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** Матюшина Павла Павловича
(ПІБ)
**академічної групи** 123-19-1
(шифр)
**спеціальності** 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

**на тему** " Комп'ютерна система ТОВ"Альфатех" з реалізацією побудови, налаштування та безпеки корпоративної мережі "
(назва за наказом ректора)

| **Керівники** | **Прізвище, ініціали** | **Оцінка за шкалою** | | **Підпис** |
|---|---|---|---|---|
| | | **рейтинговою** | **інституційною** | |
| кваліфікаційної роботи | проф. Цвіркун Л.І. | | | |
| розділів: | | | | |
| розробка апаратної частини | доц. Бешта Д.О. | | | |
| розробка корпоративної мережі | ас. Панферова Я.В. | | | |
| **Рецензент** | | | | |
| **Нормоконтролер** | проф. Цвіркун Л.І. | | | |

**Дніпро**
**2023**

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

# ЗАВДАННЯ
# на кваліфікаційну роботу ступеня бакалавр

**студента** Матюшина П.П. **академічної групи** 123-19-1
(прізвище та ініціали) (шифр)

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

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

**на тему** "Комп'ютерна система ТОВ"Альфатех" з реалізацією побудови, налаштування та безпеки корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Стан питання та постановка завдання | На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання | 17.05.2023 |
| Розробка апаратної частини | На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи | 23.05.2023 |
| Розробка корпоративної мережі | Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі | 26.05.2023 |
| Розробка компонента системи | Виконується детальна розробка компонента системи | 27.05.2023 |

**Завдання видано** _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

**Дата видачі** 19.12.2022

**Дата подання до екзаменаційної комісії** 06.06.2023

**Прийнято до виконання** _____ Матюшин П.П.

# РЕФЕРАТ

Пояснювальна записка: 66с., 22 рис., 11 табл., 1 дод., 6 джерел.

КОМПАНІЯ, ПРОДАЖІ, МЕРЕЖА, ТЕХНІКА, ТЕХНОЛОГІЯ, ОБЛАДНАННЯ, СИСТЕМА

Об’єкт розробки – комп’ютерна система для компанії з продажу спецтехніки «Альфатех», з розробкою та впровадженням корпоративної мережі.

Головна мета роботи полягає у створенні ефективної корпоративної мережі, яка дозволить компанії підвищити продуктивність та рівні продажів.

Виконано детальний аналіз структури об’єкту впровадження та його потреб. Сформовано вимоги до майбутньої системи та здійснено вибір обладнання.

Виконано розробку системи з можливістю масштабування та перепрограмування. Основна сфера застосування системи – офіси середніх та великих розмірів.

Розроблена система виконує наступний функціонал:

- зв’язок підрозділів підприємства;
- забезпечення спільного доступу до ресурсів;
- захист даних у системі.

Розробка корпоративної мережі компанії була здійснена згідно усіх поставлених вимог та рекомендацій.

Комп’ютерна мережа була змодельована у середовищі програми Cisco Packet Tracer.

Перевірка роботи спроектованої системи наводиться у пояснювальній записці та додатках до неї.

ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система.

КМ – комп’ютерна мережа.

DHCP – (Dynamic Host Configuration Protocol) є протоколом мережевого рівня, який дозволяє автоматично надавати IP-адреси та інші мережеві налаштування пристроям у комп'ютерній мережі.

NAT – (Network Address Translation) - це технологія, яка використовується для перетворення IP-адрес у пакетах мережевого трафіку при проходженні через мережевий пристрій.

ACL – (Access Control List) – це список правил, який використовується для контролю доступу до ресурсів в мережі, таких як маршрутизатори або комутатори.

VPN – це технологія, яка дозволяє створювати зашифровані тунелі через публічну мережу, таку як Інтернет.

VLAN – (Virtual Local Area Network) - це технологія, яка дозволяє розділити фізичну локальну мережу на логічно відокремлені мережеві сегменти.

OSPF – (Open Shortest Path First) - це протокол маршрутизації в мережах IP, який використовує алгоритм Dijkstra для вибору найкоротших шляхів та визначення оптимальних маршрутів.

# ВСТУП

У сучасному світі, де інформаційні технології відіграють важливу роль у діяльності підприємств, належна організація мережевої інфраструктури стає ключовим аспектом для забезпечення ефективності та продуктивності бізнесу. Корпоративна мережа є основним засобом комунікації та обміну даними всередині підприємства, а її розробка та налаштування вимагають комплексного та детального підходу.

Ця дипломна робота присвячена розробці корпоративної мережі для компанії "Альфатех". Компанія "Альфатех" є великим підприємством, яке спеціалізується на продажі спецтехніки різного призначення. З метою покращення комунікації, обміну даними та забезпечення безперебійної роботи всіх внутрішніх підрозділів компанії, розробка корпоративної мережі стає невід'ємною частиною їхньої стратегії розвитку.

У першу чергу, буде проведений детальний аналіз потреб компанії щодо мережевої інфраструктури. Вивчення робочих процесів, вимог та очікувань працівників щодо комунікації та обміну даними допоможе визначити необхідні функціональні вимоги та характеристики мережі. На основі отриманих даних буде розроблено проект корпоративної мережі для компанії "Альфатех". Це включатиме побудову фізичної топології мережі, вибір необхідного обладнання та технологій, а також розробку схеми адресації IP.

Ця дипломна робота буде спрямована на детальне опрацювання процесу розробки та налаштування корпоративної мережі для компанії "Альфатех". Результати цієї роботи будуть важливим внеском у поліпшення комунікації, ефективності та безпеки внутрішніх процесів компанії, а також відображатимуть сучасні практики в галузі мережевих технологій.

# 1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

## 1.1 Стисла характеристика галузі та умови застосування КС

Галузь продажу спецтехніки включає в себе торгівлю різноманітними видами техніки, призначеними для виконання спеціалізованих завдань в різних галузях, таких як будівництво, дорожнє будівництво, сільське господарство, лісове господарство, муніципальне господарство, металургійна та гірнича промисловість та інші.

Продаж спецтехніки зазвичай здійснюється через спеціалізовані дилерські центри або автоагентства, які співпрацюють з виробниками та іншими постачальниками техніки. Клієнтами можуть бути як великі промислові компанії, які замовляють спецтехніку для власних потреб, так і малий бізнес або приватні особи, які шукають техніку для власного використання.

Також продаж спецтехніки часто супроводжується додатковими послугами, такими як сервісне обслуговування, навчання персоналу, доставка і монтаж техніки. Також деякі дилери можуть надавати фінансові послуги, такі як лізинг, для полегшення процесу придбання спецтехніки клієнтом.

Спецтехніка може бути новою або вживаною, а також різних марок та моделей, включаючи екскаватори, бульдозери, кранів, навантажувачів, трактори, комунальну техніку та інші.

Галузь продажу спецтехніки є важливою для розвитку різних галузей економіки та підтримки інфраструктурних проєктів. Продаж спецтехніки є великим ринком з значними обсягами продажів і відповідними можливостями для підприємств.

Крім того, галузь продажу спецтехніки є досить конкурентною, оскільки на ринку працює багато постачальників і дилерів. Для підтримки конкурентоспроможності, більшість дилерів стараються пропонувати своїм клієнтам високоякісну техніку, забезпечувати якісний сервіс і консультації щодо вибору техніки, а також пропонувати прийнятні ціни та вигідні умови оплати.

Зростання інтернет-технологій дозволило створити онлайн-майданчики, де клієнти можуть шукати і купувати спецтехніку з будь-якої точки світу. Це дозволяє покупцям знайти оптимальний варіант для своїх потреб, порівняти ціни і вибрати техніку з різних виробників та дилерів.

Галузь продажу спецтехніки вимагає високого рівня експертизи технічних характеристик, особливостей використання техніки, її технічного обслуговування та ремонту. Тому, для успішної роботи у цій галузі, дилери мають мати висококваліфікованих спеціалістів з цих питань.

Узагальнюючи, дана галузь є важливою складовою розвитку різних галузей економіки, вона вимагає високої кваліфікації технічних фахівців та конкурентної боротьби між постачальниками та дилерами.

### 1.2 Характеристика і структура об’єкта впровадження

Об’єкт впровадження – Центр спецтехніки «Альфатех».

Альфатех спеціалізується на виробництві інженерної та будівельної спецтехніки, включаючи автомобільні кранові установки, бурові установки, кочегарки, спеціальні автомобілі та інші види обладнання.

Центр спецтехніки «Альфатех» був створений у 2003 році і з того часу успішно розвивається. Компанія має великий досвід у виробництві спецтехніки, а також використовує найсучасніші технології та матеріали для виробництва своєї продукції.[1]

Основними продуктами Центру спецтехніки «Альфатех» є автомобільні кранові установки, які виробляються відповідно до європейських та світових стандартів якості. Компанія пропонує широкий вибір моделей кранів, які відрізняються за типом ходової частини, грузопідйомністю та робочою висотою.

Крім того, «Альфатех» виготовляє бурові установки, які застосовуються для буріння свердловин для водопостачання, газопостачання, нафтовидобування та інших галузей. Бурові установки компанії

характеризуються високою продуктивністю та надійністю, а також можуть бути зібрані на різних базах та з різними видами приводу.[1]

Також компанія виготовляє кочегарки, які застосовуються для перевезення вантажів на великі відстані, а також спеціальні автомобілі для транспортування вантажів з особливими вимогами до перевезення.

Компанія «Альфатех» має власний виробничий потенціал та здатність виготовляти не тільки серійну продукцію, але і індивідуальні рішення для клієнтів. Крім того, компанія надає послуги зі збірки, обслуговування та ремонту спецтехніки, що забезпечує клієнтів по всій Україні високоякісне обслуговування та швидке реагування на потреби ринку.

Центр спецтехніки «Альфатех» активно працює на внутрішньому та зовнішньому ринках, співпрацюючи з провідними виробниками та постачальниками комплектуючих з усього світу. Компанія має розгалужену мережу дилерів та сервісних центрів по всій Україні, а також успішно експортує свою продукцію до країн Європи, Близького Сходу та Східної Азії.[1]

Центр спецтехніки Альфатех є ексклюзивним офіційним дилером на території України компаній Hyundai Construction Equipment та Shantui Construction Machinery Co., LTD. Вони спеціалізуються на продажу та сервісному обслуговуванні будівельної, дорожньої та промислової техніки, виробленої провідними світовими виробниками. Альфатех також є офіційним дилером техніки Bobcat, гірничорудного обладнання Astec Industries та Telsmith, а також комунальної техніки Retech та Ausa.[1]

Альфатех реалізує широкий асортимент навісного обладнання Kovaco, Hydro Khan, Bobcat, яке може використовуватися на будівельних, комунальних, гірничих підприємствах. Також в наявності широкий асортимент запасних частин і шин від відомих світових виробників.

Усі вироби «Альфатех» відповідають найвищим стандартам якості та безпеки, а також мають гарантію від виробника. Компанія постійно працює

над удосконаленням своєї продукції та розробкою нових моделей, щоб задовольнити потреби найвимогливіших клієнтів.

Робота Компанії спрямована на розвиток довгострокового партнерства. Компанія працює на українському ринку 20 років.

### 1.3 Розміщення структурних підрозділів підприємства

Структура підприємства представлена двома будівлями: центральним офісом, розміщеним за адресою Дніпровський р-н, м. Підгородне, Автодорога М04, Знам'янка-Луганськ-Ізварино, 227км+580м, Дніпропетровська обл., Україна, 52001, та сервісним центром, розміщеним у будівлі на відстані 500м від головного офісу (рисунок 1.1). [2]

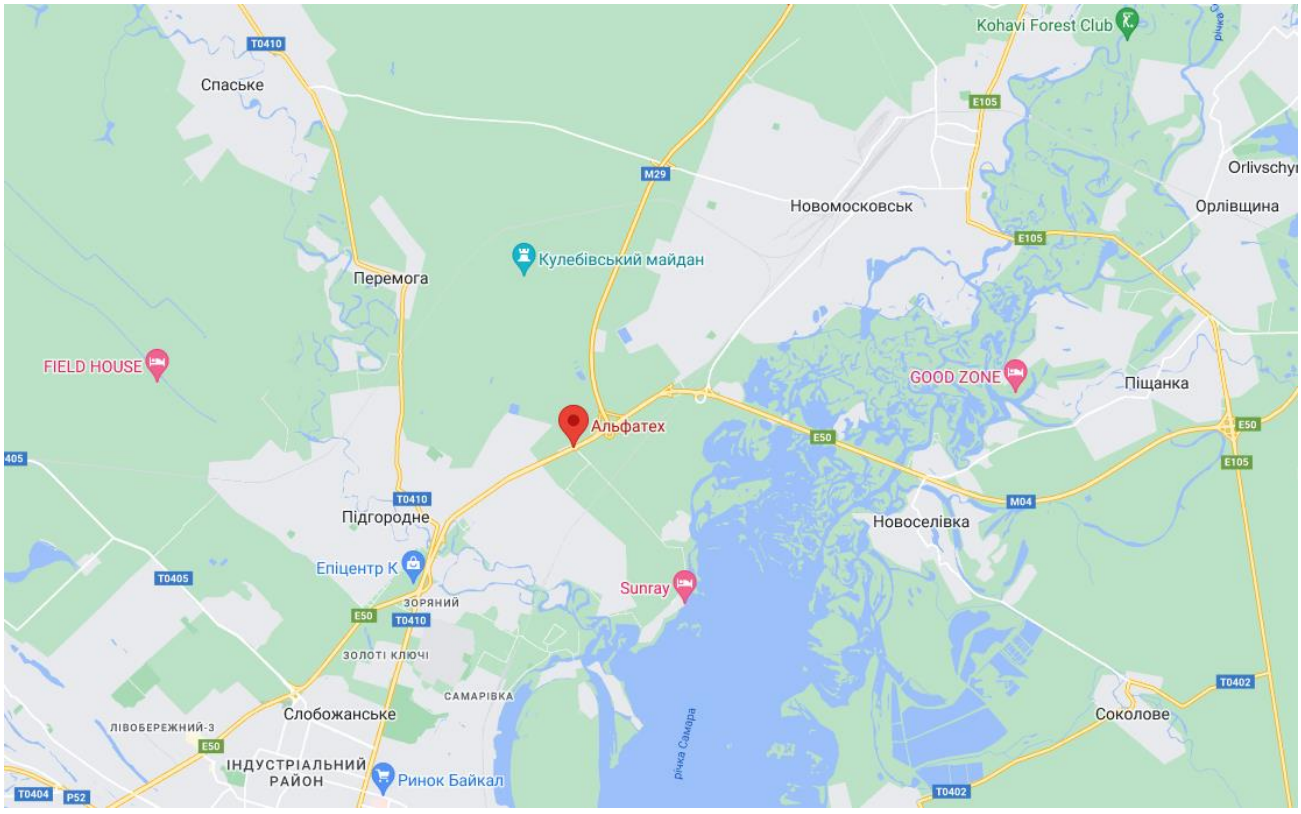


Рисунок 1.1 – Георозміщення офісу компанії «Альфатех»

На рисунку 1.2 зображено зовнішній вигляд головного офісу компанії.


Рисунок 1.2 – Будівля головного офісу

### 1.4 Організаційна структура підприємства

Організаційна структура компанії Центр спецтехніки Альфатех є ієрархічною та побудована на принципах функціонального поділу праці. Керівництво компанії складається з генерального директора, який займає вершину ієрархії, та керівників відділів.

У свою чергу, відділи компанії можуть бути розділені на підрозділи та групи. Відділи компанії Центр спецтехніки Альфатех включають такі функціональні напрямки:

1. Виробничий відділ: включає в себе інженерів, механіків та інших спеціалістів, які займаються розробкою та виготовленням спецтехніки.

2. Відділ продажів: включає в себе менеджерів з продажу, які займаються просуванням продукції на ринку та взаємодією з потенційними клієнтами.
3. Відділ логістики та постачання: включає в себе менеджерів з логістики та постачання, які забезпечують доставку та постачання комплектуючих та матеріалів для виробництва спецтехніки.
4. Відділ сервісу та технічної підтримки: включає в себе інженерів та спеціалістів, які забезпечують обслуговування та технічну підтримку клієнтів після продажу.

Загалом, організаційна структура компанії «Альфатех» є підпорядкованою, ієрархічною та побудована на принципах функціонального поділу праці з можливим застосуванням матричної структури для виконання проектних завдань. Відділи та підрозділи компанії співпрацюють між собою для досягнення загальної мети - розробки та виробництва якісної та конкурентоспроможної спецтехніки.

Схему організаційної структури компанії наведено на рисунку 1.3.

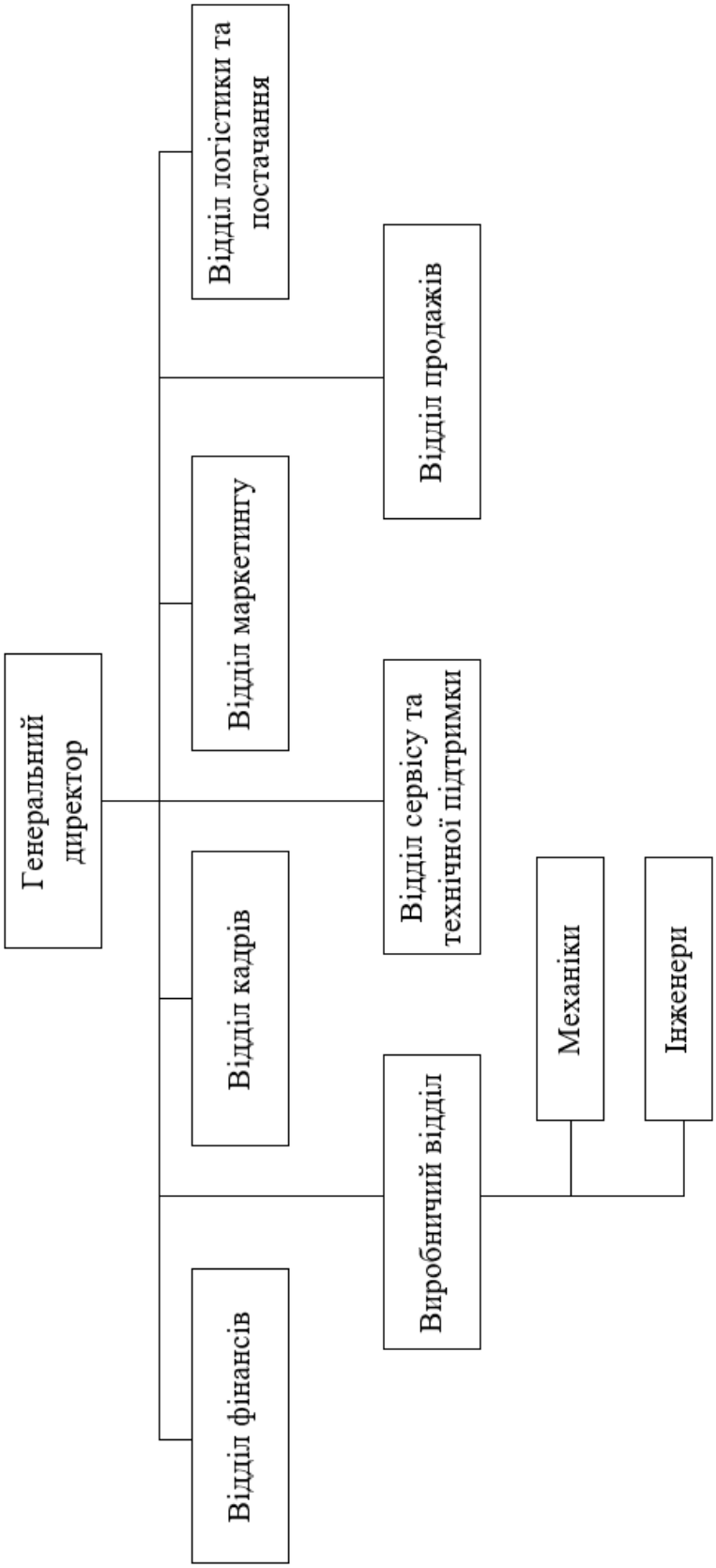


Рисунок 1.3 – Організаційна структура компанії «Альфатех»

## 1.4 Аналіз топологічної схеми розміщення структурних підрозділів підприємства

На рисунку 1.4 показано частину головного офісу підприємства, яка виділена під відділ продажу, та віддалену мережу сервісного центра, у якій розміщено відділ логістики та постачання.

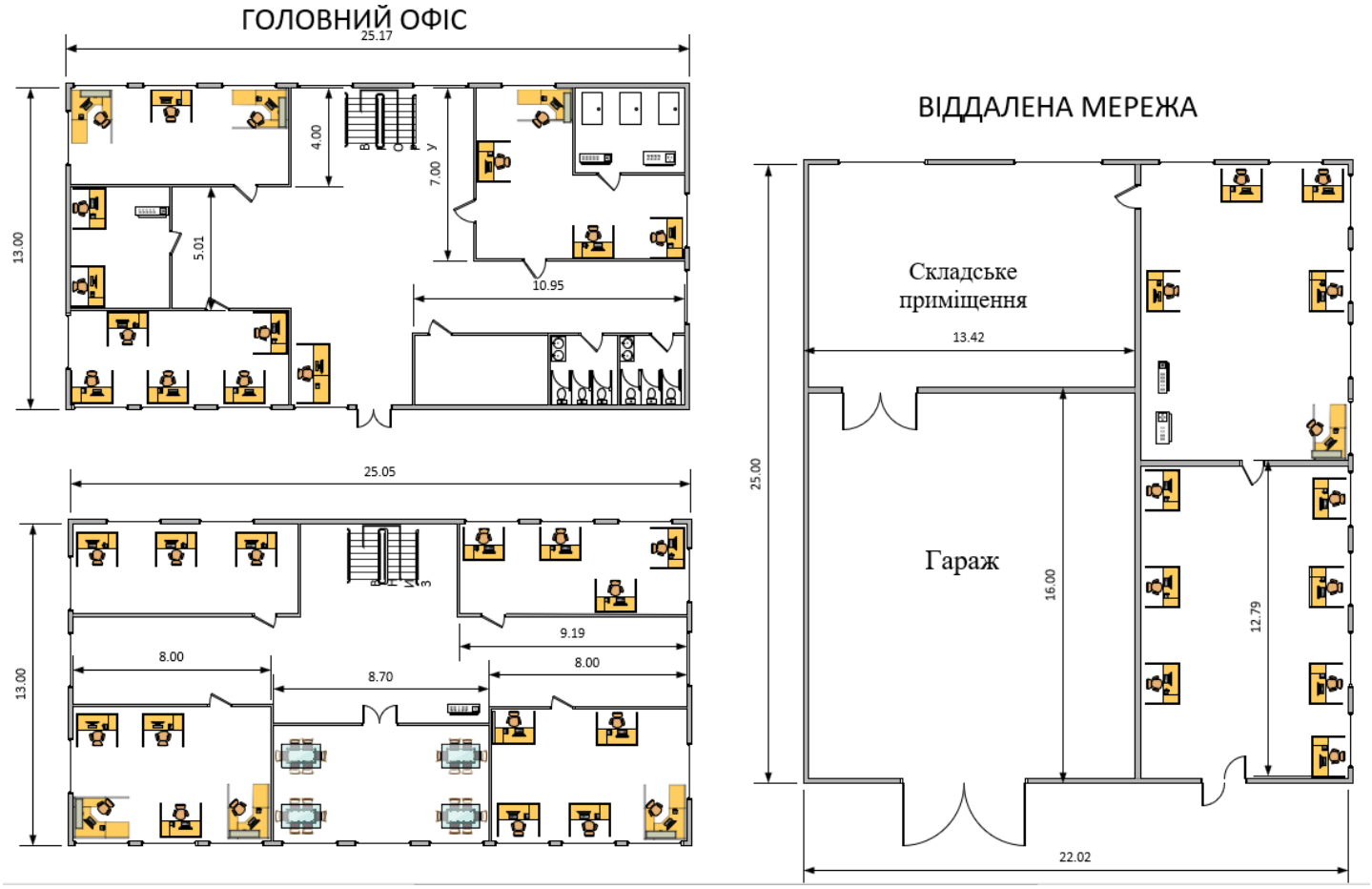


Рисунок 1.4 – Структурна схема підприємства

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

Інформаційне забезпечення компанії «Альфатех» здійснюється на основі декількох принципів, таких як:

1. Інтеграція - забезпечення взаємодії між різними системами та компонентами.

2. Автоматизація - використання програмного забезпечення та апаратних засобів для зменшення людських помилок та збільшення продуктивності роботи.
3. Захист інформації - застосування технічних та організаційних заходів для захисту інформації від несанкціонованого доступу, витоку, порушень цілісності та конфіденційності.
4. Орієнтованість на клієнта - врахування потреб та вимог клієнтів при розробці та впровадженні інформаційних рішень.

Технічні способи інформаційного забезпечення компанії включають в себе використання різноманітних інформаційних технологій та програмних засобів.

Загалом, інформаційне забезпечення компанії «Альфатех» базується на використанні передових технологій та методів, що дозволяють забезпечити високу ефективність та якість роботи. [3]

### 1.6 Аналітичний огляд існуючих способів обробки та передачі інформації

У компанії «Альфатех» використовуються різні способи обробки та передачі інформації. Для забезпечення ефективної роботи в компанії використовуються сучасні інформаційні технології та програмні засоби.

Один з найбільш важливих способів передачі інформації в компанії є електронна пошта. Цей спосіб передачі інформації є найбільш поширеним та доступним. Він дозволяє передавати повідомлення, документи та інші матеріали швидко та зручно, без необхідності фізично присутніх осіб. Крім того, електронна пошта може бути захищена від несанкціонованого доступу за допомогою різних методів шифрування та автентифікації.

Також в компанії використовуються спеціалізовані програмні засоби для передачі інформації, зокрема системи відеоконференції та месенджери. Вони дозволяють проводити зустрічі та обговорення проектів в онлайн-режимі, що дозволяє зберегти час та зменшити витрати на подорожі.

Крім того, компанія використовує спеціалізовану програмну систему для обліку та контролю за робочим часом працівників. Ця система дозволяє автоматизувати процеси обліку робочого часу та забезпечити точність розрахунку заробітної плати.[4]

Щодо обробки інформації, в компанії використовуються різні математичні методи та алгоритми для аналізу та оптимізації роботи. Наприклад, використовуються алгоритми машинного навчання для прогнозування та аналізу даних, що дозволяє забезпечити ефективну роботу техніки та зменшити витрати на її обслуговування. Крім того, в компанії застосовуються методи оптимізації роботи обладнання, що дозволяє забезпечити максимальну продуктивність та ефективність роботи. [4]

Загалом, в компанії «Альфатех» використовуються різні технічні та математичні засоби для забезпечення ефективної роботи техніки та персоналу, а також захисту інформації. Використання сучасних технологій та програмних засобів дозволяє компанії забезпечити максимальну ефективність та точність у роботі.

### 1.7 Постановка завдання та мета роботи

Основним завданням на кваліфікаційну роботу є розробка комп’ютерної системи компанії «Альфатех» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Під час виконання кваліфікаційної роботи слід виконати наступні пункти:

1. Аналіз потреб компанії у мережевому забезпеченні.
2. Визначення технічних вимог до мережі.
3. Розробка апаратної частини мережі, вибір обладнання та його специфікація.
4. Визначення топології мережі.

5. Розробка плану мережі. Необхідно розробити план мережі, який буде відображати всі складові мережі: топологію, типи з’єднань, розташування обладнання.
6. Розрахунок адресації для мережевого обладнання та вузлів.
7. Налаштування конфігурації мережевого обладнання та вузлів.
8. Тестування роботи мережі.
9. Розробка компонента системи на базі технології IoT.

### 1.8 Визначення можливих напрямків рішення поставлених завдань

Корпоративна мережа є складною інфраструктурою, що повинна задовольняти потреби компанії в передачі даних та забезпеченні безпеки і доступності інформації. В залежності від потреб компанії, можливі різні напрямки побудови корпоративної мережі.

Найпопулярнішим є варіант з побудовою провідної мережі. Цей варіант передбачає побудову мережі на основі кабельних з'єднань. Він є більш стійким і надійним, ніж бездротові мережі, і забезпечує високу швидкість передачі даних.

Також можливий варіант з побудовою бездротової мережі. Цей варіант передбачає побудову мережі на основі бездротових з'єднань. Він є більш гнучким і зручним, оскільки не потребує викладення кабелю, але може бути менш надійним та швидкість передачі даних може бути обмеженою.

Можливе використання комбінованого підходу: цей варіант передбачає використання комбінації провідних та бездротових мереж.

Корисним може бути використання віртуальних приватних мереж (VPN): цей варіант передбачає побудову мережі з використанням захищених каналів зв'язку. Він забезпечує безпеку передачі даних через Інтернет і може бути корисним для компаній з розподіленими командами або де працівники працюють з дому.

Кожен з цих напрямків має свої переваги та недоліки, і вибір конкретного напрямку буде залежати від потреб компанії, бюджету та інших

факторів. Для успішної побудови корпоративної мережі необхідно провести ретельний аналіз вимог, ресурсів та можливостей компанії та вибрати оптимальний напрямок для її побудови.

# 2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

## 2.1 Технічні вимоги до комп'ютерної системи

### 2.1.1 Вимоги до системи в цілому

#### 2.1.1.1 Вимоги до структури та функціонування системи

Для проєктування корпоративної мережі компанії замовник надав схему загальної архітектури, зображену на рисунку 2.1.

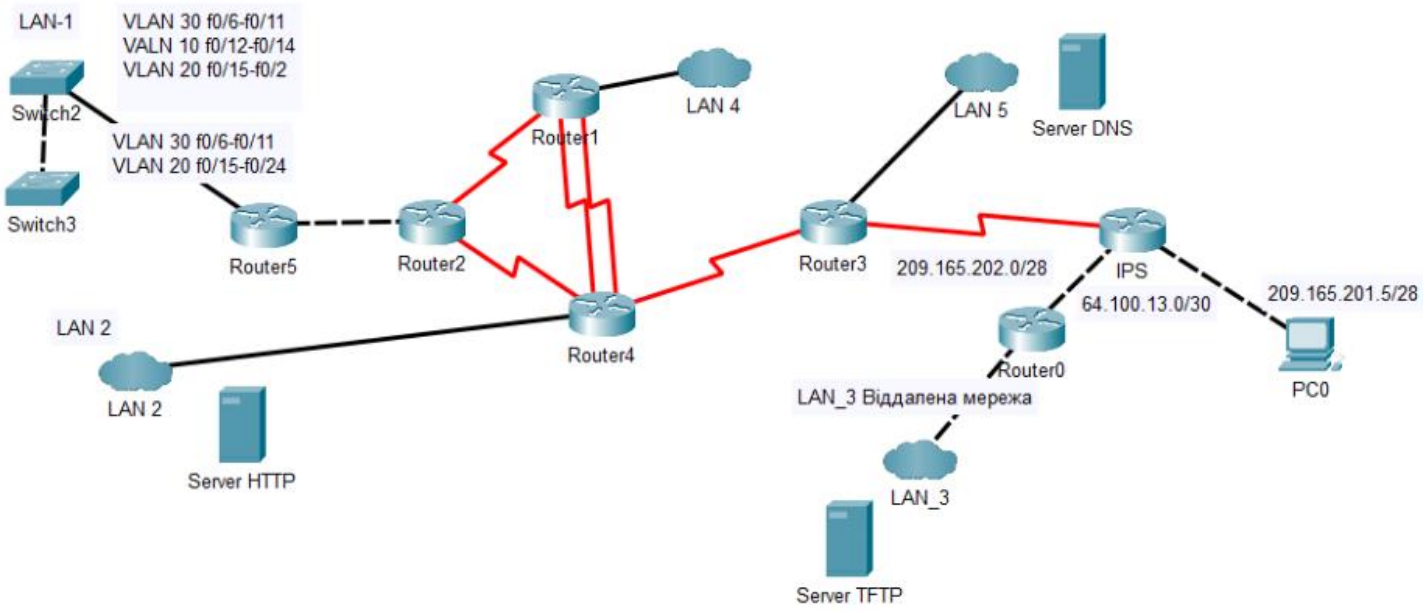


Рисунок 2.1 – Загальна архітектура мережі

Для кожної підмережі LAN замовник виділив відповідний відділ компанії:

LAN1 – відділ кадрів та фінансовий відділ (56 хостів);

LAN2 – відділ маркетингу (69 хостів);

LAN3 – відділ технічної підтримки (82 хости);

LAN4 – відділ продажу (56 хостів);

LAN5 – сервісний центр та відділ логістики та постачання (12 хостів);

#### 2.1.1.2 Вимоги до способів і засобів зв’язку між компонентами комп’ютерної системи

Для забезпечення зв’язку пристроїв в мережі необхідно використати наступні типи кабельних з’єднань:

- FastEthernet – для зв’язку з ПК;
- GigabitEthernet – для зв’язку підмереж з маршрутизаторами;
- Serial-інтерфейси – для каналів зв’язку між маршрутизаторами.

З’єднання між будівлями повинне виконуватися через VPN тунель. Всі пристрої мережі повинні мати з’єднання з мережею Internet.

Зв’язок між окремими відділами компанії необхідно забезпечити за допомогою налаштування протоколу динамічної маршрутизації.

Система повинна забезпечувати надійний зв'язок між компонентами комп'ютерної системи. Передача даних повинна бути безперервною і надійною, а кількість помилок повинна бути мінімальною.

#### 2.1.1.3 Вимоги до характеристик взаємозв'язків комп’ютерної системи

Протоколи зв'язку повинні бути спільними для створюваної системи та суміжних систем. Система повинна використовувати стек TCP/IP. Це забезпечить безперешкодну інтеграцію системи з іншими системами.

Усі зв’язки, які виконуються під час використання системи, повинні бути захищеними задля збереження конфіденційності інформації.

#### 2.1.1.4 Вимоги до режимів функціонування системи

Система повинна мати можливість працювати в безпечному середовищі, забезпечуючи захист від несанкціонованого доступу, зламів, втрати даних та інших загроз безпеці. Система повинна мати можливість відновлювати свою роботу після виникнення помилок або збоїв.

#### 2.1.1.5 Вимоги до діагностування системи

Кожні 3 місяці необхідно виконувати обстеження та діагностику стану, в якому знаходиться система, з метою виявлення та вирішення проблем та несправностей.

Повинен проводитись моніторинг стану системи, який включає збір і аналіз даних про різні параметри системи, такі як ресурси процесора, пам'ять, диски та мережеві підключення.

Також необхідний журнал подій, який збирає і реєструє інформацію про події, помилки, відомості про роботу системи та дії користувачів.

#### 2.1.1.6 Перспективи розвитку системи

Для забезпечення розвитку та модернізації комп’ютерної системи в майбутньому повинні виконуватися такі вимоги:

- система повинна бути побудована з використанням якісного та ліцензованого обладнання;
- інфраструктура мережі повинна забезпечувати масштабованість та розширення мережі. Система повинна бути гнучкою, щоб задовольняти зростаючі потреби компанії;
- для розвитку комп'ютерної системи потрібна кваліфікована команда інженерів;
- необхідно забезпечити постійне вдосконалення системи, оновлення технологій, вирішення проблем та впровадження нових функціональностей. Важливо бути в курсі останніх технологічних тенденцій і відповідати на зміни в бізнес-середовищі.

#### 2.1.1.7 Показники призначення

Комп'ютерна повинна дозволяти спілкуватися та обмінюватися інформацією між різними відділами і працівниками компанії, включаючи

передачу даних про клієнтів, замовлення, продукти, складські запаси, фінансову інформацію та інші дані, необхідні для ефективного ведення бізнесу.

Також система повинна дозволяти компанії ефективно керувати процесом продажу та взаємодіяти зі своїми клієнтами. Інформація про клієнтів, їхні замовлення, історія покупок та інші дані повинні бути централізовано збережені і доступні працівникам. Вона повинна відстежувати запаси спецтехніки, керувати поставками та логістикою, а також інформацією про наявність товарів на складі, розташування та рух товарів.

#### 2.1.1.8 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

##### 2.1.1.8.1 умови і регламент (режим) експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) системи з заданими технічними показниками, у тому числі види і періодичність обслуговування ТЗ чи системи

Для забезпечення безпечної та стабільної роботи системи, приміщення, в яких вона функціонує, повинні відповідати наступним вимогам:

- температура повітря у межах від +15 до +25 градусів за Цельсієм;
- вологість повітря не більше 75% при атмосферному тиску від 84 кПа до 107 кПа;
- напруга електромережі будівель повинна становити 220В з частотою 50 Гц.
- у приміщеннях, в яких функціонує система, повинна дотримуватися техніка пожежної безпеки;
- заборонено використання зволожувачів повітря у приміщеннях з мережевим обладнанням;

Необхідно дотримуватися усіх вимог, які вказані в документації до мережевого обладнання;

Система повинна забезпечувати функціонування при підвищенні температури повітря до 40 градусів.

**2.1.1.8.2 Вимоги до параметрів мереж енергопостачання (живлення та заземлення)**

Мережі енергопостачання повинні відповідати вимогам, стандартним на території України, а саме:

- стандартна напруга для однофазних мереж становить 220 Вольт. Частота електричного струму складає 50 герц;
- напруга та частота електричного струму повинні підтримуватись в межах допустимих відхилень. Допустимі відхилення для напруги становлять ±10%, а для частоти - ±1%;
- вимоги до заземлення включають належну електричну з'єднаність землі та електроустановок, що забезпечує безпеку електротехнічного обладнання та людей, а також допомагає уникнути статичної електрики та перенапруг;
- вимоги до якості електричного струму включають мінімізацію гармонік, флікеру, напругових переривань та інших спотворень, які можуть негативно впливати на роботу обладнання.

**2.1.1.8.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи**

Необхідно визначити достатню кількість спеціалістів, які зможуть забезпечити ефективне управління, моніторинг, технічну підтримку та розвиток мережі.

Цими завданнями займаються адміністратори системи у загальній кількості 25 працівників. Даний персонал повинен мати необхідну кваліфікацію та компетенції для роботи з комп'ютерною мережею. Це включає

знання про мережеві протоколи, оперативні системи, мережеве обладнання, засоби безпеки, а також навички в управлінні, розв'язанні проблем та комунікації з користувачами.

Режим роботи даного персоналу складається керівниками офісів, але кількість обслуговуючого персоналу, який знаходиться у офісі протягом робочого дня, не повинен складати менше 8 спеціалістів.

Обслуговуючий персонал повинен мати можливість постійного навчання та оновлення знань.

#### 2.1.1.8.4 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів

Комплект запасних виробів повинен включати основне мережеве обладнання, таке як комутатори, маршрутизатори, модеми, кабелі, конектори, адаптери тощо.

Запасні вироби повинні бути розміщені для зберігання у відповідних приміщеннях, де забезпечується відповідна температура, вологість та захист від пилу, вологи та пошкоджень. Необхідно мати впорядкований і доступний інвентарний облік запасних виробів.

Запасні вироби повинні бути збережені в захищених від стороннього доступу місцях, де забезпечується безпечне зберігання. Також необхідно встановити правила щодо перевірки та оновлення запасних виробів, щоб забезпечити їх готовність до використання.

До запасних виробів повинна бути прикладена відповідна документація та інструкції, які описують правила зберігання, використання та заміни запасних виробів. Це допоможе забезпечити правильне використання та обслуговування запасних виробів.

#### 2.1.1.8.5 Вимоги до регламенту обслуговування

Регламент включає перевірку та технічне обслуговування мережевого обладнання, перевірку стану інфраструктури мережі, оновлення програмного

забезпечення та інші необхідні дії. Регламент обслуговування повинен включати вимоги до системи моніторингу, яка надає можливість відстежувати стан мережі, виявляти проблеми та вчасно реагувати на них. Також регламент повинен включати вимоги до резервного копіювання даних та можливості відновлення мережі в разі відмови обладнання або втрати даних. Регламент повинен визначати вимоги до технічної підтримки мережі, включаючи контактну інформацію та режим реагування на заявки користувачів.

Вимоги до регламенту обслуговування повинні включати вимоги до оновлення програмного забезпечення та обладнання, а також до розвитку мережі з урахуванням потреб компанії. Це включає оцінку та впровадження нових технологій та розширення мережі для відповіді на зростаючі потреби.

#### 2.1.1.9 Вимоги до патентної чистоти

Першою вимогою є перевірка наявності ліцензій або інших дозволів для використання програмного забезпечення та інших технологічних ресурсів. Компанія повинна мати належні ліцензії на всі використовувані програми та технології. Рекомендується використання вільного програмного забезпечення (open-source software), яке має відповідні ліцензії та дозволи на використання. Використання такого програмного забезпечення знижує ризик порушення патентних прав.

Компанія повинна дотримуватись авторських прав при використанні інформації, матеріалів, зображень та інших ресурсів в мережі.

Компанія повинна проводити правовий аналіз щодо використання технологій та програмного забезпечення, а також документувати ліцензії, угоди та інші відповідні документи, які підтверджують легальність використання ресурсів.

### 2.1.2 Додаткові вимоги

#### 2.1.2.1 Вимоги до активного обладнання

Активне обладнання мережі повинно мати достатню пропускну здатність для передачі даних з вимогами до швидкості та масштабу мережі (1 Гбіт).

Обладнання повинно бути надійним і забезпечувати стабільну роботу мережі. Воно повинне забезпечувати мінімальну кількість відмов, високу стійкість до несправностей та можливість відновлення після виникнення проблем.

Активне обладнання мережі повинно бути сумісним з іншими пристроями і протоколами, що використовуються в мережі. Обладнання повинно мати можливості управління та моніторингу, що дозволяють адміністраторам контролювати та налаштовувати мережу. Також обладнання мережі повинно мати вбудовані заходи безпеки, що дозволяють захищати мережу від несанкціонованого доступу, атак та загроз.

#### 2.1.2.2 Вимоги до кабель-каналів, інформаційних та електричних розеток

Кабель-канали повинні бути виготовлені з якісних матеріалів і мати високу міцність, що забезпечує їх надійну роботу і довговічність. Вони повинні бути відповідним чином захищені від зовнішніх впливів, таких як волога, пил та удари.

Кабель-канали повинні відповідати вимогам пожежної безпеки, таким як встановлення негорючих матеріалів, додержання відстаней між кабелями та іншими елементами, забезпечення вентиляції та ефективного відведення тепла. Кабель-канали повинні бути легкими у монтажі та обслуговуванні. Вони повинні мати зручні кріплення, доступ до кабелів для проведення пересування або заміни, а також зручність у встановленні розеток та інших елементів.

Кабель-канали, інформаційні та електричні розетки повинні бути чітко позначені і ідентифіковані, щоб спростити установку, обслуговування та ремонт. Всі розетки повинні мати ступінь захисту не нижче IP20.

#### 2.1.2.3 Вимоги до комунікаційного обладнання і його розташування

Обладнання повинно розміщуватись у приміщеннях з контрольованими кліматичними умовами, щоб уникнути перегріву, конденсації і інших негативних впливів на його роботу.

Усе комунікаційне обладнання повинно бути забезпечене не менше, ніж 24 інтерфейсами FastEthernet. Комунікаційне обладнання повинно мати вбудовані засоби безпеки, такі як механізми аутентифікації, шифрування даних, захист від атак та вторгнень.

Комунікаційне обладнання повинно бути розташоване відповідно до нормативних вимог та рекомендацій. Необхідно враховувати вимоги до вентиляції, температури, вологості та інших параметрів середовища. Також необхідно враховувати фізичну доступність для обслуговування та розміщення в рекомендованих розподільних коробках чи шафах. Розташування повинно забезпечувати належну організацію кабельних систем для зменшення перешкод, запобігання пошкодженням кабелів і полегшення підключення.

#### 2.1.2.4 Вимоги до резервування

Під час виконання резервного копіювання даних у системі необхідно забезпечити регулярне створення копій, яке виконується у кінці робочого дня. Це дозволяє забезпечити актуальність копій і уникнути втрати важливих даних у разі відмови або випадкового видалення.

Процедури резервного копіювання повинні бути документовані, зрозумілі та доступні обслуговуючому персоналу. Копії даних повинні періодично перевірятися на цілісність, щоб впевнитися, що вони не

пошкоджені або неповні (перевірка хеш-сум та виконання тестового відновлення збережених даних).

Важливо застосовувати шифрування для захисту даних від несанкціонованого доступу. Ключі шифрування повинні бути безпечно зберігатися та доступні тільки обмеженому колу вповноважених осіб.

### 2.1.3 Вимоги до функцій, які виконує КС

Вимоги до функцій, які виконує комп'ютерна система компанії «Альфатех», включають наступні пункти:

1. Обробка даних: комп'ютерна система повинна забезпечувати ефективну обробку даних, включаючи збір, аналіз та зберігання даних.
2. Забезпечення безпеки даних: комп'ютерна система повинна забезпечувати захист даних компанії від несанкціонованого доступу, включаючи захист від вірусів, злочинних атак та інших загроз.
3. Підтримка роботи з документами: комп'ютерна система повинна забезпечувати підтримку роботи з документами, включаючи створення, редагування, зберігання та обмін документами між співробітниками компанії.
4. Підтримка різноманітних пристроїв: комп'ютерна система повинна підтримувати роботу з різноманітними пристроями.
5. Підтримка зв'язку: комп'ютерна система повинна забезпечувати підтримку зв'язку між співробітниками компанії, включаючи електронну пошту, чат, відеоконференції тощо.
6. Автоматизація бізнес-процесів: комп'ютерна система повинна допомагати автоматизувати бізнес-процеси компанії, включаючи управління запасами, фінансовий облік, збір та аналіз даних клієнтів та інше.

### 2.1.4 Вимоги до видів забезпечення

#### 2.1.4.1 Вимоги до інформаційного забезпечення

Інформаційна система повинна бути здатною працювати з ростом обсягу даних та збільшенням навантаження. Інформація повинна бути захищена від несанкціонованих змін, вилучень або порушень цілісності даних. Інформаційна система повинна бути надійною, що означає, що вона працездатна та доступна в будь-який час, коли її потребують користувачі.

Програмне забезпечення повинно бути зручним у використанні для користувачів комп'ютерної системи, щоб забезпечити ефективну роботу користувачів з системою.

Програмне забезпечення повинно мати підтримку від виробника або постачальника, щоб забезпечити коректну роботу системи та вчасну виправлення помилок. Програмне забезпечення повинно бути сумісним з операційною системою (Windows) та іншими програмами, які використовуються в комп'ютерній системі.

#### 2.1.4.2 Вимоги до лінгвістичного забезпечення

Комп'ютерна система повинна мати можливість працювати з різними мовами і забезпечувати підтримку багатомовності. Це включає переклад між мовами, визначення мови тексту автоматично та інші мовні операції. Комп'ютерна система повинна бути здатна до локалізації, тобто адаптації до конкретної мовної та культурної специфіки користувачів. Це включає переклад і адаптацію інтерфейсу користувача, форматування дат, часу, валют та інших локалізованих елементів.

#### 2.1.4.3 Вимоги до технічного забезпечення

Активне та комунікаційне обладнання мережі повинне закуповуватися у єдиного виробника – Cisco. Обладнання повинне постачатися у оригінальному пакуванні та комплектації.

Характеристики вузлів у мережі:

- чіп Ryzen трьохтисячної або п’ятитисячної серії або чіп Intel 8-10 покоління;
- оперативна пам’ять DDR4 8 гігабайт;
- графіка AMD Vega 7;
- жорсткий диск об’ємом не менше 500 Гб;
- блок живлення 450-600 ват;
- материнська плата повинна бути забезпечена усіма базовими інтерфейсами;
- наявність усієї базової комп’ютерної периферії.

У IoT системі зв’язок між пристроями повинен бути забезпечений з використанням технології бездротового зв’язку (Wi-Fi).

#### 2.1.4.4 Вимоги до організаційного забезпечення

В комп'ютерній системі повинен бути наявний кваліфікований персонал, який має достатні знання і навички для ефективного використання та управління системою.

Структура управління повинна бути чіткою та включати розподіл обов'язків та відповідальності між різними підрозділами та співробітниками. Це допомагає уникнути непорозумінь і забезпечити ефективну комунікацію та координацію роботи.

Організаційне забезпечення повинно включати резервне планування, яке описує дії у разі виникнення непередбачуваних ситуацій, таких як відмова обладнання, катастрофи, кібератаки тощо. Також воно повинне включати політики та процедури, спрямовані на забезпечення безпеки і конфіденційності інформації.

#### 2.1.4.5 Вимоги до методичного забезпечення

Методичне забезпечення повинно містити технічну документацію про комп'ютерну мережу, яка включає схеми мережі, конфігураційні файли, опис мережевого обладнання та інші технічні деталі. Воно повинно містити

інструкції щодо налаштування, встановлення, експлуатації та обслуговування комп'ютерної мережі. Також методичне забезпечення повинно включати навчальні матеріали, такі як презентації, відеоуроки та навчальні посібники, які допомагають персоналу компанії зрозуміти принципи роботи мережі, основні поняття і технології.

## 2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи

Виходячи із сформованих технічних вимог та аналізу структури компанії, проведеного у першому розділі, необхідно скласти структурну схему комплексу технічних засобів комп’ютерної системи (рисунок 2.2).

Схема складається з мережі Internet, рівня ядра (маршрутизатори), рівня доступу (комутатори) та рівня хостів (ПК користувачів). Зв’язок між провайдером та рівнем ядра реалізовано через Serial інтерфейси, зв’язок між рівнем ядра та рівнем доступу через Gigabit інтерфейси, зв’язок між рівнем доступу та рівнем хостів через FastEthernet інтерфейси.

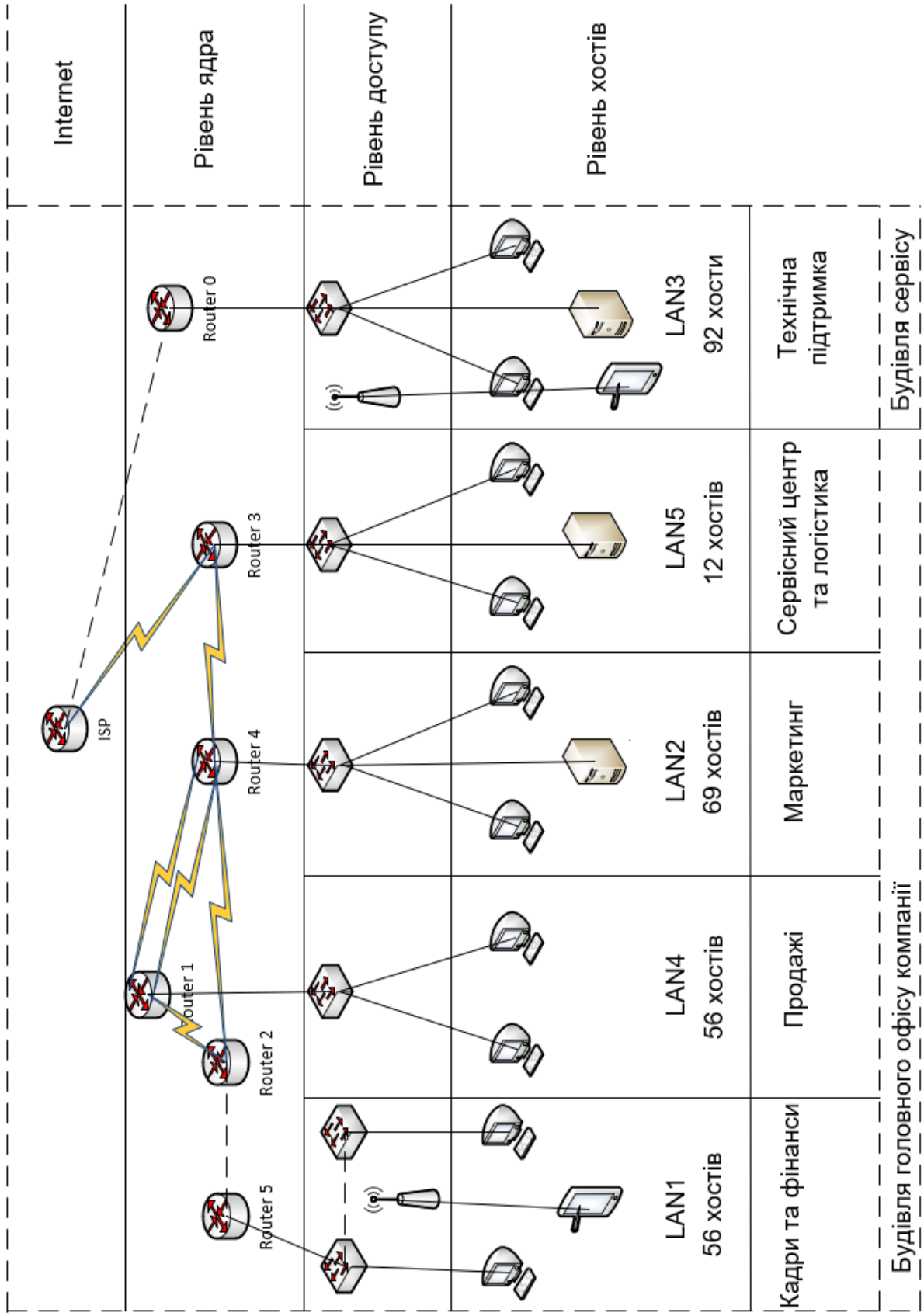


Рисунок 2.2 - Схема комплексу технічних засобів комп’ютерної системи

## 2.3 Розробка специфікації апаратних засобів комп'ютерної системи

Розглянемо специфікацію обладнання компанії на прикладі мережі віддаленого офісу LAN3.

Так як мережа віддаленого офісу невеликих розмірів, для неї було обрано маршрутизатор Cisco 1921-ADSL2/K9. Дана лінійка маршрутизаторів була розроблена спеціально для невеликих компаній та віддалених філіалів. Дані маршрутизатори мають 2 інтегрованих порти GigabitEthernet , компактний форм-фактор 1 RU та підтримують 1 інтегрований сервісний модуль (ISM). Також є 2 слоти розширення під модулі EHWIC.

Було обрано комутатор Cisco WS-C2960-24LC-S. Комутатор використовує технологію Cisco EnergyWise, яка дозволяє ефективно керувати споживанням електроенергії і знижувати витрати на електроенергію. Цей комутатор має вбудовані функції безпеки, такі як Access Control Lists (ACLs). Він підтримує різноманітні мережеві підключення, включаючи FastEthernet і GigabitEthernet порти.

Сервер було обрано моделі Cisco UCS C220 M3 LFF.

Для бездротового зв'язку з IoT компонентами було обрано маршрутизатор Cisco 881W-GN-A-K9. Даний тип маршрутизаторів має інтегровану точку доступу стандарту 802.11g для підтримки бездротових клієнтів.

Розроблену специфікацію наведено у таблиці 2.1.

Таблиця 2.1 – Специфікація обладнання офісу віддаленої мережі

| Позиція | Найменування і технічна характеристика | Тим, марка, позначення документа, опитувального листа | Одиниці виміру | Кількість | Примітки |
|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | Маршрутизатор Cisco 1921:<br>2 GE integrated;<br>2 EHWIC integrated;<br>512 MB DRAM, 256 MB flash memory. | Cisco 1921-ADSL2/K9 | од | 1 | Network Technology: 10/100/1000Base-T. Security Features: IPSec, SSL, AAA, PKI, Content Filtering, L2TP v3, GRE. |
| 2 | Комутатор Cisco WS-C2960-24LC-S:<br>24 x Fast Ethernet Network; 2 x Gigabit Ethernet Uplink;<br>64 MB DRAM; 32 flash. | Cisco WS-C2960-24LC-S | од | 1 | Management: RMON, SNMP v1,2c,3, VLAN, QoS, CLI, DHCP, Telnet, HTTP, HTTPS, Syslog. |
| 3 | Сервер Cisco UCS C220:<br>2 x Intel Xeon E5-2650L;<br>8 GB DDR3 (2 x 4 GB) | Cisco UCS C220 M3 LFF | од | 1 | RAID-контролер: Cisco UCS RAID SAS 2008M-8i Мережевий контролер: 2x порта 1 Gb Ethernet Віддалений доступ: Cisco Integrated Management Controller (CIMC) Блок живлення: 2 x 650 W |
| 4 | Маршрутизатор Cisco 881:<br>256 MB DRAM, 128 MB flash memory;<br>4 10/100BASE-T. | Cisco 881W-GN-A-K9 | од | 1 | Точка доступу стандарту IEEE 802.11n draft 2.0, сумісна 802.11 b/g; Автоматичний вибір швидкості передачі даних для 802.11g/n всеспрямовані антени 2x3 MIMO; Знімні антени |

Наступною розглянемо кабельну структуру віддаленого офісу компанії (рисунок 2.3).

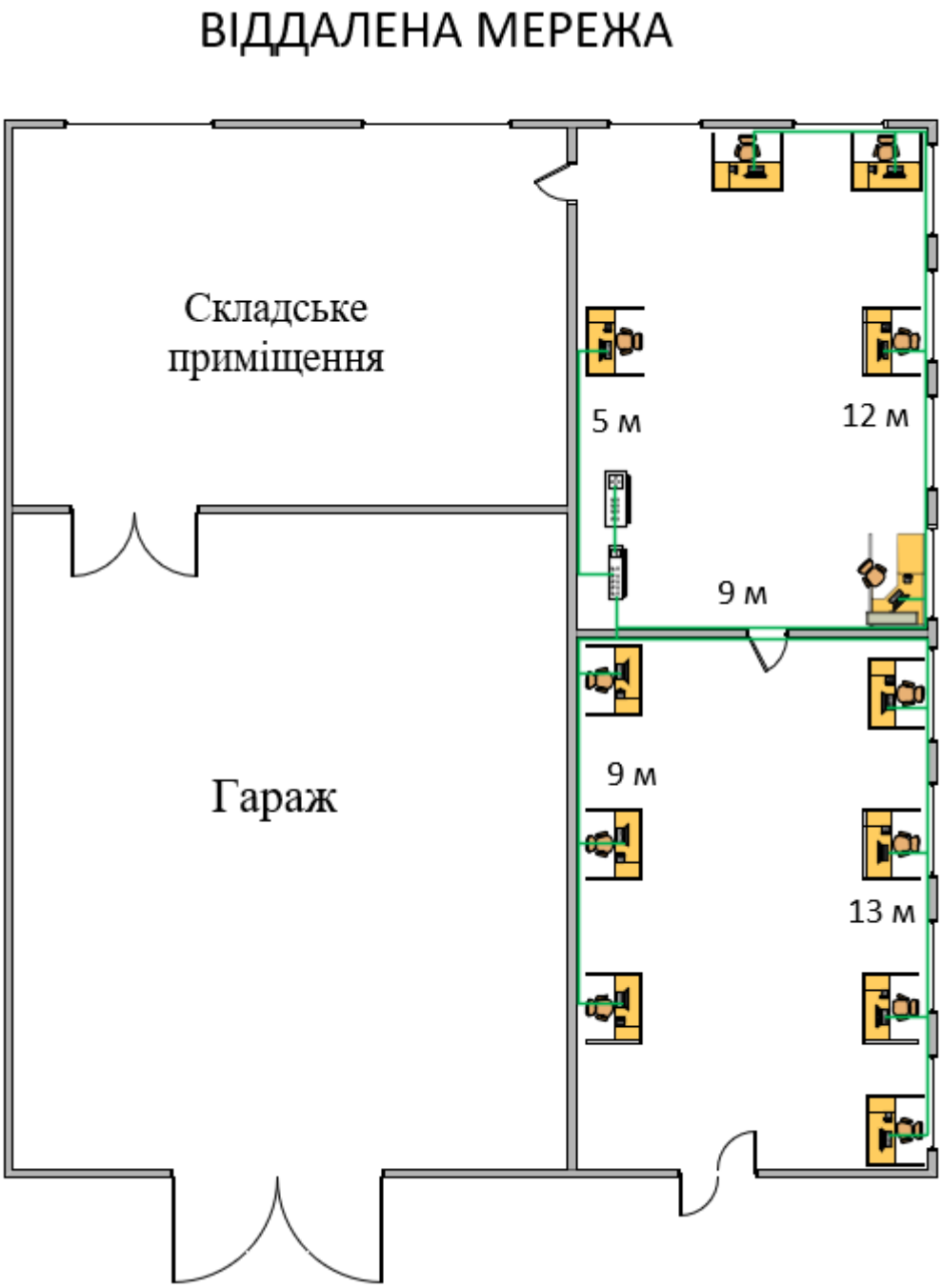


Рисунок 2.3 – Кабельна структура офісу віддаленої мережі

Специфікацію кабельної структури наведено в таблиці 2.2. Каблель-канали розміщуються на підлозі під стіною. Зв’язок вузлів з мережею реалізовується за допомогою інформаційних розеток RJ-45.

Таблиця 2.2 – Специфікація кабельної структури віддаленого офісу

| Позиція | Найменування і технічна характеристика | Тим, марка, позначення документа, опитувального листа | Одиниці виміру | Кількість | Примітки |
|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | Підлоговий кабельний канал 15х15мм | In-liner AERO | м | 50 | Алюмінієвий кабельний канал |
| 2 | Комп'ютерна розетка RJ45 UTP | Sven Comfort SE-60036-C | од | 12 | Клас захищеності: IP54 |
| 3 | Розетка із заземленням подвійна | Schneider Electric Sedna | од | 12 | Двогніздова<br>Полюси 2P + E, зі шторками<br>Вихід заземлення: бічний |
| 4 | Кабель UTP 0.48 | Каблекс | м | 60 | Тип ізоляції кабеля: ПВХ |
| 5 | Мідний провід ПВС 3х1 | МЕГА-КАБЕЛЬ™ | м | 90 | Ізоляція жил – ПВХ.<br>Струмове навантаження на провід ПВС 3х1 – 10 А. |

### 2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Найбільша підмережа має 82 вузли. Маршрутизація трафіку виконується в лінію з пропускною здатністю 1000 Мбіт/с.

Тоді, навантаження на маршрутизатор повинно бути не більше, ніж:

$$\mu_{вих}=\frac{1000000000}{650\times8}=192\ 300 \text{ пакетів/с (2.1)}$$

Кожен ПК у підмережі в середньому виробляє 105 пакетів. Виходячи з даного значення отримуємо максимальну кількість ПК, які можна під’єднати до мережі.

$$N=\frac{192300}{105}=1831 \text{ пристроїв (2.2)}$$

Для розрахунку інтенсивності трафіку помножимо кількість вузлів на середню кількість пакетів:

$$\lambda=82*105=8610 \text{ пакетів/с (2.3)}$$

Коефіцієнт затримки дорівнює:

$$\rho=\frac{\lambda}{\mu_{вих}}=8610/192300=0.04 \text{ (2.4)}$$

Коефіцієнт зайнятості маршрутизатора визначається за формулою:

$$\frac{\rho}{1-\rho}=\frac{0.04}{1-0.04}=0.04 \text{ (2.5)}$$

Середня затримка кадру, пов’язана з чергою M/M/1, дорівнює:

$$T=\frac{1}{\mu-\lambda}=\frac{1}{192300-8610}=5.4 \text{ мкс (2.6)}$$

Середня довжина черги дорівнює:

$$L_{чер}=\frac{\rho^2}{1-\rho}=\frac{0.04^2}{1-0.04}=0.0002 \text{ (2.7)}$$

Середній час перебування пакета в черзі дорівнює:

$$T_{оч}=\frac{L_{чер}}{\lambda}=\frac{0.0002}{8610}=23.2 \text{ нс (2.8)}$$

Пропускна здатність каналу дорівнює:

$$b=\lambda\times l=8610\times650\times8=44772000 \text{ біт/с} =44.7 \text{ Мбіт/с (2.10)}$$

# 3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

## 3.1 Розрахунок адресації мережі компанії «Альфатех»

Для проєктування корпоративної мережі компанії виділено блок адрес 10.23.48.0/22. В таблиці 3.1 вказано кількість вузлів для кожної з 5 підмереж компанії, виходячи з цих даних буде виконуватися розбиття головного блоку адрес на підмережі.

Таблиця 3.1 – Виділений блок адрес

| № | Блок адрес | LAN1 | LAN2 | LAN3 | LAN4 | LAN5 |
|---|---|---|---|---|---|---|
| 9 | 10.23.48.0/22 | 56 | 69 | 82 | 56 | 12 |

Для кожної LAN маємо відповідний відділ компанії:

LAN1 – відділ кадрів;

LAN2 – відділ фінансів;

LAN3 – відділ сервісу та технічної підтримки;

LAN4 – відділ продажів;

LAN5 – відділ логістики та постачання.

Для ефективного використання простору адрес розрахунок підмереж буде виконуватися за допомогою методу маски змінної довжини (VLSM). Даний метод дозволяє виділяти блоки адрес розміром ступеню двійки. У кожній виділеній підмережі дві адреси використовуються для адреси мережі та широкомовної адреси, це варто враховувати при виділенні розміру для деяких підмереж. Для того, щоб запобігти накладанню адрес, розрахунок за методом VLSM необхідно виконувати від найбільшої за розміром підмережі, до найменшої.

Найбільша підмережа (LAN3) має 82 вузли. Для того, щоб виконати розрахунок адреси підмережі, необхідно перевести частину мережі до двійкового вигляду, що дасть змогу зручніше оперувати бітами. Після цього необхідно визначитись з кількістю адрес, які буде виділено для підмережі.

Найменша кількість адрес, яку можна виділити для 82 вузлів – 128 ($2^7$). Тому відділимо з кінця адреси 7 біт.

10.23.00110000.0|0000000

Якщо перевести адресу мережі назад до десятинного вигляду, то отримаємо адресу підмережі LAN3 – 10.23.48.0/25. Виходячи з цього діапазон адрес, доступних для вузлів у підмережі, становитиме від 10.23.48.0 – 10.23.48.126. Широкомовна адреса – 10.23.48.127.

Наступним проведемо розрахунок адресації для підмережі LAN1, хоч дана підмережа і менша за розміром від LAN2, виділимо їй 128 ($2^7$) адрес, так як дана підмережа потребує розбиття на віртуальні локальні мережі за технологією VLAN.

Перед початком розрахунку збільшимо значення мережевої частини адреси на 1 біт. Знову відділимо 7 біт з правого боку адреси.

10.23.00110000.1|0000000

Якщо перевести адресу мережі назад до десятинного вигляду, то отримаємо адресу підмережі LAN1 – 10.23.48.128/25. Виходячи з цього діапазон адрес, доступних для вузлів у підмережі, становитиме від 10.23.48.129 – 10.23.48.254. Широкомовна адреса – 10.23.48.255.

Аналогічні розрахунки виконуються для LAN2.

Адреса мережі: 10.23.49.0/25.

Діапазон адрес: 10.23.49.1 – 10.23.49.126.

Широкомовна адреса: 10.23.49.127.

Аналогічні розрахунки виконуються для LAN4.

Адреса мережі: 10.23.49.128/26.

Діапазон адрес: 10.23.49.129 – 10.23.49.190.

Широкомовна адреса: 10.23.49.191.

Аналогічні розрахунки виконуються для LAN5.

Адреса мережі: 10.23.49.192/28.

Діапазон адрес: 10.23.49.193 – 10.23.49.206.

Широкомовна адреса: 10.23.49.207.

Результати розрахунків наведено у таблиці 3.2.

Таблиця 3.2 – Схема адресації мережі

| Підмережа | Розмір | Виділений розмір | Адреса | Маска | Діапазон доступних адрес |
|---|---|---|---|---|---|
| LAN1 | 56 | 128 | 10.23.48.128 | /25 | 10.23.48.129 - 10.23.48.254 |
| LAN2 | 69 | 128 | 10.23.49.0 | /25 | 10.23.49.1 - 10.23.64.126 |
| LAN3 | 82 | 128 | 10.23.48.0 | /25 | 10.23.48.1 - 10.23.48.126 |
| LAN4 | 56 | 64 | 10.23.49.128 | /26 | 10.23.49.129 - 10.23.49.190 |
| LAN5 | 12 | 16 | 10.23.49.192 | /28 | 10.23.49.193 - 10.23.49.206 |

Для каналів, які забезпечують зв’язок між маршрутизаторами, виділено блок адрес 10.1.9.0/24. Провівши розрахунок за методом VLSM виділимо 6 підмереж по 4 адреси для кожного каналу. Результати розрахунку наведено у таблиці 3.3.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами

| Підмережа | Розмір | Виділений розмір | Адреса | Маска | Діапазон доступних адрес |
|---|---|---|---|---|---|
| WAN1 | 2 | 2 | 10.1.9.0 | /30 | 10.1.9.1 - 10.1.9.2 |
| WAN2 | 2 | 2 | 10.1.9.4 | /30 | 10.1.9.5 - 10.1.9.6 |
| WAN3 | 2 | 2 | 10.1.9.8 | /30 | 10.1.9.9 - 10.1.9.10 |
| WAN4 | 2 | 2 | 10.1.9.12 | /30 | 10.1.9.13 - 10.1.9.14 |
| WAN5 | 2 | 2 | 10.1.9.16 | /30 | 10.1.9.17 - 10.1.9.18 |
| WAN6 | 2 | 2 | 10.1.9.20 | /30 | 10.1.9.21 - 10.1.9.22 |

### 3.2 Розрахунок адресації пристроїв

Після проведення усіх розрахунків необхідно призначити отримані адреси інтерфейсам маршрутизаторів.

Результати наведено у таблиці 3.4.

Таблиця 3.4 – Схема адресації маршрутизаторів

| Пристрій | Інтерфейс | IP-адреса | Маска |
|---|---|---|---|
| Matiushyn_Router_0 | Gig0/0 | 64.100.13.2 | 255.255.255.252 |
| | Gig0/1 | 10.23.48.1 | 255.255.255.128 |

Продовження таблиці 3.4

| Пристрій | Інтерфейс | IP-адреса | Маска |
|---|---|---|---|
| Matiushyn_Router_1 | Gig0/0 | 10.23.49.129 | 255.255.255.192 |
| | Se0/2/0 | 10.1.9.18 | 255.255.255.252 |
| | Se0/2/1 | 10.1.9.22 | 255.255.255.252 |
| | Se0/3/1 | 10.1.9.13 | 255.255.255.252 |
| Matiushyn_Router_2 | Gig0/0 | 10.1.9.5 | 255.255.255.252 |
| | Se0/3/0 | 10.1.9.10 | 255.255.255.252 |
| | Se0/3/1 | 10.1.9.14 | 255.255.255.252 |
| Matiushyn_Router_3 | Gig0/0 | 10.1.9.5 | 255.255.255.240 |
| | Se0/3/0 | 10.1.9.10 | 255.255.255.252 |
| | Se0/3/1 | 10.1.9.14 | 255.255.255.252 |
| Matiushyn_Router_4 | Gig0/0 | 10.23.49.1 | 255.255.255.128 |
| | Se0/2/0 | 10.1.9.17 | 255.255.255.252 |
| | Se0/2/1 | 10.1.9.21 | 255.255.255.252 |
| | Se0/3/0 | 10.1.9.9 | 255.255.255.252 |
| | Se0/3/1 | 10.1.9.2 | 255.255.255.252 |
| Matiushyn_Router_5 | Gig0/0 | 10.1.9.6 | 255.255.255.252 |
| | Gig0/0.19 | 10.23.48.129 | 255.255.255.224 |
| | Gig0/0.29 | 10.23.48.161 | 255.255.255.224 |
| | Gig0/0.39 | 10.23.48.193 | 255.255.255.224 |
| | Gig0/0.99 | 10.23.48.225 | 255.255.255.240 |
| Matiushyn_Router_ISP | Gig0/0 | 64.100.13.1 | 255.255.255.252 |
| | Gig0/1 | 209.165.201.1 | 255.255.255.240 |
| | Se0/3/0 | 209.165.202.1 | 255.255.255.252 |

Також необхідно привласнити адреси SVI-інтерфейсам комутаторів у мережі. Адреси інтерфейсів наведено у таблиці 3.5.

Таблиця 3.5 – IP-адреси комутаторів у підмережах

| Підмережа | Пристрій | IP-адреса SVI інтерфейсу | Маска підмережі | Адреса шлюзу |
|---|---|---|---|---|
| LAN1 | Matiushyn_Switch_2 | 10.23.48.226 | 255.255.255.240 | 10.23.48.225 |
| | Matiushyn_Switch_3 | 10.23.48.227 | 255.255.255.240 | 10.23.48.225 |
| LAN2 | Matiushyn_Switch_5 | 10.23.49.2 | 255.255.255.128 | 10.23.49.1 |

Продовження таблиці 3.5

| Підмережа | Пристрій | IP-адреса SVI інтерфейсу | Маска підмережі | Адреса шлюзу |
|---|---|---|---|---|
| LAN3 | Matiushyn_Switch_0 | 10.23.48.2 | 255.255.255.128 | 10.23.48.1 |
| LAN4 | Matiushyn_Switch_4 | 10.23.49.130 | 255.255.255.192 | 10.23.49.129 |
| LAN5 | Matiushyn_Switch_1 | 10.23.49.194 | 255.255.255.240 | 10.23.49.193 |

### 3.3 Налаштування моделі комп’ютерної системи

Після всіх розрахунків необхідно побудувати логічну топологію мережі у середовищі Cisco Packet Tracer. Топологію наведено на рисунку 3.1. На топології вказано усі розраховані підмережі компанії, мережеві пристрої та їх з’єднання.

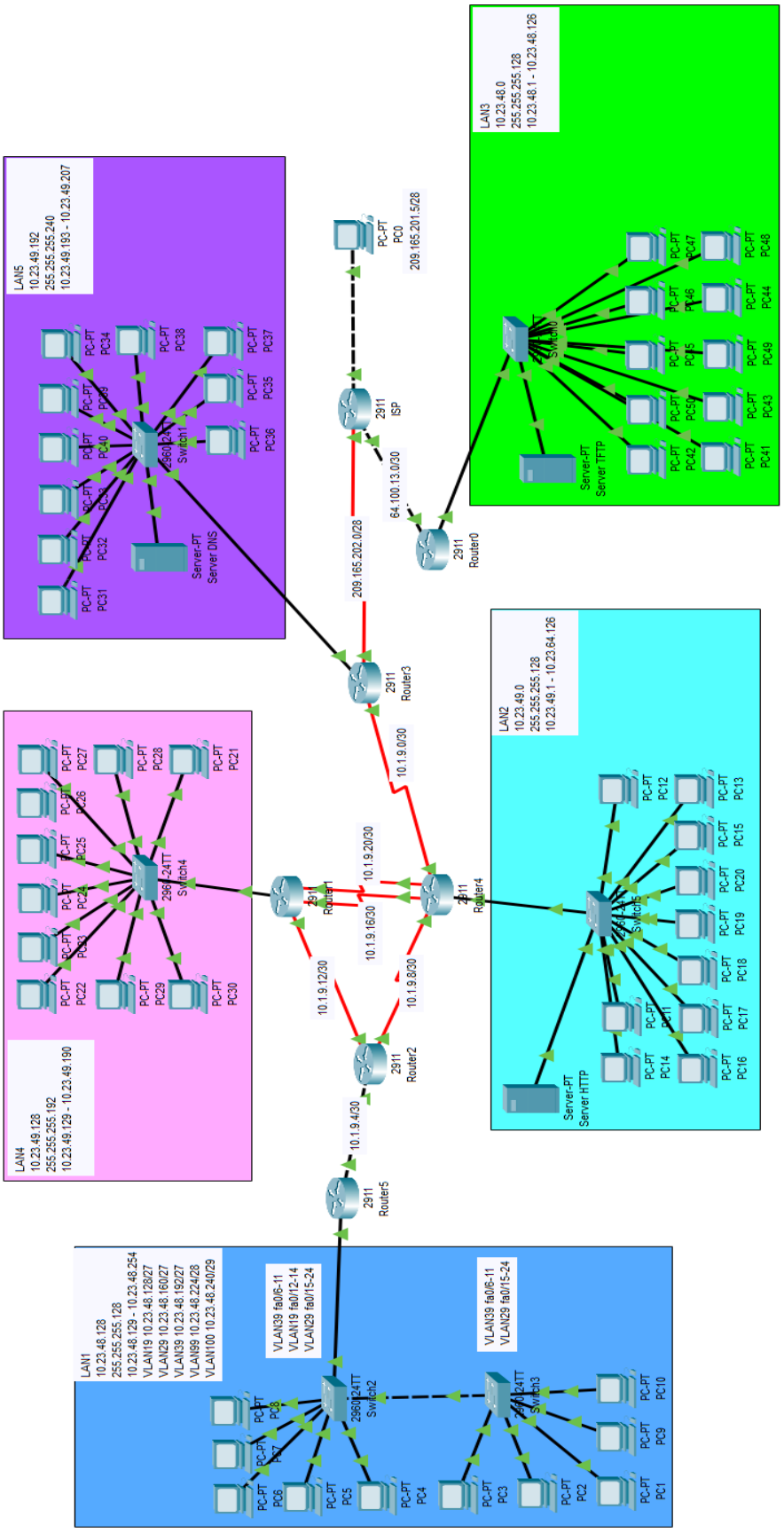


Рисунок 3.1 – Логічна топологія мережі

## 3.4 Налаштування та перевірка роботи комп’ютерної системи

### 3.4.1 Базове налаштування конфігурації пристроїв

На маршрутизаторах та комутаторах мережі необхідно виконати налаштування базової конфігурації. Необхідно надати кожному пристрою назву, встановити банер MOTD, налаштувати паролі для ліній vty та consol та привілейованого режиму. Усі паролі повинні бути зашифровані. Також необхідно створити користувача з доменним ім’ям, створити ключ за алгоритмом RSA та налаштувати використання протоколу SSH. Приклад налаштування базової конфігурації наведено нижче.

```
Enable //Переходимо до привілейованого режиму
Conf t //Переходимо в режим конфігурації
Hostname Matiushyn_Router_1 //Призначення імені пристрою
//Налаштування паролю для ліній vty та consol
Line console 0
Password cisco
Login
Line vty 0 15
Password cisco
Login
Enable secret class //Встановлення паролю для привілейованого режиму
Service password-encryption //Шифрування паролів
Banner motd ‘Matiushyn_Router_1’ //Налаштування банеру MOTD
ip domain-name Matiushyn_Router_1 //Створення доменного імені
Crypto key generate rsa //Генерування ключа RSA довжиною 1024 біт
1024
Username 123191_Matiushyn password admincisco //Сворення
користувача
//Налаштування використання протоколу SSH на лініях vty
Line vty 0 15
Transport input ssh
Login local
```

### 3.4.2 Налаштування маршрутизаторів

Після налаштування базової конфігурації на мережевих пристроях необхідно виконати налаштування маршрутизаторів. В першу чергу необхідно забезпечити маршрутизацію пакетів між підмережами, для цього використаємо протокол динамічної маршрутизації OSPF. Даний протокол буде поширювати адреси вказаних мереж з його таблиці маршрутизації на всі інтерфейси окрім тих, які вказані як пасивні. У якості пасивних інтерфейсів вкажемо інтерфейси локальних мереж, щоб не створювати зайвий трафік.

Приклад налаштування протоколу OSPF на маршрутизаторі наведено нижче.

```
router ospf 1 //Вмикаємо протокол
 passive-interface GigabitEthernet0/0 //Налаштовуємо інтерфейс локальної мережі у якості пасивного
//Вказуємо перелік мереж, які повинен поширювати маршрутизатор
 network 10.23.49.0 0.0.0.127 area 0
 network 10.1.9.16 0.0.0.3 area 0
 network 10.1.9.20 0.0.0.3 area 0
 network 10.1.9.8 0.0.0.3 area 0
 network 10.1.9.0 0.0.0.3 area 0
```

Також необхідно виконати налаштування статичних машрутів на пограничному машрутизаторі мережі. Першим створимо статичний машрут за замовчуванням, вказавши адресу інтерфейсу Se0/3/0 маршрутизатора ISP як наступний перехід.

```
ip route 0.0.0.0 0.0.0.0 209.165.202.1 //Створення статичного маршруту за замовчуванням
```

Далі налаштуємо статичний машрут, який буде забезпечувати доступ до мережі провайдера.

```
ip route 209.165.201.0 255.255.255.240 209.165.202.1 //Створення статичного маршруту до мережі провайдера
```

На всіх DCE-інтерфейсах машрутизаторів мережі необхідно встановити частоту 128000 та пропускну здатність 128. Приклад налаштування наведено нижче.

```
interface Serial0/3/0 //Вибір DCE-інтерфейсу
bandwidth 128 //Встановлення пропускної здатності
clock rate 128000 //Встановлення частоти
```

Після цього необхідно реалізувати використання служби AAA для аутентифікації на маршрутизаторах компанії. Під час налаштування необхідно призначити адресу віддаленого Radius-серверу, налаштувати аутентифікацію до консолі за протоколом Radius, а також створити локальну базу користувачів для аутентифікації на той випадок, якщо з'єднання з Radius-сервером відсутнє. У ролі Radius-сервера виступає DNS-сервер мережі компанії. Приклад налаштування служби AAA наведено нижче.

```
aaa new-model //Створення нової AAA-моделі
radius-server host 10.23.49.206 auth-port 1645 key radius123
//Призначення адреси віддаленого Radius-сервера
local //Встановлення аутентифікації на лінії consol за протоколом Radius
aaa authentication login CONSOLE group radius
line console 0
login authentication CONSOLE
//Створення локальної бази користувачів
aaa authentication login default local
username 123191_Matiushyn password admin123 //Створення
користувача
line vty 0 15
login authentication default
```

Для того, щоб забезпечити роботу служби AAA, необхідно налаштувати конфігурацію Radius-сервера. Налаштування зображено на рисунку 3.2.

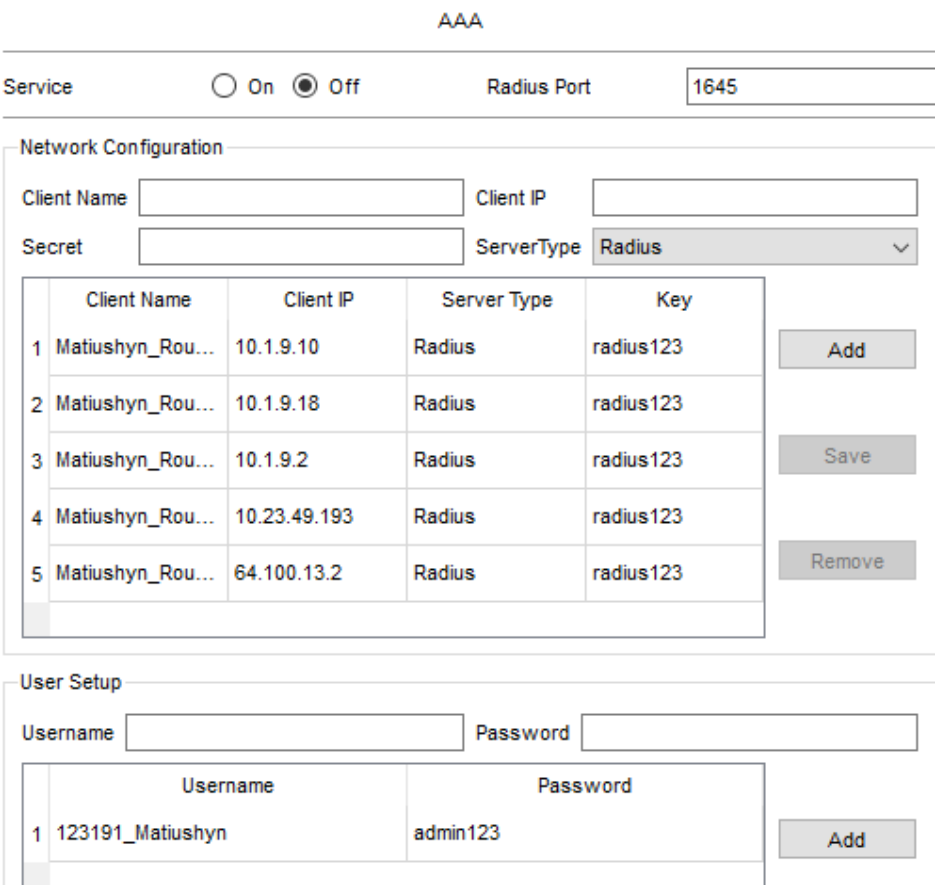


Рисунок 3.2 – Конфігурація Radius-сервера

### 3.4.3 Налаштування роботи Інтернет

Щоб забезпечити доступ до мережі інтернет з локальної мрежі компанії, необхідно виконати налаштування технології динамічного NAT на пограничних маршрутизаторах головного та віддаленого офісів. Динамічний NAT використовує виділений пул глобальних адрес для призначення хостам, які намагаються отримати доступ до інтернету. Для трансляції адрес було виділено наступний пул адрес: від 209.165.200.5 по 209.165.200.30.

Динамічний NAT виконує трансляцію трафіку звіряючись з призначеним ACL-списком, тому для його роботи необхідно створити такий список. В даному списку вкажемо трафік, який буде забороненим для трансляції (в нашому випадку це увесь трафік, який надходить з мережі головного офісу до мережі віддаленого) та дозволимо весь інший трафік. Приклад налаштування ACL-списку для NAT наведено нижче.

```
ip access-list extended NAT9 //Створюємо новий ACL-список
//Вказуємо увесь трафік, якому буде заборонено трансляцію
 deny ip 10.23.49.192 0.0.0.15 10.23.48.0 0.0.0.127
deny ip 10.23.48.128 0.0.0.127 10.23.48.0 0.0.0.127
deny ip 10.23.49.0 0.0.0.127 10.23.48.0 0.0.0.127
deny ip 10.23.49.128 0.0.0.63 10.23.48.0 0.0.0.127
deny ip 10.1.9.0 0.0.0.255 10.23.48.0 0.0.0.127
//Дозволяємо увесь інший трафік, який надходить з підмереж головного офісу компанії
permit ip 10.23.49.192 0.0.0.15 any
permit ip 10.23.48.128 0.0.0.127 any
permit ip 10.23.49.0 0.0.0.127 any
permit ip 10.23.49.128 0.0.0.63 any
permit ip 10.1.9.0 0.0.0.255 any
```

Після цього необхідно створити NAT-пул, з якого будуть обиратися адреси для трансляції. Приклад наведено нижче.

```
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
```

Після цього необхідно увімкнути трансляцію, призначивши використання створеного ACL-списку та пулу адрес. Приклад наведено нижче.

```
ip nat inside source list NAT9 pool Internet
```

Після цього налаштуємо внутрішній та зовнішній інтерфейси машрутизатора.

```
interface Serial0/3/0
ip nat outside //Призначення інтерфейсу статусу зовнішнього
interface Serial0/3/1
ip nat inside //Призначення інтерфейсу статусу внутрішнього
```

За вимогою замовника необхідно налаштувати HTTP-сервер таким чином, щоб щоб на вузлах при введенні в рядку браузера http://123.dnipro.ua (http://209.165.200.4) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу. Щоб реалізувати дану функцію необхідно

налаштувати статичну трансляцію локальної адреси сервера в адресу 209.165.200.4, а також виконати налаштування DNS-сервера таким чином, щоб доменному імені 123.dnipro.ua відповідала глобальна адреса 209.165.200.4.

Спершу налаштуємо статичну трансляцію NAT на пограничному машрутизаторі мережі.

```
ip nat inside source static 10.23.49.19 209.165.200.4
```

Далі створимо доменне ім’я 123.dnipro.ua на DNS-сервері (рисунок 3.3).

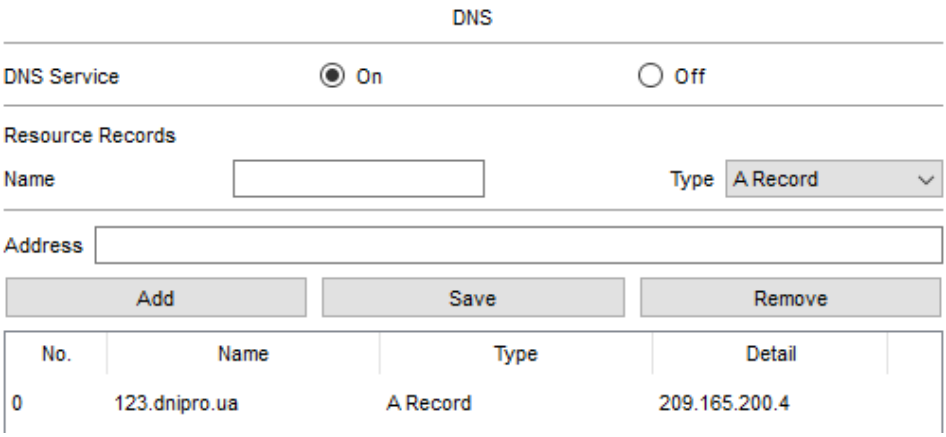


Рисунок 3.3 – Створення доменного імені

Створений сайт показано на рисунку 4.4.

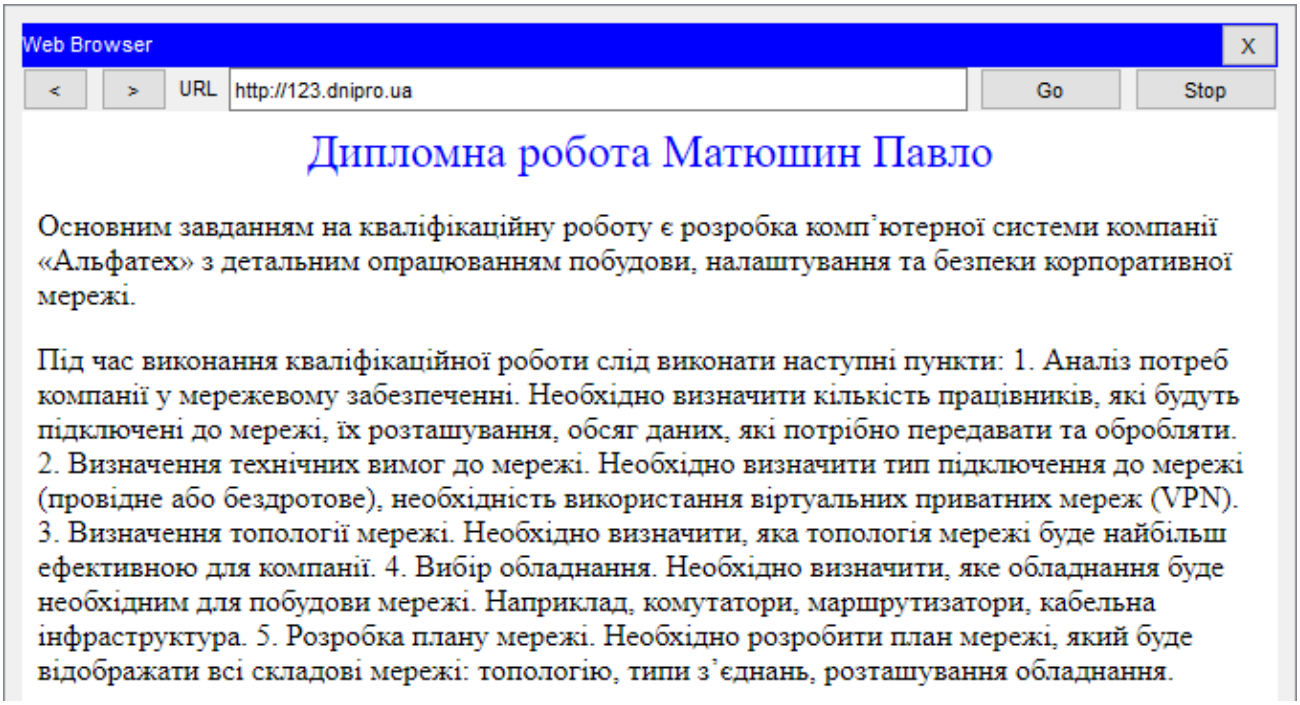


Рисунок 3.4 – Створений сайт

Для того, щоб забезпечити зв’язок між головним та віддаленим офісами компанії, необхідно створити захищений канал передачі даних за допомогою використання технології VPN на основі протоколу IPsec. Дана технологія потребує створення ACL-списку, за яким вона буде обирати трафік, який буде шифруватися та передаватися через канал. Створений ACL-список з пограничного машрутизатора головного офісу наведено нижче.

```
ip access-list extended VPN9 //Створюємо новий список
//Дозволяємо проходження трафіку з підмереж головного офісу до мережі віддаленого офісу
permit ip 10.23.49.192 0.0.0.15 10.23.48.0 0.0.0.127
permit ip 10.23.48.128 0.0.0.127 10.23.48.0 0.0.0.127
permit ip 10.23.49.0 0.0.0.127 10.23.48.0 0.0.0.127
permit ip 10.23.49.128 0.0.0.63 10.23.48.0 0.0.0.127
permit ip 10.1.9.0 0.0.0.255 10.23.48.0 0.0.0.127
```

Далі необхідно виконати конфігурацію маршрутизатора на роботу VPN. Приклад налаштування наведено нижче.

```
license boot module c2900 technology-package securityk9 //Вмикаємо модуль безпеки, необхідний для роботи протоколу
 crypto isakmp policy 10 //Створюємо нову політику ISAKMP
 encr 3des //Встановлюємо використання алгоритму 3des для шифрування даних
 hash md5 //Налаштовуємо hash
 authentication pre-share //Обираємо тип аутентифікації
 group 2 //Обираємо групу
crypto isakmp key cisco address 64.100.13.2 //Створюємо ключ cisco та вказуємо адресу зовнішнього інтерфейсу пограничного маршрутизатора віддаленого офісу
crypto ipsec transform-set TS esp-3des esp-md5-hmac //Створюємо набір перетворень
crypto map MAP 10 ipsec-isakmp //Створюємо нове криптографічне зіставлення
 set peer 64.100.13.2 // Вказуємо адресу зовнішнього інтерфейсу пограничного маршрутизатора віддаленого офісу
```

set transform-set TS //Встановлюємо використання створеного набору перетворень

match address VPN9 //Вказуємо використання створеного ACL-списку

interface Serial0/3/0

crypto map MAP //Вмикаємо роботу зіставлення на зовнішньому інтерфейсі машрутизатора

На пограничному маршрутизаторі віддаленого офісу було виконано аналогічні налаштування.

## 3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

### 3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Захист інформації в комп'ютерній системі є важливим аспектом забезпечення безпеки даних. Існує багато методів і технік, які можна використовувати для захисту інформації в комп'ютерній системі. Ось декілька найпоширеніших методів:

Встановлення паролів: Використання сильних паролів для всіх облікових записів і зміна їх регулярно. Краще використовувати комбінацію великих і малих літер, цифр і спецсимволів.

Шифрування даних: Використання шифрування для захисту конфіденційних даних. Шифрування може бути застосоване до файлів, дискових просторів, електронної пошти, з'єднань тощо.

Оновлення програмного забезпечення: Регулярне оновлення всіх програм, операційних систем і антивірусного програмного забезпечення на комп'ютерних системах, оскільки вони містять виправлення для виявлених вразливостей.

Використання фаєрволу: Встановлення програмного або апаратного забезпечення фаєрволу, яке контролює мережевий трафік і блокує небажані з'єднання або атаки.

Антивірусне програмне забезпечення: Встановлення надійного антивірусного програмного забезпечення та регулярне оновлюйте його визначення, щоб виявляти інфіковані файли та шкідливі програми.

Заборона доступу: Встановлення належної політики доступу до даних і ресурсів. Обмеження доступу до конфіденційної інформації лише необхідним користувачам.

### 3.5.2 Налаштування віртуальних мереж VLAN

У підмережі LAN1 головного офісу компанії необхідно реалізувати технологію VLAN. Потреба використання даної технології виникла через бажання замовника розділити робітників на три робочі групи. Створені віртуальні локальні мережі наведено у таблиці 3.6.

Таблиця 3.6 – Мережі VLAN

| Номер VLAN | Ім’я VLAN | Примітка |
|---|---|---|
| 19 | VLAN19 | Закупівля техніки |
| 29 | VLAN29 | Зв’язок з клієнтами |
| 39 | VLAN39 | Закупівля запчастин |
| 1 | Default | Не використовується |
| 99 | Management | Для керування пристроями |
| 100 | Native | Власна |

Після розподілення робітників на групи необхідно виконати розрахунок адресації для підмереж VLAN. Результати розрахунку за методом VLSM наведено у таблиці 3.7.

Таблиця 3.7 – Схема адресації VLAN

| Назва підмережі | Розмір | Виділений розмір | Адреса | Маска | Діапазон доступних адрес |
|---|---|---|---|---|---|
| VLAN19 | 32 | 32 | 10.23.48.128 | /27 | 10.23.48.129–10.23.48.158 |
| VLAN29 | 32 | 32 | 10.23.48.160 | /27 | 10.23.48.161–10.23.48.190 |
| VLAN39 | 32 | 32 | 10.23.48.192 | /27 | 10.23.48.193–10.23.48.222 |
| Management | 16 | 16 | 10.23.48.224 | /28 | 10.23.48.225–10.23.48.238 |

Продовження таблиці 3.7

| Назва підмережі | Розмір | Виділений розмір | Адреса | Маска | Діапазон доступних адрес |
|---|---|---|---|---|---|
| Native | 8 | 8 | 10.23.48.240 | /29 | 10.23.48.241–10.23.48.246 |

У таблиці 3.8 вказано інтерфейси комутаторів, які відповідають виділеним VLAN.

Таблиця 3.8 – Розподіл портів комутаторів

| Назва підмережі | VLAN | Розподіл портів |
|---|---|---|
| VLAN19 | 19 | Fa0/12-Fa0/14 |
| VLAN29 | 29 | Fa0/15-Fa0/24 |
| VLAN39 | 39 | Fa0/6-Fa0/11 |

У таблиці 3.9 наведено адреси портів пристроїв у мережі LAN1.

Таблиця 3.9 – Адресація портів пристроїв

| Пристрій | Інтерфейс | IP-адреса | Маска | Шлюз | VLAN |
|---|---|---|---|---|---|
| Matiushyn_Switch_2 | SVI | 10.23.48.226 | /28 | 10.23.48.225 | 99 |
| Matiushyn_Switch_3 | SVI | 10.23.48.227 | /28 | 10.23.48.225 | 99 |
| Matiushyn_Router_5 | G0/0.19 | 10.23.48.129 | /27 | - | 23 |
| | G0/0.29 | 10.23.48.161 | /27 | - | 33 |
| | G0/0.39 | 10.23.48.193 | /27 | - | 43 |
| | G0/0.99 | 10.23.48.225 | /28 | - | 99 |

Після всіх розрахунків необхідно налаштувати порти комутаторів на відповідні їм VLAN. Приклад налаштування наведено нижче.

```
int range fa0/6-11 //Вибираємо діапазон інтерфейсів
```

switchport mode access //Вмикаємо режим роботи access
switchport access vlan 39 //Призначаємо обрним інтерфейсам VLAN
int range fa0/15-24
switchport mode access
switchport access vlan 29
int range Gig0/1-2
switchport mode trunk //Налаштовуємо режим роботи trunk
switchport trunk native vlan 100 //Призначаємо native VLAN
switchport trunk allowed vlan 19,29,39,99-100 //Вказуємо VLAN, яким дозволено пересилання трафіку

Після налаштування комутаторів необхідно налаштувати маршрутизатори таким чином, щоб забезпечити машрутизацію між VLAN. Приклад налаштування наведено нижче.

interface GigabitEthernet0/1.19 //Створюємо під-інтерфейс
encapsulation dot1Q 19 //Вмикаємо інкапсуляцію
ip address 10.23.48.129 255.255.255.224 //Призначаємо адресу
interface GigabitEthernet0/1.29
encapsulation dot1Q 29
ip address 10.23.48.161 255.255.255.224
interface GigabitEthernet0/1.39
encapsulation dot1Q 39
ip address 10.23.48.193 255.255.255.224
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 10.23.48.225 255.255.255.240

### 3.5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

Необхідно реалізувати динамічне призначення адрес для вузлів у підмережах VLAN. Для цього використаємо протокол DHCP.

Приклад налаштування наведено нижче.

//Виключаємо з роздачі перші 10 адрес з кожної підмережі
ip dhcp excluded-address 10.23.48.129 10.23.48.138

```
ip dhcp excluded-address 10.23.48.161 10.23.48.170
ip dhcp excluded-address 10.23.48.193 10.23.48.202
//Створюємо новий DHCP-пул
ip dhcp pool VLAN19
network 10.23.48.128 255.255.255.224 //Налаштовуємо адресу мережі для розподілення адрес
default-router 10.23.48.129 // Вказуємо шлюз за замовчуванням
dns-server 10.23.49.206 //Вказуємо DNS-сервер
ip dhcp pool VLAN29
 network 10.23.48.160 255.255.255.224
default-router 10.23.48.161
dns-server 10.23.49.206
ip dhcp pool VLAN39
network 10.23.48.192 255.255.255.224
default-router 10.23.48.193
dns-server 10.23.49.206
```

Після цього необхідно забезпечити безпеку портів комутаторів, до яких під’єднано сервери. Для цього дозволимо лише двом унікальним пристроям доступ до порту та налаштуємо динамічне розпізнавання MAC-адреси з додаванням в поточну конфігурацію. Приклад налаштування наведено нижче.

```
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
```

# 4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

## 4.1 Інженерне рішення по розробці компонента системи

IoT - це скорочення від "Internet of Things" (інтернет речей). Це назва мережі взаємопов'язаних фізичних пристроїв, транспортних засобів, приладів та інших об'єктів, вбудованих датчиками, програмним забезпеченням та мережевим з'єднанням, що дозволяють їм збирати та обмінюватися даними.

Головний та віддалений (сервісний центр) офіси компанії потребують впровадження власних систем IoT.

Система головного офісу повинна забезпечувати виконання наступних завдань:

1. Відмикання дверей за допогою RFID-зчитувача та карток. В тому разі, якщо картка не дійсна, двері замикаються, зачиняються вікна та вмикається сирена. Якщо картка дійсна, то двері відмикаються, відчиняються вікна та вмикається світло;
2. В разі спрацювання датчика вогню вмикається сирена та відмикаються двері;
3. При спрацюванні датчика руху вмикається сирена, замикаються двері та вікна.

Система сервісного центра повинна забезпечувати виконання наступних завдань:

1. При спрацюванні сирени на датчику рівня CO2 повинні відчинятися ворота гаража.
2. Двері повинні відмикатися за допогою RFID-карток аналогічно до головного офісу.
3. В разі спрацювання датчика вогню вмикається сирена та відмикаються двері, а також вмикається пожежний розпилювач та відчиняються ворота гаража.

### 4.2 Налаштування обладнання та сервісів системи IoT

Усі пристрої повинні бути об’єднані у локальну мережу через підключення до HomeGateway (з’єднання повинно бути захищеним за протоколом WPA2-PSK). HomeGateway виступає у ролі IoT-сервера.

Для бездротового з’єднання з HomeGateway необхідно увести на пристрої SSID та пароль WPA2-PSK (рисунок 4.1).

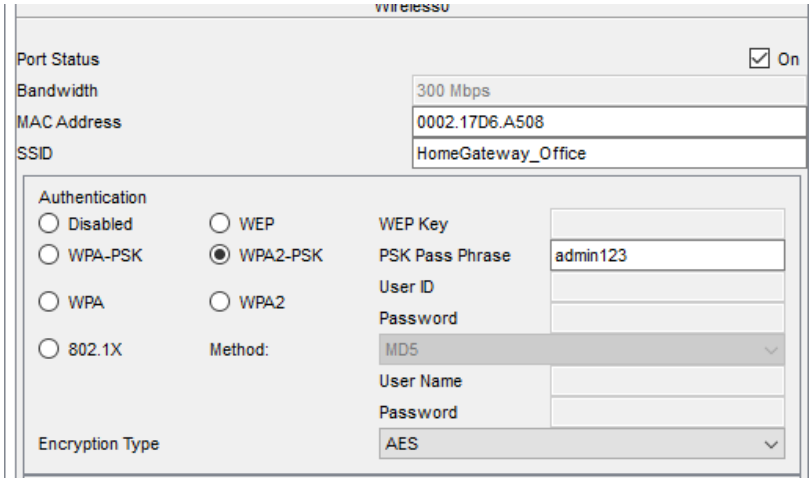


Рисунок 4.1 – З’єднання пристрою з HomeGateway

Після цього необхідно увімкнути DHCP та вказати використання HomeGateway в ролі IoT-сервера (рисунок 4.2).

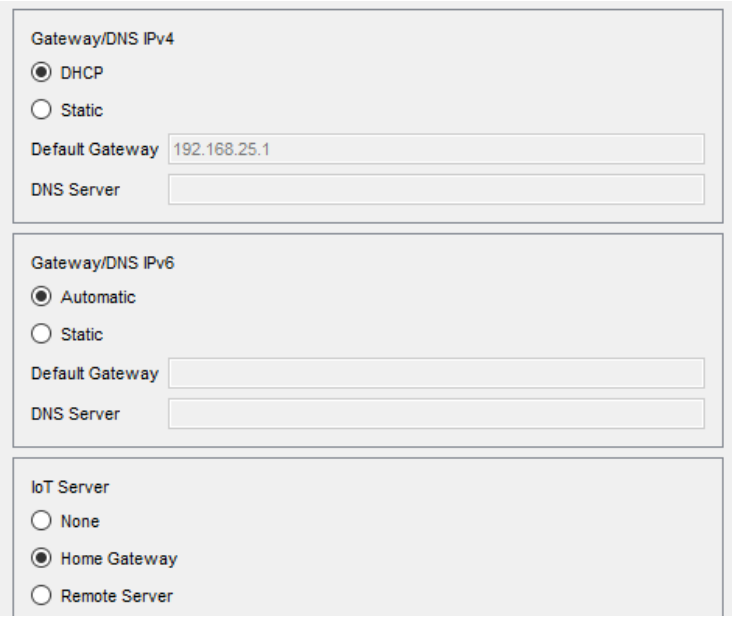


Рисунок 4.2 – Налаштування пристрою

Після успішного налаштування пристроїв можна побачити їх список на домашній сторінці IoT-сервера (рисунок 4.3).

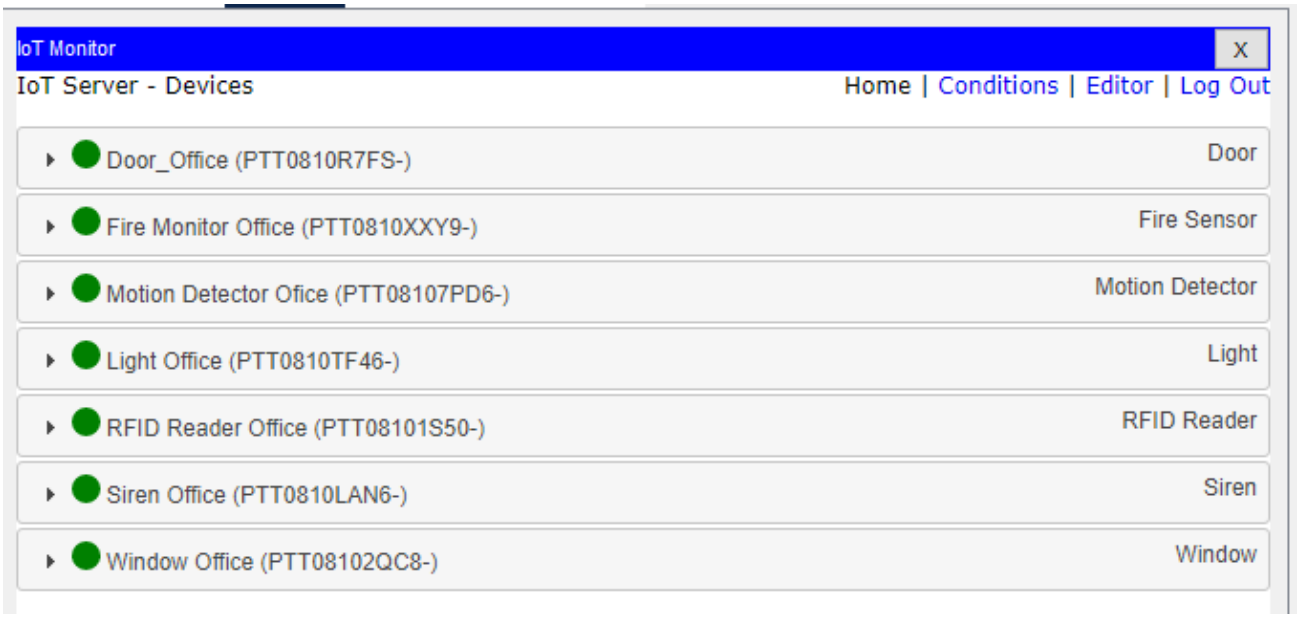


Рисунок 4.3 – Домашня сторінка IoT-серверу головного офісу

Далі перейдемо до створення сценаріїв на сервері. Спершу налаштуємо роботу RFID-зчитувача. Налаштування сценаріїв наведено на рисунку 4.4 та рисунку 4.5.

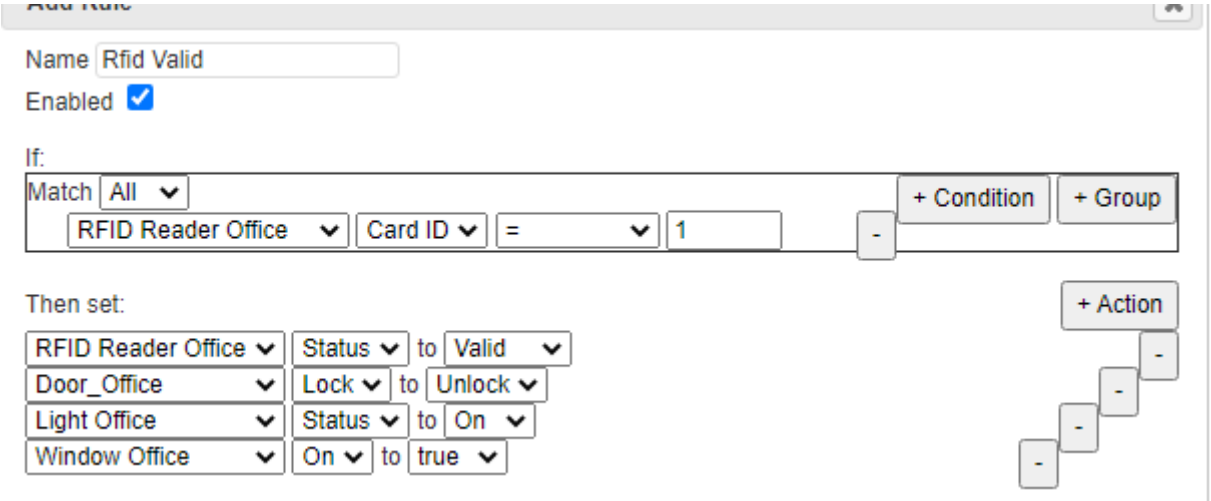


Рисунок 4.4 – Спрацювання RFID-зчитувача при правильному ID картки

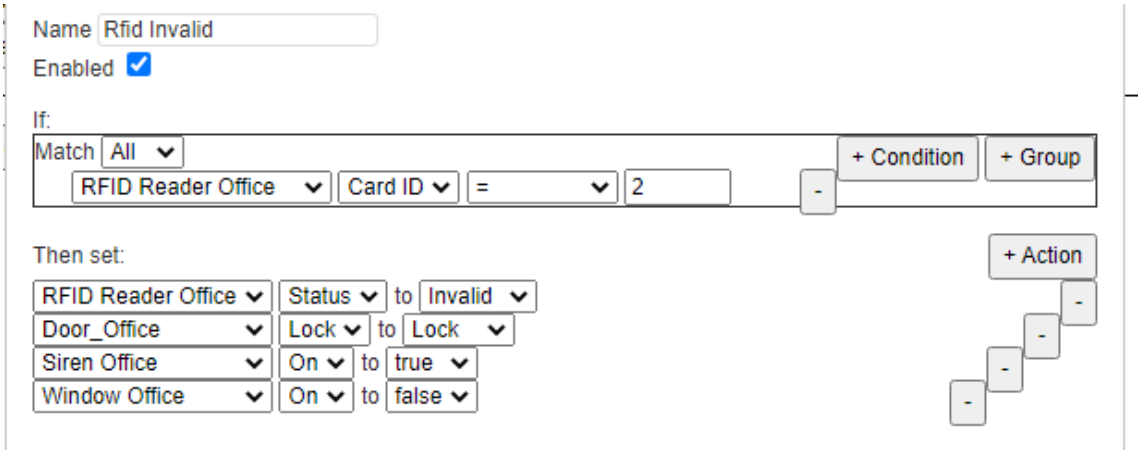


Рисунок 4.5 – Спрацювання RFID-зчитувача при неправильному ID картки

Після налаштування RFID виконаємо налаштування роботи детектору вогню. Сценарій зображено на рисунку 4.6.

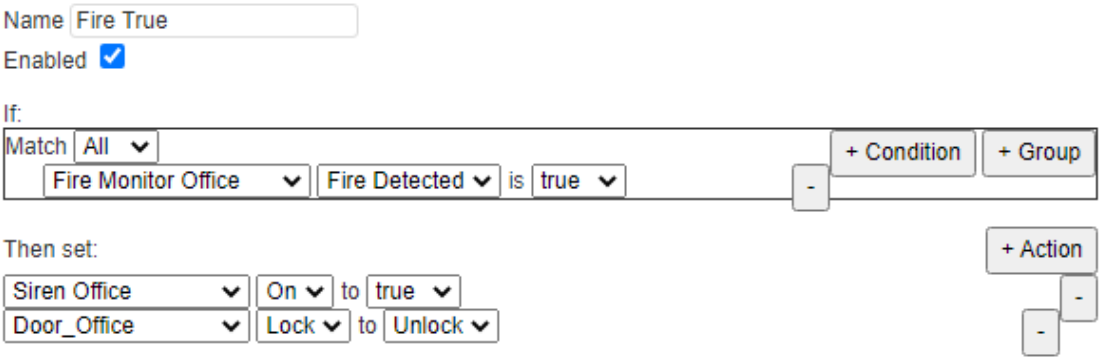


Рисунок 4.6 – Спрацювання детектору вогню

Наступним налаштуємо роботу пристроїв при спрацюванні детектора руху. Сценарій зображено на рисунку 4.7.

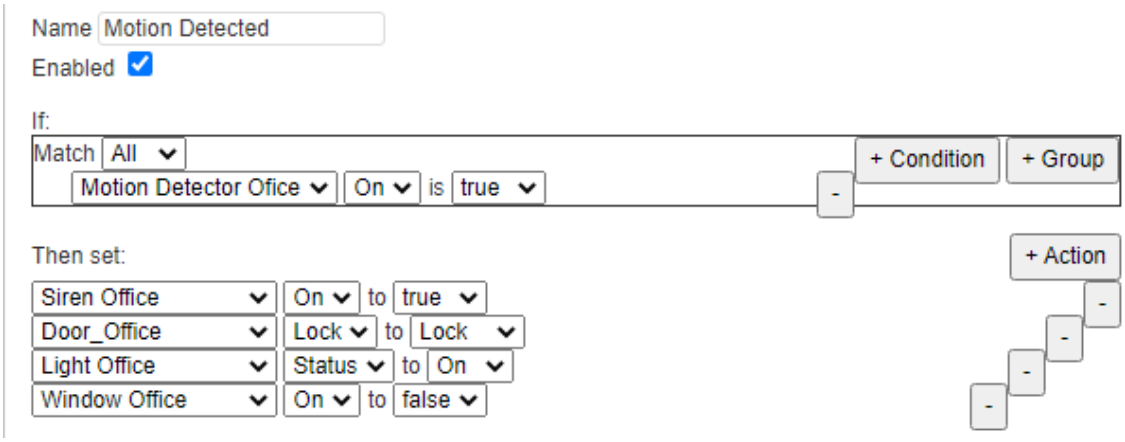


Рисунок 4.7 – Спрацювання детектора руху

Після цього створимо сценарій, який спрацює у випадку, якщо всі показники датчиків знаходяться в нормі (рисунок 4.8).

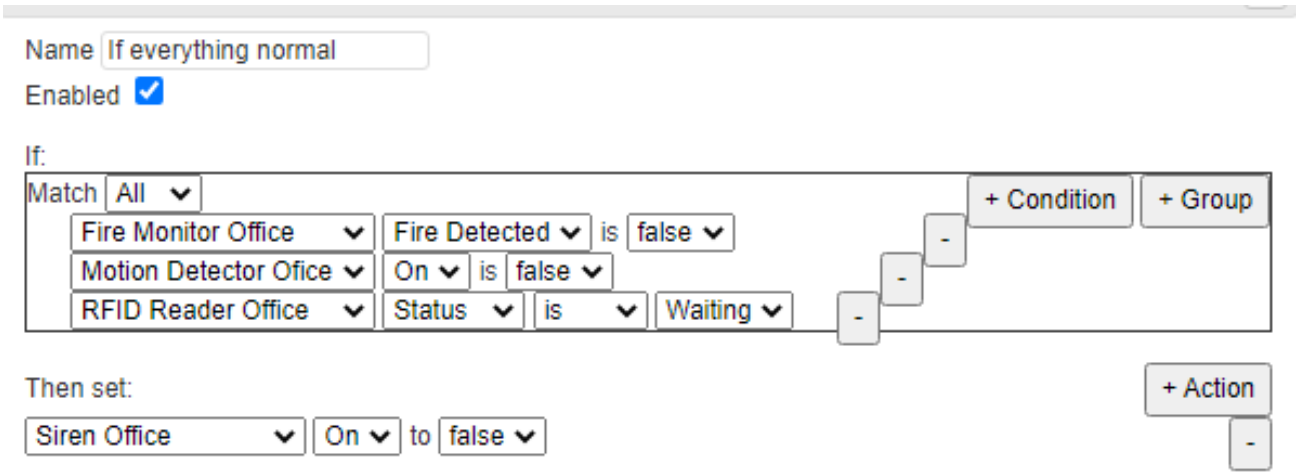


Рисунок 4.8 – Відсутність роботи датчиків

Список усіх сценаріїв для головного офісу зображено на рисунку 4.9.

| Actions | Enabled | Name | Condition | Actions |
|---|---|---|---|---|
| Edit Remove | Yes | Rfid Valid | RFID Reader Office Card ID = 1 | Set RFID Reader Office Status to Valid<br>Set Door_Office Lock to Unlock<br>Set Light Office Status to On<br>Set Window Office On to true |
| Edit Remove | Yes | Rfid Invalid | RFID Reader Office Card ID = 2 | Set RFID Reader Office Status to Invalid<br>Set Door_Office Lock to Lock<br>Set Siren Office On to true<br>Set Window Office On to false |
| Edit Remove | Yes | Fire True | Fire Monitor Office Fire Detected is true | Set Siren Office On to true<br>Set Door_Office Lock to Unlock |
| Edit Remove | Yes | Motion Detected | Motion Detector Ofice On is true | Set Siren Office On to true<br>Set Door_Office Lock to Lock<br>Set Light Office Status to On<br>Set Window Office On to false |
| Edit Remove | Yes | If everything normal | Match all:<br>• Fire Monitor Office Fire Detected is false<br>• Motion Detector Ofice On is false<br>• RFID Reader Office Status is Waiting | Set Siren Office On to false |

Add

Рисунок 4.9 – Список створених сценріїв головного офісу

Після налаштування роботи системи головного офісу виконаємо налаштування роботи системи сервісного центру. Усі налаштування сценаріїв

виконуються за аналогічним принципом. Перелік створених сценаріїв для сервісного центру зображено на рисунку 4.10.

IoT Monitor

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

| Actions | Enabled | Name | Condition | Actions |
|---|---|---|---|---|
| Edit Remove | Yes | Rfid Valid | RFID Reader Service Card ID = 1 | Set RFID Reader Service Status to Valid<br>Set Door service Lock to Unlock |
| Edit Remove | Yes | Rfid Invalid | RFID Reader Service Card ID = 2 | Set RFID Reader Service Status to Invalid<br>Set Door service Lock to Lock<br>Set Siren Service On to true<br>Set Garage door On to false |
| Edit Remove | Yes | CO2 Detected | Carbon Detector Alarm is true | Set Garage door On to true |
| Edit Remove | Yes | Fire True | Fire monitor Service Fire Detected is true | Set Siren Service On to true<br>Set Door service Lock to Unlock<br>Set Garage door On to true<br>Set Fire sprinker Status to true |
| Edit Remove | Yes | Fire False | Fire monitor Service Fire Detected is false | Set Fire sprinker Status to false |
| Edit Remove | Yes | Motion Detected | Motion detector Service On is true | Set Siren Service On to true<br>Set Door service Lock to Lock<br>Set Garage door On to false |
| Edit Remove | Yes | Everything normal | Match all:<br>• Fire monitor Service Fire Detected is false<br>• Motion detector Service On is false | Set Siren Service On to false |

Рисунок 4.10 – Перелік створених сценаріїв для сервісного центру

Результуючу топологію з усіма IoT-пристроями зображено на рисунку 4.11.

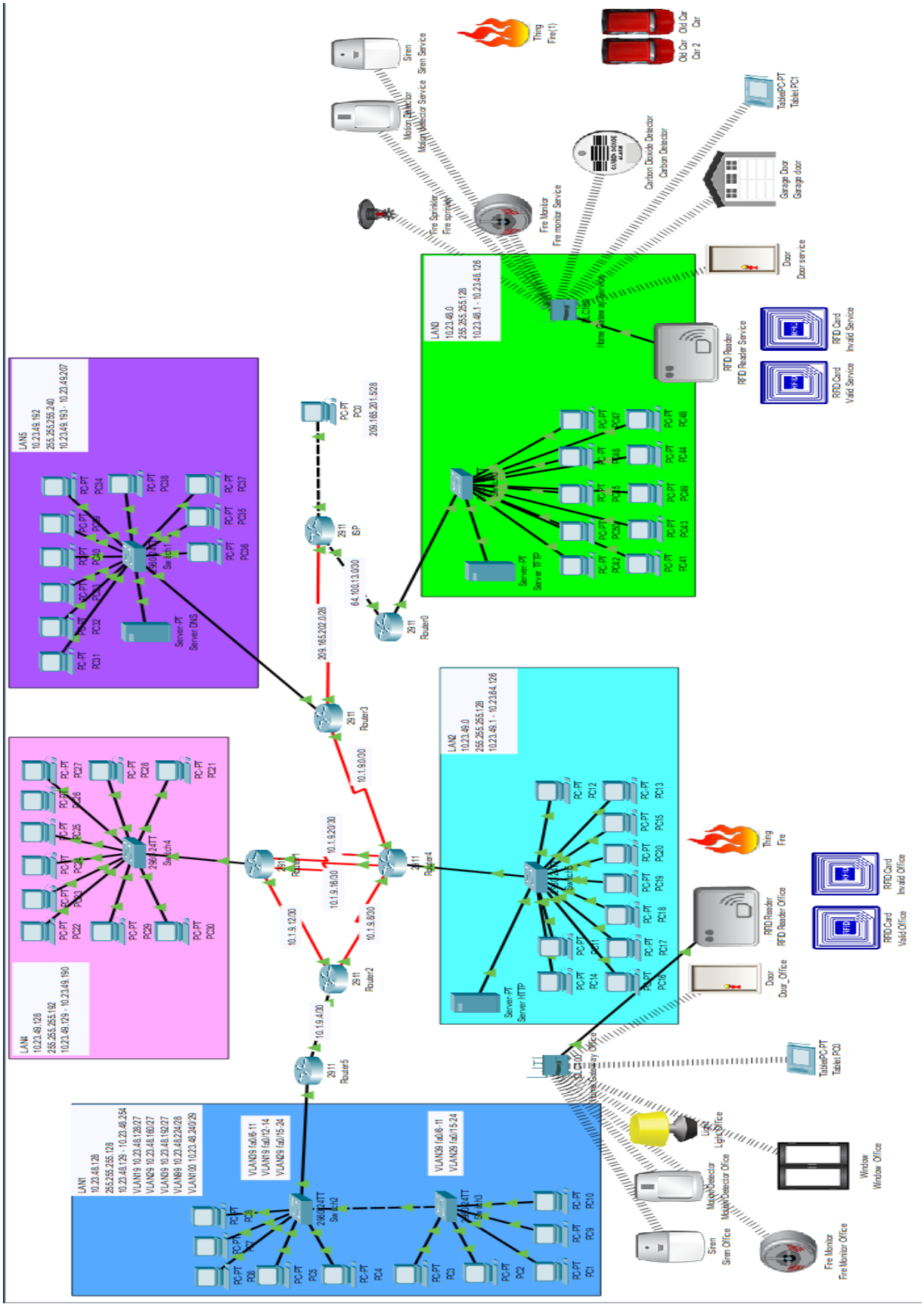


Рисунок 4.11 – Логічна топологія з підключеннями IoT-пристроїв

# ВИСНОВКИ

В рамках даної кваліфікаційної роботи було проведено дослідження та розробку корпоративної мережі, спрямованої на забезпечення ефективної комунікації та обміну даними в організаційному середовищі. Отримані результати свідчать про відповідність сучасному рівню наукових і технічних знань у галузі комп'ютерних мереж.

Підприємство, для якого виконувалася розробка та впровадження корпоративної мережі – центр спецтехніки «Альфатех».

Під час виконання проєкту було налаштовано такі технології, як NAT, VPN, VLAN, DHCP, AAA, OSPF та інші.

Розроблена корпоративна мережа відповідає поточним тенденціям технологічного розвитку та враховує сучасні вимоги організаційного середовища. Вона забезпечує надійність, безпеку та ефективність комунікаційних процесів, сприяючи підвищенню продуктивності та конкурентоспроможності підприємства.

Можливі галузі використання результатів даної роботи охоплюють широкий спектр сфер, включаючи бізнес, урядові структури, освітні заклади та інші організації, які потребують ефективної корпоративної мережі. Розроблена модель та рекомендації можуть бути використані як основа для побудови або модернізації мереж в цих галузях.

Можливі напрямки подальших досліджень включають впровадження передових технологій, розробку механізмів захисту мереж та аналіз впливу нових тенденцій, таких як штучний інтелект чи розширена реальність, на корпоративні мережі.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Центр спецтехніки Альфатех – [Електронний ресурс] – https://alfatech.com.ua/ (дата звернення 12.05.2023)

2. Альфатех, регіональні представництва – [Електронний ресурс] – https://alfatech.com.ua/contacts (дата звернення 12.05.2023)

3. Інформаційне забезпечення діяльності підприємства – [Електронний ресурс] - https://moodle.znu.edu.ua/pluginfile.php/722218/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%2010-11%20%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%20%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%96%20%D0%A1%D0%93%D0%94.pdf (дата звернення 15.05.2023)

4. Основи обробки текстової та графічної інформації – [Електронний ресурс] - https://elearning.sumdu.edu.ua/free_content/lectured:c5dfdb13db13a6099b7e1489d805156fd10127f0/20200921190435//1782687/index.html (дата звернення 16.05.2023)

5. Що таке VPN – [Електронний ресурс] – https://experience.dropbox.com/uk-ua/resources/what-is-vpn (дата звернення 25.05.2023)

6. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2022. – 62 с.

# ДОДАТОК А

Текст програми налаштування обладнання корпоративної мережі

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

# ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.2309-01 12 01

Листів 10

2023

# АНОТАЦІЯ

У додатку представлено програмне забезпечення налаштувань мережевого обладнання Cisco у середовищі моделювання "Cisco Packet Tracer".

Тексти програм викладені за допомогою мови конфігураційних сценаріїв для мережевого обладнання Cisco.

Програма призначена для забезпечення конфігурації DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній, а також створення віртуальних приватних мереж (VPN) та домену комп'ютерної системи.

# ЗМІСТ

## 1.Скрипт налаштування Router3

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Matiushyn_Router_3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 10.23.49.193 10.23.49.194
ip dhcp excluded-address 10.23.49.206
!
ip dhcp pool LAN5
network 10.23.49.192 255.255.255.240
default-router 10.23.49.193
dns-server 10.23.49.206
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username 123191_Matiushyn password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524RLX9-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
```

```
!
crypto isakmp key cisco address 64.100.13.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 64.100.13.2
set transform-set TS
match address VPN9
!
!
!
!
ip domain-name Matiushyn_Router_3
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 10.23.49.193 255.255.255.240
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/3/0
ip address 209.165.202.2 255.255.255.240
ip nat outside
crypto map MAP
!
interface Serial0/3/1
ip address 10.1.9.1 255.255.255.252
ip nat inside
clock rate 2000000
!
```

```
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute static subnets
passive-interface GigabitEthernet0/0
network 10.1.9.0 0.0.0.3 area 0
network 209.165.202.0 0.0.0.31 area 0
network 10.23.49.192 0.0.0.15 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224
ip nat inside source list NAT9 pool Internet
ip nat inside source static 10.23.49.19 209.165.200.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 209.165.201.0 255.255.255.240 209.165.202.1
ip route 209.165.202.0 255.255.255.252 Serial0/3/0
!
ip flow-export version 9
!
!
ip access-list extended VPN9
permit ip 10.23.49.192 0.0.0.15 10.23.48.0 0.0.0.127
permit ip 10.23.48.128 0.0.0.127 10.23.48.0 0.0.0.127
permit ip 10.23.49.0 0.0.0.127 10.23.48.0 0.0.0.127
permit ip 10.23.49.128 0.0.0.63 10.23.48.0 0.0.0.127
permit ip 10.1.9.0 0.0.0.255 10.23.48.0 0.0.0.127
ip access-list extended NAT9
deny ip 10.23.49.192 0.0.0.15 10.23.48.0 0.0.0.127
deny ip 10.23.48.128 0.0.0.127 10.23.48.0 0.0.0.127
deny ip 10.23.49.0 0.0.0.127 10.23.48.0 0.0.0.127
deny ip 10.23.49.128 0.0.0.63 10.23.48.0 0.0.0.127
deny ip 10.1.9.0 0.0.0.255 10.23.48.0 0.0.0.127
permit ip 10.23.49.192 0.0.0.15 any
permit ip 10.23.48.128 0.0.0.127 any
permit ip 10.23.49.0 0.0.0.127 any
permit ip 10.23.49.128 0.0.0.63 any
permit ip 10.1.9.0 0.0.0.255 any
!
banner motd ^CMatiushyn_Router_3^C
!
radius server 10.23.49.206
address ipv4 10.23.49.206 auth-port 1645
key radius123
!
!
!
line con 0
```

```
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
end
```

### 2. Скрипт налаштування Router0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Matiushyn_Router_0
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 10.23.48.1 10.23.48.10
ip dhcp excluded-address 10.23.48.19
!
ip dhcp pool LAN3
network 10.23.48.0 255.255.255.128
default-router 10.23.48.1
dns-server 10.23.49.206
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
!
!
!
!
!
ip cef
```

```
no ipv6 cef
!
!
!
username 123191_Matiushyn password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524I40E-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 209.165.202.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 209.165.202.2
set transform-set TS
match address VPN9
!
!
!
!
ip domain-name Matiushyn_Router_0
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 64.100.13.2 255.255.255.252
ip nat outside
duplex auto
speed auto
crypto map MAP
!
interface GigabitEthernet0/1
ip address 10.23.48.1 255.255.255.128
```

```
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip nat pool Internet 209.165.205.5 209.165.205.30 netmask
255.255.255.224
ip nat inside source list NAT9 pool Internet
ip classless
ip route 0.0.0.0 0.0.0.0 64.100.13.1
ip route 64.100.13.0 255.255.255.252 64.100.13.1
ip route 209.165.201.0 255.255.255.240 64.100.13.1
!
ip flow-export version 9
!
!
ip access-list extended VPN9
permit ip 10.23.48.0 0.0.0.127 10.23.49.192 0.0.0.15
permit ip 10.23.48.0 0.0.0.127 10.23.48.128 0.0.0.127
permit ip 10.23.48.0 0.0.0.127 10.23.49.0 0.0.0.127
permit ip 10.23.48.0 0.0.0.127 10.23.49.128 0.0.0.63
permit ip 10.23.48.0 0.0.0.127 10.1.9.0 0.0.0.255
ip access-list extended NAT9
deny ip 10.23.48.0 0.0.0.127 10.23.49.192 0.0.0.15
deny ip 10.23.48.0 0.0.0.127 10.23.48.128 0.0.0.127
deny ip 10.23.48.0 0.0.0.127 10.23.49.0 0.0.0.127
deny ip 10.23.48.0 0.0.0.127 10.23.49.128 0.0.0.63
deny ip 10.23.48.0 0.0.0.127 10.1.9.0 0.0.0.255
permit ip 10.23.48.0 0.0.0.127 any
!
banner motd ^CMatiushyn_Router_0^C
!
radius server 10.23.49.206
address ipv4 10.23.49.206 auth-port 1645
key radius123
!
!
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
```

```
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
end
```