5 Топологічна схема компанії

Комп’ютерна мережа компанії, що займається монтажем і обслуговуванням ліфтів, побудована за ієрархічною топологією з використанням розподіленої структури, яка охоплює п’ять локальних мереж (LAN). Для забезпечення ефективного управління, безпеки та масштабованості, мережа організована на базі чотирьох розподільчих маршрутизаторів та одного спеціалізованого маршрутизатора з функціями міжмережевого екрану (IPS).

Основні елементи мережі:

– IPS-маршрутизатор центральний шлюз до Інтернету з вбудованим інструментом для захисту від вторгнень;

– R1, R2, R3, R4 розподільчі маршрутизатори, що відповідають за підключення LAN2–LAN5.

– R0 маршрутизатор віддаленої мережі, який забезпечує зв’язок з окремою інфраструктурною локацією підприємства.

– LAN1–LAN5 — локальні мережі, організовані для підтримки окремих підрозділів компанії.

Переваги топології:

– гнучкість і масштабованість (легке додавання нових підмереж або підрозділів);

– сегментація мережі через VLAN (покращення безпеки та керованості трафіку);

– розподілене навантаження (завдяки багаторівневій маршрутизації);

– інтеграція IoT-підсистеми (безпосередній збір та обробка даних із ліфтових об'єктів)

– захищений доступ до віддаленої мережі (з використанням сучасних методів шифрування).

Схема топології мережі наочно ілюструє логічні зв’язки між компонентами комп’ютерної системи компанії (див. рисунок 1.2).

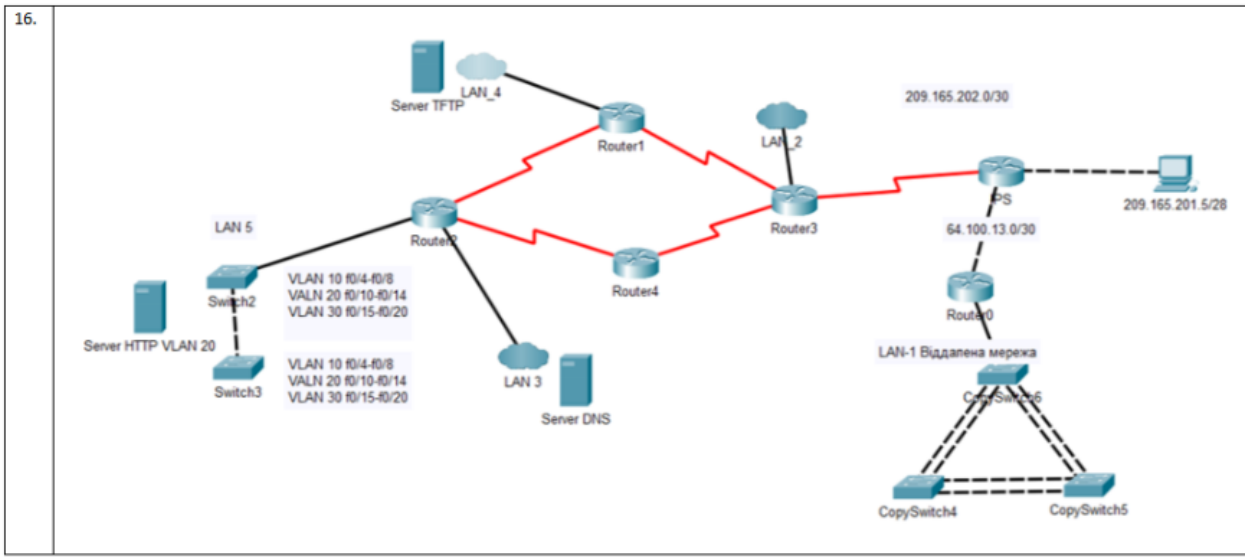

Рисунок 1.2 – Топологічна схема комп’ютерної мережі підприємства

1.3 Огляд існуючих аналогів систем, технологій, архітектур та програмних рішень

В умовах сучасної цифровізації особливої популярності набувають системи моніторингу стану обладнання, управління обслуговуванням, а також кіберзахисту інформаційної інфраструктури підприємств.

1.3.1 Існуючі програмно-апаратні рішення

Серед комерційних систем, які застосовуються у сфері моніторингу та диспетчеризації ліфтів, виділяються наступні:

– Orona 3G Smart – система для моніторингу ліфтового обладнання в реальному часі, з використанням GSM-модулів та хмарної платформи;

– Schindler Ahead – IoT-рішення для прогнозного обслуговування та аналітики, яке включає сенсори, хмарну інфраструктуру та мобільний застосунок;

– KONE 24/7 Connected Services – інтелектуальна система, що використовує машинне навчання для аналізу даних із ліфтів та ескалаторів;

– локальні SCADA-системи (наприклад, WinCC, MasterSCADA) – широко застосовуються для візуалізації, збору та зберігання даних в межах одного або кількох об’єктів.

1.3.2 Технології та архітектури

Інтегровані системи для обслуговування технічних об’єктів зазвичай будуються за багаторівневою архітектурою.

Периферійний рівень: датчики, контролери, пристрої збору даних (Edge-обчислення).

Комунікаційний рівень: передача даних через Ethernet, Wi-Fi, GSM/4G, LoRaWAN або NB-IoT.

Серверний рівень: обробка, архівування та аналітика даних, зазвичай з використанням баз даних SQL/NoSQL.

Клієнтський рівень: доступ до інформації через веб-інтерфейси, мобільні додатки або HMI-панелі.

1.3.3 Програмні засоби

У контексті розробки власного програмного забезпечення для моніторингу та обслуговування технічних приміщень, найчастіше використовуються такі засоби:

Node-RED – графічне середовище для побудови логіки IoT-додатків;

MQTT/HTTP APIs – протоколи обміну даними між пристроями та сервером;

Grafana/ThingsBoard/OpenHAB – платформи для візуалізації даних з сенсорів;

Python/C++/JavaScript – як основні мови програмування для створення серверної та клієнтської логіки.

1.3.4 Аналіз аналогів

Існуючі рішення, попри свою функціональність, здебільшого мають комерційний характер або обмежені можливості кастомізації. Крім того, деякі з них вимагають високих фінансових вкладень на впровадження та обслуговування. Тому розробка адаптованої під потреби конкретної компанії комп'ютерної системи із відкритою архітектурою, підтримкою IoT та сучасних протоколів безпеки є доцільною, як з технічної, так і з економічної точки зору.

1.4 Обґрунтування напрямку вирішення задачі для об'єкта впровадження

У сучасних умовах експлуатації ліфтового обладнання особливу актуальність набуває не лише технічна надійність, а й можливість своєчасного моніторингу технічного стану, реагування на аварійні ситуації, ведення журналу обслуговування, а також централізоване управління з урахуванням географічної розподіленості об'єктів. Впровадження комп'ютерної системи із включенням IoT-компонентів дозволяє якісно підвищити рівень контролю, автоматизації та інформаційної безпеки в діяльності компанії.

1.4.1 Проблематика та необхідність автоматизації

На момент розробки система управління ліфтовими приміщеннями в компанії базується на фрагментованих рішеннях: локальні контролери, відсутність централізованої обробки даних, слабкий моніторинг стану обладнання в реальному часі та низький рівень автоматизації обслуговування. Також існують труднощі з доступом до аналітики з різних філій або віддалених об'єктів.

Враховуючи ці проблеми, доцільним є впровадження єдиної комп'ютерної системи з модульною архітектурою, яка об'єднує:

– апаратну частину (сервера, маршрутизатори, комутатори, сенсори, мікроконтролери);

– програмне забезпечення для збору, обробки, передачі та візуалізації даних;

– IoT-підсистему для автоматичного контролю стану приміщень та обладнання.

1.4.2 Ідея реалізації

Основна ідея проекту полягає у створенні багаторівневої комп'ютерної системи, що охоплює центральний офіс та віддалені об'єкти обслуговування. У кожному приміщенні з ліфтовим обладнанням передбачається розгортання локальних обчислювальних вузлів на базі мікроконтролерів (ESP32 або Raspberry Pi) із підключеними сенсорами, такими як температура, вологість, відкриття дверей та присутність персоналу. Всі вузли об'єднуються в єдину мережу через VPN-з'єднання з маршрутизацією між LAN через захищені канали. Для обміну даними між вузлами та центральним сервером використовується протокол MQTT, що забезпечує ефективну взаємодію. Передбачається розробка веб-панелі для візуалізації стану об'єктів, отримання сповіщень, перегляду історичних даних та керування обладнанням. Також впроваджуються механізми безпеки, включаючи контроль доступу, ізоляцію VLAN, міжмережеві екрани та аудит дій користувачів.

1.4.3 Очікуваний результат

Запропонований підхід дозволить досягти таких результатів:

– централізація даних з усіх ліфтових приміщень у межах єдиної системи;

– підвищення ефективності технічного обслуговування завдяки ранньому виявленню відхилень;

– можливість дистанційного моніторингу та реагування;

– покращення кіберзахисту даних;

– зменшення простоїв обладнання та підвищення його надійності.

Таким чином, обґрунтований вибір напрямку базується на поєднанні сучасних IoT-технологій, мережевих рішень і адаптованого програмного забезпечення, що разом утворюють ефективну та масштабовану систему для підприємства.

1.5 Функціональна структура об’єкту професійної діяльності

1.5.1 Основні функціональні напрями діяльності компанії

Проєктно-монтажний напрям, забезпечення встановлення нового ліфтового обладнання на об’єктах замовника, включно з проєктуванням, закупівлею комплектуючих та пусконалагоджувальними роботами.

Сервісне обслуговування, регулярне технічне обслуговування ліфтів відповідно до регламенту, виявлення та усунення несправностей, аварійно-диспетчерське реагування.

Моніторинг та контроль стану обладнання, збір і аналіз даних про технічний стан обладнання через IoT-компоненти, зокрема з ліфтових машинних приміщень, що дозволяє виконувати превентивне обслуговування.

Адміністративне управління, планування ресурсів, формування графіків робіт, бухгалтерія, звітність, кадрове діловодство.

Інформаційна підтримка, робота з базами даних об’єктів, історією обслуговування, сервісними заявками, підтримка клієнтів через IT-системи.

1.5.2 Функціональні компоненти комп’ютерної системи

Центральний серверний сегмент, який використовується для обробки даних з усіх підрозділів, зберігання журналів обслуговування, обліку запчастин, обліку звернень та керування обліковими записами співробітників.

IoT-підсистема контролю ліфтових приміщень, яка складається з мікроконтролерів та датчиків (температура, вологість, дим, доступ), з’єднаних з мережею компанії через маршрутизатори. Передає дані у центральну систему за допомогою MQTT.

Локальні офіси та філії, які використовують термінали доступу до бази даних, локальні мережі (LAN) та засоби зв’язку для обміну інформацією з головним офісом.

Мобільні робочі місця персоналу. Техніки мають планшети або смартфони з доступом до внутрішньої системи для перегляду заявок, введення результатів обслуговування, фіксації несправностей у реальному часі.

Система безпеки та резервного копіювання, впроваджені VLAN для поділу трафіку, IPS-маршрутизатор для фільтрації, механізми автентифікації та резервне копіювання на хмарне або локальне сховище.

1.5.3 Взаємозв'язок функціональних блоків

Усі блоки взаємодіють через корпоративну IP-мережу, побудовану за ієрархічною топологією. Дані з віддалених об’єктів (через VPN або LTE-з’єднання) надходять до центрального сервера, де обробляються та архівуються. Програмне забезпечення забезпечує доступ керівництва до аналітики, а персоналу – до функціональних даних для поточної роботи.

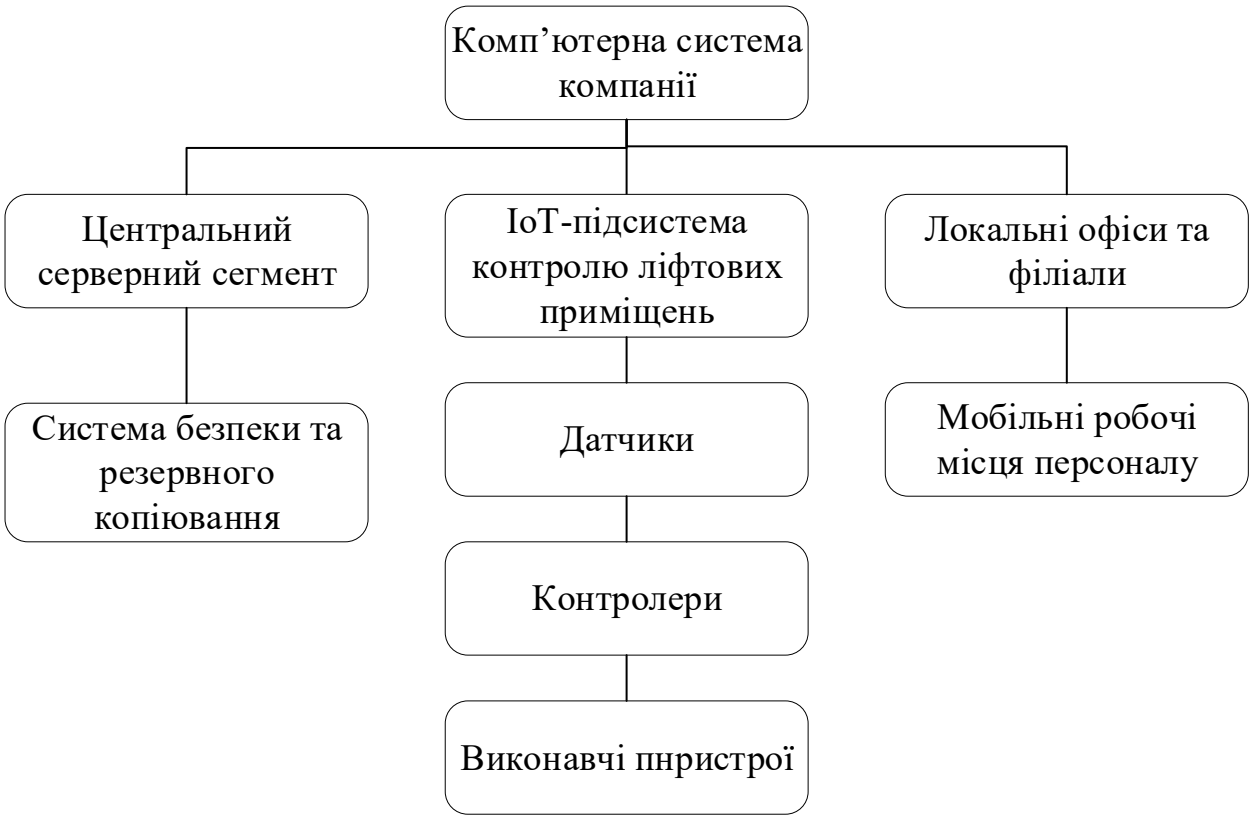

Рисунок 1.3 – Взаємозв'язок функціональних блоків

1.6 Мета і задачі роботи

Мета роботи: метою даної кваліфікаційної роботи є розробка комп’ютерної системи для компанії, що спеціалізується на монтажі та технічному обслуговуванні ліфтів, з детальним опрацюванням побудови та налаштування

організаційної мережі. У рамках роботи також передбачається впровадження IoT-підсистеми для моніторингу технічного стану ліфтових приміщень, з метою підвищення надійності обладнання та ефективності сервісного обслуговування.

Основні задачі роботи:

– провести огляд науково-технічних джерел для обґрунтування актуальності розробки;

– сформувати технічні вимоги до комп’ютерної системи та її складових.

– розробити структуру корпоративної мережі підприємства з урахуванням сучасних принципів безпеки та сегментації (у тому числі VLAN);

– розробити апаратну частину системи, враховуючи вимоги до продуктивності, масштабованості та енергоспоживання;

– розробити топологічну схему мережі з урахуванням декількох локальних мереж (LAN), маршрутизаторів розподілу та IPS-фільтрації;

– визначити IP-адресацію вузлів комп’ютерної системи та правила керування доступом до інформаційних ресурсів;

– проаналізувати існуючі програмно-апаратні рішення для віддаленого моніторингу та керування об'єктами;

– розробити програмну частину IoT-підсистеми на базі мікроконтролерів для збору та передавання даних з ліфтових приміщень.

2. ТЕХНІЧНІ ВИМОГИ ДО КОМП’ЮТЕРНОЇ СИСТЕМИ

Повна назва: «Комп'ютерна система компанії з монтажу та обслуговування ліфтів», далі Система.

Система призначена для поліпшення основних процесів діяльності компанії, що спеціалізується на монтажі та технічному обслуговуванні ліфтів, з акцентом на централізоване управління інформаційними потоками, підвищення надійності сервісного обслуговування та впровадження моніторингу технічного стану об’єктів за допомогою IoT-підсистеми. Вона забезпечує збір, обробку та збереження даних про об’єкти обслуговування, дозволяє диспетчерам і технічному персоналу своєчасно отримувати інформацію про стан ліфтового обладнання, планувати обслуговування, фіксувати виконані роботи, а також оперативно реагувати на аварійні ситуації.

Комплексне поєднання програмного й апаратного забезпечення дозволяє реалізувати сучасний підхід до управління сервісною інфраструктурою з можливістю масштабування та віддаленого доступу.

2.1 Вимоги до структури і функціонування Системи

2.1.1 Перелік функціональних складових чи підсистем, їхнє призначення

Система має модульну архітектуру та складається з кількох функціональних складових (підсистем), кожна з яких виконує визначену роль у загальній структурі інформаційного середовища підприємства.

Підсистема керування обслуговуванням ліфтів. Забезпечує ведення обліку об’єктів обслуговування, реєстрацію заявок, планування профілактичних робіт, фіксацію результатів технічного огляду та ремонту. Підтримує формування графіків робіт та звітної документації.

IoT-підсистема моніторингу ліфтових приміщень. Включає мікроконтролери, датчики (температури, вологості, задимлення, відкриття дверей тощо) та відповідне програмне забезпечення. Призначена для збору й передавання

інформації про стан середовища в машинних приміщеннях у реальному часі для виявлення потенційних відхилень або небезпечних ситуацій.

Підсистема управління мережею та безпекою. Складається з маршрутизаторів, комутаторів, міжмережевих екранів (у тому числі IPS) і програмного забезпечення для управління мережею. Забезпечує сегментацію мережі на основі VLAN, контроль доступу, шифрування даних і захист від зовнішніх загроз.

Інформаційно-аналітична підсистема. Збирає та агрегує дані з усіх компонентів системи, надаючи інструменти для статистичного аналізу, візуалізації технічного стану обладнання, формування звітів і аналітичних довідок для управлінського персоналу.

Підсистема обліку персоналу та доступу. Відповідає за реєстрацію користувачів, управління правами доступу, ведення журналів дій та інтеграцію з внутрішніми або зовнішніми системами ідентифікації.

Підсистема резервного копіювання та відновлення. Призначена для автоматичного створення резервних копій даних, налаштувань мережі та системного програмного забезпечення. Забезпечує відновлення працездатності системи у разі збоїв або втрати інформації.

2.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи

Комунікаційна інфраструктура повинна гарантувати цілісність та доставку даних у режимі реального часу, особливо між IoT-пристроями та центральним сервером. Це критично важливо для оперативного виявлення аварійних ситуацій у ліфтових приміщеннях.

У системі повинно передбачатися використання як дротових (Ethernet), так і бездротових (Wi-Fi, LTE, LoRa або ZigBee) каналів зв’язку. Дротовий зв’язок застосовується в межах корпоративної локальної мережі (LAN), а бездротовий – для підключення віддалених або важкодоступних IoT-пристроїв.

Зв’язок між сегментами мережі має здійснюється за допомогою керованих комутаторів із підтримкою VLAN, а також маршрутизаторів з функціями фільтрації трафіку, управління пропускною здатністю та маршрутизації між підмережами.

Всі компоненти системи мають взаємодіяти через основний сервер (чи кластер серверів), який виступає в ролі вузла обробки запитів, збереження даних, аналітики та адміністрування.

Інформаційний обмін має здійснюватися з використанням захищених протоколів передачі (HTTPS, MQTT з TLS, VPN-тунелі тощо). Це забезпечує захист конфіденційної інформації від перехоплення, модифікації або втрати.

Компоненти IoT-підсистеми повинні підтримувати стандартизовані протоколи (MQTT, Modbus TCP, HTTP/REST API), що забезпечує легку інтеграцію, гнучкість та можливість масштабування системи.

У разі зростання навантаження в мережі повинна зберігатися пріоритетність критичного трафіку (сигнали тривоги з датчиків, повідомлення про відмови тощо).

2.1.3 Вимоги до характеристик взаємозв'язків створюваної Системи із суміжними Системами

Система повинна мати відкриті прикладні програмні інтерфейси (API) для взаємодії з іншими інформаційними системами, зокрема: бухгалтерськими та ERP-системами (наприклад, BAS ERP або 1C); системами контролю доступу персоналу; хмарними сервісами зберігання або аналітики.

Комунікація між системами має відбуватися із використанням шифрування (TLS/SSL), з автентифікацією запитів та журналюванням взаємодії.

Взаємозв’язки із суміжними системами повинні підтримувати як односторонню передачу (наприклад, експорт звітності до ERP), так і двосторонню синхронізацію даних (наприклад, отримання оновлених графіків обслуговування з центральної бази).

Система має підтримувати механізми синхронізації часових міток та періодичної актуалізації даних з урахуванням заданих інтервалів оновлення (real-time або пакетна передача).

При збільшенні кількості зовнішніх систем або користувачів, Система повинна забезпечити стабільну роботу каналів зв’язку, можливість горизонтального масштабування API та обробку більших обсягів запитів без деградації продуктивності.

У випадку використання датчиків або контролерів сторонніх постачальників, Система має бути сумісною з протоколами MQTT, CoAP, BACnet або іншими, що підтримуються цими пристроями.

2.1.4 Вимоги до режимів функціонування Системи

Система повинна функціонувати в кількох основних режимах, у кожному з яких ключову роль відіграє стабільна та захищена робота комп’ютерної мережі організації.

У нормальному штатному режимі вся інфраструктура локальних мереж (LAN) та маршрутизаторів повинна забезпечувати безперебійний обмін даними між центральним сервером, робочими станціями, мережевими сховищами та периферійними вузлами. Мережеве обладнання повинно гарантувати низьку затримку, високу пропускну здатність та підтримку пріоритету трафіку для критично важливих служб.

У режимі технічного обслуговування система дозволяє гнучко виводити з роботи окремі сегменти мережі (наприклад, VLAN або віддалені вузли), не порушуючи загальної функціональності, при цьому зберігається можливість моніторингу та журналювання змін через адміністраторські консолі.

В аварійному режимі система повинна швидко реагувати на мережеві збої, спроби несанкціонованого доступу, відмову маршрутизаторів або комутаторів, миттєво повідомляючи через резервні канали зв’язку (наприклад, мобільний інтернет) та активуючи політики резервного маршрутизації або VPN-з’єднання.

У режимі резервного живлення повинні підтримуватись ключові мережеві компоненти: маршрутизатори рівня розподілу, комутатори критичних LAN-сегментів та сервери безпеки, що дозволяє зберігати мінімально необхідну мережеву функціональність для координації роботи системи в умовах обмеженого енергоживлення.

Режим діагностики та тестування призначений для перевірки цілісності мережевої інфраструктури: проводяться пінг-тести, аналіз трасування маршрутів, перевірка пропускної здатності каналів та доступності серверів.

2.1.5 Межі розвитку, модернізації Системи

З метою забезпечення довготривалої ефективності та адаптивності Системи, необхідно передбачити можливості її подальшого розвитку та модернізації. Система повинна бути побудована за модульним принципом, що забезпечить гнучке масштабування як апаратної, так і програмної складових без потреби повного переоснащення інфраструктури.

Мережеве обладнання має підтримувати сучасні стандарти зв’язку (Gigabit Ethernet, IPv6, VLAN, VPN, QoS), а також мати резерв ємності по пропускній здатності портів і обробці трафіку. У перспективі має бути можлива інтеграція нових локальних мереж (LAN), включення додаткових вузлів (наприклад, сервісних офісів або технічних приміщень) та безболісне розширення існуючих підмереж без порушення загальної логіки маршрутизації.

Програмне забезпечення має мати підтримку оновлення версій, модифікації інтерфейсів користувача та розширення функціоналу без переривання сервісів. Важливим є забезпечення зворотної сумісності між компонентами, що дозволить виконувати поетапну модернізацію. Особливу увагу слід приділити питанням кібербезпеки: система повинна передбачати можливість інтеграції нових механізмів захисту, зокрема шифрування даних, багатофакторної автентифікації, сучасних міжмережевих екранів та систем виявлення вторгнень.

Також система повинна бути готова до переходу на хмарні сервіси або гібридну модель з частковою віртуалізацією, що забезпечить гнучке управління ресурсами, відмовостійкість та ефективне резервне копіювання.

Таким чином, у вимогах до розвитку комп’ютерної системи необхідно передбачити:

– можливість горизонтального та вертикального масштабування;

– модернізацію програмної платформи без зупинки системи;

– гнучке керування мережею з підтримкою централізованого адміністрування;

– інтеграцію з новими цифровими сервісами (IoT, аналітика, мобільний доступ);

– стійкість до змін нормативно-правової бази та технічних стандартів.

2.2 Вимоги до показників призначення

Система повинна відповідати визначеним технічним, функціональним та експлуатаційним вимогам, що відображають її здатність виконувати поставлені завдання з високою ефективністю та надійністю.

Продуктивність мережевої інфраструктури – не менше 1 Гбіт/с для основних магістралей, з можливістю масштабування до 10 Гбіт/с у майбутньому. Пропускна здатність комутаторів та маршрутизаторів повинна забезпечувати обробку пікових навантажень без втрати пакетів.

Надійність – середній час безвідмовної роботи (MTBF) для критичних компонентів системи (маршрутизатори, сервери, комутатори) має становити не менше 30 000 годин.

Відмовостійкість – реалізація резервних маршрутів передачі даних, наявність джерел безперебійного живлення (UPS), можливість швидкого відновлення сервісів після аварійних ситуацій.

Затримка передачі даних – не більше 5 мс у межах локальної мережі та до 20 мс між віддаленими вузлами.

Безпека – підтримка міжмережевих екранів, сегментації трафіку (VLAN), систем виявлення вторгнень (IDS), багаторівневого контролю доступу.

Масштабованість – можливість додавання нових вузлів у систему без необхідності суттєвої реконфігурації мережі або зупинки її роботи.

Основне обладнання встановлюється у приміщеннях класу С, тобто з обмеженим доступом, захистом від пилу, вологи та перепадів температури (робочий діапазон: +10 °С … +35 °С).

Частина мережевого обладнання (наприклад, віддалені вузли або IoT-комутатори) може розміщуватись на відкритому повітрі, отже вимагається захист згідно з класом IP65 або вище, робота при температурах від -20 °С до +50 °С, в умовах підвищеної вологості.

У вибухонебезпечних або агресивних середовищах встановлення активного мережевого обладнання не передбачено; для таких зон передбачається прокладання кабелів з відповідною сертифікацією та використання захищених корпусів.

2.3 Додаткові вимоги

2.3.1 Вимоги до налаштувань Системи

Комп’ютерна мережа системи повинна включати п’ять сегментів: LAN1-LAN5. Кількість вузлів у кожному сегменті має становити до 66, 170, 233, 201 і 227 відповідно. Для підмереж передбачено адресний блок: 172.24.IPn.0/21, де IPn дорівнює 128.

Необхідно розробити систему адресації для вузлів мережі відповідно до встановлених вимог.

Для налаштування слід:

− використати блок адрес IPv4;

− виділити адреси з діапазону 10.0.16.0/24 для каналів між маршрутизаторами;

− призначити перші можливі IP-адреси інтерфейсам і підінтерфейсам маршрутизаторів у LAN;

− надати другі можливі IP-адреси комутаторам у LAN;

− визначити IP-адреси серверів за формулою: перший доступний адрес у мережі + 9 + 16;

− використовувати останні доступні IP-адреси для вузлів;

− налаштувати адресацію кінцевих пристроїв у VLAN через DHCP.

Необхідно виконати початкове налаштування мережевих пристроїв, яке включає такі дії:

− присвоїти пристроям імена у форматі: *Moiseenko_тип пристрою_номер пристрою*;

− встановити пароль "*cisco*" для доступу до консолі та vty на всіх пристроях;

− налаштувати пароль "class" для привілейованого режиму;

− зашифрувати всі паролі, що зберігаються у відкритому вигляді;

− розробити банер MOTD для інформаційних повідомлень;

− активувати SSH на всіх лініях vty;

− створити користувача *123211_Moiseenko* із паролем "*admincisco*";

− використовувати ім'я пристрою як доменне ім'я;

− згенерувати RSA-ключ довжиною 1024 біт для захисту даних;

− встановити тактову частоту 128000 на DCE-інтерфейсах маршрутизаторів;

− налаштувати аудит та надсилання повідомлень про початок і завершення процесу *exec* із використанням локальної бази.

2.3.2 Вимоги до структурованої кабельної системи

СКС є основою для побудови надійної, масштабованої та високопродуктивної комп’ютерної мережі компанії. Відповідність СКС сучасним стандартам забезпечує стабільну передачу даних, гнучкість у модернізації та зручність в обслуговуванні системи.

Основні вимоги до СКС включають:

Відповідність міжнародним стандартам: проектування та монтаж СКС повинні відповідати вимогам стандартів ISO/IEC 11801, TIA/EIA-568, EN 50173,

які регламентують типи кабелів, способи прокладання, організацію точок підключення та допустимі рівні електромагнітних перешкод.

Тип середовища передачі: основним типом кабелю є виті пари категорії Cat 6 або Cat 6A для горизонтальної підсистеми, що забезпечує швидкість передачі даних до 1–10 Гбіт/с. Для магістрального з'єднання між розподільними щитами використовується оптоволоконний кабель (типу OM3/OM4), що дозволяє передавати дані на великі відстані з високою пропускною здатністю.

Гнучка топологія: СКС повинна забезпечувати можливість легкого підключення нових робочих місць, серверів, контролерів та інших мережевих пристроїв без необхідності зміни всієї кабельної інфраструктури.

Централізація та зонування: рекомендується організувати кабельну інфраструктуру за допомогою телекомунікаційних шаф (TR) у кожній локальній зоні (LAN), зв'язаних між собою через головний комутаційний вузол (MDF). Це дозволяє локалізувати несправності та спростити адміністрування.

Пожежна безпека та захист: всі компоненти СКС (кабелі, розетки, патч-панелі) повинні мати сертифікати пожежної безпеки, а траси мають бути прокладені у металевих лотках або коробах, особливо у виробничих приміщеннях або шахтах ліфтів. Важливим є дотримання розділення силових та слабкострумових ліній.

Резервування та відмовостійкість: передбачається наявність резервних каналів між критичними вузлами мережі, що дозволяє підтримувати працездатність системи у разі обриву кабелю або виходу з ладу окремого сегмента.

Інвентаризація та маркування: усі кабелі, розетки та порти мають бути чітко промарковані згідно з планом СКС, що дозволяє швидко ідентифікувати з'єднання під час обслуговування чи оновлення мережі.

Урахування зовнішніх умов: при прокладанні кабелів у зоні шахт або відкритих приміщень слід використовувати кабелі у захищеній оболонці (екрановані, з додатковим ізоляційним шаром), які витримують вологість, механічні навантаження та перепади температур.

2.3.3 Вимоги до параметрів мереж енергопостачання Системи

1. Номінальні параметри електромережі: напруга живлення: ~220 В (±10%) для однофазного обладнання, частота: 50 Гц (±1 Гц), коефіцієнт потужності: не менше 0,9 для споживачів ІТ-інфраструктури.

2. Категорія надійності електропостачання: усі критичні компоненти системи (серверне обладнання, комутатори, маршрутизатори, контролери) мають бути підключені до джерела живлення II категорії надійності, що передбачає резервне живлення з двох незалежних джерел або автономного живлення при відмові основного.

3. Безперебійне живлення: для серверного обладнання та ключових вузлів мережі передбачається встановлення джерел безперебійного живлення (UPS) з часом автономної роботи не менше 15–30 хвилин. UPS мають підтримувати функцію автоматичного завершення роботи серверів у разі тривалого відключення живлення. Бажано використання подвійного живлення (redundant power supply) для серверів та комутаторів рівня ядра.

4. Захист електроживлення: усі силові лінії мають бути обладнані пристроями захисту від перенапруги (SPD), а також автоматичними вимикачами відповідного номіналу. У розподільчих шафах передбачено заземлення відповідно до вимог ПУЕ, ізольоване від сигнального заземлення ІТ-обладнання.

5. Енергоспоживання: має бути передбачено попередній розрахунок споживаної потужності кожного сегменту Системи, із запасом не менше 30% від максимальної потужності. Енергоспоживання окремих підсистем має фіксуватися за допомогою інтелектуальних лічильників або вбудованих функцій моніторингу в UPS.

6. Розділення силових та слабкострумових мереж: кабелі живлення мають бути прокладені в окремих лотках або трубах, з відстанню не менше 20 см до мережевих кабелів передачі даних, щоб уникнути електромагнітних перешкод.

7. Умови експлуатації: обладнання встановлюється в опалюваних, вентильованих приміщеннях із температурним режимом +10 °C … +35 °C та вологістю не більше 80%. Для віддалених мережевих вузлів, які розташовані на

відкритому повітрі або в шахтах ліфтів, передбачено герметичні щити з автономними джерелами живлення та відповідним ступенем захисту (IP65).

2.3.4 Вимоги до регламенту обслуговування Системи

Регламент обслуговування охоплює профілактичні, діагностичні, ремонтні та оновлювальні заходи, які повинні здійснюватися регулярно та відповідно до затвердженого графіка.

Основні вимоги до регламенту обслуговування.

Огляд працездатності активного мережевого обладнання (маршрутизатори, комутатори, сервери) – щомісяця.

Перевірка цілісності кабельної інфраструктури, стану з’єднань і маркування – раз на квартал.

Чищення пилу, перевірка вентиляції та температурних режимів у серверних приміщеннях –раз на місяць.

Тестування резервного живлення (UPS, батареї) – раз на квартал.

Повна перевірка усієї мережевої інфраструктури на наявність збоїв та втрат – раз на півроку.

Оновлення прошивок мережевого обладнання та системного ПЗ – відповідно до графіка вендора, але не рідше одного разу на півроку.

Регулярне резервне копіювання критичних даних і конфігурацій – щодня / щотижня відповідно до критичності систем.

Перевірка журналів подій, виявлення підозрілої активності та вторгнень – щотижня.

Аудит безпеки доступу до мережі, облікових записів і паролів – раз на квартал.

Усі дії, пов’язані з обслуговуванням Системи, мають фіксуватись у відповідному журналі технічного обслуговування.

Ведення електронної бази з історією збоїв, обслуговування та модернізації.

Формування звітів про стан системи після кожної профілактики.

За кожен сегмент системи має бути призначена відповідальна особа або підрозділ (мережева інфраструктура, серверне обладнання, клієнтські станції, резервне живлення тощо).

У разі виявлення критичної несправності відповідальні особи зобов’язані вжити заходів щодо її усунення не пізніше ніж за 4 години з моменту виявлення.

Обслуговуючий персонал повинен бути забезпечений необхідними засобами діагностики, тестерами, ноутбуками для підключення до обладнання, комплектами запасних частин.

Критичне обладнання повинно мати гарячі резерви або швидкий доступ до заміни, щоб мінімізувати час відновлення системи.

Обмеження фізичного доступу до серверних кімнат, розподільчих шаф та інших чутливих елементів Системи.

Ведення обліку осіб, які мали доступ до елементів системи з обов’язковою реєстрацією часу входу/виходу.

3. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ

3.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи компанії

При розробці комп’ютерної системи для компанії, що займається монтажем і обслуговуванням ліфтів, ключовим завданням є створення надійної, масштабованої та керованої інфраструктури, яка забезпечує безперервний обмін інформацією між усіма підрозділами підприємства, а також дозволяє здійснювати моніторинг і контроль за об’єктами обслуговування в реальному часі.

З огляду на особливості діяльності компанії, до складу технічного комплексу обрано такі компоненти.

Центральний серверний вузол, розміщений у головному офісі. Він містить сервери файлового обміну, контролери домену, системи віртуалізації, антивірусного захисту та резервного копіювання.

Клієнтські комп’ютери та термінали, встановлені у відділах адміністрації, технічного обліку, складу та інженерної підтримки. Кожен пристрій під’єднаний до внутрішньої мережі через комутатори другого рівня.

Маршрутизатори розподілу (4 одиниці), які забезпечують логічне сегментування мережі за підрозділами компанії, підвищуючи безпеку та зменшуючи трафік між підмережами.

Маршрутизатор із системою виявлення вторгнень (IPS) на межі з Інтернетом для забезпечення кіберзахисту.

Виділена мережа для IoT-підсистем, яка працює окремо в межах VLAN4 на двох керованих комутаторах, для передачі даних з апаратно-програмного комплексу моніторингу ліфтових приміщень.

Віддалений офіс, підключений через VPN через маршрутизатор та три комутатори для повноцінної інтеграції в загальну мережу.

Обрана структурна схема є гібридною, поєднуючи класичну зіркову топологію з сегментованими мережами VLAN та маршрутизованим ядром.

Такий підхід дозволяє:

– оптимізувати трафік між підрозділами;

– підвищити рівень інформаційної безпеки завдяки розмежуванню зон довіри;

– забезпечити масштабованість – у разі розширення організації не виникає потреби в повній реконструкції мережі;

– інтегрувати IoT-рішення без впливу на основну корпоративну мережу;

– надійно під’єднати віддалені офіси, зберігаючи єдину архітектуру системи.

– кожен компонент системи має резервування (двійне живлення, резервні комутатори, RAID-масиви на серверах), що мінімізує ймовірність збоїв та втрати даних.

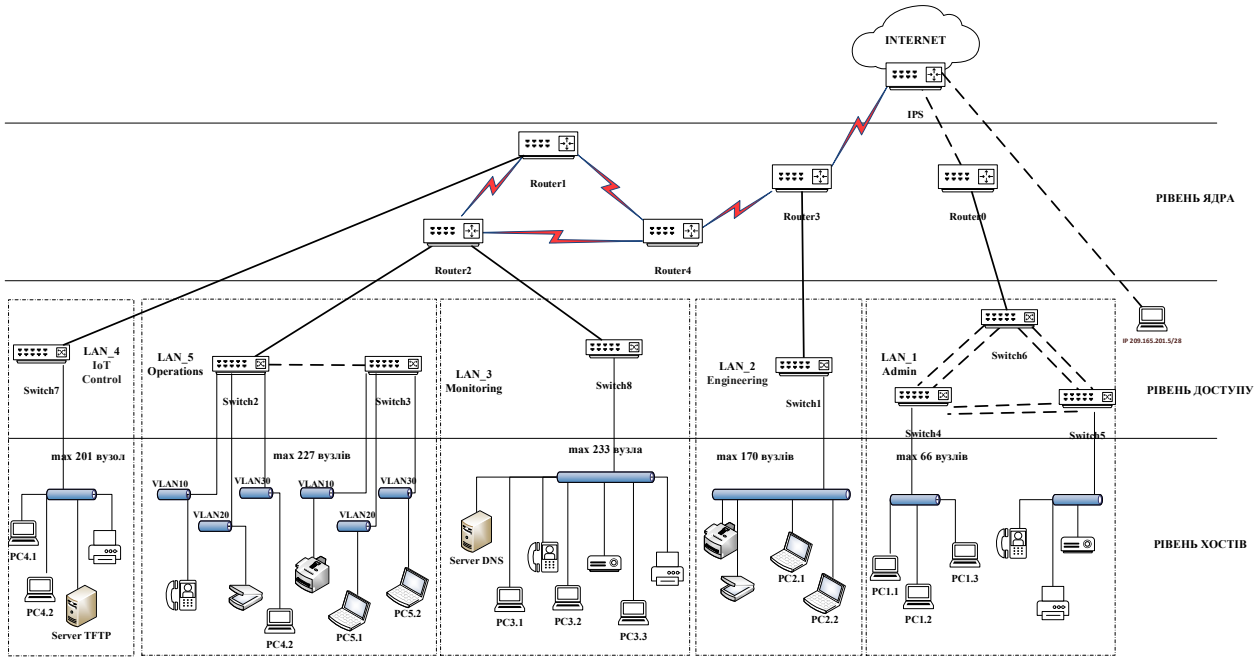

Рисунок 3.1 – Структурна схема комплексу технічних засобів комп’ютерної системи компанії

Структурна схема повністю відповідає потребам компанії, враховує вимоги до безпеки, продуктивності та зручності експлуатації, а також передбачає перспективу розвитку та інтеграції нових технологій.

3.2 Розробка специфікації апаратних засобів комп’ютерної мережі

Для забезпечення стабільної, швидкої та безпечної роботи комп’ютерної мережі компанії необхідно підібрати відповідні апаратні засоби, здатні підтримувати задану топологію, обсяг трафіку та функціональні потреби підприємства.

Основні критерії відбору обладнання:

– підтримка гігабітного Ethernet (10/100/1000 Мбіт/с);

– можливість конфігурування VLAN і підтримка QoS;

– наявність резервування живлення або портів;

– вбудовані засоби безпеки (фільтрація, контроль доступу, IPS);

– простота адміністрування та масштабованість.

Загальна специфікація обраного обладнання представлена у таблиці 3.1.

Таблиця 3.1 – специфікація апаратних засобів

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1.	Маршрутизатори ядра	Cisco ISR 4331 або аналог	од.	4	Підтримка до 100 пристроїв на кожну мережу; шифрування IPsec VPN; підтримка динамічної маршрутизації (OSPF, EIGRP, BGP); Інтерфейси: 3 × GE WAN/LAN, 1 × SFP; можливість віддаленого керування (SSH, SNMP, HTTPS)

Продовження таблиці 3.1

1	2	3	4	5	6
2.	Граничний маршрутизатор з IPS	Cisco Firepower 1010	од.	1	Інтегрована система виявлення та запобігання вторгненням (IPS/IDS); апаратне прискорення фільтрації пакетів; VPN шлюз для віддалених підключень; захист мережевого периметру
3.	Керований комутатор	Cisco Catalyst 2960-X або аналог	од.	8	24 або 48 портів Gigabit Ethernet; підтримка VLAN, STP, RSTP два оптичних uplink-порти SFP; резервування живлення (опціонально); використовуються для LAN-сегментів та VLAN4 з IoT
4.	Комутатори віддаленого офісу	TP-Link JetStream T1600G-28TS або подібні	од.	3	Підтримка L2 функцій та VLAN; увімкнення/вимкнення портів, дзеркалювання; просте адміністрування через веб-інтерфейс
5.	Серверна інфраструктура	HPE ProLiant DL360 Gen10	од.	2	Процесор: Intel Xeon Silver; Оперативна пам’ять: 32–64 ГБ DDR4; СХД: RAID-масив на SSD+HDD; Підтримка віртуалізації, AD DS, файловий сервер, моніторинг
6.	Робочі станції	Dell OptiPlex 7000 або еквівалент	од.	20	Intel Core i5 / i7; 16 ГБ RAM, SSD 512 ГБ; Підключення по Ethernet; ОС: Windows 11 Pro

Закінчення таблиці 3.1

7.	Джерела безперебійного живлення (UPS)	APC Smart-UPS 1500VA	од.	6	Для серверної та маршрутизаторів. Автономність: 15–30 хв; USB / SNMP моніторинг; Можливість автоматичного вимкнення обладнання

Розглянемо варіанти кабельної системи для офісу «Служби інформаційних технологій». Для цього визначимо розташування вузлів комп'ютерної мережі та створимо схему прокладання кабелів. У результаті отримаємо план, представлений на рисунку 3.2.

Згідно зі схемою, передбачено чотири основні кабельні гілки:

– кабель, що забезпечує з'єднання з провайдером;

– кабель для підключення комутатора до маршрутизатора;

– два кабелі, призначені для підключення оргтехніки;

– п’ять кабелів для з'єднання ПК та серверу.

Літерою «К» позначено місце розташування комутаційної коробки для кабелю живлення.

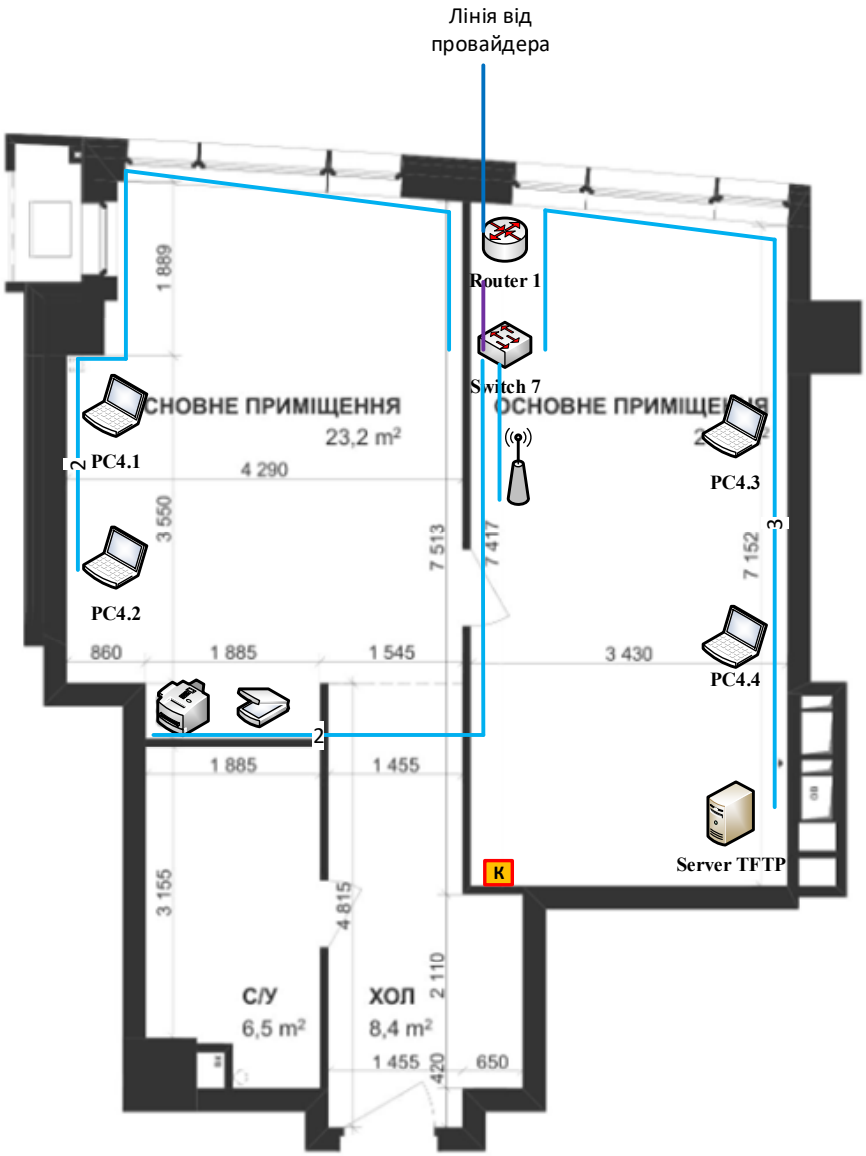

Рисунок 3.2 – Схема розташування кабельних трас офісу «Служби інформаційних технологій»

Враховуючи розташування вузлів, кількість кабелів у кожній гілці та геометричні параметри приміщення, формується специфікація (див. таблицю 3.2).

Таблиця 3.2 – Специфікація СКС

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1.	Вита пара КПВ-ВП (350) 4х2х0,51 U/UTP-cat.5E	Одескабель	м	70	
2.	Кабельканал LHD 40х20	KOPOS	м	34	Організація укладки UTP проводу
3.	Розетка подвійна комп'ютерна Asfora, RJ45	Schneider Electric	од.	7	
4.	Кабельканал LHD 40х20	KOPOS	м	38	Організація укладки кабелю живлення
5.	Розетка подвійна із заземленням Deriy 16 А 250 В без шторок	Lezard	од.	7	
6.	Кабель силовий ПВС 3*0,75	Одескабель	м	97	
7.	Зовнішня розподільна коробка і12 (85х85х37) (sp33291201) IP55	Spelsberg	од.	1	
8.	Патч-панель 24xRJ-45 19" 1U 24 порти CAT6 UTP (P6024)	Atcom	од.	1	
9.	Серверна шафа 4U, 600х350х284 скло	EServer	од.	1	

3.3 Розробка моделі та налаштувань корпоративної мережі

3.3.1 Розрахунок схеми адресації корпоративної мережі

Корпоративна комп’ютерна мережа компанії складається з п’яти логічно ізольованих підмереж (LAN_1…LAN_5), що взаємодіють через рівень маршрутизаторів. LAN_4 додатково розподілена на декілька віртуальних локальних мереж (VLAN), що забезпечує сегментацію трафіку за ролями або

службами. Зовнішнє з'єднання виконується через маршрутизатор з вбудованим IPS-модулем.

Уся адресація базується на приватному IP-просторі IPv4 з класу 172.24.128.0/21, що дозволяє гнучко розподіляти підмережі:

– базова адреса: 10.0.0.0/8

– маска: /24 для звичайних LAN, /30 – для точка-точка каналів.

Таблиця 3.3 – Блок адрес мережі та кількість вузлів в кожній з підмереж

№	Блок адрес	LAN_1	LAN_2	LAN_3	LAN_4	LAN_5
16	172.24.128.0/21	66	170	233	201	227

Для розподілу мережі компанії відповідно до організаційних підрозділів слід враховувати принципи функціонального або структурного поділу підмереж:

LAN_1 – Admin, адміністрація, бухгалтерія;

LAN_2 – Engineering, технічний відділ;

LAN_3 – Monitoring, Відеоспостереження, SCADA;

LAN_4 – IoT Control, Обладнання контролю приміщень;

LAN_5 – Operations, Офісні працівники, VLAN-и.

Схема адресації підмереж у таблиці 3.3 розроблена з урахуванням кількості вузлів у кожному сегменті. Для підмереж із понад 170 пристроями (LAN_2 – LAN_5) обрано маску /24 (254 IP-адреси), для LAN_1 з 66 вузлами – маску /25 (126 адрес), що дозволяє оптимізувати використання адресного простору.

Використано діапазон приватних IP-адрес класу B (172.24.0.0/21), що забезпечує достатній резерв для масштабування. Адресація структурована логічно, з розділенням мереж за призначенням. Передбачено резерв для майбутнього розширення, що гарантує гнучкість та надійність корпоративної мережі.

Таблиця 3.4 – Схема адресації підмереж підприємства

Назва мережі	Необхідна кількість вузлів	Виділена кількість вузлів	Адреса підмережі	Префікс	Діапазон допустимих IP-адрес вузлів
1	**2**	**3**	**4**	**5**	**6**
LAN_3	233	254	172.24.128.0 255.255.255.0	/24	172.24.128.1 - 172.24.128.254
LAN_5	227	254	172.24.129.0 255.255.255.0	/24	172.24.129.1 - 172.24.129.254
LAN_4	201	254	172.24.130.0 255.255.255.0	/24	172.24.130.1 - 172.24.130.254
LAN_2	170	254	172.24.131.0 255.255.255.0	/24	172.24.131.1 - 172.24.131.254
LAN_1	66	126	172.24.132.0 255.255.255.128	/25	172.24.132.1 - 172.24.132.126

Адресація VLAN-сегментів у межах LAN_5 виконана з урахуванням кількості вузлів у кожній логічній групі, що дозволило ефективно розподілити підмережу 172.24.129.0/21 без втрати IP-простору.

Для VLAN Subscriber, Office_Meneg та Executive, де потрібно до 62 хостів, обрано маску /26 (255.255.255.192), яка надає по 62 адреси в кожному сегменті. Це оптимальне рішення, що забезпечує необхідну кількість IP і залишає резерв для розширення.

VLAN Managment потребує лише 14 адрес, тому використано маску /28 (255.255.255.240), яка забезпечує до 14 доступних IP – цього достатньо для адміністративних пристроїв та службових вузлів.

Уся підмережа LAN_5 (172.24.129.0/24) розбита на чотири логічні VLAN із чітко визначеними межами адрес, що спрощує маршрутизацію, покращує безпеку та дозволяє гнучке управління трафіком між сегментами. Такий підхід відповідає принципам структурованої адресації у VLAN - мережах.

Таблиця 3.5 – Схема адресації мереж VLAN підмережі LAN_5

Назва	Розмір	Адреса	Префікс мережі	Діапазон адрес
1	**2**	**3**	**4**	**5**
Subscriber	62	172.24.129.0 255.255.255.192	/26	172.24.129.1 - 172.24.129.62

Закінчення таблиці 3.5

1	2	3	4	5
Office_Meneg	62	172.24.129.64 255.255.255.192	/26	172.24.129.65 - 172.24.129.126
Executive	62	172.24.129.128 255.255.255.192	/26	172.24.129.129 - 172.24.129.190
Managment	14	172.24.129.192 255.255.255.240	/28	172.24.129.193 - 172.24.129.206

Адресація каналів зв’язку між маршрутизаторами реалізована на основі використання підмереж з префіксом /30 (255.255.255.252), що є стандартним і доцільним підходом для точка-точка (point-to-point) з’єднань.

Кожна з підмереж WAN_1 – WAN_4 включає лише дві корисні IP-адреси (наприклад, 10.0.16.1 і 10.0.16.2), що ідеально підходить для зв'язку між двома маршрутизаторами, не витрачаючи зайві IP-адреси. Це дозволяє:

–зменшити споживання IP-простору;

–упорядкувати логіку адресації;

–полегшити супровід і виявлення несправностей.

Обрана адресна область 10.0.16.0/24 дозволяє створити до 8 таких підмереж, із яких у таблиці задіяно чотири – цього достатньо для побудови чотирьох фізичних або логічних каналів зв’язку між маршрутизаторами ядра та периферійними вузлами.

Загалом, реалізація забезпечує ефективне використання адрес, підтримку масштабованості та спрощення конфігурації маршрутизації.

Таблиця 3.6 – Схема адресації каналів між маршрутизаторами

Назва підмережі	Адреса підмережі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса
WAN_1	10.0.16.0	/30	10.0.16.1-10.0.16.2	10.0.16.3
WAN_2	10.0.16.4	/30	10.0.16.5-10.0.16.6	10.0.16.7
WAN_3	10.0.16.8	/30	10.0.16.9-10.0.16.10	10.0.16.11
WAN_4	10.0.16.12	/30	10.0.16.13-10.0.16.14	10.0.16.15

При розробці детальної й структурованої адресації інтерфейсів усіх маршрутизаторів було використано Gigabit Ethernet-інтерфейси для з'єднання маршрутизаторів із внутрішніми сегментами мережі (LAN), обираючи маски відповідно до потреб кожного сегмента, що дозволяє максимально ефективно використовувати IP-адреси без перевитрати.

Для організації WAN-з’єднань між маршрутизаторами застосовано підмережі з префіксом /30, оскільки вони ідеально підходять для з’єднань типу "точка-точка" (тільки дві корисні адреси на підмережу).

Прив’язка адрес до топології дозволила спростити подальшу маршрутизацію та управління, оскільки легко ідентифікувати кожен пристрій за IP-адресою та інтерфейсом.

Враховано і взаємодію з провайдером через публічні IP-адреси та резервне з'єднання через зовнішній маршрутизатор, що забезпечує стійкість до відмов.

Також у схемі реалізовано підтримку VLAN (напр., у LAN_5), що передбачає налаштування SVI-інтерфейсів, і їхні адреси були закладені відповідно до раніше спроєктованої адресної структури VLAN-сегментів.

Ця таблиця є базою для побудови всієї маршрутизованої інфраструктури мережі, дозволяючи коректно налаштувати маршрути, реалізувати безпечний доступ між сегментами та інтеграцію з зовнішніми мережами. Це підвищує масштабованість та керованість системи.

Таблиця 3.7 – Схема адресації маршрутизаторів КС КМІ

Пристрій	Інтерфейс	IP-адрес	Маска мережі	Префікс
1	**2**	**3**	**4**	**5**
Moiseenko_R1	Gig0/1	172.24.130.1	255.255.255.0	/24
	Serial0/0/1	10.0.16.5	255.255.255.252	/30
	Serial0/1/0	10.0.16.1	255.255.255.252	/30
Moiseenko_R2	Gig0/1	172.24.129.193	255.255.255.240	/28
	Gig0/2	172.24.128.1	255.255.255.0	/24
	Serial0/1/0	10.0.16.2	255.255.255.252	/30
	Serial0/1/1	10.0.16.9	255.255.255.252	/30

Закінчення таблиці 3.7

1	2	3	4	5
Moiseenko_R3	Serial0/1/0	10.0.16.14	255.255.255.252	/30
	Serial0/0/0	209.165.202.2	255.255.255.252	/30
	Serial0/0/1	10.0.16.6	255.255.255.252	/30
	Gig0/1	172.24.131.1	255.255.255.224	/27
Moiseenko_R4	Serial0/1/0	10.0.16.13	255.255.255.252	/30
	Serial0/1/1	10.0.16.10	255.255.255.252	/30
Moiseenko_R0	Gig0/2	172.24.132.1	255.255.255.128	/25
	Gig0/1	64.100.13.1	255.255.255.252	/30
Rout_ISP	Serial0/0/0	209.165.202.2	255.255.255.252	/30
	Gig0/0	209.165.201.1	255.255.255.252	/28
	Gig0/1	64.100.13.2	255.255.255.252	/30

Адреси SVI-інтерфейсів комутаторів налаштовано відповідно до схеми сегментації мережі КС КМІ.

Під час розробки схеми адресації SVI-інтерфейсів комутаторів потрібно було забезпечити логічну й узгоджену IP-структуру для керованих комутаторів, які обслуговують відповідні підмережі. SVI (Switched Virtual Interface) використовується для віртуального інтерфейсу VLAN на 3-рівневих комутаторах і дає змогу здійснювати маршрутизацію між VLAN або керування мережею.

Адреси SVI-інтерфейсів були підібрані так, щоб залишити перші кілька IP-адрес у кожній підмережі для комутаційної інфраструктури, забезпечуючи легке адміністрування й уніфікацію. У кожній підмережі адреса шлюзу (вказана в колонці) відповідає IP-адресі на маршрутизаторі, що обслуговує цю підмережу.

У LAN_1, яка використовує маску /25, передбачено три окремі комутатори з унікальними адресами. Це дозволяє мати кілька керованих точок у межах однієї логічної підмережі. Усі вони використовують один шлюз – 172.24.132.1.

У LAN_2, LAN_3 і LAN_4 використані стандартні маски /24, що забезпечує достатній обсяг адрес для поточних і майбутніх потреб. Комутатори мають чітко виділену адресу, а шлюзи відповідають маршрутизаторам згідно з таблицею маршрутизаторів.

Для LAN_5, де реалізовано сегментацію через VLAN, призначено окремі комутатори з адресами в межах підмережі /28 – це дає змогу розмежовувати підрозділи, а IP-адреси узгоджені з таблицею VLAN-мереж.

Уніфікація нумерації комутаторів (наприклад, Sw1.1, Sw5.2) відображає їхнє розташування в структурі, полегшує адміністрування та дозволяє швидко локалізувати проблеми.

Схема забезпечує ефективне керування, логічну адресацію і зручність розгортання VLAN, а також узгоджується з маршрутизованою інфраструктурою підприємства, описаною в попередніх таблицях.

Таблиця 3.8 – Схема адресації SVI-інтерфейсів комутаторів

Підмережа	Пристрій	IP-адрес	Маска мережі	Адреса шлюзу
LAN_1	Moiseenko_Sw1.1	172.24.132.2	255.255.255.128	172.24.132.1
	Moiseenko_Sw1.2	172.24.132.3	255.255.255.128	172.24.132.1
	Moiseenko_Sw1.3	172.24.132.4	255.255.255.128	172.24.132.1
LAN_2	Moiseenko_Sw2	172.24.131.2	255.255.255.0	172.24.131.1
LAN_3	Moiseenko_Sw3	172.24.128.2	255.255.255.0	172.24.128.1
LAN_4	Moiseenko_Sw4	172.24.129.2	255.255.255.0	172.24.130.1
LAN_5	Moiseenko_Sw5.1	172.24.129.194	255.255.255.240	172.24.129.193
	Moiseenko_Sw5.2	172.24.129.195	255.255.255.240	172.24.129.193
	Moiseenko_Sw5.3	172.24.129.195	255.255.255.240	172.24.129.193

Топологічна схема корпоративної мережі була розроблена на основі таблиць адресації й відображає логічну та фізичну структуру системи. Вона побудована за ієрархічним принципом: ядро, дистрибуція та доступ. Усі LAN-сегменти мають власні підмережі, маршрутизатори й комутатори з призначеними IP-адресами (відповідно до таблиць 3.3–3.8).

У VLAN-сегменті LAN_5 реалізовано логічне розділення трафіку за функціональними групами. Міжмаршрутизаторні з’єднання виконані через /30-

мережі, забезпечуючи ефективне використання адресного простору. Вихід до зовнішньої мережі реалізовано через маршрутизатор ISP. Схема є узгодженою, масштабованою й готовою до моделювання в середовищі Packet Tracer.

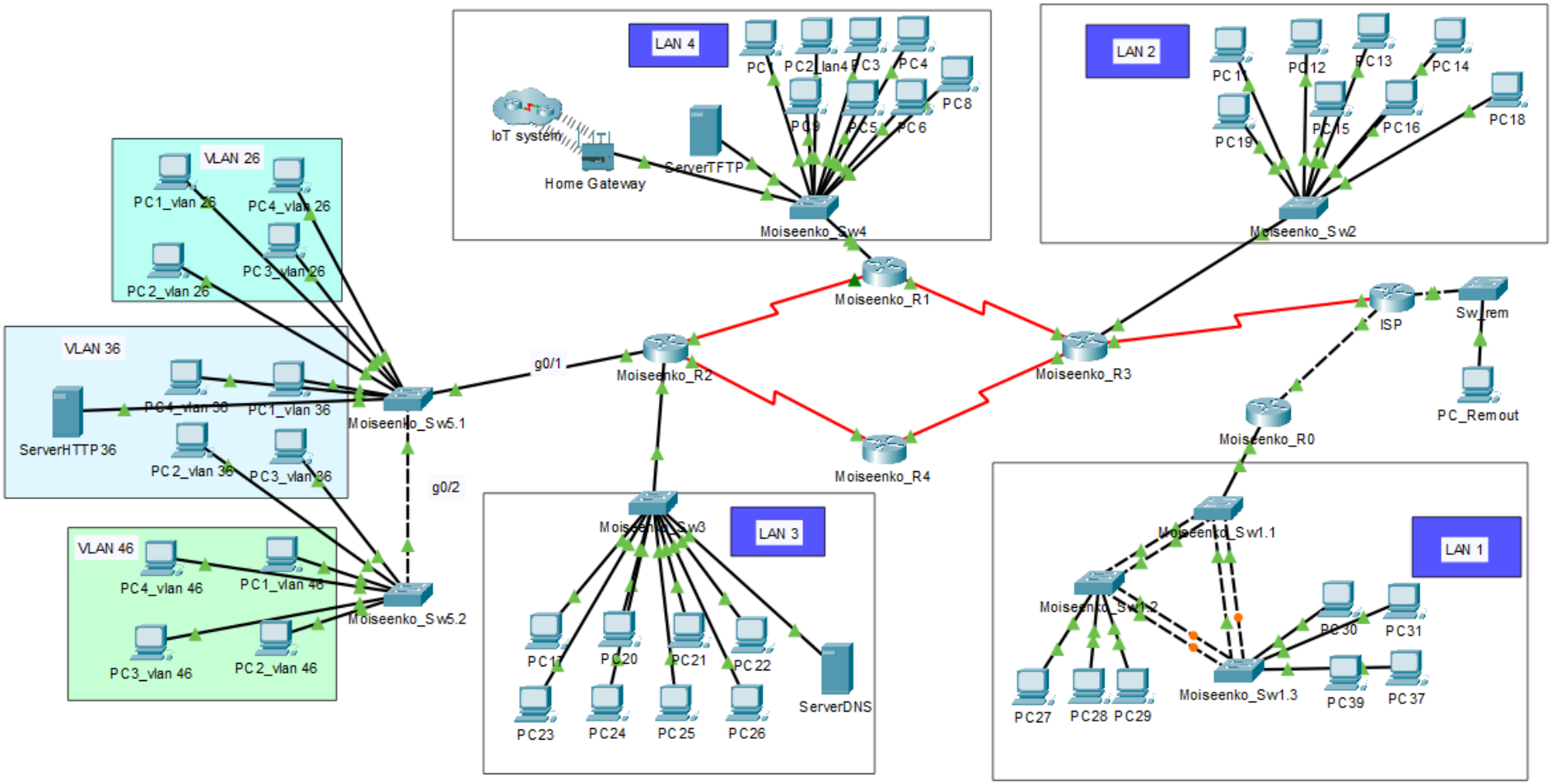

Рисунок 3.3 – Топологічна схема корпоративної мережі КМІ

3.3.2 Налаштування моделі комп’ютерної мережі

3.3.2.1 Налаштування маршрутизаторів

Розглянемо ключові етапи налаштування маршрутизаторів корпоративної мережі, зокрема базове налаштування маршрутизатора Moiseenko_R1, конфігурація інтерфейсів, запуск протоколу маршрутизації EIGRP, а також налаштування та перевірка служби DHCP на інших маршрутизаторах.

На маршрутизаторі Moiseenko_R1 було здійснено стандартне початкове налаштування: встановлення імені пристрою, паролів доступу, увімкнення інтерфейсів та призначення IP-адрес. Команди базового налаштування:

```
Router(config)#hostname Moiseenko_R1
Moiseenko_R1(config)#no ip domain-lookup
Moiseenko_R1(config)#service password-encryption
Moiseenko_R1(config)#enable secret cisco
Moiseenko_R1(config)#line console 0
Moiseenko_R1(config-line)#password cisco
Moiseenko_R1(config-line)#login
Moiseenko_R1(config-line)#exit
Moiseenko_R1(config)#line vty 0 15
Moiseenko_R1(config-line)#password cisco
Moiseenko_R1(config-line)#login
Moiseenko_R1(config-line)#trans inp ssh
Moiseenko_R1(config-line)#exit
Moiseenko_R1(config)#banner motd #123-21-1 Moiseenko. authorized users only#
Moiseenko_R1(config)#username 12321Mois password cisco
Moiseenko_R1(config)#ip domain-name Moiseenko_R1.com
Moiseenko_R1(config)#cryp key g r
The name for the keys will be: Moiseenko_R1.Moiseenko_R1.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Рисунок 3.4 – Базове налаштування маршрутизатора Moiseenko_R1

Інтерфейс Serial0/1/0 маршрутизатора Moiseenko_R1 використовується для зв’язку з маршрутизатором Moiseenko_R2. Налаштування:

```
Moiseenko_R1(config)#int s0/0/1
Moiseenko_R1(config-if)#description WAN2
Moiseenko_R1(config-if)#ip add 10.0.16.5 255.255.255.252
Moiseenko_R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Moiseenko_R1(config-if)#clock rate 128000
Moiseenko_R1(config-if)#bandwidth 128
Moiseenko_R1(config-if)#exit
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

Рисунок 3.5 – Налаштування послідовного інтерфейсу

На маршрутизаторі Moiseenko_R1 реалізовано динамічну маршрутизацію за допомогою EIGRP (номер автономної системи – 100). Усі необхідні мережі додаються вручну:

```
Moiseenko_R2(config)#router eigrp 16
Moiseenko_R2(config-router)#redistribute static
Moiseenko_R2(config-router)#network 10.0.16.8 0.0.0.3
Moiseenko_R2(config-router)#network 10.0.16.0 0.0.0.3
Moiseenko_R2(config-router)#network 172.24.129.0 0.0.0.63
Moiseenko_R2(config-router)#network 172.24.129.64 0.0.0.63
Moiseenko_R2(config-router)#network 172.24.129.128 0.0.0.63
Moiseenko_R2(config-router)#network 172.24.129.192 0.0.0.15
Moiseenko_R2(config-router)#network 172.24.128.0 0.0.0.255
Moiseenko_R2(config-router)#pas g0/1.26
Moiseenko_R2(config-router)#pas g0/1.36
Moiseenko_R2(config-router)#pas g0/1.46
Moiseenko_R2(config-router)#pas g0/1.99
Moiseenko_R2(config-router)#exit
Moiseenko_R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
```

Рисунок 3.6 – Налаштування протоколу маршрутизації EIGRP

```
Moiseenko_R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D       10.0.16.0/30 [90/21024000] via 10.0.16.5, 00:12:58, Serial0/0/1
C       10.0.16.4/30 is directly connected, Serial0/0/1
L       10.0.16.6/32 is directly connected, Serial0/0/1
D       10.0.16.8/30 [90/21024000] via 10.0.16.13, 00:12:53, Serial0/1/0
C       10.0.16.12/30 is directly connected, Serial0/1/0
L       10.0.16.14/32 is directly connected, Serial0/1/0
     172.24.0.0/16 is variably subnetted, 8 subnets, 4 masks
D       172.24.128.0/24 [90/21024256] via 10.0.16.5, 00:12:58, Serial0/0/1
                        [90/21024256] via 10.0.16.13, 00:12:53, Serial0/1/0
D       172.24.129.0/26 [90/21026560] via 10.0.16.5, 00:12:58, Serial0/0/1
                        [90/21026560] via 10.0.16.13, 00:12:53, Serial0/1/0
D       172.24.129.64/26 [90/21026560] via 10.0.16.5, 00:12:58, Serial0/0/1
                         [90/21026560] via 10.0.16.13, 00:12:53, Serial0/1/0
D       172.24.129.128/26 [90/21026560] via 10.0.16.5, 00:12:58, Serial0/0/1
                          [90/21026560] via 10.0.16.13, 00:12:53, Serial0/1/0
D       172.24.129.192/28 [90/21026560] via 10.0.16.5, 00:12:58, Serial0/0/1
                          [90/21026560] via 10.0.16.13, 00:12:53, Serial0/1/0
D       172.24.130.0/24 [90/20512256] via 10.0.16.5, 00:12:58, Serial0/0/1
C       172.24.131.0/24 is directly connected, GigabitEthernet0/1
L       172.24.131.1/32 is directly connected, GigabitEthernet0/1
```

Рисунок 3.7 – Приклад таблиці маршрутизації на Moiseenko_R3

Після завершення налаштувань здійснено перевірку доступності мережевих вузлів за допомогою команди *ping*.

Successful	PC1_vlan 36	PC11	ICMP	
Successful	PC1_vlan 26	PC1	ICMP	
Successful	PC11	PC1	ICMP	
Successful	PC12	ServerTFTP	ICMP	
Successful	ServerTFTP	ServerDNS	ICMP	

Рисунок 3.8 – Пінгування хостів в різних підмережах

DHCP-сервер реалізований на маршрутизаторі Moiseenko_R2 для автоматичної видачі IP-адрес підмережі VLAN_36:

```
Moiseenko_R2(config)#ip dhc ex 172.24.129.1 172.24.129.10
Moiseenko_R2(config)#ip dhc ex 172.24.129.65 172.24.129.75
Moiseenko_R2(config)#ip dhc ex 172.24.129.129 172.24.129.139
Moiseenko_R2(config)#ip dhc pool POOL_VLAN26
Moiseenko_R2(dhcp-config)#net 172.24.129.0 255.255.255.192
Moiseenko_R2(dhcp-config)#def 172.24.129.1
Moiseenko_R2(dhcp-config)#dns 172.24.128.10
Moiseenko_R2(dhcp-config)#ip dhc pool POOL_VLAN36
Moiseenko_R2(dhcp-config)#net 172.24.129.64 255.255.255.192
Moiseenko_R2(dhcp-config)#def 172.24.129.65
Moiseenko_R2(dhcp-config)#dns 172.24.128.10
Moiseenko_R2(dhcp-config)#ip dhc pool POOL_VLAN46
Moiseenko_R2(dhcp-config)#net 172.24.129.128 255.255.255.192
Moiseenko_R2(dhcp-config)#def 172.24.129.129
Moiseenko_R2(dhcp-config)#dns 172.24.128.10
Moiseenko_R2(dhcp-config)#ex
```

Рисунок 3.9 – Налаштування DHCP на маршрутизаторі Moiseenko_R2

На маршрутизаторі Moiseenko_R4, підключеному до VLAN_36, перевірено отримання IP-адреси через DHCP.

Перевірка результату здійснювалась з застосуванням команди *show ip dhcp binding.*

```
Moiseenko_R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.24.129.11    0050.0FEB.316A           --                     Automatic
172.24.129.12    00D0.D325.8A20           --                     Automatic
172.24.129.13    0001.9761.159A           --                     Automatic
172.24.129.14    0002.4A15.3A15           --                     Automatic
172.24.129.76    00D0.FF6D.E865           --                     Automatic
172.24.129.77    00D0.5801.7D40           --                     Automatic
172.24.129.78    000C.CF11.611D           --                     Automatic
172.24.129.79    0001.42A5.6127           --                     Automatic
172.24.129.80    00D0.589A.925B           --                     Automatic
172.24.129.140   000A.F32D.CC0B           --                     Automatic
172.24.129.141   000A.F386.C433           --                     Automatic
```

Рисунок 3.10 – Результат застосування DHCP на Moiseenko_R4

Для підтримки технології DHCP також відповідним чином повинен бути налаштований хост даної мережі.

На клієнтському ПК, що входить до VLAN_36, також успішно спрацювало динамічне отримання IP-адреси:

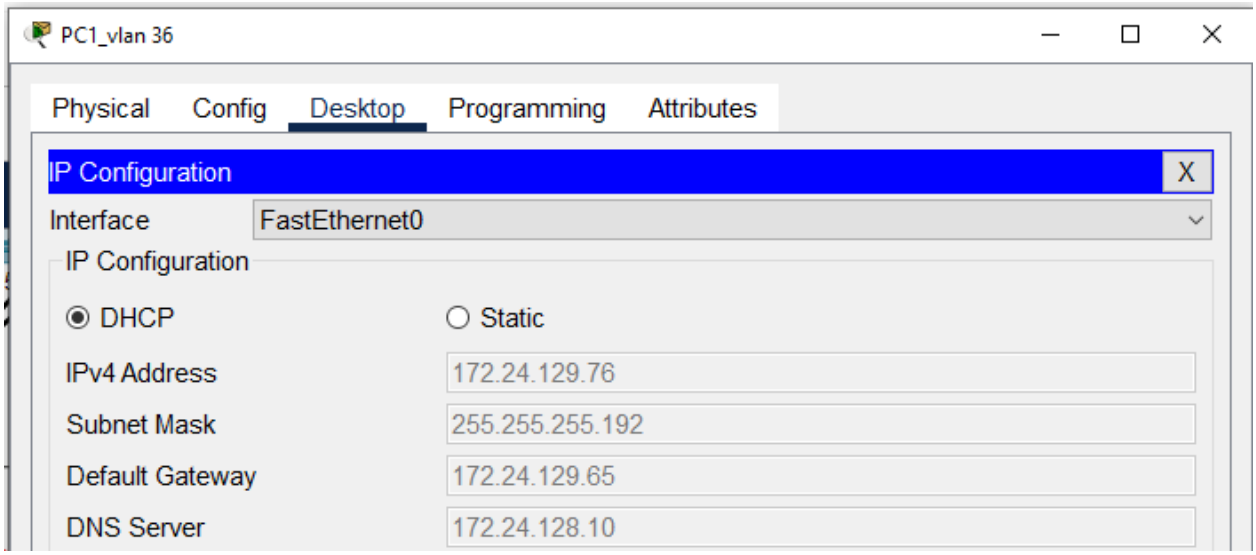

Рисунок 3.11 – Результат застосування DHCP на ПК PC1_vlan36

Виконаємо логічну сегментацію мережі на основі VLAN, що забезпечує розмежування трафіку між різними функціональними зонами корпоративної мережі. Така сегментація дозволяє підвищити безпеку, ефективність та керованість інфраструктури, як показано в таблиці 3.8.

VLAN 1 (Default) – зарезервована за замовчуванням на більшості комутаторів. Поточна підмережа не використовується для передачі даних, щоб уникнути потенційних конфліктів і зловживань.

VLAN 24 (Service area) – виділена для обслуговування клієнтів. Це дозволяє ізолювати касові системи та робочі термінали від решти мережі, мінімізуючи ризики витоку даних чи впливу атак.

VLAN 34 (Office) – призначена для адміністративного персоналу. Такий розподіл дозволяє організувати доступ до відповідних серверів, принтерів та офісної інфраструктури, не змішуючи її з іншими сегментами.

VLAN 44 (Cameras) – використовується для IP-камер. Відокремлення відеоспостереження від основної мережі дозволяє гарантувати стабільну пропускну здатність і захист відеопотоків.

VLAN 99 (Managment) – керівна VLAN, через яку здійснюється адміністрування мережевих пристроїв. Це стандартна практика, що підвищує

безпеку мережі, дозволяючи контролювати доступ до комутаторів і маршрутизаторів.

VLAN 100 (Native) – вказана як "власна мережа", тобто VLAN, що використовується як native VLAN на транкових портах. Це необхідно для коректної передачі нетегованих кадрів у змішаному середовищі.

Таблиця 3.9 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
1	Default	Не використовується
24	Service area	Для зони обслуговування
34	Office	Для адміністрації крамниці
44	Cameras	Для IP-камер
99	Managment	Для управління пристроями
100	Native	Власна мережі

```
Moiseenko_Sw5.1(config)#vlan 26
*Mar 1 2:0:37.418: %SSH-5-ENABLED: SSH 1.99 has been enabled
Moiseenko_Sw5.1(config-vlan)#name Subscriber
Moiseenko_Sw5.1(config-vlan)#vlan 36
Moiseenko_Sw5.1(config-vlan)#name ffice_Meneg
Moiseenko_Sw5.1(config-vlan)#vlan 46
Moiseenko_Sw5.1(config-vlan)#name Executive
Moiseenko_Sw5.1(config-vlan)#vlan 99
Moiseenko_Sw5.1(config-vlan)#name Management
Moiseenko_Sw5.1(config-vlan)#vlan 100
Moiseenko_Sw5.1(config-vlan)#name Native
Moiseenko_Sw5.1(config-vlan)#exit
```

Рисунок 3.12 – Номери та назви мереж VLAN

Налаштування фізичних портів комутатора для відповідних VLAN-мереж є критично важливим етапом при налаштуванні комутаційного обладнання в корпоративній мережі.

Прив’язка портів до VLAN реалізує фізичну сегментацію мережевих пристроїв відповідно до їх ролі в організаційній структурі. Такий підхід забезпечує логічну ізоляцію трафіку, зменшуючи ризики несанкціонованого доступу та підвищуючи продуктивність.

Таблиця 3.10 – Розподіл портів для окремих мереж VLAN

Назва	VLAN	Порти
Subscriber	26	f0/10-f0/14
Office_Menag	36	f0/4-f0/8
Executive	46	f0/15-f0/20

VLAN 26 (Subscriber) – виділені порти f0/10–f0/14, що можуть обслуговувати термінали самообслуговування, пристрої клієнтської зони або POS-системи. Вони фізично відокремлені від офісної і керівної частини мережі.

VLAN 36 (Office_Menag) – порти f0/4–f0/8 призначені для офісного персоналу або керівників середньої ланки. Це дозволяє реалізувати доступ до адміністративних ресурсів без конфлікту з іншими потоками даних.

VLAN 46 (Executive) – порти f0/15–f0/20 зарезервовані для вищого керівництва або критично важливих вузлів мережі. Це дозволяє забезпечити для них підвищений рівень контролю та безпеки.

Адресація пристроїв в підмережі зони обслуговування представлена в таблиці 3.11.

Таблиця 3.11 – Адресація пристроїв в підмережі крамниці 1 КС КМІ

Пристрій	Інтерфейс	Адреса	Маска мережі	Шлюз	VLAN
Moiseenko_Sw5	SVI	172.24.129.194	255.255.255.240	172.24.129.193	99
Moiseenko_Sw5	SVI	172.24.129.195	255.255.255.240	172.24.129.193	99
Moiseenko_R2	G0/0.26	172.24.129.1	255.255.255.192	-	26
	G0/0.36	172.24.129.65	255.255.255.192	-	36
	G0/0.46	172.24.129.129	255.255.255.192	-	46
	G0/0.99	172.24.129.193	255.255.255.240	-	99

У корпоративній мережі компанії реалізовано маршрутизування між VLAN за допомогою технології "router-on-a-stick", де один фізичний інтерфейс GigabitEthernet 0/1 маршрутизатора Moiseenko_R2 поділений на чотири логічні підінтерфейси відповідно до кількості VLAN у підмережі LAN_5. Кожному

підінтерфейсу призначено окрему IP-адресу згідно з таблицею 3.11, а для передачі VLAN-трафіку використано інкапсуляцію 802.1Q.

```
Moiseenko_R2(config-if)#int g0/1.26
Moiseenko_R2(config-subif)#enc d 26
Moiseenko_R2(config-subif)#ip add 172.24.129.1 255.255.255.192
Moiseenko_R2(config-subif)#no shut
Moiseenko_R2(config-subif)#exit
Moiseenko_R2(config)#int g0/1.36
Moiseenko_R2(config-subif)#enc d 36
Moiseenko_R2(config-subif)#ip add 172.24.129.65 255.255.255.192
Moiseenko_R2(config-subif)#no shut
Moiseenko_R2(config-subif)#exit
Moiseenko_R2(config)#int g0/1.46
Moiseenko_R2(config-subif)#enc d 46
Moiseenko_R2(config-subif)#ip add 172.24.129.129 255.255.255.192
Moiseenko_R2(config-subif)#no shut
Moiseenko_R2(config-subif)#exit
Moiseenko_R2(config)#int g0/1.99
Moiseenko_R2(config-subif)#enc d 99
Moiseenko_R2(config-subif)#ip add 172.24.129.193 255.255.255.240
Moiseenko_R2(config-subif)#no shut
Moiseenko_R2(config-subif)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

Рисунок 3.13 – Налаштування протоколу 802.1Q trunking

Фізичний інтерфейс G0/1 не отримує IP-адресу напряму, а використовується як базовий для створення підінтерфейсів.

Кожен підінтерфейс, наприклад G0/1.26, G0/1.36, G0/1.46, G0/1.99, відповідає певній VLAN.

На кожному підінтерфейсі використано команду: *enc d <номер VLAN>*, що дозволяє визначити трафік відповідної VLAN.

Також кожному підінтерфейсу присвоєно IP-адресу шлюзу для відповідної VLAN, яка використовується кінцевими пристроями як шлюз за замовчуванням.

Результат перевірки налаштування 802.1Q наведено на рисунку 3.14.

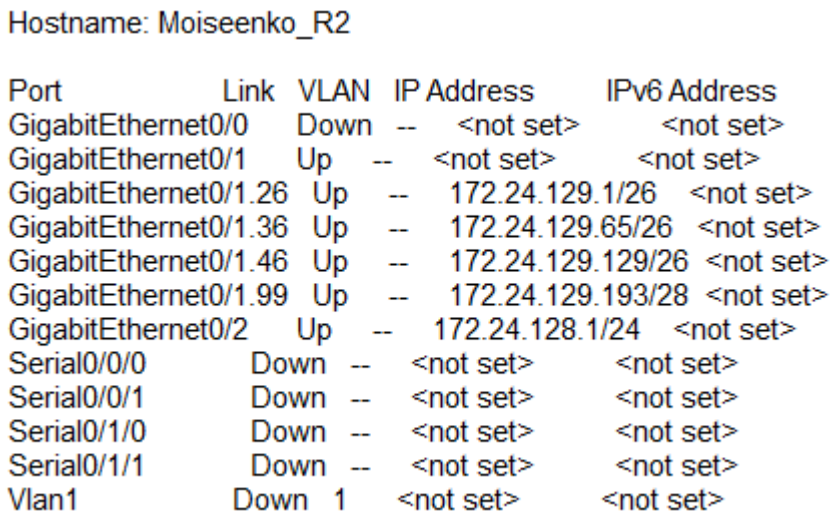

Рисунок 3.14 – Результат перевірки налаштування 802.1Q

3.3.2.2 Налаштування комутаторів

У процесі конфігурації комутатора Moiseenko_Sw4.1 було виконано базове налаштування віртуальних локальних мереж (VLAN), з метою логічного розділення трафіку між підрозділами підприємства в підмережі LAN_4.

Створення VLAN здійснюється за допомогою команди *vlan [ідентифікатор VLAN]*, яка ініціює створення нової віртуальної локальної мережі. Ідентифікатор VLAN має бути числом у діапазоні від 1 до 4094. Для зручності в адмініструванні можна задати мережі описову назву за допомогою команди *name [назва VLAN]*.

Призначення портів до VLAN виконується шляхом налаштування відповідного інтерфейсу комутатора для роботи з обраною VLAN. Для цього використовується команда *switchport mode access*, яка встановлює порт у режим доступу, та команда *switchport access vlan [ідентифікатор VLAN]*, що прив’язує порт до конкретної VLAN. У режимі доступу порт обробляє трафік лише однієї VLAN.

```
Moiseenko_Sw5.2(config-if-range)#int r f0/10-14
Moiseenko_Sw5.2(config-if-range)#switchport mode access
Moiseenko_Sw5.2(config-if-range)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to down
Moiseenko_Sw5.2(config-if-range)#switchport access vlan 26
```

Рисунок 3.15 – Призначення портів VLAN

У підмережі простору обслуговування комп'ютерної мережі потрібно забезпечити передачу трафіку трьох VLAN між двома комутаторами. Для цього необхідно налаштувати Trunk-порт, використовуючи команди *switchport mode trunk* та *switchport trunk encapsulation dot1q*, що відповідає протоколу 802.1Q. Далі, за допомогою команди *switchport trunk allowed vlan [список VLAN]* можна визначити, які VLAN будуть передаватися через Trunk.

```
Moiseenko_Sw5.1(config)#int g0/1
Moiseenko_Sw5.1(config-if)#switchport mode trunk

Moiseenko_Sw5.1(config-if)#switchport trunk native vlan 100
Moiseenko_Sw5.1(config-if)#switchport trunk allowed vlan 26,36,46,99-100
Moiseenko_Sw5.1(config-if)#no shutdown
Moiseenko_Sw5.1(config-if)#exit
```

Рисунок 3.16 – Налаштування Trunk порт

VLAN 99 використовується як VLAN управління. Призначення IP-адрес виконане відповідно до таблиці 3.9. З цієї мережі призначаються адреси для маршрутизатора Moiseenko_R2 та комутаторів.

```
Moiseenko_Sw5.1(config)#int vlan 99
Moiseenko_Sw5.1(config-if)#description LAN Vnutr_99
Moiseenko_Sw5.1(config-if)#ip add 172.24.129.194 255.255.255.240
Moiseenko_Sw5.1(config-if)#no shut
Moiseenko_Sw5.1(config-if)#ip default-gateway 172.24.129.193
Moiseenko_Sw5.1(config)#exit
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Рисунок 3.17 – Налаштування VLAN 99

Перевірка налаштувань VLAN виконується командами show vlan brief та show interface [інтерфейс] switchport, що дозволяють перевірити поточні налаштування VLAN та інтерфейсів.

```
Moiseenko_Sw5.1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/9
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
26   Subscriber                       active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14
36   ffice_Meneg                      active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8
46   Executive                        active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20
99   Management                       active
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.18 – Результат перевірки налаштувань VLAN

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC4_vlan 46	PC2_vlan 36	ICMP	
	Successful	PC1_vlan 46	PC1_vlan 26	ICMP	
	Successful	PC1_vlan 26	PC1_vlan 36	ICMP	
	Successful	PC1_vlan 26	PC3_vlan 46	ICMP	
	Successful	ServerHTTP36	PC1_vlan 26	ICMP	

Рисунок 3.19 – Результат перевірки пінгування між хостами трьох VLAN

У підмережі LAN1, відповідно до технічних вимог, для забезпечення високої пропускної здатності, балансування навантаження та підвищення надійності з’єднання, виконано агрегування портів комутаторів Moiseenko_Sw1.1, Moiseenko_Sw1.2 та Moiseenko_Sw1.3.

У цій підмережі використовується технологія агрегування портів LACP (Link Aggregation Control Protocol), що відповідає стандарту IEEE 802.3ad. Вона автоматично й динамічно об’єднує порти в агрегований канал, забезпечуючи рівномірний розподіл навантаження та підвищену стійкість з’єднання.

```
Moiseenko_Sw1.1(config)#interface range f0/1-2
Moiseenko_Sw1.1(config-if-range)#channel-group 1 mode auto
Moiseenko_Sw1.1(config-if-range)#interface range f0/3-4
Moiseenko_Sw1.1(config-if-range)#channel-group 3 mode auto
Moiseenko_Sw1.1(config-if-range)#interface Port-channel 1
Moiseenko_Sw1.1(config-if)# switchport mode trunk
Moiseenko_Sw1.1(config-if)#interface Port-channel 3
Moiseenko_Sw1.1(config-if)# switchport mode trunk
Moiseenko_Sw1.1(config-if)#int v 1
Moiseenko_Sw1.1(config-if)#ip add 172.24.132.2 255.255.255.128
Moiseenko_Sw1.1(config-if)#ip def 172.24.132.1
Moiseenko_Sw1.1(config)#ex
```

Рисунок 3.20 – Налаштування LACP на Moiseenko_Sw1.1

Для LACP обрали порти Fa1/0–2 та Fa3/0–4 на Moiseenko_Sw1.1 і перевели їх у режим агрегації командами:

channel-group 1 mode auto

channel-group 3 mode auto

Одночасно ці інтерфейси налаштовано як trunk. На кожному комутаторі SVI-інтерфейсу призначено IP-адресу з діапазону підмережі LAN1.

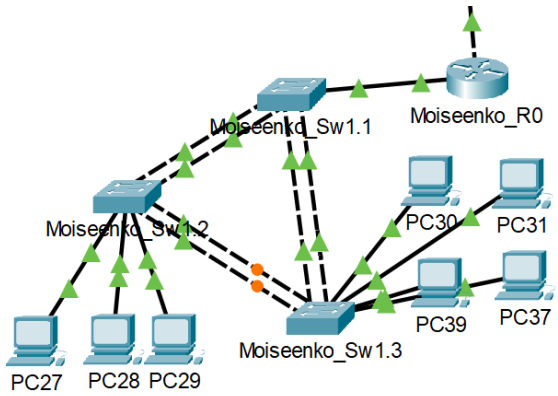

Рисунок 3.21 – Результат впровадження LACP для LAN1

```
Moiseenko_Sw1.1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

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

1      Po1(SU)           PAgP   Fa0/1(P) Fa0/2(P)
3      Po3(SD)           PAgP   Fa0/3(I) Fa0/4(I)
```

Рисунок 3.22 – Пеервірка LACP на Moiseenko_Sw1.1

3.3.3 Налаштування роботи з Інтернет

Для забезпечення виходу хостів комп'ютерної мережі в Інтернет застосовується технологія NAT.

Маршрутизатор Moiseenko_R3 виконує роль пограничного пристрою, підтримує NAT і має два інтерфейси: внутрішній (LAN) та зовнішній (WAN).

Глобальну IP-адресу, яку надає інтернет-провайдер, призначають на WAN-інтерфейс для зв'язку з мережею Інтернет.

Під час налаштування NAT на Moiseenko_R3 створюється пул глобальних адрес для трансляції, вказується NAT-адреса для серверів та позначаються інтерфейси як *inside* і *outside*.

```
Moiseenko_R3(config)#access-list 16 permit 172.24.128.0 0.0.7.255
Moiseenko_R3(config)#ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224
Moiseenko_R3(config)#ip nat inside source list 16 pool Internet
Moiseenko_R3(config)#ip nat inside source static 172.24.130.10 209.165.200.3
Moiseenko_R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
Moiseenko_R3(config)#interface s0/0/0
Moiseenko_R3(config-if)#ip nat outside
Moiseenko_R3(config-if)#interface s0/0/1
Moiseenko_R3(config-if)#ip nat inside
Moiseenko_R3(config-if)#interface s0/1/0
Moiseenko_R3(config-if)#ip nat inside
Moiseenko_R3(config-if)#interface g0/1
Moiseenko_R3(config-if)#ip nat inside
Moiseenko_R3(config-if)#exit
```

Рисунок 3.23 – Налаштування NAT Moiseenko_R3

```
Moiseenko_R3#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.6:4   172.24.129.143:4   209.165.201.5:4    209.165.201.5:4
icmp 209.165.200.7:3   172.24.129.80:3    209.165.201.5:3    209.165.201.5:3
icmp 209.165.200.8:13  172.24.128.11:13   209.165.201.5:13   209.165.201.5:13
icmp 209.165.200.9:1   172.24.128.12:1    209.165.201.5:1    209.165.201.5:1
---  209.165.200.3     172.24.130.10      ---                ---

Moiseenko_R3#
```

Рисунок 3.24 – Результат перевірки налаштувань NAT

3.3.4 Захист інформації в комп’ютерній Системі

3.3.4.1 Налаштування контролю доступу

Для захисту та контролю доступу до мережевих ресурсів комп’ютерної мережі підприємства впроваджено технологію AAA, що дозволяє централізовано керувати ідентифікацією користувачів, їхніми правами доступу та обліком активності.

Під час налаштування вибрано аутентифікацію через протокол RADIUS, який переносить перевірку облікових даних на зовнішні сервери, забезпечуючи гнучкіше й централізоване керування.

Авторизація визначає, до яких ресурсів та команд матиме доступ користувач після успішної аутентифікації, а адміністратори можуть призначати різні рівні привілеїв для різних груп.

Модуль обліку (accounting) реєструє дії користувачів – команди та час роботи в мережі, що дає змогу відстежувати активність, виявляти проблеми та забезпечувати відповідність політикам безпеки.

```
Moiseenko_R4(config)#aaa new-model
Moiseenko_R4(config)#aaa authentication login default local
Moiseenko_R4(config)#aaa authentication login Login group radius local
Moiseenko_R4(config)#line vty 0 4
Moiseenko_R4(config-line)#login authentication default
Moiseenko_R4(config-line)#radius-server host 172.24.130.10 auth-port 1645
%New type server exists with same address port combination.
Moiseenko_R4(config)#radius-server key radius123
Moiseenko_R4(config)#exit
Moiseenko_R4#
%SYS-5-CONFIG_I: Configured from console by console

Moiseenko_R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Moiseenko_R4(config)#aaa authentication login SSH-LOGIN local
Moiseenko_R4(config)#line vty 0 4
Moiseenko_R4(config-line)#login authentication SSH-LOGIN
Moiseenko_R4(config-line)#transport input ssh
Moiseenko_R4(config-line)#exit
Moiseenko_R4(config)#radius-server host 172.24.130.10
%New type server exists with same address port combination.
Moiseenko_R4(config)#radius-server key radius123
Moiseenko_R4(config)#aaa authentication login default group radius local
Moiseenko_R4(config)#exit
```

Рисунок 3.25 – Налаштування служби AAA на роутері Moiseenko_R4

У процесі налаштування служби AAA було виконано нижченаведені етапи.

1) Налаштування аутентифікації для доступу до консольного порту. Створено список методів аутентифікації, який змушує пристрій звертатися до RADIUS-сервера для перевірки облікових даних користувача при спробі підключитися до консолі. Призначено цей список консольному інтерфейсу, щоб жоден користувач без валідної обліковки на RADIUS не міг отримати доступ.

2) Конфігурація RADIUS-сервера. Визначено ім’я (alias) та IP-адресу маршрутизаторів, які будуть клієнтами RADIUS. Задано спільний ключ (shared secret) для захищеного обміну запитами аутентифікації між мережевими пристроями та сервером. Налаштовано порти та необхідні таймаути/повторні спроби для коректної взаємодії з сервером.

3) Впровадження аутентифікації на віртуальні лінії (VTY). Для всіх VTY-ліній (доступ по Telnet/SSH) застосовано той самий список методів аутентифікації RADIUS, що і для консолі. Встановлено рівні привілеїв, які присвоюються після успішного входу, відповідно до ролі користувача.

4) Підготовка AAA-сервера. Налаштовано базову мережеву конфігурацію: призначено IP-адресу, маску та шлюз за замовчуванням. Додано в конфігурацію імена (hostname) всіх мережевих пристроїв, які будуть звертатися за аутентифікацією, щоб спростити адміністрування та моніторинг. Створено облікові записи користувачів із паролями, групами та рівнями привілеїв, що дозволяє централізовано керувати доступом до мережевого обладнання.

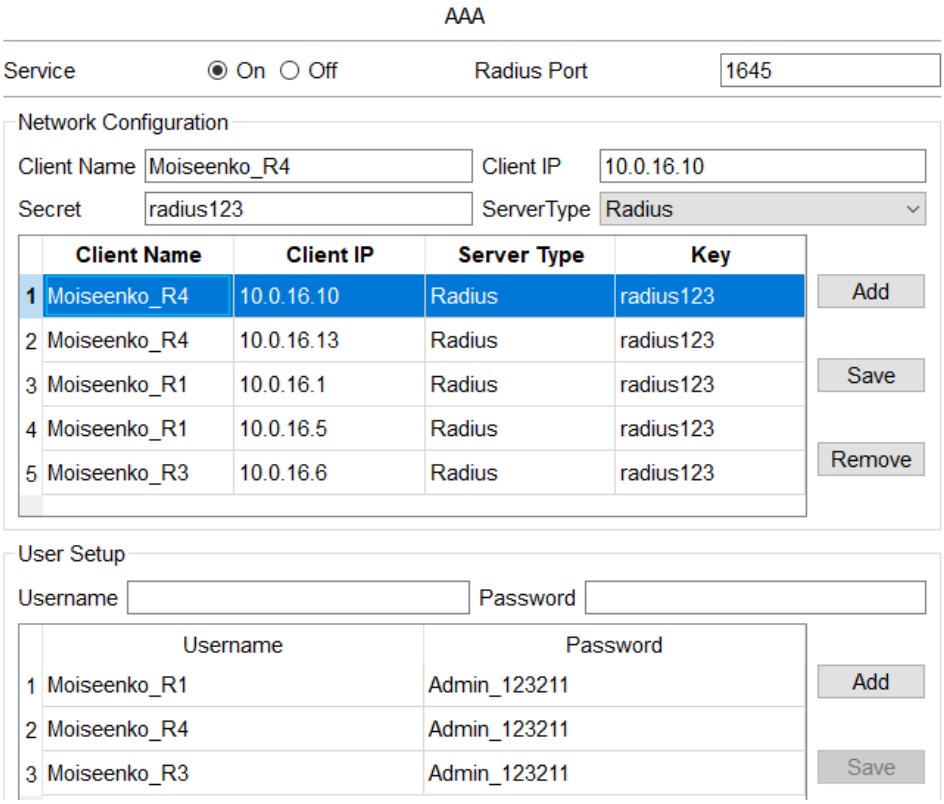

Рисунок 3.26 – Налаштування серверу AAA

```
123-21-1 Moiseenko. authorized users only

User Access Verification

Username: Moiseenko_R3
Password:
Moiseenko_R3>enable
Password:
Moiseenko_R3#sh
Moiseenko_R3#show ?
  aaa                 Show AAA values
  access-lists        List access lists
  arp                 Arp table
```

Рисунок 3.27 – Перевірка служби AAA

У підмережах LAN_5, 4 та 3 знаходяться сервери підприємства. На комутаторі відповідної локальної мережі (наприклад, Moiseenko_Sw5.1, де до порту Fa0/6 підключений HTTP-сервер) слід реалізувати заходи безпеки для всіх портів, до яких підключені сервери.

Застосовані команди: *switchport port-security mac-address sticky* // налаштування автоматичного розпізнавання MAC-адресу з додаванням його в поточну конфігурацію; *switchport port-security violation restrict* // налаштування.

```
Moiseenko_Sw5.1(config)#int f0/6
Moiseenko_Sw5.1(config-if)#no shut
Moiseenko_Sw5.1(config-if)#switchport mode access
Moiseenko_Sw5.1(config-if)#switchport port-security
Moiseenko_Sw5.1(config-if)#switchport port-security maximum 2
Moiseenko_Sw5.1(config-if)#switchport port-security mac-address sticky
Moiseenko_Sw5.1(config-if)#switchport port-security violation restrict
Moiseenko_Sw5.1(config-if)#exit
```

Рисунок 3.28 – Налаштування безпеки порту Fa0/6

Перевірка налаштувань безпеки порту комутатора, підключеного до серверу IoT, на прикладі Moiseenko_Sw6 є важливим етапом для забезпечення захисту мережі. Ця перевірка дозволяє виявити та запобігти можливим загрозам, таким як несанкціонований доступ або атаки на мережеву інфраструктуру.

Для виконання перевірки використовується команда *show port-security*, яка дозволяє отримати детальну інформацію про статус безпеки порту. При її запуску адміністратор може переглянути такі параметри:

– стан безпеки порту (включено чи вимкнено);

– кількість дозволених MAC-адрес та фактично підключені MAC-адреси;

– тип порушень безпеки (наприклад, перевищення ліміту MAC-адрес);

–дія при порушенні (обмеження, блокування чи захист);

Процедура перевірки може включати такі етапи:

– підключення до комутатора через консоль або SSH;

– виконання команди *show port-security interface [інтерфейс]* для отримання даних;

– аналіз отриманої інформації та внесення необхідних змін у конфігурацію для посилення безпеки.

```
Moiseenko_Sw5.1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-----------------------------------------------------------------------
        Fa0/6        2          1                0         Restrict
-----------------------------------------------------------------------
```

Рисунок 3.29 – Перевірка безпеки порту

Для забезпечення безпеки віддаленого доступу до маршрутизаторів у корпоративній мережі було впроваджено протокол SSH версії 2 (Secure Shell). Це критично важливий захід для захисту мережевого обладнання від несанкціонованого доступу, атак типу «людина посередині» (MITM) та перехоплення даних.

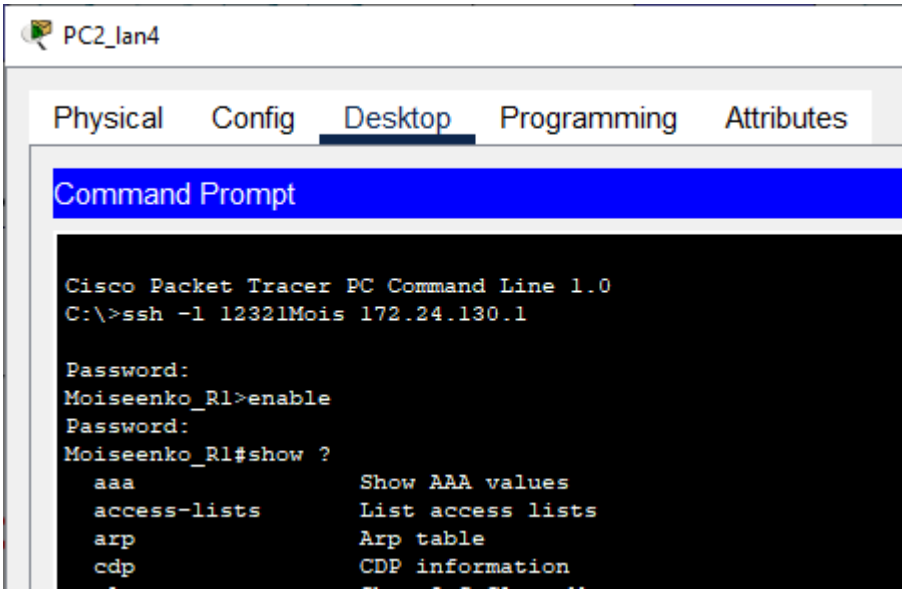

Рисунок 3.30 – Перевірка доступу а протоколом SSH

3.3.4.2 Налаштування віртуальної приватної мережі VPN

З метою забезпечення безпечного обміну даними між віддаленими сегментами корпоративної комп’ютерної системи компанії, було реалізовано налаштування віртуальної приватної мережі (VPN). Така технологія дозволяє

створити захищене з’єднання поверх публічної або незахищеної мережі, наприклад, Інтернету, за допомогою шифрування та аутентифікації учасників з’єднання.

У рамках проєкту було налаштовано VPN-з’єднання між маршрутизатором компанії Moiseenko_R0 та провайдером Rout_ISP. Для реалізації VPN використовувалась технологія IPSec, що забезпечує шифрування трафіку та перевірку цілісності даних.

Основні етапи налаштування включали:

– створення списку доступу (Access List) для визначення трафіку, який підлягає шифруванню, створюється ACL;

– налаштування ISAKMP політик (фаза 1) налаштовується політика шифрування між VPN-партнерами;

– задання спільного ключа (pre-shared key);

– налаштування IPSec тунелю (фаза 2) створюється трансформ-сет і криптомапа;

– прив’язка криптомапи до зовнішнього інтерфейсу маршрутизатора;

Налаштування з боку ISP (Rout_ISP) аналогічні налаштування виконуються на провайдерському маршрутизаторі, з урахуванням зворотних IP-адрес та ідентичного pre-shared key;

Перевірка роботи VPN здійснюється пінг між вузлами в мережах 172.24.132.0/25 та 172.24.130.0/24, які мають бути з’єднані через зашифрований тунель.

```
Moiseenko_R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Moiseenko_R0(config)#access-list 110 permit ip 172.24.131.0 0.0.0.255 172.24.132.0
0.0.0.127
Moiseenko_R0(config)#crypto isakmp policy 10
Moiseenko_R0(config-isakmp)#encryption aes
Moiseenko_R0(config-isakmp)#authentication pre-share
Moiseenko_R0(config-isakmp)#group 2
Moiseenko_R0(config-isakmp)#ex
Moiseenko_R0(config)#crypto isakmp key cisco address 64.100.13.2
Moiseenko_R0(config)#crypto ipsec transform-set VPN-CONF esp-3des esp-sha-hmac
Moiseenko_R0(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Moiseenko_R0(config-crypto-map)#description VPN connection to Moiseenko_R3
Moiseenko_R0(config-crypto-map)#set peer 64.100.13.2
Moiseenko_R0(config-crypto-map)#set transform-set VPN-CONF
Moiseenko_R0(config-crypto-map)#match address 110
Moiseenko_R0(config-crypto-map)#ex
Moiseenko_R0(config)#interface GigabitEthernet 0/1
Moiseenko_R0(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Moiseenko_R0(config-if)#ex
```

Рисунок 3.31 – Налаштування VPN на роутері Moiseenko_R0

```
Moiseenko_R0#show crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: VPN-MAP, local addr 64.100.13.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.24.131.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.24.132.0/255.255.255.128/0/0)
   current_peer 209.165.202.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 64.100.13.2, remote crypto endpt.: 209.165.202.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x0(0)
```

Рисунок 3.32 – Перевірка технології VPN

3.4 Розробка конфігурації IoT-рішень

В основі IoT-системи для приміщення електрощитової ліфтового господарства застосований спеціалізований бездротовий маршрутизатор DLC-100, який є шлюзом для підключення розумних пристроїв до корпоративної мережі. За протоколом DHCP маршрутизатор DLC-100 отримує TCP/IP

налаштування інтерфейсу Internet від роутера Moiseenko_R1 з діапазону адрес 172.24.130.0/24 підмережі LAN4.

DLC-100 за бездротовою технологією WiFi з діапазону приватних IP-адрес 192.168.25.1/24 розподіляє мережні налаштування "розумним речам" у крамниці.

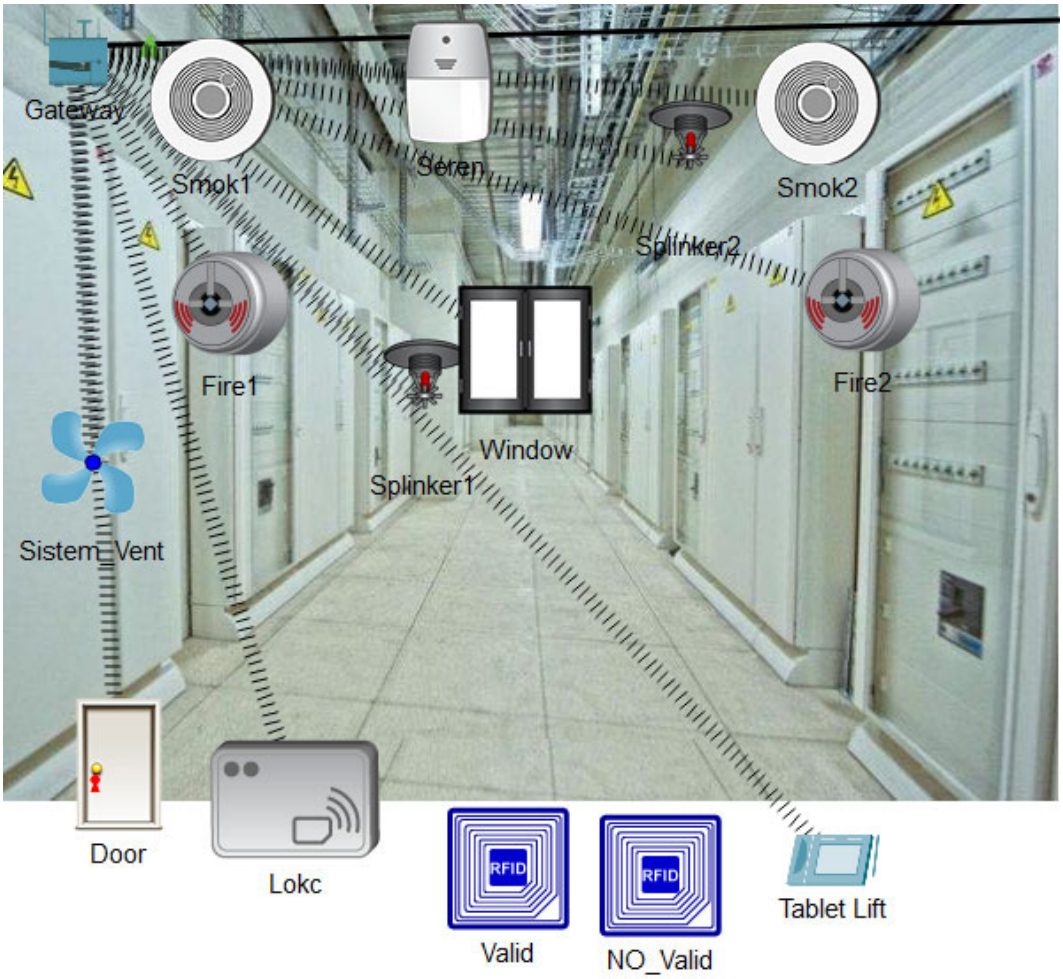

Рисунок 3.33 – Архітектура IoT-системи

Таблиця 3.12 – Мережні налаштування IoT-шлюзу

Параметр	Значення
1	**2**
IP-адреса інтерфейсу Internet	172.24.130.14
Маска домашньої підмережі	255.255.255.0
SSID бездротової домашньої мережі	Lift
Метод автентифікації	WPA2-PSK AES

Ключ автентифікації (*пароль*)	Moiseenko

Функції, що виконуються "Розумними речами":

– виявлення задимленості і сповіщення за допомогою звукового сигналу та відображення їх на хмарній платформі;

– виявлення вогню (різке зростання температури) і сповіщення за допомогою звукового сигналу, ввімкнення пристроїв пожежогасіння та відображення їх на хмарній платформі;

– керування доступом в приміщення електрощитової.

Хмарні сервіси надає сервер з сервісами IoT, який розташований в підмережі LAN-4 з IP-адресою 172.24.130.8/24.

За підтримку WiFi-мережі, відповідає роутер DLC-100. Для налаштування його на підтримку мережі необхідно виконати налаштування ідентифікатора мережі, обрати метод аутентифікації із зазначенням паролю доступу та обрати алгоритм шифрування.

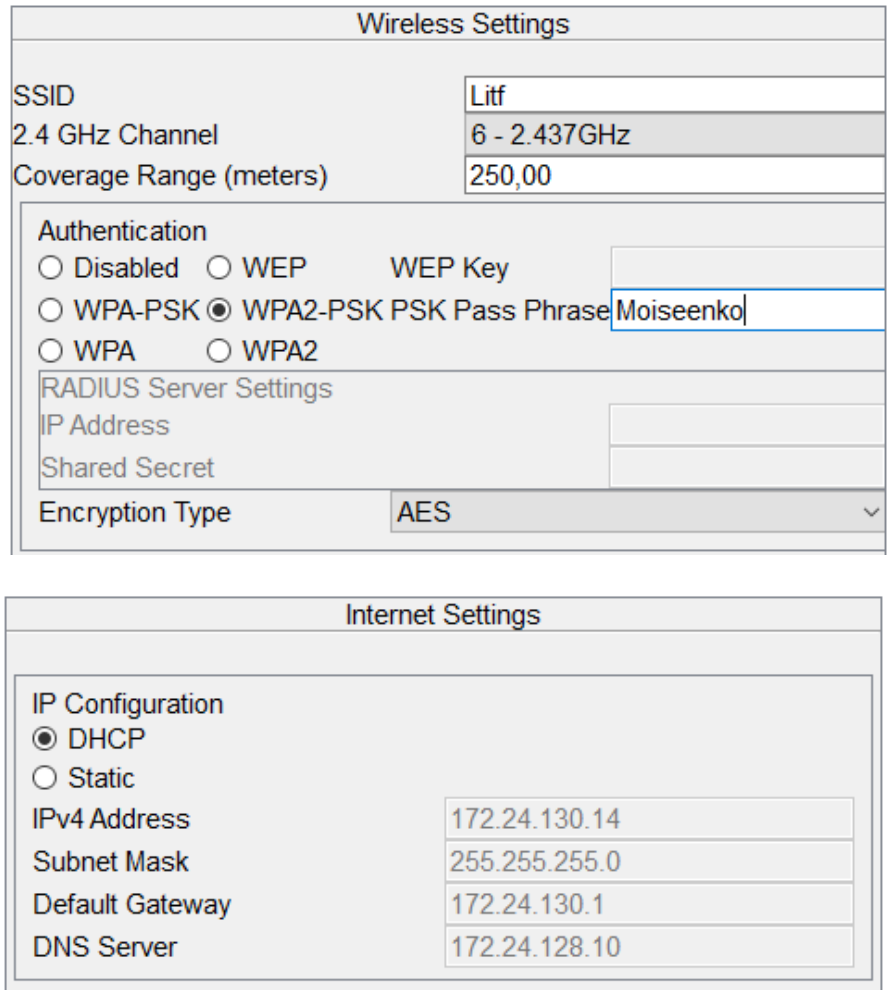

Рисунок 3.34 – Перевірка налаштувань шлюза IoT

IoT-система побудована таким чином, що всі зібрані "розумними речами" дані надходять на IoT-сервер, який розміщений у підмережі "IoT Control" компанії. Саме цей сервер є центральним вузлом для обробки, аналізу та збереження інформації. Він виконує важливі функції, серед яких моніторинг стану датчиків, виявлення аномалій та автоматичне реагування на нестандартні ситуації. Крім того, IoT-сервер має веб-інтерфейс, що дозволяє користувачам, наприклад співробітникам магазину чи службі безпеки, отримувати актуальну інформацію у реальному часі. Це дає можливість бачити стан датчиків пожежної безпеки, рівень задимленості чи температури, а також готовність пристроїв пожежогасіння до активації. Завдяки цьому компанія має повний контроль над критично важливими процесами та може оперативно реагувати на потенційні загрози. IoT-технологія значно підвищує ефективність управління системами

безпеки та автоматизації, оптимізуючи роботу підприємства та зменшуючи ризики аварійних ситуацій. Якщо потрібно більше деталей, можу доповнити текст технічними аспектами або конкретними сценаріями використання.

При налаштуванні «розумних» речей необхідно зазначити необхідні налаштування підключення до WIFi-мережі та параметри підключення до віддаленого серверу.

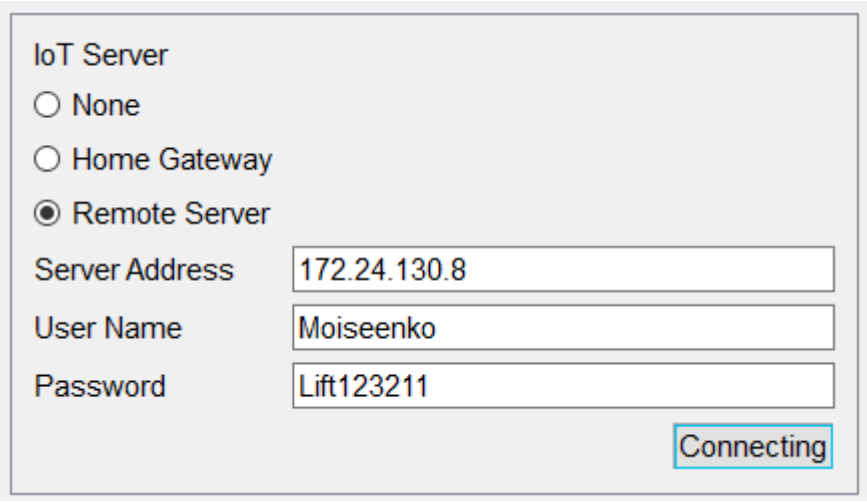

Рисунок 3.35 – Підключення до серверу в LAN-4

За допомогою веб-інтерфейса IoT-сервера є доступ до моніторінгу та керування IoT-пристроями ліфтового господарства.

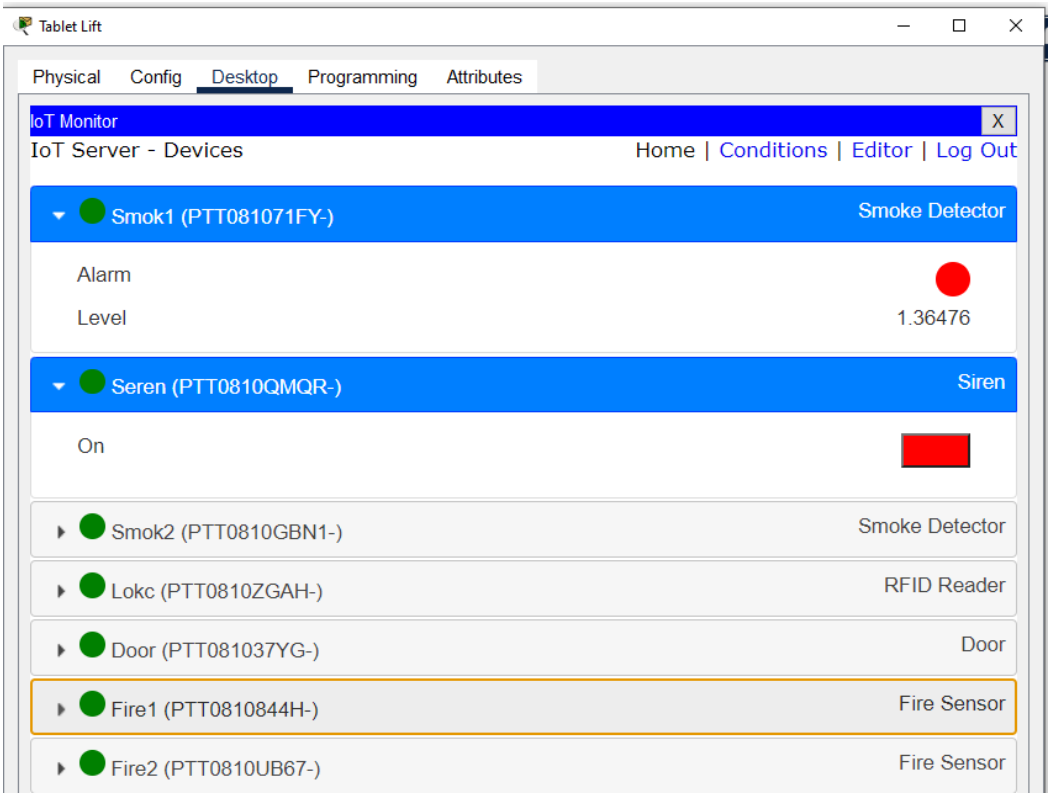

Рисунок 3.36 – Перевірка підключення речей до серверу IoT

Сценарії, створені за допомогою сервісу IoT-серверу виконують автоматичні дії у відповідь на наступні події:

–при перевищенні рівня задимленості вище 40% вмикати звукову сирену та систему вентиляції відчиняти вікно, при зниженні до рівня 30% – вимкнути сирену та вентиляцію, зачинити вікно;

–активувати пристрої пожежогасіння та звукову сигналізацію при виявленні пожежі, при зниженні показника нище порогового значення – вимкнути;

–керувати доступом до приміщення но основі RFID-технології. Валідні RFID-мітки знаходяться в діапазоні 500-600. За умови виявлення валідної RFID-мітки, двері будуть відчинені.

Tablet Lift

Physical Config Desktop Programming Attributes

IoT Monitor X

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Door_ON	Lokc Card ID is between 490 and 600	Set Door Lock to Unlock
Edit Remove	Yes	Door_OFF	Match all: • Lokc Card ID > 600 • Lokc Card ID < 490	Set Door Lock to Lock
Edit Remove	Yes	Smoke_Alarm_ON	Match any: • Smok1 Level > 40 • Smok2 Level > 40	Set Seren On to true Set Window On to true Set Sistem_Vent Status to High
Edit Remove	Yes	Smoke_Alarm_OFF	Match all: • Smok1 Level < 30 • Smok2 Level < 30	Set Seren On to false Set Window On to false Set Sistem_Vent Status to Off
Edit Remove	Yes	Fire_Alarm_ON	Match any: • Fire1 Fire Detected is true • Fire2 Fire Detected is true	Set Seren On to true Set Splinker1 Status to true Set Splinker2 Status to true
Edit Remove	Yes	Fire_Alarm_OFF	Match all: • Fire1 Fire Detected is false • Fire2 Fire Detected is true	Set Splinker1 Status to false Set Splinker2 Status to true Set Seren On to false

Рисунок 3.37 – Сценарії, створені за допомогою сервісу IoT-серверу

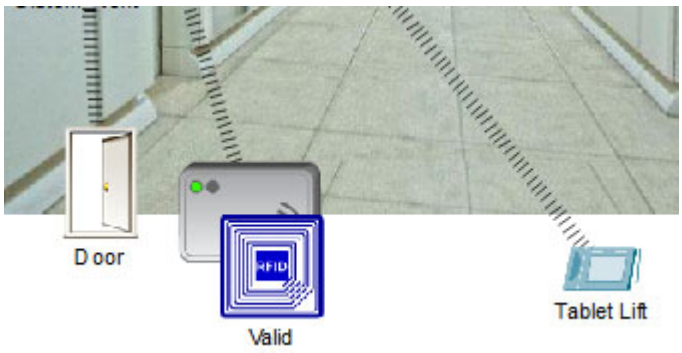

Рисунок 3.38 – Перевірка сценарію керування дверима щитової

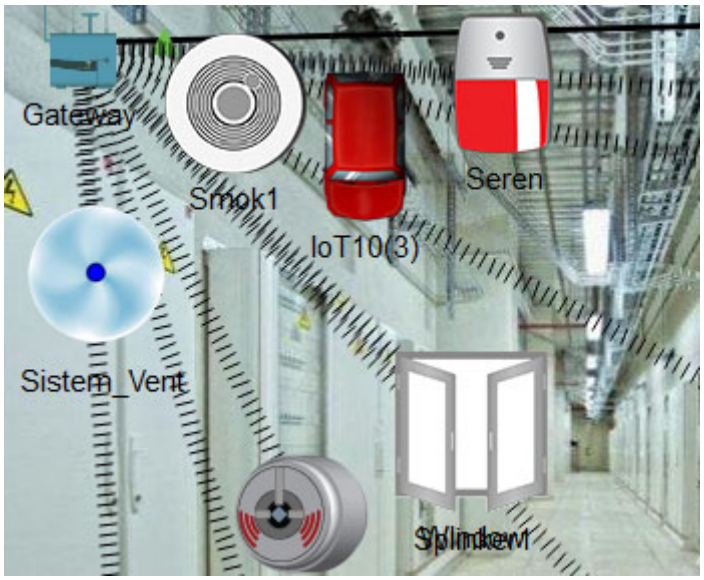

Рисунок 3.39 – Перевірка сценарію виявлення задимленості

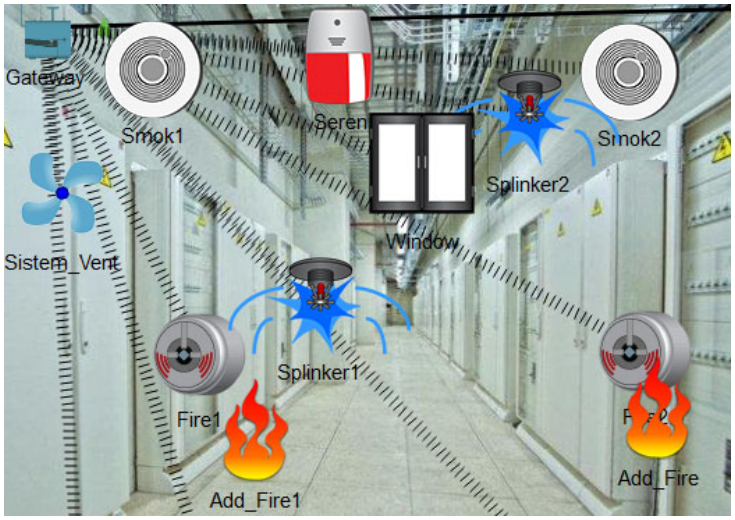

Рисунок 3.40 – Перевірка сценарію виявлення пожежі

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи на тему «Комп'ютерна система компанії з монтажу та обслуговування ліфтів з детальним опрацюванням побудови та налаштування мережі організації» було досягнуто поставленої мети – розроблено та обґрунтовано структуру, технічну реалізацію та логічну конфігурацію корпоративної мережі, що відповідає сучасним вимогам надійності, безпеки та масштабованості.

У процесі виконання проєкту:

– Проаналізовано потреби компанії в автоматизації та інформаційному обміні між підрозділами, що дало змогу визначити ключові функціональні та технічні вимоги до комп’ютерної системи.

– Обґрунтовано вибір структури мережі, зокрема поділ її на п’ять окремих LAN-сегментів із використанням VLAN-технологій для підвищення логічної безпеки та ефективного управління трафіком.

– Розроблено адресну схему, у якій враховано реальні потреби кожного сегмента, резервування IP-адрес та оптимальне використання простору адрес IPv4.

– Налаштовано ключові мережеві пристрої, зокрема маршрутизатори та комутатори, із впровадженням протоколів маршрутизації (EIGRP), механізмів VLAN, DHCP-серверів, SVI-інтерфейсів.

– Реалізовано функціональну VPN-інфраструктуру, що дозволяє створювати захищене підключення між офісами компанії через публічні мережі.

– Побудовано топологічну схему в середовищі Cisco Packet Tracer, яка візуально відображає логіку побудови мережі, взаємозв’язки між пристроями, шлюзи, маршрути та конфігурацію портів.

Отримані результати підтверджують доцільність використання багаторівневої корпоративної мережі з логічною сегментацією. Запропоноване рішення дозволяє:

– покращити керованість та масштабованість мережі;

– підвищити рівень безпеки інформаційної взаємодії;

– забезпечити резервування та стійкість до збоїв;

– спростити адміністрування та централізований контроль за трафіком і доступом.

Таким чином, розроблена комп’ютерна система є ефективним технічним рішенням, яке відповідає реальним потребам компанії з монтажу та обслуговування ліфтів і може бути впроваджене у виробничу діяльність.

Перелік посилань

1. Атестаційна робота бакалавра. Методичні рекомендації до виконання та оформлення кваліфікаційних робіт бакалаврів для здобувачів ступеня бакалавра галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / В.В. Гнатушенко, Л.І. Цвіркун, С.М. Ткаченко, Д.О. Бешта, Л.В. Бешта, Я.В. Панферова. – Д.: НТУ «ДП», 2025. – 40 с.
2. Звіти у сфері науки і техніки. Структура і правила оформлення. ДСТУ 3008:2015 [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://surl.li/dcevgv (дата звернення 28.04.2025).
3. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.
4. Маршрутизатор Cisco ISR 4331 [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://surl.li/dyxctl (дата звернення 01.06.2025).
5. Маршрутизатор Cisco Firepower 1010 [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://surl.lu/ubvqsg (дата звернення 05.06.2025).
6. Комутатор Cisco Catalyst 2960-X [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://surl.li/vqspjb (дата звернення 08.06.2025).
7. Комутатор TP-Link JetStream T1600G-28TS [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://surl.li/ainiuw (дата звернення 08.06.2025).

Додаток А

Текст програми налаштування мережі комп’ютерної системи

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.25016-01 12 01

Листів 7

2025

АНОТАЦІЯ

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

ЗМІСТ

1. Налаштування маршрутизатора Moiseenko R2

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Moiseenko_R2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 172.24.129.1 172.24.129.10
ip dhcp excluded-address 172.24.129.65 172.24.129.75
ip dhcp excluded-address 172.24.129.129 172.24.129.139
ip dhcp excluded-address 172.24.128.1 172.24.128.10
!
ip dhcp pool POOL_VLAN26
 network 172.24.129.0 255.255.255.192
 default-router 172.24.129.1
 dns-server 172.24.128.10
ip dhcp pool POOL_VLAN36
 network 172.24.129.64 255.255.255.192
 default-router 172.24.129.65
 dns-server 172.24.128.10
ip dhcp pool POOL_VLAN46
 network 172.24.129.128 255.255.255.192
 default-router 172.24.129.129
 dns-server 172.24.128.10
ip dhcp pool POOL_LAN3
 network 172.24.128.0 255.255.255.0
 default-router 172.24.128.1
 dns-server 172.24.128.10
!
aaa new-model
!
aaa authentication login Login group radius local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local
!
username 12321Mois password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX1524M7I7-
!
no ip domain-lookup
ip domain-name Moiseenko_R3.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.26
 encapsulation dot1Q 26
 ip address 172.24.129.1 255.255.255.192
!
interface GigabitEthernet0/1.36
 encapsulation dot1Q 36
 ip address 172.24.129.65 255.255.255.192
!
interface GigabitEthernet0/1.46
 encapsulation dot1Q 46
 ip address 172.24.129.129 255.255.255.192
!
interface GigabitEthernet0/1.99
 encapsulation dot1Q 99
 ip address 172.24.129.193 255.255.255.240
!
```

```
interface GigabitEthernet0/2
 ip address 172.24.128.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/0
 description WAN1
 bandwidth 128
 ip address 10.0.16.2 255.255.255.252
!
interface Serial0/1/1
 description to WAN3
 bandwidth 128
 ip address 10.0.16.9 255.255.255.252
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 16
 redistribute static
 passive-interface GigabitEthernet0/1.26
 passive-interface GigabitEthernet0/1.36
 passive-interface GigabitEthernet0/1.46
 passive-interface GigabitEthernet0/1.99
 network 10.0.16.8 0.0.0.3
 network 10.0.16.0 0.0.0.3
 network 172.24.129.0 0.0.0.63
 network 172.24.129.64 0.0.0.63
 network 172.24.129.128 0.0.0.63
 network 172.24.129.192 0.0.0.15
 network 172.24.128.0 0.0.0.255
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
banner motd #123-21 Moiseenko.
authorized users only#
!
radius server 172.24.130.10
 address ipv4 172.24.130.10 auth-port
1645
!
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
!
end
```

2. Налаштування комутатора Moiseenko_Sw5.1

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Moiseenko_Sw5.1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip domain-name Moiseenko_Sw51.com
!
username 12321_Moiseenko privilege 1 password 7 0822455D0A16
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 36
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/7
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 36
 switchport mode access
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 26
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 46
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 46
 switchport mode access
```

```
!
interface FastEthernet0/17
 switchport access vlan 46
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 46
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 46
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 46
 switchport mode access
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan
26,36,46,99-100
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk native vlan 100
 switchport trunk allowed vlan
26,36,46,99-100
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 description LAN Vnutr_99
 ip address 172.24.129.194
255.255.255.240
!
ip default-gateway 172.24.129.193
!
banner motd #123-21-1 Moiseenko.
authorized users only#
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
end
```