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

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

# ПОЯСНЮВАЛЬНА ЗАПИСКА
**кваліфікаційної роботи ступеню** бакалавра
(бакалавра, магістра)

студента Вахрушева Вадима Вячеславовича
(ПІБ)
академічної групи 123-19-1 ФІТ
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему «**Комп'ютерна система підтримки прийняття рішень ТОВ «Стеко» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»**
(назва за наказом ректора)

| **Керівники** | **Прізвище, ініціали** | **Оцінка за шкалою** | | **Підпис** |
|---|---|---|---|---|
| | | **рейтинговою** | **інституційною** | |
| кваліфікаційної роботи | Ткаченко С.М. | | | |
| 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)
«____» _____2023 року

**ЗАВДАННЯ**
**на кваліфікаційну роботу**
**ступеню** ____бакалавра_____
(бакалавра, магістра)

студенту ____Вахрушеву В.В.___ академічної групи _____123-19-1 ФІТ____
(прізвище та ініціали) (шифр)

спеціальності _____123 Комп'ютерна інженерія_____

за освітньо-професійною програмою _____Комп'ютерна інженерія_____
(офіційна назва)

на тему **«Комп'ютерна система підтримки прийняття рішень ТОВ «Стеко» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»**

затверджену наказом ректора НТУ «Дніпровська політехніка» від 11.04.2023 № 256-с

| **Розділ** | **Зміст** | **Термін виконання** |
|---|---|---|
| Стан питання та постановка завдання | Постановка завдання та мети роботи, основуюичсь на матеріалах виробничих практик | 15.05.2023 |
| Розробка апаратної частини | Формулювання технічних вимог до комп'ютерної мережі та розробка апаратної частини системи | 22.05.2023 |
| Розробка корпоративної мережі | Розрахунок налаштувань та перевірка роботи мережі, розробка методів захисту та налаштування обладнання інформаційної системи. | 26.05.2023 |
| Розробка компонента системи | Розробка компонента система | 31.05.2023 |

Завдання видано _____ ___проф. Цвіркун Л.І.___
(підпис керівника) (прізвище, ініціали)

Дата видачі 01.03.2023 р.

Дата подання до екзаменаційної комісії 01.06.2023 р.

Прийнято до виконання _____ _Вахрушев В.В.
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 64с., 23 рис., 11 табл., 2 додатки, 12 джерел.

Об’єкт розробки: комп’ютерна система для компанії — «Steko» та налаштуванням корпоративної мережі.

Мета: розробка комп’ютерної системи для компанії — «Steko»

Розроблена комп’ютерна мережа з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову систем контролю та редагування для компанії — «Steko» в м.Дніпро, а також для збору і підготовки статистичної інформації.

Розробка комп’ютерної мережі виконана відповідно до завдання на дипломну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Також технологія проектування мережі включає захист всього обладнання внутрішньої мережі від несанкціонованого доступу.

Результати перевірки у вигляді таблиць, графіків описані і знаходяться у пояснювальній записці або додатках.

КЛЮЧОВІ СЛОВА: КОМП’ЮТЕРНА МЕРЕЖА, МАРШРУТИЗАТОР, КОМУТАТОР, CISCO, CISCO PACKET TRACER, DHCP, VLAN, NAT, VPN.

# ЗМІСТ

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПК – Персональний комп’ютер .

ПЗ – Програмне забезпечення.

КМ – Комп’ютерна мережа.

VLAN – Virtual Local Area Network – віртуальна локальна комп'ютерна мережа.

ACL – Access Control List – список контролю доступу.

VPN – Virtual Private Network – віртуальна приватна мережа.

DHCP – Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла

NAT – Network Address Translation – перетворення мережевих адрес.

# ВСТУП

У сучасному бізнес-середовищі, де швидкість прийняття рішень і ефективне управління є ключовими факторами успіху, комп'ютерні мережі підтримки прийняття рішень стають невід'ємною частиною розвитку підприємств. Технологічний прогрес і постійне зростання обсягів даних створюють потребу у високопродуктивних і надійних інформаційних системах, які забезпечують швидкий доступ до інформації та надійний аналіз даних для прийняття обґрунтованих рішень.

Ця дипломна робота присвячена розробці комп'ютерної системи підтримки прийняття рішень для ТОВ «Стеко», організації, яка спеціалізується у виробництві та постачанні продуктів для будівельної галузі. Метою даної роботи є побудова, налаштування та забезпечення безпеки корпоративної мережі, що дозволить підвищити ефективність процесів управління та прийняття рішень в організації.

У процесі виконання дипломної роботи будуть проведені аналітичні процеси з метою визначення потреб і вимог ТОВ «Стеко» щодо комп'ютерної системи. На основі цього аналізу буде розроблена концепція комп'ютерної системи підтримки прийняття рішень, що враховує специфіку бізнесу ТОВ «Стеко» та вимоги до надійності, швидкодії та безпеки.

Дана дипломна робота має на меті не лише дослідження теоретичних аспектів комп'ютерних систем підтримки прийняття рішень та безпеки мереж, але й практичне впровадження розробленої системи в середовище ТОВ «Стеко». Це дозволить показати шляхи вдосконалення процесів управління та прийняття рішень, які забезпечать високу доступність та захист інформації.

В цілому, дана дипломна робота повина вирішувати важливу проблему побудови, налаштування та забезпечення безпеки корпоративної мережі в організації ТОВ «Стеко». Вона сприятиме підвищенню ефективності та якості процесів управління, а також забезпечить захист конфіденційної інформації.

# 1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

## 1.1 Характеристика галузі та умови застосування КМ

Комп’ютерна мережа буде створюватися для компанії, яка спеціалізується на виробництві металево-пластикових віконних конструкцій. Це означає, що співпраця буде виконуватися із виробничою галуззю.

Виробнича галузь відноситься до гілки економіки, яка обробляє різноманітну сировину та матеріали, для виготовлення конкретних товарів. Ця галузь має великий вплив на розвиток економіки країни, тому що охоплює багато галузей, наприклад: машинобудування, хімічна промисловість, харчова промисловість, металообробка, електроніка та багато іншого. Така всеохоплююча галузь створює багато робочих місць для людей. Хто завгодно може стати різноробочим та працювати у виробничій галузі. Однак технології розвиваються та внедряються в усі галузі, через це комп’юетрні мережі стають більш корисними для покращення виробництва, ща несе за собою автоматизацію на підприємстві. Через це робочих місць стає менше, а для влаштування на роботу потрібно мати певні кваліфіковані навички.

Комп’ютерні мережі це системи, що з'єднують комп'ютери та пристрої для обміну даними та ресурсами. Основні характеристики комп'ютерних мереж включають топологію, протоколи передачі даних, швидкість передачі, безпеку та доступність ресурсів. Ці технології забезпечують ефективний обмін даними та зручний доступ до інформації. Сьогодні комп'ютерні мережі стали необхідною складовою як повсякденного життя, так і бізнесу. Завдяки постійному розвитку технологій, комп'ютерні мережі стають надзвичайно корисними для виробничої галузі. Сучасне виробництво вже майже повністю автоматизоване та поєднане з комп'ютерними технологіями. Комп'ютерні мережі забезпечують швидкий та надійний обмін інформацією між комп'ютерами та пристроями на виробничій лінії, що підвищує продуктивність та якість виробництва. Крім того, комп'ютерні мережі забезпечують чіткий контроль над процесом виробництва, допомагаючи виявляти та усувати можливі неполадки швидше. Також на виробництві можна

використовувати комп'ютерні мережі для збору даних продуктивності, що дозволяє знайти шляхи оптимізації процесів виробництва.

Отже, автоматизація виробничого процесу полегшує роботу на виробництві, тому що це потужний інструмент, який дозволяє не тільки підтримувати рівень виробництва, але й підвищувати його.

## 1.2 Стисла характеристика та структура об’єкта реалізації

### 1.2.1 Характеристика об’єкта реалізації

Вікна Steko – це компанія, яка спеціалізується на виготовленні та установці вікон та дверей з ПВХ профілю. Українська компанія була заснована в 1999 році, з того часу вона стала однією з провідних компаній на ринку України. Компанія має два заводи, в Дніпропетровській та Львівській областях, окрім заводів також є безліч салонів по всій країні.

Компанія «Steko» виготовляє металопластикові конструкції, це не лише вікна та двері, але й підвіконня, профільні системи, фурнітура та інші дрібниці пов’язанні з ПВХ профілем. На виробництві в компанії дотримуються високих стандартів якості та використовують найсучасніші технології. Steko мають розвинену дилерську мережу та партнерські відносини з провідними виробниками, що дозволяє пропонувати високоякісні продукти клієнтам.

Компанія має відносини з великою кількістю партнерів, для реклами своєї продукції. За бажанням можно самому стати дилером та співпрацювати з компанією. Через широку мережу дилерів та велику кількість щодених доставок, у компанії добре розвинена логістика та взаємовідносини з клієнтами.

Окрім виробництва, компанія «Steko» надає усі послуги пов’язанні з монтажем вікон та дверей. Для цього вона має власних сертифікованих працівників, які проведуть заміри, демонтаж старих та монтаж нових конструкцій.

Для виробництва компанія співпрацює за архітекторами та дизайнерами, що дозволяє розширити власний асортимент та сторювати індивідуальні вікна та двері для своїх клієнтів. Компанія має власну дизайнерську студію, де

розробляються прототипи нової продукції. Щоб покращити продукцію, компанія організувала власний дослідницький центр, де проводяться долсідження, тестування та розробка нових конструкцій.

### 1.2.2 Організаційна структура підприємства

Компанія «Steko» має функціональну структуру управління. У такій структурі компанія має функціональні підрозділи, які організовані за функціями (наприклад, виробництво, маркетинг, логістика тощо). Кожен функціональний підрозділ має свого керівника, який відповідає за організацію роботи свого підрозділу, прийняття рішень та забезпечення виконання поставлених завдань. Всі підрозділи взаємодіють між собою для досягнення загальних цілей компанії та забезпечення високої якості продукції для задоволення потреб клієнтів.

Організаційна структура компанії Steko має основні рівні та підрозділи:

1. Вище керівництво, до складу входять:
    - генеральний директор – особа, яка відповідає за загальне керівництво компанією;
    - виконавчий директор – заступник генерального директора, керує окремими відділами, або підрозділами компанії.
2. Функціональні підрозділи:
    - відділ маркетингу, який відповідальний за розробку та реалізацію маркетингових стратегій, рекламу та просування продукції компанії.
    - відділ продажу, займається продажем продукції Steko, веденням ділових відносин з клієнтами та дилерами.
    - відділ дизайну, розробляє дизайн продукції, складається з команд архітекторів та дизайнерів.
    - відділ виробництва, що включає підрозділи, які займаються виробництвом вікон, дверей, профільних систем та інших продуктів.
    - відділ логістики, цей відділ відповідає за планування та здійснення доставки продукції до клієнтів та між різними підрозділами компанії.

- відділ технічної підтримки, забезпечує технічну підтримку клієнтів, включаючи консультації та післяпродажне обслуговування.

3. Регіональні підрозділи:

- салони продажу, які розташовані по всій країні і відповідають за прийом замовлень та консультування клієнтів.
- дилерські партнери, це люди, які співпрацюють з компанією Steko в якості офіційних дилерів та представляють продукцію на ринку.

У Дніпропетровській області знаходиться головний завод компанії Steko, на території цього заводу знаходиться й головний офіс компанії. До головного офісу належать вище керівництво, відділ дизайну, відділ виробництва, відділ маркетингу та частина технічної підтримки. Відділ продажу та більша друга частина відділу технічної підтримки знаходяться у віддаленому офісі, який також розташован у місті Дніпро.

На рисунку 1.1 зображена схема організаційної структури компанії «Steko».

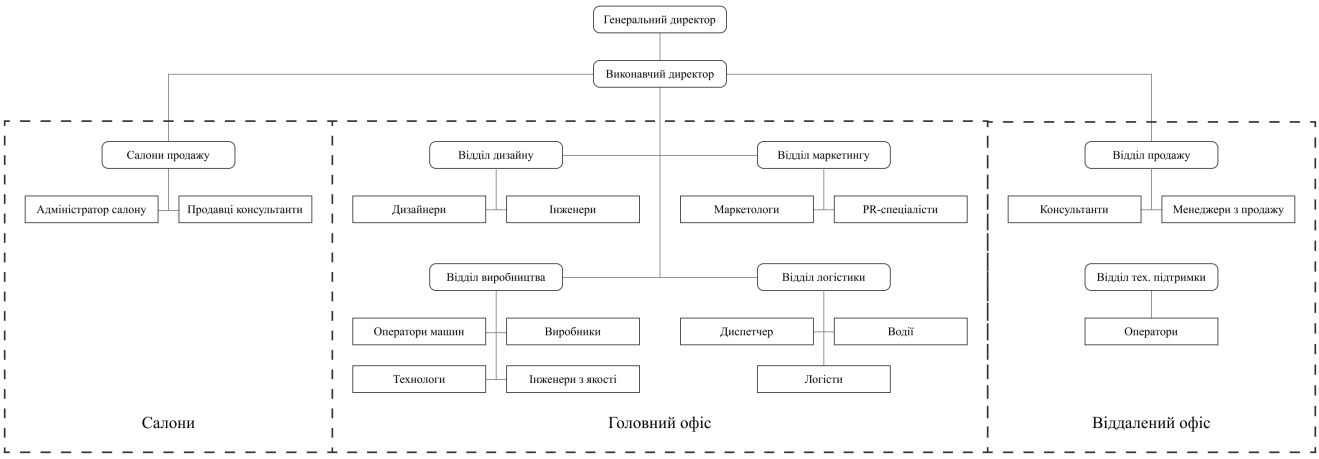


Рисунок 1.1 – Організаційна структура підприємства Steko.

### 1.2.3 Розташування структурних підрозділів компанії Steko

Головний офіс компанії знаходиться на лівому березі Дніпра за адресою вулиця Артільна, 2, м.Дніпро, Дніпропетровська область, 49000. Цей офіс знаходиться на території заводу та представляє собою чотирьох поверхову будівлю, від’єднану від виробничого цеху. Віддалений офіс знаходиться ближче до центра міста вже на правому березі, за адресою проспект Дмитра Яворницького,

93, м.Дніпро, Дніпропетровська область, 49000. На мапі зазначено, що відстань між офісами 4,7 км та займає приблизно 10 хвилин шляху на автівці.

Схему гео-розміщення офісів зображено на рисунку 1.2

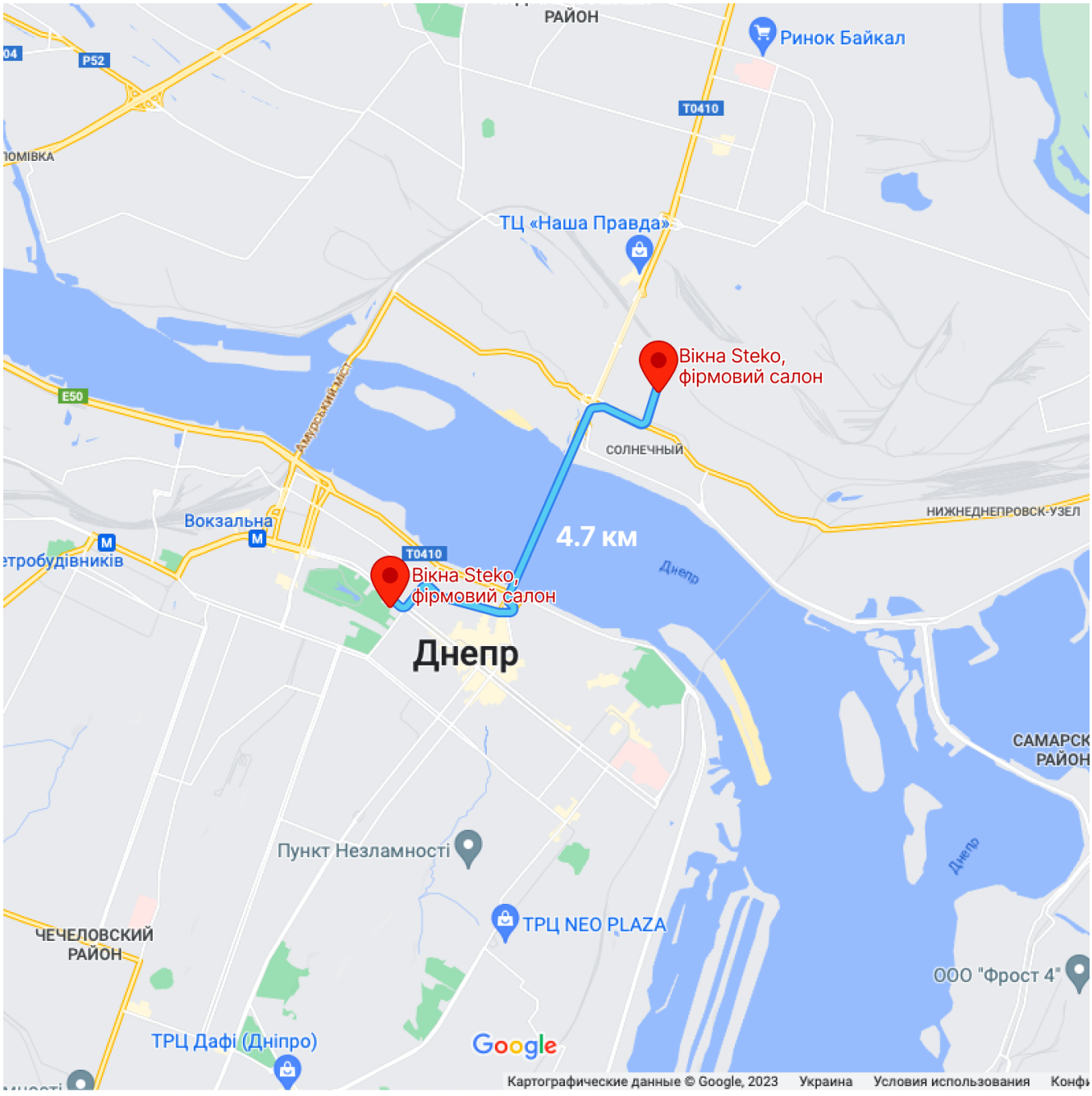


Рисунок 1.2 – Схема гео-розміщення офісів виробничої компанії «Steko».

Структурну схему розміщення відділів підприємства розглянемо на відділах корпоративного, цивільного, господарського та податкового права, що знаходяться у головному офісі (рисунок 1.3), та на відділах судової практики та юридичного обслуговування бізнесу, що знаходяться у віддаленому офісі (рисунок 1.4).

Для зручності покажемо частину структурної схеми розміщення відділів у головному офісі, це будуть відділи маркетингу та частина відділу технічної підтримки (рисунок 1.3). Також покажемо структурну схему віддаленного офісу в якому розміщується відділ продажу та друга частина відділу технічної підтримки (рисунок 1.4).

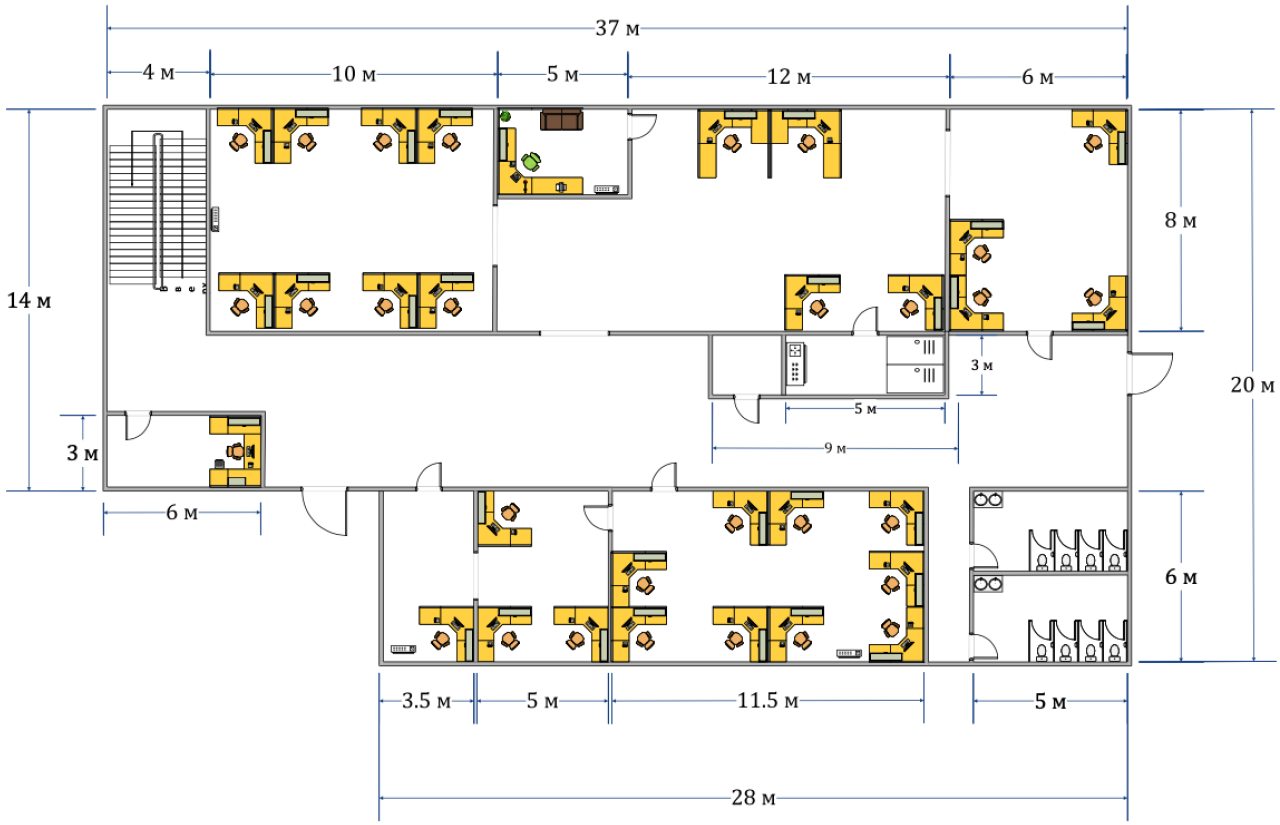


Рисунок 1.3 – Структурна схема першого поверху головного офісу, який складається з відділу маркетингу та частини відділу тех.підтримки.

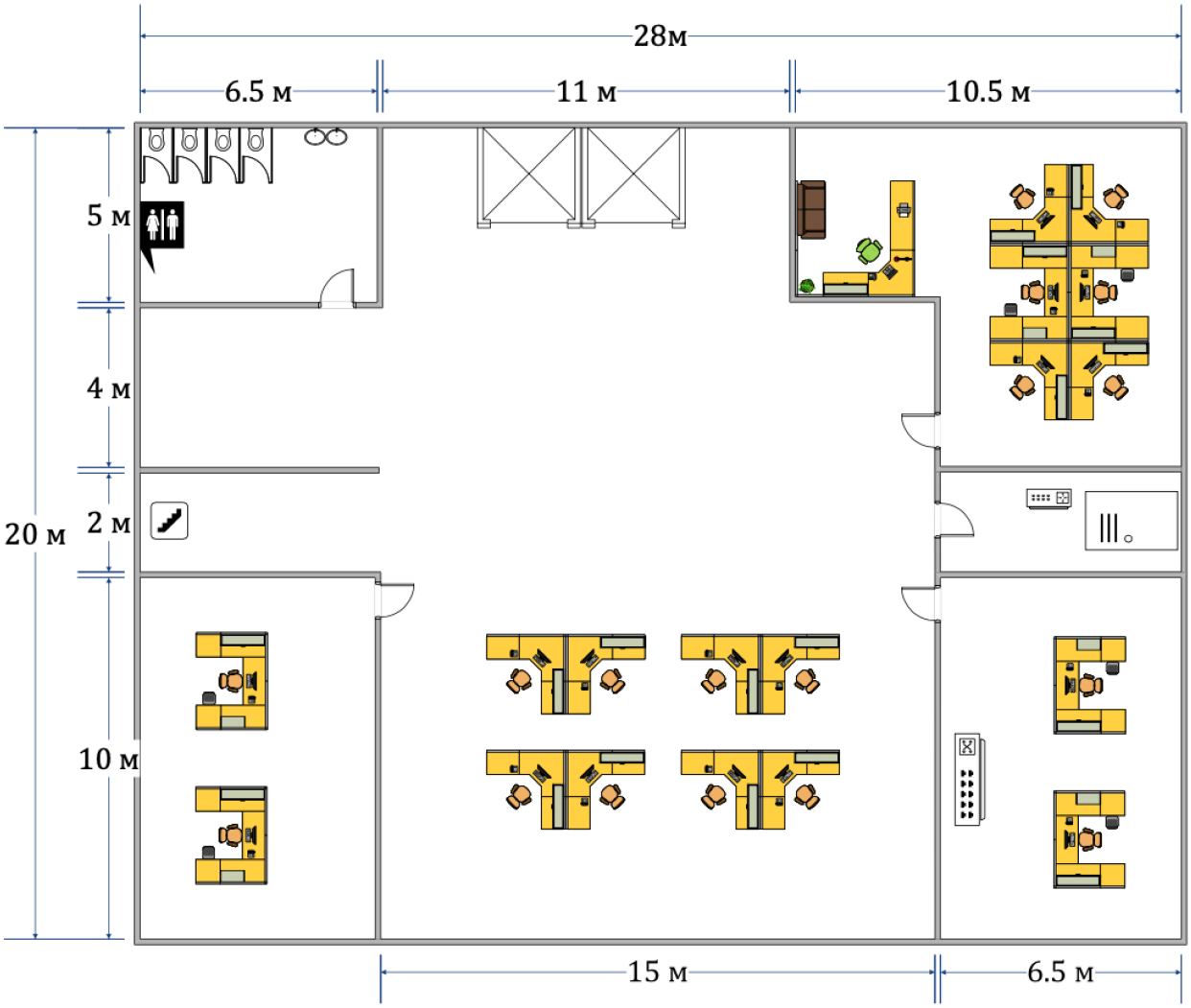


Рисунок 1.4 – Структурна схема віддаленого офісу, до складу якої входить відділ продажу та частина відділу тех.підтримки.

### 1.3 Принципи та технічні методи забезпечення інформації для об’єкта реалізації

Компанія Steko йде у ногу із часом, тому використовує інформаційні технології, щоб пришвидшити та покращити робочі процеси. Для цього в них є список принципів та технічних методів, яких вони дотримуються:

1. Авторизація на підприємстві. Кожен співробітник отримує біометричний пропуск, який дозволяє відвідувати різні території підприємства. Ці пропуски мають різні рівні допуску, завдяки чому працівники не можуть відвідувати будь-які місця на території. Наприклад, різноробочий не зможе увійти до серверної тому що в нього інший рівень допуску.

2. Електронне зберігання даних. Використовучи електронні таблиці та бази даних, зберігається, аналізується та оброблюється велика кількість даних, що дозволяє швидко та безпечного обмінуватися інформацією та документами між усіма підрозділами компанії. Щоб не втратити дані, регулярно створюють резервні копіїї даних, які зберігаються у безпечних місцях. Ці копії використовуються для відновлення даних, якщо ті були втраченні, або пошкодженні.

3. Аутентифікація. Працівник, який має доступ до критично важливої інформації, обов'язково використовує двофакторну аутентифікацію. Таких підхід виключає можливість під'єднання до мережі, без перевірки ідентичності користувача. Інші працівники, які мають доступ до менш важливої інформацію обов'язково використовують «сильні» паролі, та періодично змінюють їх.

4. Моніторинг дій. Компанія використовує систему моніторингу, щоб відслідкувати несанкціоновану діяльність на робочих приладах. Для автоматизації існують журнали подій, в яких прописані шляхи забезпечення безпеки при виявлені загрози.

5. Автоматизація виготовлення. На підприємстві використовують системи автоматизації виробництва такі як електронні датчики кількості та якості матеріалу, це дозволяє знизити витрати на ручну працю та прискорити виробництво. Цифрове проектування, або автоматичне проектування, заощаджує дизайнерам та архітекторам час проектування вікон, та зменшує кількість помилок при виготовленні. Системи розрахунку виробничих процесів використовуються для розподілу матеріалів, зменшення витрат на транспортування та забезпечення мінімальної кількості відходів. Роботизовані системи обробки матеріалів та збору конструкцій.

### 1.4 Огляд аналітичних методів для обробки та передачі інформації

На такому виробництві, як у компанії Steko щоденно використовується та обмінюється велика кількість документації та інформації, яка є важливою для компанії. Щоб знизити ризики втрачі інформації, необхідно забезпечити її

високим рівнем безпеки та конфіденційності. Для цього можна використовувати різноманітні способи обробки та передачі даних, такі як:

- Електронна пошта є одним з найпоширеніших способів обміну інформацією на підприємствах. Для забезпечення безпеки інформації можна використовувати шифрування електронної пошти та електронного підпису. Ці засоби забезпечують аутентифікацію відправника та захист від перехоплення та зміни інформації в процесі передачі.

- Електронні підписи дозволяють забезпечити аутентифікацію користувача та підтвердження аутентичності документів. Електронні підписи можуть бути використані для підписування документів та відправки електронної пошти.

- Файлові сервери дозволяють зберігати та обмінюватися документами та іншою інформацією в межах внутрішньої мережі. Для покращення безпеки використовують системи контролю доступу, шифрування даних та резервне копіювання даних.

- Хмарні сховища є зручним способом зберігання та обміну документами та іншою інформацією. Для забезпечення безпеки можна використовувати шифрування даних на рівні сервера та на рівні клієнта, а також контроль доступу до даних.

- Віртуальна приватна мережа (VPN) надає безпечний доступ до інформації з будь-якого місця з Інтернет-підключенням. За допомогою VPN можна шифрувати трафік та забезпечувати аутентифікацію користувача перед доступом до інформації.

У кожного зі способів обробки та передачі інформації є свої переваги та недоліки, тому важливо обрати той, що найкраще відповідає потребам компанії. Наприклад, якщо важливо забезпечити максимальний рівень безпеки та конфіденційності, то можна використовувати VPN та електронний підпис. Якщо ж важливо забезпечити зручний доступ до інформації, то можна використовувати хмарні сховища та файлові сервери.

### 1.5 Постановка завдання та мета роботи

Метою кваліфікаційної роботи є організація комп'ютерної мережі для компанії по виготовленню металево-пластикових конструкцій «Steko».

Для вирішення данної мети, необхідно виконати список завдань:

- обрати архітектуру для комп'ютерної мережі;
- визначити кабельну систему корпоративної мережі;
- провести аналіз мережевого трафіку;
- розробити фізичну та логічну топології комп'ютерної мережі;
- провести конфігурацію мережевого обладнання.

Як результат, мережа має бути надійною та швидкою, гнучкою та масштабованою.

### 1.6 Визначення можливих альтернативних рішень поставлених завдань

Побудова нової комп'ютерної мережі є важливим кроком для покращення стану компанії та фіксації її, як одного з лідерів на ринку. Оновлена мережа дозволить покращити зберігання та обробку великої кількості клієнтських даних. Тобто оновлення підвищіть продуктивність працівників, тому що з'явиться можливість автоматизувати деякі рутинні помилки (наприклад, надсилання факсів, звітування, обмін інформацією тощо).

Для покращення мережі та вирішення поставлених задач можливі наступні напрямки:

1.Вибір архітектура мережі для компанії «Steko»:

- централізована мережева архітектура, усі ресурси та обчислювальні потужності зосереджені в центральному вузлі мережі;
- Розподілена мережева архітектура, усі ресурси та обчислювальні потужності розподілені між вузлами мережі;

2. Вибір кабельної системи корпоративної мережі:

- вита пара, яка забезпечить добру якість сигналу та підтримку високих швидкостей на середній дистанції;

- оптоволоконний кабель, який забезпечить якістний сигнал на великій дистанції.

3.Аналіз трафіку:

- використання програмного забезпечення для моніторингу трафіку та аналізу мережевої активності;
- визначення та призначення пріоритетів для різних типів трафіку.

4. Розробка фізичної та логічної топології:

- застосування стандартних топологій, таких як зірка або дерево;
- розробка індивідуальної топології, яка відповідатиме потребам компанії.

5. Конфігурація мережевого обладнання:

- встановлення мережевих пристроїв, з урахуванням потреб виробництва та обраних мережевих архітектур та топологій;
- налаштування мережевої безпеки та захисту даних.

Враховуючи ці рішення, можна створити надійну, масштабовану, гнучку, безпечну та швидку корпоративну мережу для компанії «Steko». Проте слід мати на увазі, що конкретні рішення залежатимуть від потреб підприємства, його бюджету та доступних ресурсів.

# 2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА STEKO

## 2.1 Технічні вимоги до комп'ютерної мережі виробничої компанії Steko

### 2.1.1 Загальні вимоги до системи

#### 2.1.1.1 Вимоги структури і функціонування системи підрозділів

Основними вимогами структури та функціонування комп'ютерної мережі є:

1. Надійна система, яка працюватиме стабільно та безперебійно, уникачи віруси та інші зовнішні загрози.
2. Безпечна система, яка є захищеною від несанкціонованого доступу до даних. Належне забезпечення мережевої безпеки, аутентифікація користувачів та криптографічний захист.
3. Масштабована система, яка готова до змін та розширення залежно від потреб підприємства.
4. Гнучка система повинна дозволяти використовувати різні програмні засоби, залежно від потреб користувачів.
5. Швидка та продуктивна система для забезпечення швидкого доступу до даних, з можливістю швидкої обробки.
6. Автоматизована система, яка мінімізує ручну працю та оптимізує процеси за допомогою автоматизації.
7. Система повинна мати належну систему резервного копіювання даних та можливість відновлення даних в разі втрати.
8. Система повинна бути сумісною з іншим програмним забезпеченням та обладнанням, що використовують на виробництві.
9. Система повинна мати підтримку з боку виробників та постачальників програмного забезпечення та обладнання.

Система повинна забезпечувати безперебійни роботу інформаційної стрктури, навіть якщо відмовили деякі кімпонентів системи, щоб не припиняти роботу під час технічного обслуговування.

Потрібен механізм захисту від несанкціонованого доступу до даних, захист від вірусів, шпигунського програмного забезпечення та інших інформаційних загроз.

Нова система повина бути легкою у використанні, швидкою та продуктивною, щоб забезпечувати швидкий доступ до даних, з можливістью швидкої обробки. За можливістью система має автоматизувати ручну працю та оптимізувати робочі процеси.

Обладнання та програмне забезпечення, яке буде використовуватися у системі, має бути ліцензійним та сумісним. Обладнання системи необхідно регулярно перевіряти для виявлення можливих пошкоджень. Перевірку обладнання не слід робити самостійно, краще визвати майстрів, які знатимуть усі норми і правила техніки безпеки. Також дуже важливо мати запасне обладнання, для швидкої заміни. Програмне забезпечення має оновлятися та мати підтримку з боку постачальників.

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

Для забезпечення взаємодії між підсистемами, мають використовуватися спільний інформаційний простір та стандартизовані протоколи та формати обміну даними. Всі програмні компоненти підсистем працюють в рамках єдиного логічного простору, що забезпечується інтегрованими рішеннями серверів даних та серверів додатків.

#### 2.1.1.3 Вимоги до взаємодії та сумісності створеної мережі з суміжними системами і характеристики зв'язків між ними.

Програмне забезпечення системи забезпечує інтеграцію та сумісність на інформаційному рівні з іншими системами шляхом експорту та імпорту XML-документів. Архітектура взаємодії системи повинна відповідати таким умовам:

1. Дотримання регламентів використання системи, встановлених у процесі розробки.

2. Використання відкритих форматів обміну даними при організації взаємодії між підсистемами та системами, що використовуються на об’єкті.

3. Гарантована сумісність з існуючими і стандартними протоколами обміну даними, такими як HTTP, FTP, SOAP, REST тощо.

#### 2.1.1.4 Вимоги до режимів функціонування системи

Система повинна працювати стабільно та безперебійно, забезпечуючи неперервну доступність та працездатність для користувачів. При цьому системуа має працювати ефективно, щоб швидко оброблювати дані та запити користувачів. Система має бути забезпечена можливістью розширення, на випадок збільшення потреб користувачів, або обсягу даних.

#### 2.1.1.5 Вимоги діагностування системи

При діагностуванні системи можуть використовуватися наступні пункти:

1. Перевірка наявності та якості з'єднання між компонентами системи. Ця процедура включає перевірку кабелів, роз'ємів, підключень та антен.

2. Перевірка правильності налаштування IP-адрес, підмереж, шлюзів, DNS-серверів та інших мережевих параметрів. Включає перевірку наявності конфліктів IP-адрес та переконання в правильності налаштувань протоколів маршрутизації.

3. Перевірка доступності мережевих пристроїв та ресурсів (серверів, принтерів, інших комп'ютерів) у мережі. Включає пінгування, тестування з'єднання та перевірку стану служб.

4. Моніторинг та аналіз пакетів, що пересилаються в мережі, для виявлення аномалій, затримок, пакетних втрат, конфліктів IP-адрес та інших проблем.

5. Виявлення та локалізація джерел інтерференції та шуму, які можуть впливати на якість мережевого з’єднання.

6. Вимірювання швидкості передачі даних у мережі для оцінки пропускної здатності та виявлення можливих обмежень.

7. Аналіз мережевої активності та виявлення підозрілих пакетів, атак, вторгнень та інших безпекових загроз.

### 2.1.1.6 Моливі перспективи до розвитку мережі

З метою забезпечення довгого терміну служби та сталого розвитку комп'ютерної мережі, рекомендується враховувати наступні аспекти:

При проектуванні та реалізації системи слід враховувати використання стандартизованих протоколів, форматів даних та інших компонентів. Це дозволить забезпечити сумісність з іншими системами і легкість підтримки.

Рекомендується реалізувати комп'ютерну систему як відкриту, що допускає можливість розширення функціональності. Це дозволить впроваджувати нові функції і модулі, які задовольнять зростаючі потреби користувачів.

Комп'ютерна мережа повинна бути готовою до модернізації, як заміною технічного та програмного забезпечення, так і поліпшенням інформаційного забезпечення. Це дозволить вдосконалити функціональність та продуктивність мережі в майбутньому.

Комп'ютерна мережа має бути гнучкою і адаптивною, щоб враховувати майбутні потреби та зміни в технологічному середовищі. Вона повинна бути здатна до швидкого реагування на зміни та впровадження нових розробок.

При розробці мережі важливо враховувати довгострокові вимоги і стандарти. Технології та підходи, що використовуються, повинні бути масштабованими та стійкими до змін у майбутньому.

Забезпечення цих аспектів сприятиме сталому розвитку та удосконаленню комп'ютерної мережі, забезпечуючи її ефективність, надійність та здатність відповідати зростаючим потребам бізнесу.

### 2.1.1.7 Показники призначення

Комп'ютерна мережа призначена для легкого та швидкого спілкування та обміну інформацією між співробітниками, відділами та підрозділами компанії. Це сприяє швидкому та ефективному обміну документами, електронними

повідомленням, даними про замовлення та іншою важливою інформацією. Система дозволяє співробітникам Стеко спільно використовувати ресурси, такі як принтери, сканери, сховища даних та програмне забезпечення. Це полегшує спільну роботу над проектами, спільний доступ до документів та співпрацю між різними відділами компанії. Система забезпечує централізоване управління комп'ютерами, користувачами, даними та безпекою в компанії. Адміністратори мережі можуть надавати доступ до ресурсів, встановлювати політики безпеки, контролювати роботу мережі та забезпечувати резервне копіювання даних. Комп'ютерна система призначена автоматизувати рутинні завдання, спрощувати обробку даних, прискорювати комунікацію та сприяти підвищенню продуктивності співробітників.

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

**2.1.1.8.1Необхідні умови та режими експлуатації для забезпечення використання технічних засобів системи з заданими технічними характеристиками.**

Для забезпечення використання технічних засобів (ТЗ) системи з заданими технічними показниками, система повинна функціонувати безперервно цілодобово, забезпечуючи неперервну доступність та забезпечуючи час, необхідний для технічного обслуговування.

В системних приміщеннях рівень масової концентрації пилу в повітрі не повинен перевищувати 0,75 мг/м³, а електрична складова електромагнітного поля не повинна перевищувати 0,3 Н/м в діапазоні частот від 0,15 до 300,00 МГц. Напруга живлення мережі повинна бути 220 В, 50 Гц.

Необхідно дотримуватися вимог щодо пожежної безпеки та електробезпеки, зокрема заземлення, у приміщеннях згідно з відповідними нормативними документами, такими як ГОСТ 12.1.004-91 "ССБТ. Пожежна безпека. Загальні вимоги", ГОСТ Р 50571.22-2000 "Електроустановки будівель. Частина 7. Вимоги до спеціальних електроустановок. Розділ 707. Заземлення устаткування обробки

інформації", Правила улаштування електроустановок та Правила техніки безпеки при експлуатації електроустановок споживачів. Приміщення для експлуатації системи повинні відповідати вимогам ГОСТ 15150-69 (зі змінами 2004) "Машини, прилади та інші технічні вироби. Виконання для різних кліматичних районів. Категорії, умови експлуатації, зберігання і транспортування в частині впливу кліматичних факторів зовнішнього середовища" для виду кліматичного виконання УХЛ категорії 4.2.

Мережа повинна забезпечувати свою працездатність в умовах нормальних кліматичних умов, де температура навколишнього повітря коливається від +15°С до +25°С, відносна вологість навколишнього повітря становить до 75% при атмосферному тиску від 84 кПа до 107 кПа. Крім того, система повинна бути стійкою й працездатною при впливі екстремальних кліматичних факторів, таких як температура навколишнього повітря від 10°С до 45°С, відносна вологість повітря від 40% до 80% при температурі +10°С та атмосферний тиск від 84 кПа до 107 кПа.

Дотримання цих умов та вимог забезпечить надійну та безперебійну роботу системи відповідно до заданих технічних показників.

**2.1.1.8.2 Вимоги до параметрів мереж енергопостачання**

Для забезпечення безпечної та надійної експлуатації системи необхідно враховувати наступні вимоги до параметрів мереж енергопостачання:

Кожне працююче місце повинно мати електричні розетки з напругою 220 В і частотою 50 Гц, які мають заземлюючий контакт. Це забезпечить сумісність зі стандартами електричної мережі та забезпечить безпеку підключених пристроїв.

Відповідно до НАПБ А 01.001-2004, заборонено наступні дії:

- експлуатація кабелів та проводів з пошкодженою або втраченою захисною ізоляцією, а також залишення під напругою кабелів та проводів з неізольованими провідниками;
- використання саморобних подовжувачів, які не відповідають вимогам переносних електропроводок;

- користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електричними пристроями, а також лампами, скло яких має сліди затемнення або випинання;
- використання електроапаратури та приладів в умовах, що не відповідають рекомендаціям виробників;

дотримання цих вимог допоможе уникнути небезпечних ситуацій та забезпечить безпеку під час використання електроенергіїЖ

**2.1.1.8.3 Вимоги щодо кількості, кваліфікації персоналу, який забезпечує обслуговування, і вимоги до робочого режиму цього персоналу.**

Перед тим, як наймати персонал обслуговування мережі, необхідно розрахувати оптимальну кількість працівників, відповідно до обсягу та складності робіт. Персонал повинен мати відповідну кваліфікацію, зокрема знання технічних аспектів системи та вміння ефективно виконувати свої обов’язки. Потрібно розробити режим роботи, який буде включати часи обслуговування, планові перерви та виконання завдань у встановлені терміни. Персонал повинен бути дисциплінованим та готовим діяти відповідно до встановлених процедур і стандартів.

Також необхідно зібрати відповідну команду до якої будуть входити:

1. Адміністратори системи – спеціалісти, відповідальні за виконання спеціальних технологічних завдань та управління компанією в цілому. Вони повинні мати доступ до Інтернету, серверів і здатність взаємодіяти між підсистемами.
2. Команда експлуатації, яка забезпечить нормальне функціонування технічних і програмних засобів системи.
3. Відділ кадрів: який відповідатиме за пошук нових кваліфікованих працівників. Вони також повинні мати доступ до Інтернету, серверів і здатність взаємодіяти між підсистемами.

**2.1.1.8.4 Критерії для компонування, розташування та зберігання запасних виробів і пристроїв.**

На складі обов’язково мають бути резервні компоненти комп'ютерної мережі, включаючи мережеві комутатори, маршрутизатори, бездротові точки доступу, кабелі, роз'єми і конектори, кабелі Ethernet і бездротові антени Також слід виділити місце для запасних блоків живлення для комп'ютерів, серверів та мережевих пристроїв, запасні комп’ютери та ноутбуки також повинні бути.

Запасні вироби і прилади мають зберігатись в безпечному і захищеному приміщенні. Наявність замків, системи безпеки і контролю доступу до приміщення, де зберігаються запасні вироби, допоможе у випадку крадіжок. Бажано упорядкувати склад використовуючи спеціальні стелажі, шафи або контейнери, це дозволить швидше та легше перераховувати запаси.

Зберігати компоненти потрібно в приміщеннях з контрольованою температурою і вологістю, щоб уникнути пошкоджень від екстремальних умов. Запасні вироби і прилади повинні зберігатися у спеціальних антистатичних упаковах, та бути захищеними від прямих сонячних променів, пилу, вологи і корозії

Записи про всі запасні вироби та прилади повинні бути точними і актуальними. Регулярно проводити інвентаризації та оновлення списку запасних виробів. При створенні списку варто вказувати дати придбання, гарантійного терміну та інших важливих відомостей про запасні вироби.

**2.1.1.8.5 Вимоги до регламенту обслуговування**

Для підтримки комп’ютерної мережі необходно розробити графік обслуговування, який включатиме технічні огляди і профілактичні роботи. Регулярні діагностики обладнання допоможуть виявити можилві неполадки. Також слід оновлювати програмне забезпечення, включаючи операційну систему, антивірусне програмне забезпечення та драйвери. Для антивірусного програмного забезпечення оновлення слід проводити щодня. Для пришвидшення виявлення

можливих несправностей в мережі та комп’ютерах, слід встановити систему моніторингу.

Мережа має працювати цілодобово, для цього варти встановити резервне живлення, щоб уникнити проблем при переобої електропостачання. Також необхідно проводити регулярні перевірки і тестування запасних виробів та компонентів для виключеннях можливих відмов при заміні.

#### 2.1.1.9 Вимоги до патентної чистоти

Розробники технологій та програмних забезпечень повинні забезпечити патентну чистоту та захист від претензій виробників.

### 2.1.2 Додаткові вимоги

#### 2.1.2.1 Вимоги до активного обладнання, його функціонування, кількості портів та їх резерву, варіантів встановлення та технічних характеристик.

Загальна мета вимог до активного обладнання полягає в забезпеченні надійного та ефективного функціонування комп'ютерної мережі в компанії Стеко, щоб задовольняти потреби співробітників у швидкому та безперебійному обміні даними.

Активне обладнання повинно забезпечувати надійну та ефективну роботу мережі Стеко, забезпечуючи стабільну передачу даних і безперебійне підключення пристроїв.

Активне обладнання повинно мати достатню кількість портів для підключення всіх пристроїв у мережі, враховуючи поточні потреби і можливе майбутнє збільшення кількості пристроїв.

Обладнання повинно мати різноманітні варіанти встановлення, такі як монтаж на стіну, стійку або в шафу, це забезпечить гнучкість і зручність при розміщенні обладнання в мережі.

Активне обладнання повинно відповідати вимогам щодо продуктивності, швидкості передачі даних, низького рівня шуму та витрати енергії. Також

важливо, щоб обладнання мало довгий термін служби і було легким у керуванні та обслуговуванні.

Активне обладнання повинно мати достатню пропускну здатність, щоб забезпечити ефективну передачу даних між пристроями в мережі Стеко. До цих потреп входить пропускна здатність портів та швидкість передачі даних.

Активне обладнання повинно бути сумісним з встановленими стандартами мережі, такими як Ethernet, Wi-Fi, TCP/IP, IPv6 і т.д. Воно повинно підтримувати різні протоколи комунікації і забезпечувати сумісність з іншими пристроями у мережі Стеко.

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

У приміщеннях з підвищеною вологістю, таких, як їдальня, на підприємстві Стеко застосовуються спеціальні вимоги щодо кабель-каналів, інформаційних та електричних розеток. Нижче перераховані деякі з цих вимог:

1. Розетки та вимикачі повинні бути розташовані на поверхні, а не вмонтовані, що забезпечує безпеку та запобігає окисленню контактів.
2. Для розеток необхідно встановити пристрій захисного відключення. Ступінь захисту не повинен бути нижче IP44, що забезпечує захист від вологи та пилу.
3. У підрозетках необхідно забезпечити нерозривне під'єднання захисного провідника за допомогою варіння, опресовування, пружинних клем і т.д.
4. Електричні кабелі повинні бути вмонтовані в металеві коробки. При прокладці кабелів в кабельних каналах на поверхні стін або стелі також слід використовувати металеві коробки.
5. Кабель-канали інформаційної кабельної підсистеми повинні відповідати наступним вимогам:
    - простота монтажу;
    - стійкість та надійність в роботі;
    - достатня механічна цілісність та гнучкість;

- забезпечення швидкого доступу для обслуговування;
- наявність додаткового захисту від фізичних та хімічних пошкоджень.

Ці вимоги спрямовані на забезпечення безпеки та надійності електроустановок у приміщеннях з підвищеною вологістю на підприємстві Стеко.

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

Для забезпечення належного функціонування та безпеки комунікаційного обладнання у компанії Steko рекомендується розміщувати його в спеціальних мережевих шафах. Мережева щафа – пристрій для розміщення, організації та захисту комунікаційного обладнання комп'ютерної мережі. Така шафа є точкою в якій збираються усі комунікаційні з'єднання, кабелі та активне обладнання.
Мережева шафа повинна бути в захищеному від вологи та агресивного середовища місці. Для цих цілей можна виділити місце у серверній, або технічному приміщені.

Шафа може бути виготовлена з металу чи пластику, але обов'язково має бути заземлена. Без заземлення мережева шафа не зможе гарантувати електричної безпеки. Всередині шафа має вбудовані рейки, каркаси або кріплення для розміщення комунікаційних пристроїв, наприклад, комутаторів, маршрутизаторів, патч-панелей, серверів і т.д. Щоб шафа не нагрівалась від великої кількості процесів активного обладнання, в неї вбудовують систему охолодження.

**2.1.2.4 Вимоги до резервування**

З метою забезпечення резервування даних та можливості їх відновлення, рекомендується налаштувати систему для автоматичного резервного копіювання даних щодня. Ці налаштування можуть включати функції створення резервних копій на зовнішніх носіях, наприклад, жорсткі диски або хмарні сховища. Для економії простору можна використовувати інкрементальне копіювання. Ця процедура передає тільки змінені, або нові дані з попередньої резервної копії. Окрім автоматичного копіювання, варто також самостійно робити повне

копіювання даних. Повне копіювання необхідно робити хоча б декілька разів на місяць, щоб була можливість повного відтворення інформації.

Такий підхід зможе забезпечити регулярне резервне копіювання даних та відтворення даних у разі необхідності.

### 2.1.3 Вимоги до функцій, які виконує комп’ютерна мережа

Для того, щоб полегшити використовування комп’ютерної мережі, потрібно поділити мережу на підмережі, які будуть з’єднуватися між собою за допомогою кабелів, таких як FastEthernet та GigabitEthernet. Ці кабелі забезпечують з'єднання між різними комутаторами, які, у свою чергу, підключені до маршрутизаторів.

Комп’ютерна мережа повинна забезпечувати швидкий та безперебійний доступ до інформації, яку вона зберігає. Мережа має реєстратувати, аналізувати та контролювати усі ресурси, які використовуються. Для надійного захисту від внутрішніх загроз, необхідно завантажити ліцензійні антивіруси та програмне забезпечення які захищають від інфо-атак. Щоб покращити захист, система має бути забезпечена автоматизованим контролем безпеки та підтримкою резервного копіювання. Аби зайвий раз не лізти у мережу, можна забезпечити систему моніторингу та аналізу системи. Таке рішення дозволить дистанційно й швидко реагувати та вирішувати проблеми.

Такий підхід допоможе забезпечити ефективну роботу комп'ютерної системи для Steko, збереже конфіденційні дані та мінімізує ризики інформаційних атак.

### 2.1.4 Вимоги до видів забезпечення комп’ютерної мережі Steko

#### 2.1.4.1 Вимоги до програмного забезпечення

Інформаційне забезпечення - це система процесів та технологій, які спрямовані на забезпечення безпеки, надійності, конфіденційності й доступності інформації в системі. Воно забезпечує захист від вірусів, шпигунського програмного забезпечення, хакерьских атак та інших інформаційних загроз. Окрім безпеки, інформаційне забезпечення також має повищувати продуктивність, шляхом зручного використання, яке надає швидкий доступ до необхідної

інформаціїї та можливих з нею процедур. Щоб під’єднати інформаційне забезпечення, воно має бути сумісним з іншими додатками та системами, які використовує компанія Steko. При гарній сумісності треба забезпечети масштабованість системи, щоб її можно було розширити при необхідності. Для розширення системи необхідно продумати можливості додавання нових функцій, які можуть бути додані у майбутньому.

#### 2.1.4.2 Вимоги до лінгвістичного забезпечення

У компанії стеко працівники спілкуються українською мовою. Тому варто враховувати, що графічний інтерфейс у підсистемі повинен бути максимально перекладений для зручності користувача, адже він має бути зрозумілим та простим. Довідники та шаблони також мають бути створенні та перекладені на українську мову. Окрім довідників та шаблонів, варто мати підказки для уникнення помилок користувача, та базу додаткової інформації, до якої можна звернутися у разі незвичайної ситуації.

## 2.2 Розробка апаратної частини комп’ютерної системи

Враховуючи організаційну структуру компанії Steko, яка зображена на рисунку 1.1, та топологічних схем розміщення структурних відділів, які зображені на рисунку 1.3 та рисунку 1.4, потрібно розробити структурну схему комплексу технічних засобів комп’ютерної мережі.

При побудові мережі треба зсилатися на технічних вимогах до системи, які були описані у попередніх пунктах. Мережа буде поділена на підмережі, ділення буде розраховане відносно до структурної схеми. У підмережами пересилання трафіку має здійснюватись за рахунок протоколоу OSPF. Цей протокол використовується для в комп’ютерних мережах для обміну інформацією про маршрутизацію. Протокол є гарним рішенням, тому що дозволяє маршрутизаторам автоматично визначати найкоротший шлях для передачі даних.

На рисунках 2.1 та 2.2 зображені структурна схема апаратної частини та загальна архітектура мережі.

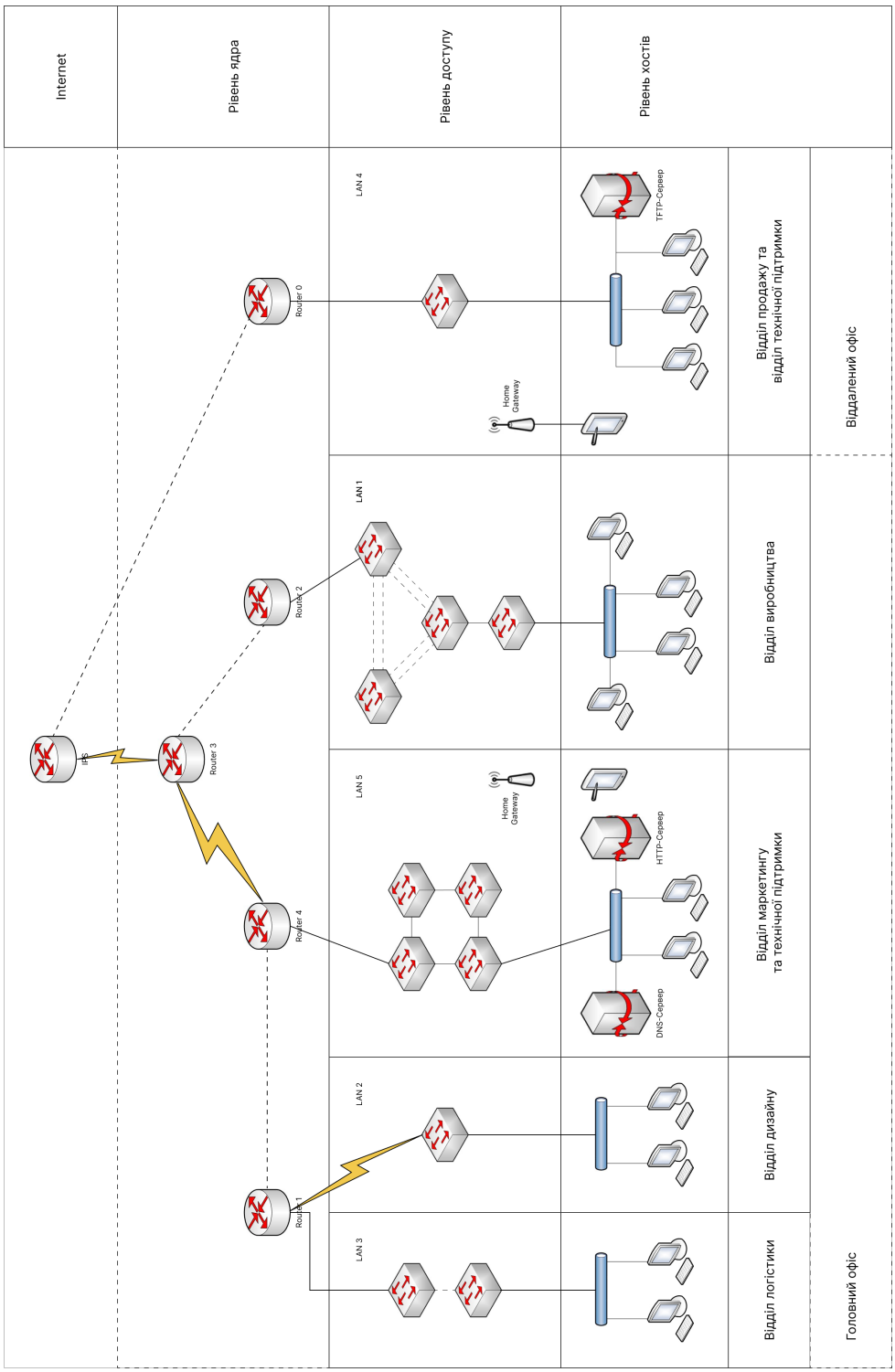


Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної системи

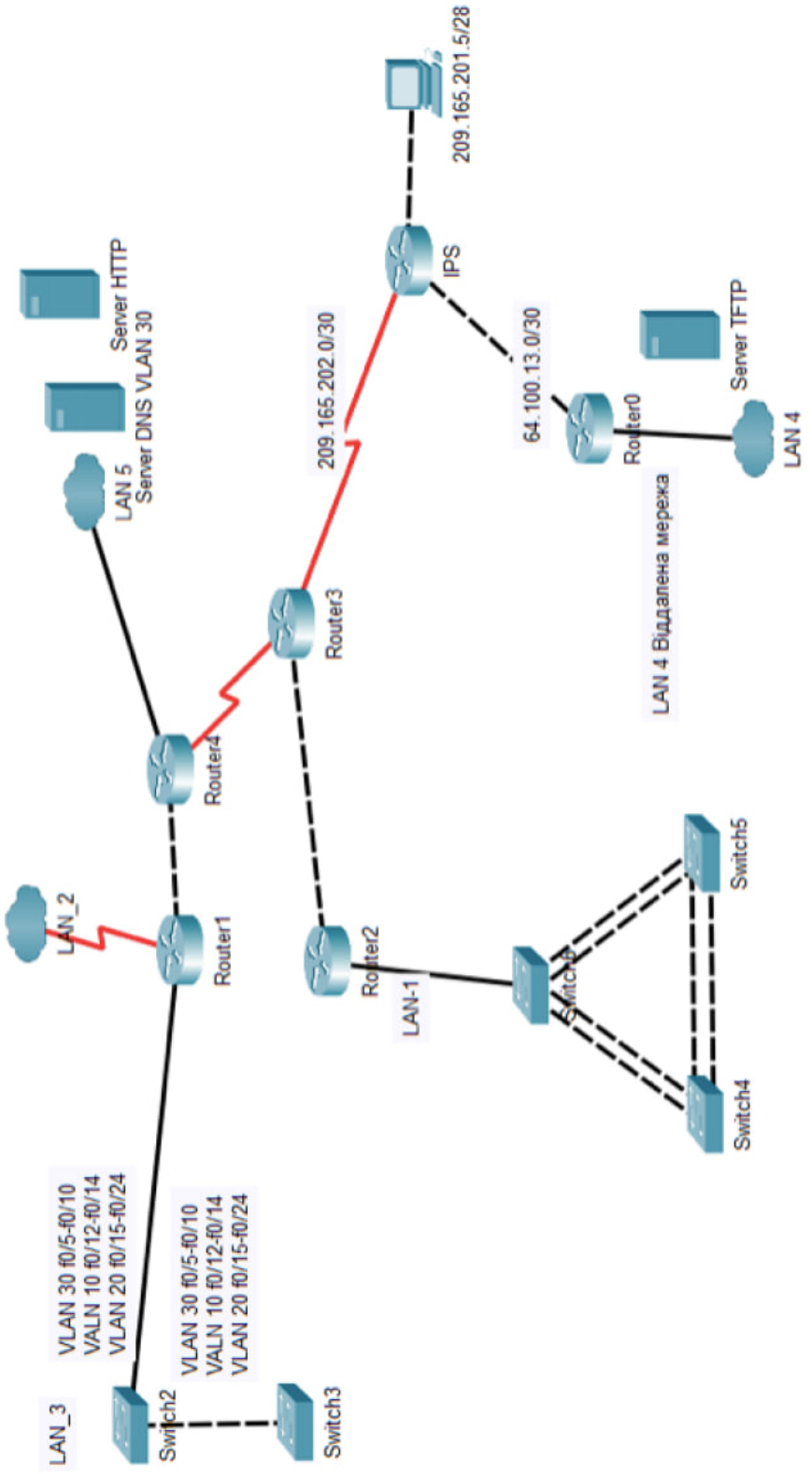


Рисунок 2.2 – Загальна архітектура мережі підприємства Стеко

### 2.2.1 Розробка специфікації апаратних засобів комп'ютерної системи

Компанія з виробки металевопластикових вікон «Steko» має одну власну чотирьох поверхову офісну будівлю, яка розташована на території заводу та орендує офіс, ближче до центру міста.

LAN1 містить в собі 75 вузлів враховуючи 10% запасу портів, потрібно обрати 4 комутатори по 24 порти. Загальна кількість портів у підмережі – 96 штук.

LAN2 містить в собі 11 вузлів, враховуючи 10% запасу портів, потрібно обрати 1 комутатор з 24 портами. Загальна кількість портів у підмережі – 24 штуки.

LAN3 містить в собі 30 вузлів, враховуючи 10% запасу портів, потрібно обрати 2 комутатора по 24 порти. Загальна кількість портів у підмережі – 48 штуки.

LAN4 містить в собі 19 вузлів, враховуючи 10% запасу портів, потрібно обрати 1 комутатор з 24 портами. Загальна кількість портів у підмережі – 24 штуки.

LAN5 містить 78 вузлів відповідно, враховуючи 10% запасу портів, потрібно обрати 4 комутатори по 24 порти. Загальна кількість портів у підмережах – 96 штук.

Загальна кількість та специфікація використаних пристроїв компанії Cisco представлена у таблиці 2.1.

Таблиця 2.1 – Специфікація обладнання, використаного під час створення корпоративної мережі для компанії «Steko»

| Позиція | Найменування і технічна характеристика | Тип, марка, позначення документа, опитувального листа | Одиниці виміру | Кількість | Примітки |
|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | Маршрутизатор серії Cisco 2911:<br>3 integrated GigabitEthernet<br>4x EHWIC slots<br>2x onboard DSP slots<br>1x ISM slot<br>512 - 2048 MB DRAM<br>256 MB Compact Flash | Cisco 2900 | од | 6 | За структурною схемою: Router0-5<br>Детальні характеристики: https://www.cisco.com/c/en/us/support/routers/2911-integrated-services-router-isr/model.html#~tab-specs |
| 2 | Комутатор серії Catalyst 2960:<br>24x 10/100 Ethernet Ports<br>2x 1GSFP amd RJ-45 combo uplinks | Cisco 2960-24PS | од | 12 | Детальні характеристики: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html |
| 3 | Маршрутизатор серії VDSL2:<br>4x 10/100/1000 LAN ports<br>1x 10/100/1000 Gigabit Ethernet WAN port<br>1x VDSL2<br>IEEE 802.11ac wireless access-point | Cisco RV134W VDSL2 | од | 2 | Детальні характеристики: https://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/datasheet-c78-736465.html |

Об’днання до одніє мережі усіх пристроїв потребує потужного обладнання, тому було вирішено використовувати три сервери: DNS-сервер, HTTP-сервер та TFTP-сервер. Для об’єднання маршрутизаторів між собою, використовується Serial, а для під’єднання комп’ютерів до маршрутизаторів необідно використовувати порти FastEthernet.

Прикладом структурованної кабельної мережі стане віддалений офіс, тому що він менший і на ньому буде легче показати план розміщення вузлів комп’ютерної мережі. На рисунку 2.3 зображена спроектована схема розміщення кабелів.

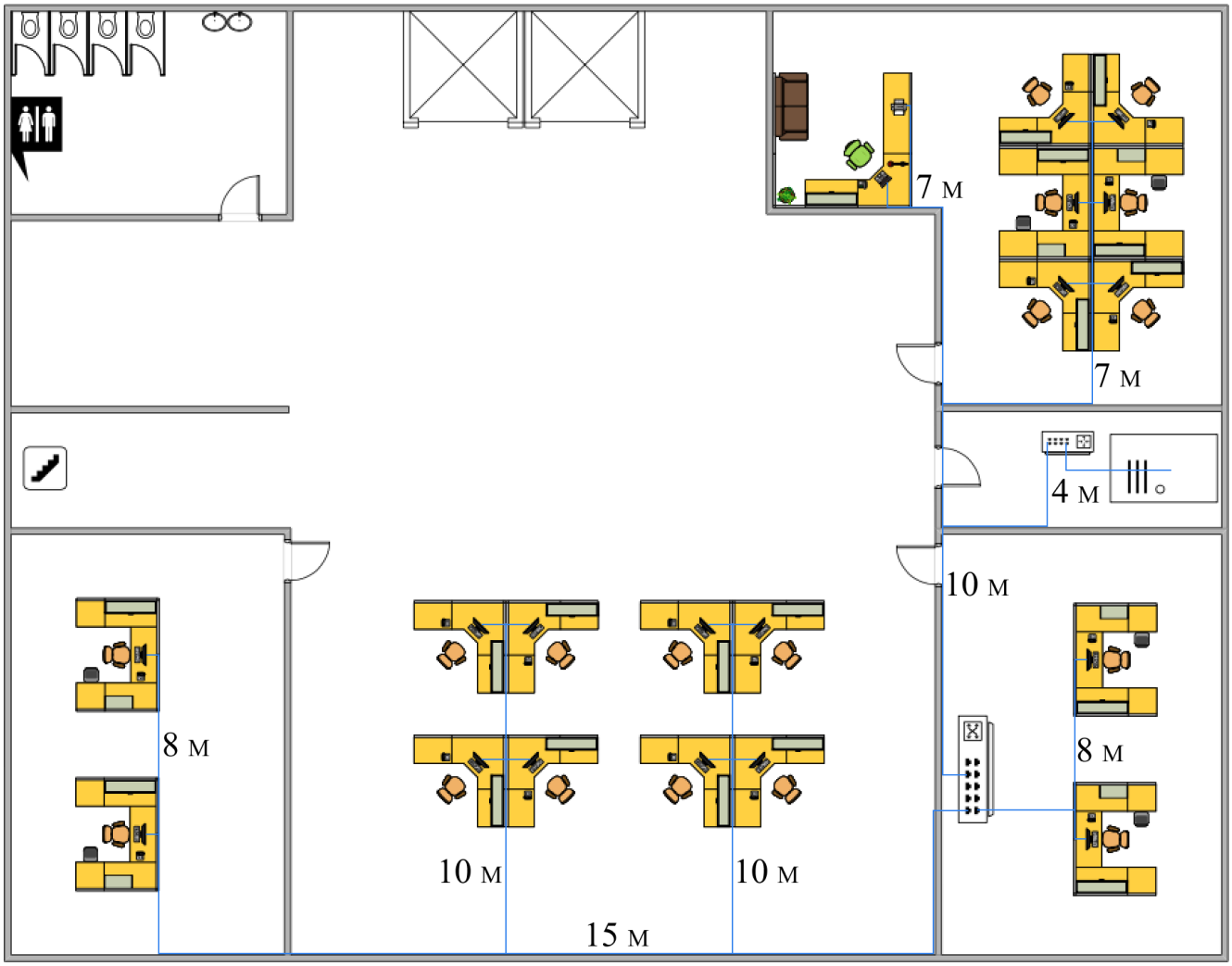


Рисунок 2.3 – Схема розміщення кабельних мереж віддаленого офісу Steko

Для віддаленого офісу було вирішено використовувати розташовувати кабельні канали у підлозі вдовж стін з використанням комп’ютерних розеток, які мають роз’єм RJ-45. У таблиці 2.2 знаходиться специфікація СКМ віддаленного офісу, яка враховує фізичні розміри приміщення та розташування вузлів.

Таблиця 2.2 – Специфікація структурованої кабельної мережі

| Позиція | Найменування і технічна характеристика | Тип, марка, позначення документа, опитувального листа | Одиниці виміру | Кількість | Примітки |
|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | Підлоговий кабельний канал алюмінієвий 18х15мм | Simon | м | 80 | За проєктом LAN4 для крученої пари |
| 2 | Розетка комп'ютерна RJ45 UTP кат. 5E подвійна | Asfora | од | 24 | За проєктом LAN4 |
| 3 | Розетка із заземленням подвійна | Mono | од | 48 | За проєктом LAN4 |
| 4 | LAN-кабель U/UTP кат 5E | OK-Net | м | 110 | За проєктом LAN4 |
| 5 | Кабель живлення ПВС 3х1 | Одес-Кабель | м | 90 | За проєктом LAN4 |
| 6 | Кабельний канал пластиковий 20х40 | Simon | м | 100 | За проєктом LAN4 |

### 2.3 Розробка специфікації апаратних засобів комп'ютерної мережі

Під час розробки мережі, було вирішено використовувати маршрутизатори моделі Cisco 2911 та комутатори Cisco Catalyst 2960, які будуть забезпечувати зв'язок між комп'ютерами. Комп'ютери були обрані стандартні офісні моделі ARTLINE Business B47v11Win з шестиядерним процесором AMD Ryzen 8 5700G (3.8 - 4.6 ГГц), оперативною пам'яттю 16 ГБ, твердотільним SSD накопичувачем обсягом 480 ГБ, відеокартою AMD Radeon Vega 8 та з попередньо встановленою операційною системою Windows 11 Pro.

Сервера для мережі були обрані моделі Cisco UCS C220 M3 LFF. Це звичайний сервер, який має процессор: 2 шт x Intel Xeon E5-2650L v2, 16 GB DDR3 (2 x 8 GB) RAID-контроллер: Cisco UCS RAID SAS 2008M-8i Mezzanine Card UCSC-RAID-11-C220 74-10149-01, Мережевий контролер: 2x порти 1 Gb Ethernet.

Для комп'ютерної мережі було обрано мережеве обладнання від виробника Cisco, таке рішення має вилучити проблеми із сумісностью компонентів.

### 2.4 Визначення показників інтенсивності вихідного трафіку найбільшої локальної мережі підприємства.

Вихідний трафік маршрутизується в лінію з пропускною здатністю у 1000 Мбіт на секунду.

Важливо не перенавантажувати маршрутизатора, для цього швидкість надходження пакетів повинна бути меншої за швидкість відправлання пакетів.

Для проведення розрахунків, візьмемо значення рівне максимальному розміру навантаження пакетів у канальному рівні моделі OSI:

$$\mu_{вих} = 1000000000/(650*8) = 192307,7 \text{ пакетів/с} \quad (2.1)$$

Оскільки в середньому, кожне джерело виробляє 85 пакетів/с, то маршрутизатор обмежен кількістю приєднань з наступної формули:

$$N = 192307,7/85 = 2262 \text{ джерел.} \quad (2.2)$$

Що задовольняє нашу найбільшу локальну мережу, яка складається з 78 ПК.

Кожен з 78 ПК посилає потік заявок з інтенсивністю у 85 кадрів/с. Інтенсивність вихідного трафіку:

$$\lambda = 78*85 = 6630 \text{ пакетів/с.} \quad (2.3)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{6630}{192307,7} = 0,03 \quad (2.4)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0,03}{1-0,03} = 0,03 \quad (2.5)$$

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

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{(192307,7 - 6630)} = 5,38 мкс \quad (2.6)$$

Це значення задовольняє нашим вимогам.

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0.03^2}{1-0.03} = 0.001 \quad (2.7)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0,001}{6630} = 1,5 мкс \quad (2.8)$$

Пропускна здатність каналу:

$$b = \lambda * \text{довжина кадру} = 6630*650*8 = 34476000 \text{біт/с} = 34,5 \text{Мбіт/с} \quad (2.9)$$

Це задовольняє пропускній здатності каналу в 1000Мбіт/с.

Висновки: Була розроблена структера комп’ютерної мережі для компанії Steko, мережева архітектура мережі задовольнє отримане від компанії завдання, а пропускна здатність каналу також задовольняє вимоги, що підтверджується аналізом трафіку мережі.

# 3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

## 3.1 Розрахунок адресації корпоративної мережі

Використовуючи структуру мережі компанії Steko, яку наведено на рисунку 2.2, необхідно створити модель комп'ютерної мережі.

В кожній підмережі має бути мережна адреса, яка надається за принципом 10.23.20.0/22 відповідно до таблиці 3.1.

Таблиця 3.1 – Виділений блок адрес для компанії

| № | Адреса мережі | LAN_1 | LAN_2 | LAN_3 | LAN_4 | LAN_5 |
|---|---|---|---|---|---|---|
| 2 | 10.23.20.0 | 75 | 11 | 30 | 19 | 78 |

Комп'ютерна мережа компанії Steko буде поділена на 5 підмереж, с загальною кількістю у 213 користувачів.

Опираючись на кількість пристроїв у кожній підмережі, можна поділити діапазон на два відрізки по 128 адрес, два відрізки по 32 адреси та один відрізок з 16 адресами.

Для виділення переведемо адресу мережі в двійковий вид і відокремимо незадіяну в операції частину: 10.23.00010100.00000000.

Підмережа LAN_1, містить 75 користувачів. Для неї мінімальний блок адрес дорівнює 128 адресам.

Для розрахунків отримуємо кінець діапазону: 10.23.00010100.01111111

Отриману адресу 10.23.00010100.01111111 переводимо в десятичні значення та отримаємо адресу 10.23.20.128 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.20.255 та діапазоном доступних адрес 10.23.20.129 - 10.23.20.254.

Наступні підмережі рахуемо так само, додаючи по 1 біту до мережевої частини, після розрахунків отримали настпуні результати.

Адресацію з урахуванням вимог до мережі представлено у таблиці 3.2

Таблиця 3.2 – Схема адресації мережі

| Підмережа | Розмір | Виділений розмір | Адреса | Маска | Діапазон доступних адрес | Широкомовна адреса |
|---|---|---|---|---|---|---|
| LAN1 | 75 | 128 | 10.23.20.128 | /25 | 10.23.20.129 - 10.23.20.254 | 10.23.20.255 |
| LAN2 | 11 | 32 | 10.23.21.160 | /27 | 10.23.21.161 - 10.23.21.190 | 10.23.21.191 |
| LAN3 | 30 | 128 | 10.23.21.0 | /25 | 10.23.21.1 - 10.23.21.126 | 10.23.21.127 |
| LAN4 | 19 | 32 | 10.23.21.128 | /27 | 10.23.21.129 - 10.23.21.158 | 10.23.21.159 |
| LAN5 | 78 | 128 | 10.23.20.0 | /25 | 10.23.20.1 - 10.23.20.126 | 10.23.20.127 |

У наступній таблиці 3.3 продемонстрована схема адресації каналів WAN між маршрутизаторами з діапазону 10.1.2.0/24.

Таблиця 3.3 – Підмережі каналів WAN між маршрутизаторами

| Підмережа | Розмір | Виділений розмір | Адреса | Маска | Діапазон доступних адрес | Широкомовна адреса |
|---|---|---|---|---|---|---|
| WAN1 | 2 | 4 | 10.1.2.0 | /30 | 10.1.2.1 - 10.1.2.2 | 10.1.2.3 |
| WAN2 | 2 | 4 | 10.1.2.4 | /30 | 10.1.2.5 - 10.1.2.6 | 10.1.2.7 |
| WAN3 | 2 | 4 | 10.1.2.8 | /30 | 10.1.2.9 - 10.1.2.10 | 10.1.2.11 |

### 3.2 Розрахунок адресації пристроїв

Для зручності подальшої роботи, задокументуємо у таблиці 3.4 адресацію всіх маршрутизаторів мережі. Цей підхід дозволить швидко відновити адресацію у разі випадкових несправностей.

Таблиця 3.4 – Схема адресації пристроїв

| Пристрій | Інтерфейс | IP-адреса | Маска |
|---|---|---|---|
| Vakhrushev_Router_0 | Gig0/0 | 10.1.2.10 | 255.255.255.252 |
| | Gig0/1.12 | 10.23.21.33 | 255.255.255.224 |
| | Gig0/1.22 | 10.23.21.65 | 255.255.255.224 |
| | Gig0/1.32 | 10.23.21.1 | 255.255.255.224 |
| | Gig0/1.99 | 10.23.21.97 | 255.255.255.240 |
| | Gig0/1.2 | 10.23.21.161 | 255.255.255.224 |
| Vakhrushev_Router_1 | Gig0/0 | 10.1.2.9 | 255.255.255.252 |
| | Gig0/1 | 10.23.20.1 | 255.255.255.128 |
| | Se0/3/1 | 10.1.2.2 | 255.255.255.252 |
| Vakhrushev_Router_2 | Gig0/0 | 10.1.2.6 | 255.255.255.252 |
| | Gig0/1 | 10.23.20.129 | 255.255.255.128 |
| Vakhrushev_Router_3 | Gig0/0 | 10.1.2.5 | 255.255.255.252 |
| | Se0/3/0 | 209.165.202.2 | 255.255.255.252 |
| | Se0/3/1 | 10.1.2.1 | 255.255.255.252 |
| Vakhrushev_Router_5 | Gig0/0 | 64.100.13.2 | 255.255.255.252 |
| | Gig0/1 | 10.23.21.129 | 255.255.255.224 |
| Vakhrushev_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 |

До таблиці 3.5 занесемо адреси інтерфейсів комутаторів в підмережах. Для п’яти підмережм ми маємо вісім комутаторів.

Таблиця 3.5 – IP-адреси комутаторів в підмережах відділів

| Підмережа | Пристрій | IP-адреса SVI інтерфейсу | Маска підмережі | Адреса шлюзу |
|---|---|---|---|---|
| LAN1 | Vakhrushev_Switch_0 | 10.23.20.13 | 255.255.255.224 | 10.23.20.129 |
| | Vakhrushev_Switch_6 | 10.23.20.13 | | |
| | Vakhrushev_Switch_5 | 10.23.20.13 | | |
| LAN2 | Vakhrushev_Switch_2 | 10.23.21.16 | 255.255.255.22 | 10.23.21.161 |
| LAN3 | Vakhrushev_Switch_3 | 10.23.20.98 | 255.255.255.240 | 10.23.20.97 |
| | Vakhrushev_Switch_7 | 10.23.20.99 | | |
| LAN4 | Vakhrushev_Switch_4 | 10.23.21.13 | 255.255.255.22 | 10.23.21.129 |
| LAN5 | Vakhrushev_Switch_1 | 10.23.20.2 | 255.255.255.12 | 10.23.20.1 |

### 3.3 Налаштування моделі комп’ютерної мережі корпоративної мережі

Корпоративна мережа складається з головного та віддаленого офісу. На рисунку 3,1 зображена топологічна схема, яка складається з корпоративної мережі та мережі провайдера. На схемі головний офіс складається з усіх LAN`ів, окрім LAN_4, томе що він характеризує віддалений офіс. Усі компоненти мережі з’єднуються за допомогою кабелів Serial, Ethernet та GigabitEthernet.

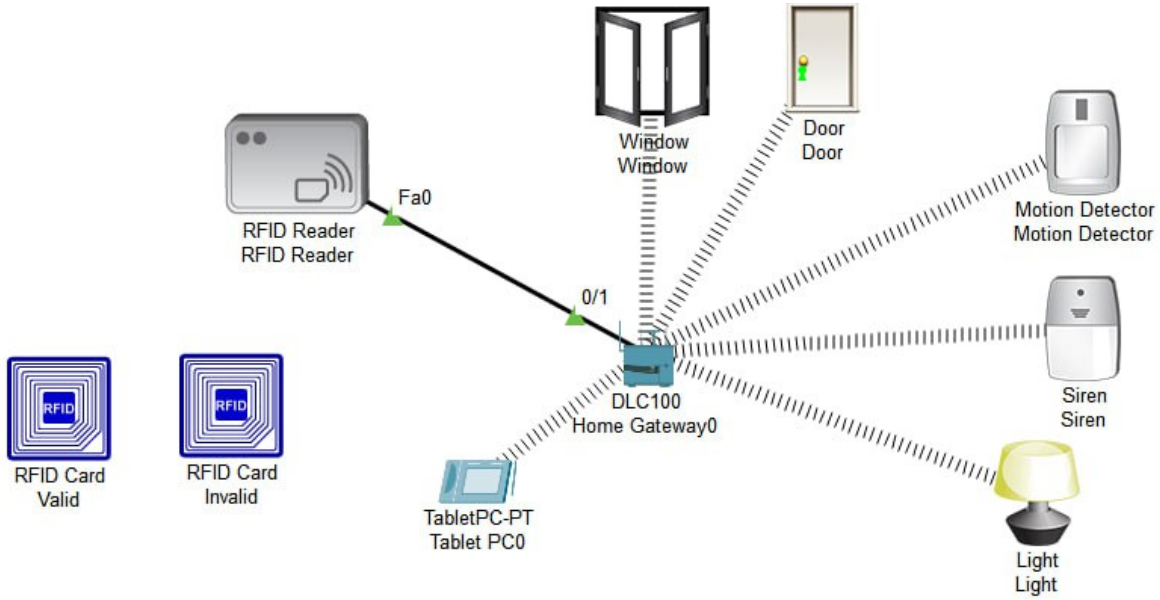


Рисунок 3.1 – Схема компонентів для корпоративної мережі виборбничої компанії «Steko»

### 3.4 Налаштування та перевірка роботи комп'ютерної мережі

#### 3.4.1 Базове налаштування конфігурації пристроїв

Для захисту обладнання від несанкціонованого доступу виконаємо базове налаштування пристроїв на прикладі Vakhrushev_Router_5:

enable // вмикає привілеї підтримки на роутері

conf t // перехід в режим конфігурації роутера

hostname Vakhrushev_Router_5 // зміна назви маршрутизатора

line console 0

password cisco // встановлює пароль "cisco" для доступу до порту консолі

login

line vty 0 15

password cisco // встановлює пароль "cisco" для доступу до віртуальних терміналів

login

enable secret class // встановлює зашифрований пароль для підтвердження підвищених привілеїв

service password-encryption // вмикає шифрування паролів в конфігурації

banner motd 'Vakhrushev_Router_5' // встановлення повідомлення MOTD ("Message of the Day")

ip domain-name Vakhrushev_Router_5 // встановлення доменного ім’я для роутера

crypto key generate rsa // генерує RSA ключ для шифрування трафіку.

1024 // встановлення кількості бітів ключа

username 123191_Vakhrushev password admincisco // створює користувача

line vty 0 15

transport input ssh // встановлює протокол SSH для входу в віртуальні термінали

login local

Ці строки коду виконують налаштування роутера, встановлюють паролі, шифрують паролі, створюють користувачів та встановлюють засоби аутентифікації для доступу до роутера.

### 3.4.2 Налаштування маршрутизаторів корпоративної мережі

Для взаємодії користувачів між різними підмережами, необхідно налаштувати маршрутизації на маршрутизаторах комп’ютерної мережі.

Маршрутизацію можна виконати, як статично, додав маршрути, або динамічно за допомогою протоколу динамічної маршрутизації.

Для комп’ютерної мережі компанії «Steko» був обран протокол маршрутизації OSPF, тому що це відкритий протокол маршрутизації, який працює на обладнанні будь-якого виробника, на відмінну від протоколу EIGRP, який працює тільки на обладнані Cisco.

Налаштування OSPF включає в себе оголошення безпосередньо підключених локальних мереж та відключення поширення оновлень маршрутизації на інтерфейси локальних мереж.

Налаштування протоколу OSPF на Vakhrushev_Router_2:

router ospf 1 // входить в режим налаштування OSPF та надає номер процесу

passive-interface default // встановлює всі інтерфейси роутера в пасивний режим за замовчуванням

no passive-interface Serial0/3/0 // видаляє інтерфейс Serial0/3/0 з пасивного режиму OSPF, що дозволяє роутеру оголошення через цей інтерфейс

no passive-interface Serial0/3/1

network 10.23.21.160 0.0.0.31 area 0 // додає мережі необхідні для маршрутизації мереж

network 10.23.21.0 0.0.0.31 area 0

network 10.23.21.32 0.0.0.31 area 0

network 10.23.21.64 0.0.0.31 area 0

network 10.1.2.8 0.0.03 area 0

Налаштуємо маршрут за замовчуванням на маршрутизаторі Vakhrushev_Router_5, який має пряме підключенням до ISP. Це необхідно для його розповсюдження, далі наведені приклади команд:

ip route 0.0.0.0 0.0.0.0 64.100.13.1 // встановлює маршрут за замовчуванням, що означає, що будь-який пакет, для якого немає конкретного маршруту

redistribute static subnets // вмикає розповсюдження статичних маршрутів через протокол OSPF

Додаємо статичний маршрут до мережі провайдера ISP:

ip route 64.100.13.1 255.255.255.252 64.100.13.1

Проводимо налаштування пропускної здатності та тактової частоти на прикладі Serial-інтерфейсів на маршрутизаторі Vakhrushev_Router_1.

int se0/3/1 // обирає конкретний інтерфей

bandwidth 128 // налаштовує пропускну здатність на значення 128 Кб/с

clock rate 2000000 // встановлює тактову частоту у 2000000 bps на DCE-інтерфейсах мрушрутизаторів

Узявши для прикладу прилад Vakhrushev_Router_3, налаштуємо підтримку служби AAA. Після вдалого налаштування, виконуємо процедуру для усіх маршрутизаторів. Для виконання налаштувань використовувалися наступні команди:

aaa new-model // вмикає нову модель AAA (Authentication, Authorization, Accounting)

radius-server host 10.23.20.12 auth-port 1645 key radius123 // налаштовує адресу RADIUS та порт підключення

aaa authentication login CONSOLE group radius local // Налаштовує аутентифікації для групи CONSOLE через RADIUS-сервер

line console 0

login authentication CONSOLE // Налаштовує аутентифікації для консольного порту

aaa authentication login default local // створює локальну базу даних користувачів

username Vakhrushev_Router_3 password admin123 // налаштовує логін та пароль для локальної бази

line vty 0 15

login authentication default

### 3.5 Перевірка роботи комп'ютерної мережі

Перевірку роботи комп'ютерної мережі починаємо з перевірки DHCP-серверів. Для перевірки необхідно відкрити інтерфейм ПК, та на вкладці «Desktop» потрібно включити отримання адрес через DHCP. Ці кроки необхідно виконати на кожному комп'ютері підмережі маршрутизатора.

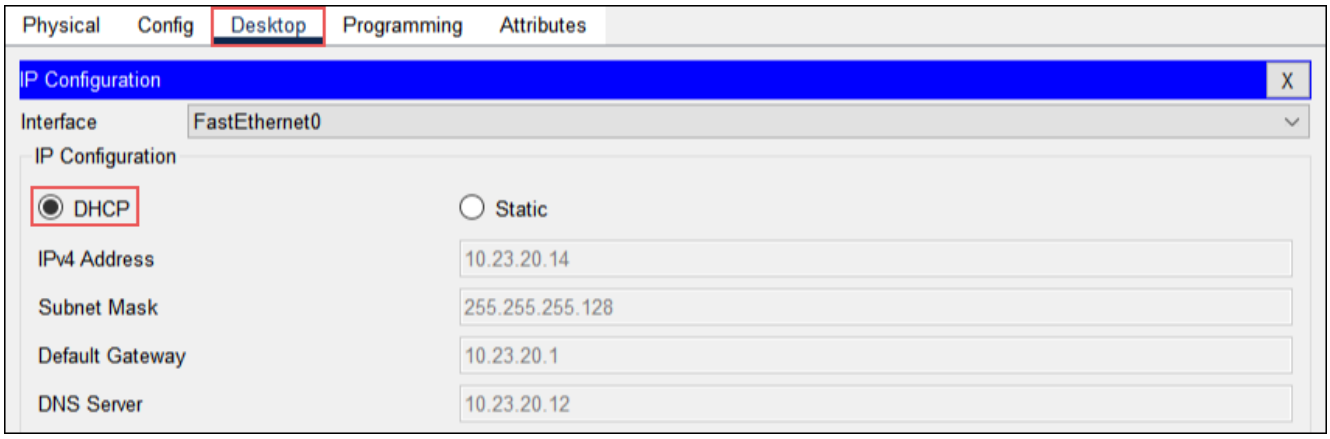


Рисунок 3.2 – Перевірка роботи DHCP-серверу

Комп'ютер успішно отримав адресу через DHCP та інформацію про DNS-сервер та мережу.

Далі надсилаємо Ping-пакет від помп'юетра з підмережі LAN_2 до комп'ютера з підмережі LAN_3. Ці дії виконуються для перевірки протоколу OSPF. Open Shortest Path First – це протокол динмаічної маршрутизації, який використовується для визначення найкоротших шляхів передачі даних.

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|---|---|---|---|---|---|---|---|---|---|
| | Successful | PC1(1) | PC6 | ICMP | | 3.539 | N | 0 | (edit) |
| | Successful | PC2(1) | PC8 | ICMP | | 5.755 | N | 1 | (edit) |
| | Successful | PC3(1) | PC6 | ICMP | | 7.536 | N | 2 | (edit) |

Рисунок 3.3 – Перевірка роботи маршрутизації

Тепер перевіримо роботу NAT. Для перевірки потрбіно надіслати Ping-пакет від комп'ютера з мережі організації до комп'ютера у мережі провайдера. Під час перевірки також зафіксуємо статистику перетворень NAT (рисунки 3.4-6)

```
Vakhrushev_Router_3#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.4     10.23.20.10        ---                ---
tcp 209.165.200.4:80   10.23.20.10:80     209.165.205.5:1025 209.165.205.5:1025
tcp 209.165.200.4:80   10.23.20.10:80     209.165.205.5:1026 209.165.205.5:1026
```

Рисунок 3.4 – Статистика перетворень до надсилання пакетів

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|---|---|---|---|---|---|---|---|---|---|
| | Successful | PC10(1) | PC0 | ICMP | | 1.663 | N | 5 | (edit) |
| | Successful | PC2(1) | PC0 | ICMP | | 4.602 | N | 6 | (edit) |
| | Successful | PC3(1) | PC0 | ICMP | | 4.602 | N | 7 | (edit) |

Рисунок 3.5 – Успішний результат пересилки пакетів

```
Vakhrushev_Router_3#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.5:4   10.23.20.145:4     209.165.201.5:4    209.165.201.5:4
icmp 209.165.200.6:3   10.23.20.144:3     209.165.201.5:3    209.165.201.5:3
icmp 209.165.200.7:1   10.23.20.148:1     209.165.201.5:1    209.165.201.5:1
---  209.165.200.4     10.23.20.10        ---                ---
tcp 209.165.200.4:80   10.23.20.10:80     209.165.205.5:1025 209.165.205.5:1025
tcp 209.165.200.4:80   10.23.20.10:80     209.165.205.5:1026 209.165.205.5:1026
```

Рисунок 3.6 – Статистика перетворень після надсилання пакетів

Під час виконання роботи був створен сайт, роботу якого необхідно перевірити. Цей крок необхідний у якості практики візиту веб-сайту. Перевірка проходить на будь-якому ПК у мережі (рисунок 3.7).

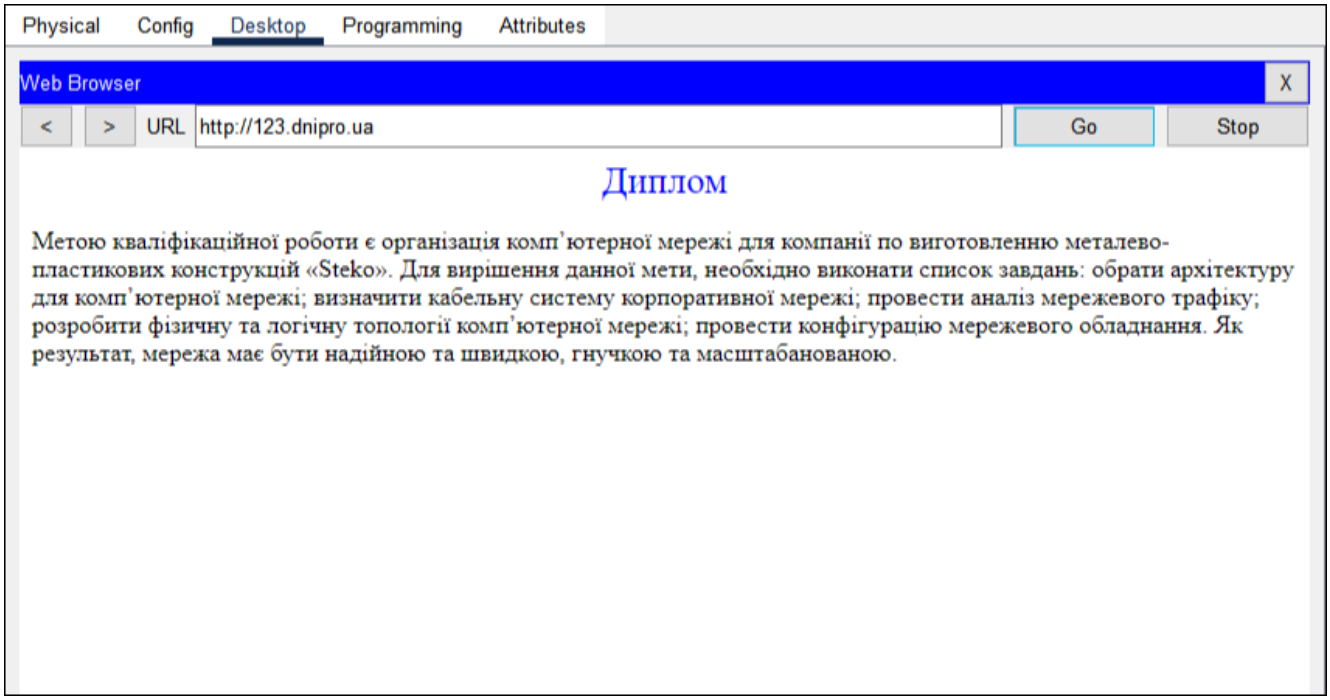


Рисунок 3.7 – Перевірка роботи тестового сайту за адресою 123.dnipro.ua

Залишилось виконати перевірку роботи VPN. Для цього до основної мережі потрібно відправити Ping-пакет з віддаленої мережі, під час перевірки зафіксуємо статистику перетворень, щоб була можливість побачити результати (рисунки 3.8-10).

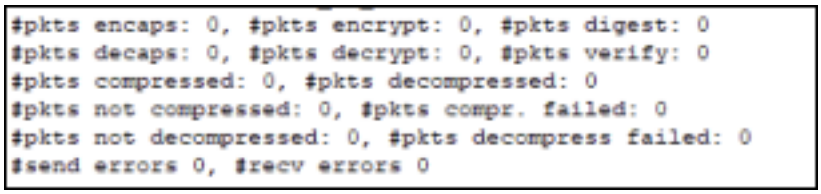


Рисунок 3.8 – Статистика перетворень до надсилання пакетів


Рисунок 3.9 – Успішна робота VPN

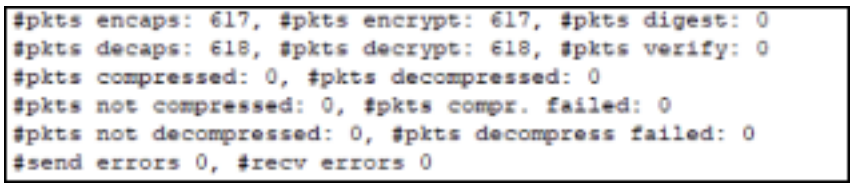


Рисунок 3.10 – Статистика перетворень після надсилання пакетів

### 3.6 Захист інформації від несанкціонованого доступу

При з'єднанні з мережею, хакер може збирати конфідеційну інформацію. Для уникнення таких ситуацій необхідне налаштування мережі, яке дозволить вчасно виявляти потенційні загрози, що допомооже захистити систему від несанкціонованого доступу та знизити шанс витрати інформації. Комп’ютерна мережа компанії Steko має три основні типи захисту конфідеційної інформації:

1. Фізичний захист, що включає заходи забезпечення безпеки кабельної системи, електроживлення та засоби архівації.
2. Адміністративний захист, що включає контроль доступу до приміщень, розробку стратегії безпеки компанії та планування дій у надзвичайних ситуаціях.
3. Програмний захист, що включає використання антивірусних програм, систем розмежування повноважень та програм контролю доступу.

Завдяки взаємодії між собою, створюється комплексна система захисту, яка зберігає інформацію та запобігаю спробам несанкіцонованого доступу

### 3.7 Налаштування мереж VLAN

Для виконання налаштувань підмережа LAN_3 була розділена на три підмережі VLAN. Номери використаних VLAN мереж внесено до таблиці 3.6

Таблиця 3.6 – Мережі VLAN

| Номер VLAN | Ім’я VLAN | Примітка |
|---|---|---|
| VLAN1 | Default | Не використовується |
| VLAN99 | Management | Для керування пристроями |
| VLAN100 | Native | Власна |

Таблиця 3.7 – Схеми адресації підмереж VLAN

| Назва | Розмір | Адреса | Маска | Діапазон адрес | Широкомовна адреса |
|---|---|---|---|---|---|
| VLAN32 | 32 | 10.23.21.0 | 255.255.255.224 | 10.23.21.1 - 10.23.21.30 | 10.23.21.31 |
| VLAN12 | 32 | 10.23.21.32 | 255.255.255.224 | 10.23.21.33 - 10.23.21.62 | 10.23.21.63 |
| VLAN22 | 32 | 10.23.21.64 | 255.255.255.224 | 10.23.21.65 - 10.23.21.94 | 10.23.21.95 |
| VLAN99 | 16 | 10.23.21.96 | 255.255.255.240 | 10.23.21.97 - 10.23.21.110 | 10.23.21.111 |
| VLAN100 | 8 | 10.23.21.112 | 255.255.255.248 | 10.23.21.113 - 10.23.21.118 | 10.23.21.119 |

Таблиця 3.8 – Розподіл портів для окремих мереж VLAN

| Назва | VLAN | Розподіл портів |
|---|---|---|
| VLAN32 | 32 | F0/5-f0/10 |
| VLAN12 | 12 | F0/12-f0/14 |
| VLAN22 | 22 | F0/15-f0/24 |

Таблиця 3.9 – Адресація пристроїв в LAN_3.

| Пристрій | Інтерфейс | Адреса | Маска | Шлюз | VLAN |
|---|---|---|---|---|---|
| Switch2 | SVI | 10.23.21.162 | 255.255.255.224 | 10.23.21.161 | 99 |
| Router1 | G0/1.12 | 10.23.21.33 | 255.255.255.224 | 10.23.21.32 | 12 |
| | G0/1.22 | 10.23.21.65 | 255.255.255.224 | 10.23.21.64 | 22 |
| | G0/1.32 | 10.23.21.1 | 255.255.255.224 | 10.23.21.0 | 32 |
| | G0/1.99 | 10.23.21.97 | 255.255.255.240 | 10.23.21.96 | 99 |

Для пояснення було вирішено описати налаштування технології VLAN на прикладі комутатора Vakhrushev_Switch_2, далі наведені строки коду, використанні під час налаштувань

int range fa0/5-10 // вибирає діапазон інтерфейсів FastEthernet від 5 до 10.

switchport mode access // встановлює режим роботи інтерфейсу як "access", що означає, що інтерфейс використовується для підключення кінцевих пристроїв

switchport access vlan 32 // присвоює вказаному діапазону інтерфейсів VLAN 32 як вхідний VLAN

```
int range fa0/12-14
switchport mode access
switchport access vlan 12
int range fa0/15-24
switchport mode access
switchport access vlan 22
int range fa0/1-4
```

switchport mode trunk // інтерфейс використовується для передачі даних між комутаторами і підтримує різні VLAN

```
switchport trunk native vlan 100
switchport trunk allowed vlan 32,12,22,99-100
```

Налаштування портів на комутаторах, які привласнили адреси з мережі Management VLAN:

```
int vlan 99
ip address 10.23.21.162 255.255.255.224
ip default-gateway 10.23.21.161
```

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

Для надання мережних налаштувань користувачам в кожній з підмереж VLAN компанії використовується протокол динамічної адресації DHCP. Щоб забезпечити цю функціональність, потрібно налаштувати маршрутизатор, який виконує маршрутизацію між мережами VLAN, у якості DHCP-сервера.

ip dhcp excluded-address 10.23.21.1 10.23.21.10 // виключає діапазон IP-адрес, що означає, що ці адреси не будуть назначатись DHCP-клієнтам

```
ip dhcp excluded-address 10.23.21.33 10.23.21.42
```

ip dhcp excluded-address 10.23.21.65 10.23.21.74

ip dhcp excluded-address 10.23.21.161 10.23.21.170

ip dhcp pool VLAN12 // створення пулу адрес для VLAN12

network 10.23.21.32 255.255.255.224 // визначає мережу як частину пулу VLAN12

default-router 10.23.21.33 // встановлює IP-адресу маршрутизатора за замовчуванням

dns-server 10.23.20.12 // встановлює IP-адресу сервера DNS

ip dhcp pool VLAN22

network 10.23.21.64 255.255.255.224

default-router 10.23.21.65

dns-server 10.23.20.12

ip dhcp pool VLAN32

network 10.23.21.0 255.255.255.224

default-router 10.23.21.1

dns-server 10.23.20.12

Також налаштуємо функцію безпеки портів на комутаторах:

int f0/8 // входить в режим налаштування інтерфейсу FastEthernet

switchport mode acces // встановлює режим доступу, порт стає призначенийм для підключення кінцевого пристрою

switchport port-security // вмикає функцію безпеки порту

switchport port-security maximum 2 // встановлює максимальну кількість дозволених MAC-адрес на порту комутатора

switchport port-security mac-address sticky // додає MAC-адреси автоматично в таблицю безпеки порту

switchport port-security violation restrict // становлює дію, яка відбувається, коли порушується безпека порту

Ці строки коду налаштовують порт комутатора, включаючи режим доступу, функцію безпеки порту і обмеження доступу до порту згідно з параметрами

безпеки, такими як максимальна кількість MAC-адресів і дія при порушенні безпеки.

Висновок: По зовершенню моделювання комп’ютерної мережі у просторі Cisco Packet Tracer, була отримана мережа для компанії Steko, яка задовольня поставлені задачі, такі як встановлення NAT чи VPN. Перед сдачею, мережа була перевірена на функціонування та відповідність нормам.

# 4 РОЗРОБКА КОМПОНЕНТУ ДЛЯ КОНТРОЛЮ ДОСТУПУ

## 4.1 Інженерне рішення по розробці компонента системи

Інтернет речей (IoT) став невід'ємною складовою сучасних комп'ютерних систем і був успішно впроваджений в комп'ютерну мережу компанії "Steko" відповідно до вимог замовника. IoT-система безпеки офісу включає різні пристрої, такі як IoT-двері, вікна, датчики вогню, сирени та RFID-зчитувачі з картками.

Робота IoT-системи виглядає наступним чином: RFID-зчитувач перевіряє ідентифікаційні картки. Якщо ідентифікатор на картці співпадає з дозволеним, сигнал надсилається на IoT-сервер, який розблоковує двері та відчиняє вікна. У разі неспівпадіння ідентифікатора з дозволеним, спрацьовує сирена, а вікна, якщо вони були відчинені, автоматично закриваються.

Також, якщо датчик вогню виявляє вогонь, він відправляє сигнал на IoT-сервер, який активує сирени для сповіщення про небезпеку. Для забезпечення зв'язку між пристроями був використаний HomeGateway, який виступає в ролі сервера IoT. Пристрої підключаються до HomeGateway бездротовим зв'язком, який базується на стандарті IEEE 802.11 (Wi-Fi).

## 4.2 Налаштування обладнання та сервісів системи IoT

Перед тим як створити IoT- систему безпеки, необхідно оновити топологічну схему, шляхом додавання в неї IoT пристроїв, та під’єднати їх до HomeGateway.

Для забезпечення цього, необхідно на HomeGateway налаштувати бездротову точку доступу з іменем Vakhrushev-123-19-1 у головному офісі компанії і Vakhrushev-123-19-1-2 у віддаленому офісі. Для забезпечення безпеки мережі, ми обираємо протокол WPA2-PSK із паролем cisco123. Топологічну схему корпоративної мережі з позиціонованими пристроями IoT можна побачити на рисунку 4.1.

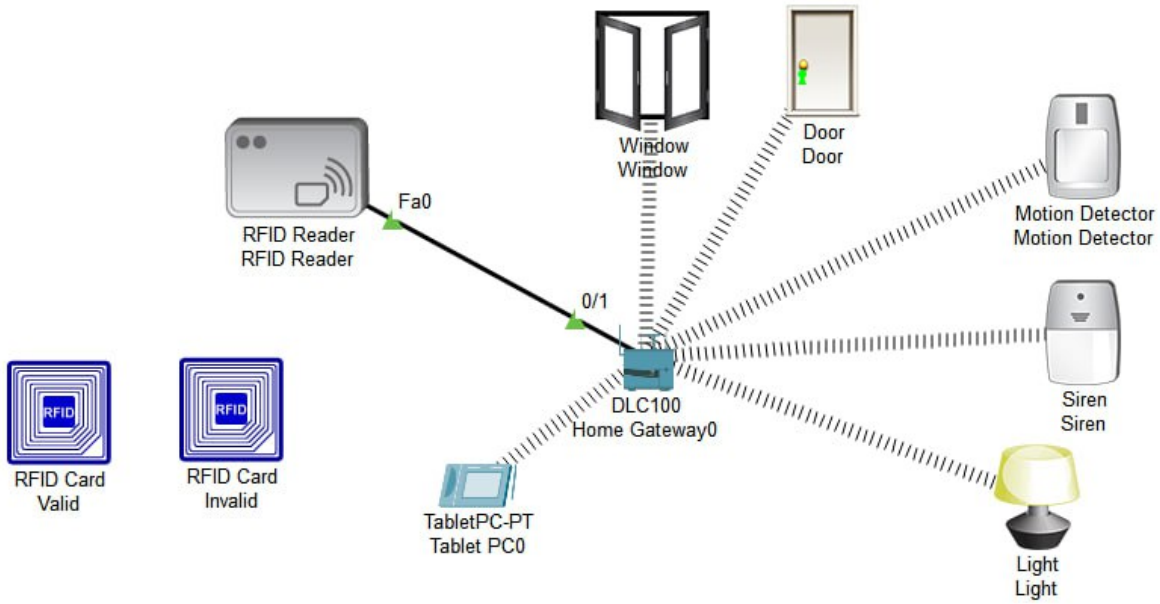


Рисунок 4.1 – Топологічна схема компонентів IoT-систнми безпеки компанії «Steko»

Налаштування IoT-системи були виконані на планшетних ПК, які під’єднані до однієї мережі за IoT-пристроями.

Для налаштування системи, на сервері потрібно створити сценарії роботи для кожного IoT-пристрої. Налаштування виконуються у планшетному-ПК, який підключен до мережі серверу. Щоб розпочати налаштування необхідно відкрити на планшеті вкладку «IoT Monitor», потім ввести логін та пароль, після чого відкриється вкладка «Home» на якій є список усіх підключених пристроїв. Налаштування сценаріїв виконуєтсья на вкладці «Conditions» (рисунок 4.2).

Для цього через додані підключений до мережі серверу планшет відкриваємо IoT Monitor, вводимо дані логіну та паролю, після чого потрапляємо на сторінку з усіма підключеними пристроями. Для налаштування сценаріїв переходимо на вкладку «Conditions», яку зображено на рисунку 4.2.

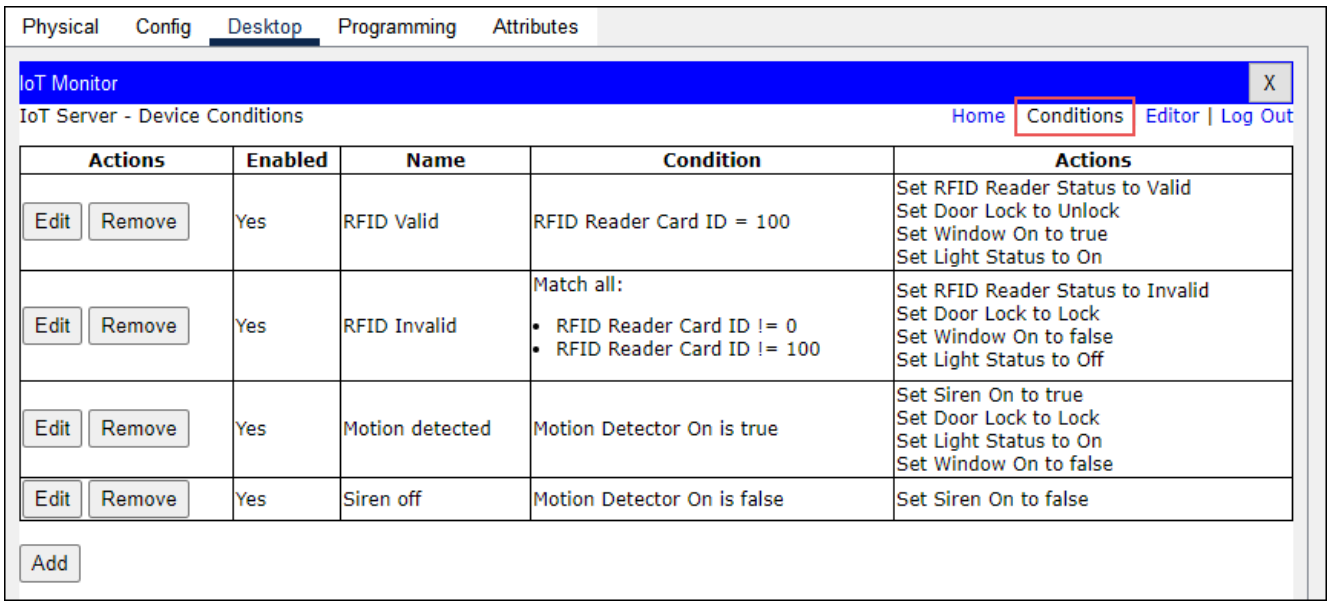


Рисунок 4.2 – Основний вигляд вкладки «Conditions»

Для забезпечення безпеки, на території компанії Steko працівники використовують особисті ID-картки, завдяки яким вони мають доступ до різних відділів на території підприємства. Для моделювання роботи ID-картки використовується RFID-зчитувач.

RFID-зчитувач має дві повевідинки, коли ID-картка підходить та коли вона не підходить. У разі використовування правильної ID-картки, можна відчинити двері, та вікна та увімкнути світло. Якщо ID-картка не буде підходити, тоді двері та вікна будуть зачинені, а світло буде вимкнутим.

На рисунках 4.3-4 зображені сценарії RFID-зчитувачів.

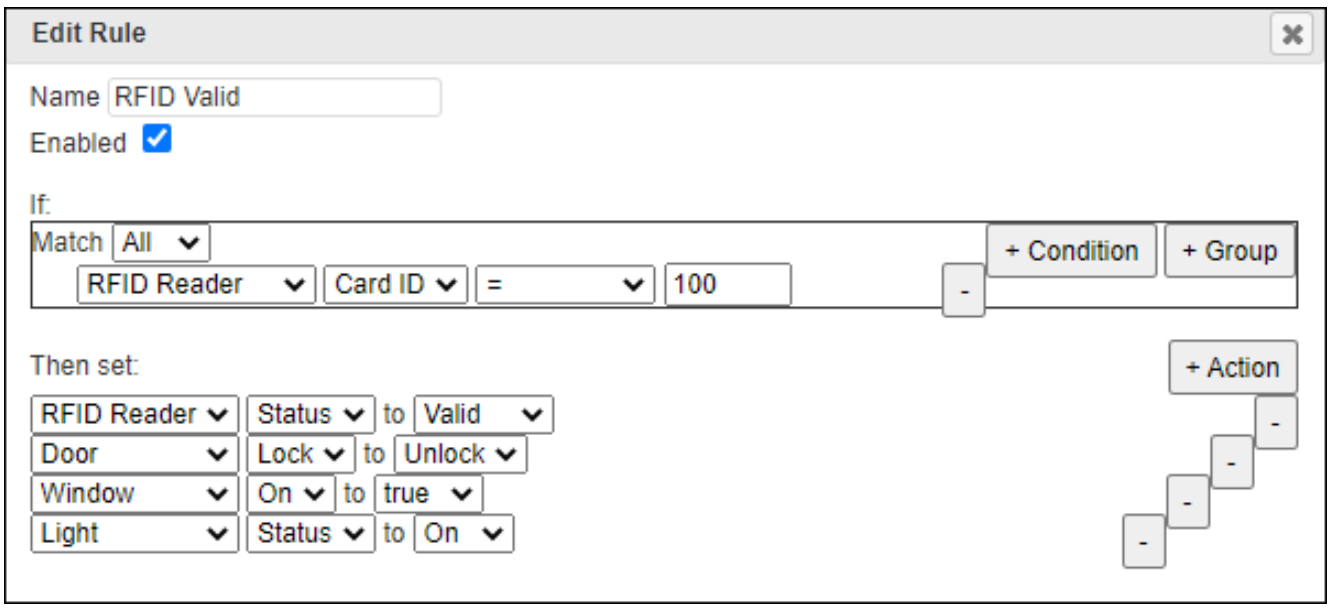

Рисунок 4.3 – Сценарій RFID-зчитувача, якщо картка підходить

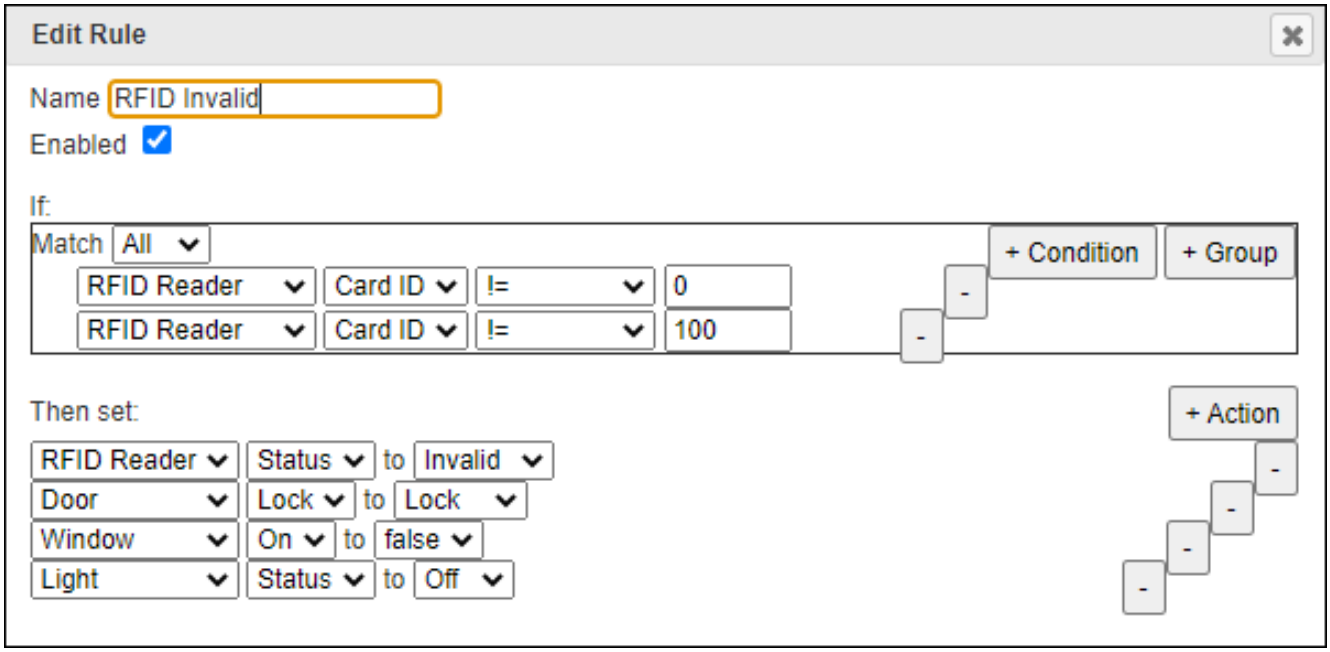


Рисунок 4.4 – Сценарій RFID-зчитувача, якщо картка не підходить

Окрім RFID-зчитувачів, також треба налаштувати детектор руху. У разі несанкціонованого вторгнення, детектор руху повинен зафіксувати підозрілу активнсіть, після чого зачиняються усі двері та вікна, та вмикається світло разом з сиреною охорони. Приклад налаштованого сценарію наведено на рисунку 4.5

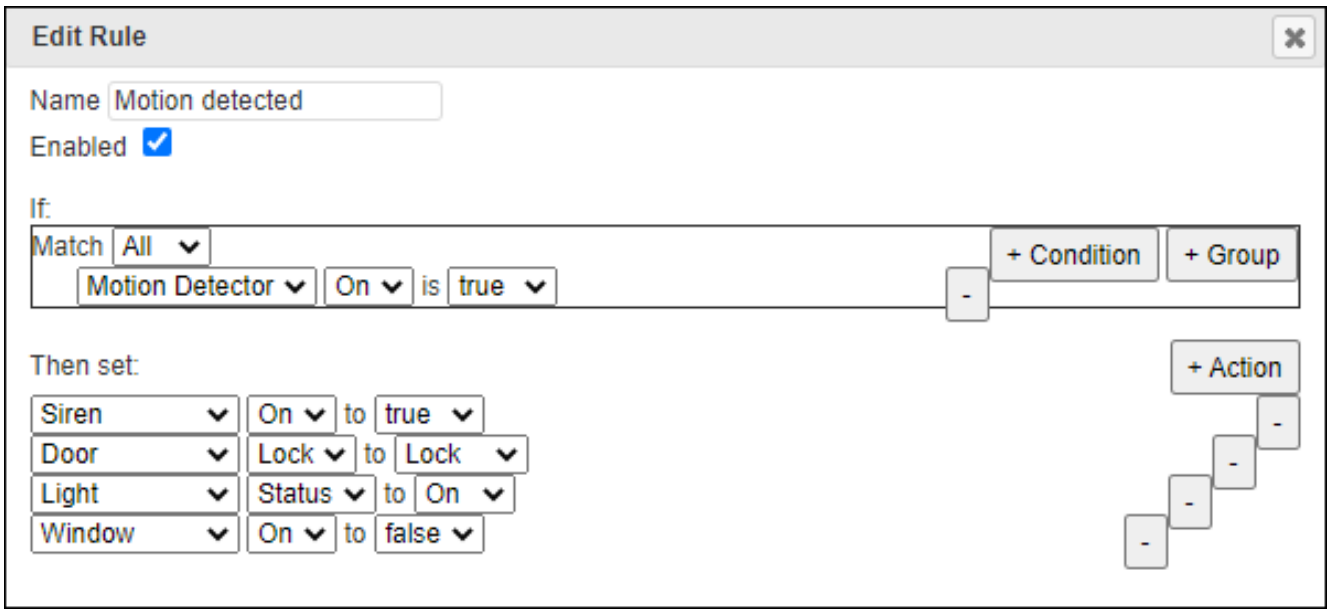


Рисунок 4.5 – Сценарій детектору руху

Оскільки сирена пов’язана з детектором руху, необхідно її відповідно налаштувати. Сирена має бути вимкнена, якщо детектор має значення «false» та вмикатися, коли значення змінюється на «true». Сценарій наведено на рисунку 4.6

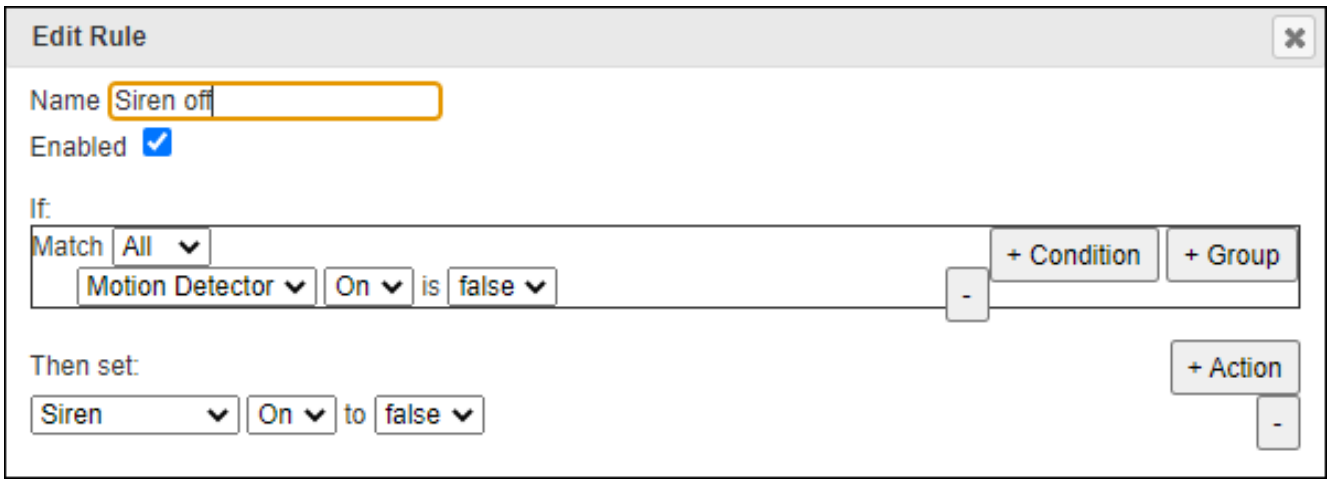


Рисунок 4.6 – Сценарій сирени у стані спокою

Висновки: Для виробничої компанії «Steko» була розроблена система інтернет речей. Метою системи було покращення захисту та безпеки офісів компанії. Замовника дуже торбувало питання ідентифікації персоналу, з чим дуже дуже добре справилися RFID-зчитувачі для ID-карток. Тепер на території офісу та заводу не буде постороніх осіб.

# Висновки

Під час виконання кваліфікайіної роботи була проведена комплексна аналітична робота, спрямована на розробку та впровадження ефективної комп'ютерної мережі підтримки прийняття рішень в організації ТОВ «Стеко».

Узявши до уваги потреби і вимоги компанії, вдалось визначити оптимальну архітектуру мережі для забезпечення ефективного обміну даними та забезпечення безпеки і захищеності інформації. Було проведено аналіз і вибір необхідного обладнання, такого як комутатори, маршрутизатори, сервери інші мережеві пристрої, з урахуванням потреб компанії.

У роботі описані процеси побудови мережі, такі як фізичне розташування пристроїв, конфігурацію мережевих параметрів, налаштування VLAN і сегментування мережі для забезпечення ефективного управління трафіком та підвищення безпеки. Були виконані заходи забезпечення безпеки, включаючи налаштування системи виявлення вторгнень, використання шифрування трафіку і встановлення політик безпеки. Були розроблені процедури резервного копіювання даних та відновлення системи для забезпечення високої доступності і захисту інформації.

Після успішного впровадження комп'ютерної мережі ТОВ «Стеко» отримає приріст продуктивності та ефективності в своїй діяльності. Забезпечення безпеки і надійності мережі дозволяє компанії захищати конфіденційну інформацію і запобігати потенційним загрозам з боку зовнішніх атак.

## Перелік посилань


1. Компанія «Steko» [Електронний ресурс] - https://steko.ua
2. Старий сайт компанії «Steko» [Електронний ресурс] – https://steka.online
3. Дилерська программа [Електронний ресурс] – https://dealer.steko.com.ua/index.php?product
4. Вікна «Steko» [Електронний ресурс] – https://steko.okna.ua/ua/
5. Досье компанії «Steko» [Електронний ресурс] – https://youcontrol.com.ua/catalog/company_details/38114294/
6. Корпоративна мережа [Електронний ресурс] - https://www.wiki-data.uk-ua.nina.az/%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%96_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96.html
7. Комп’ютерна мережа [Електронний ресурс] - https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0
8. Захист інформації в локальних мережах [Електронний ресурс] - https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97_%D0%B2_%D0%BB%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0%D1%85
9. Сервер Cisco [Электронный ресурс] : https://servak.com.ua/servers/servery-cisco/server-cisco-ucs-c220-m3-lff.html?gclid=CjwKCAjw9e6SBhB2EiwA5myr9qWr2RJOq2eELoFd3imggWeEIEeYVBto-J8tjfxnbfmhjmP5oHa3WhoCLioQAvD_BwE
10. ДСТУ “ГОСТ 12.1.004-91 "ССБТ. Пожежна безпека. Загальні вимоги»”.

11. ДСТУ “ГОСТ Р 50571.22-2000. "Електроустановки будівель. Частина 7. Вимоги до спеціальних електроустановок. Розділ 707. Заземлення устаткування обробки інформації»”.
12. ДСТУ “ГОСТ 15150-69 (зі змінами 2004) "Машини, прилади та інші технічні вироби. Виконання для різних кліматичних районів. Категорії, умови експлуатації, зберігання і транспортування в частині впливу кліматичних факторів зовнішнього середовища" для виду кліматичного виконання УХЛ категорії 4.2”.

# Додаток А

## Загальна архітектура мережі

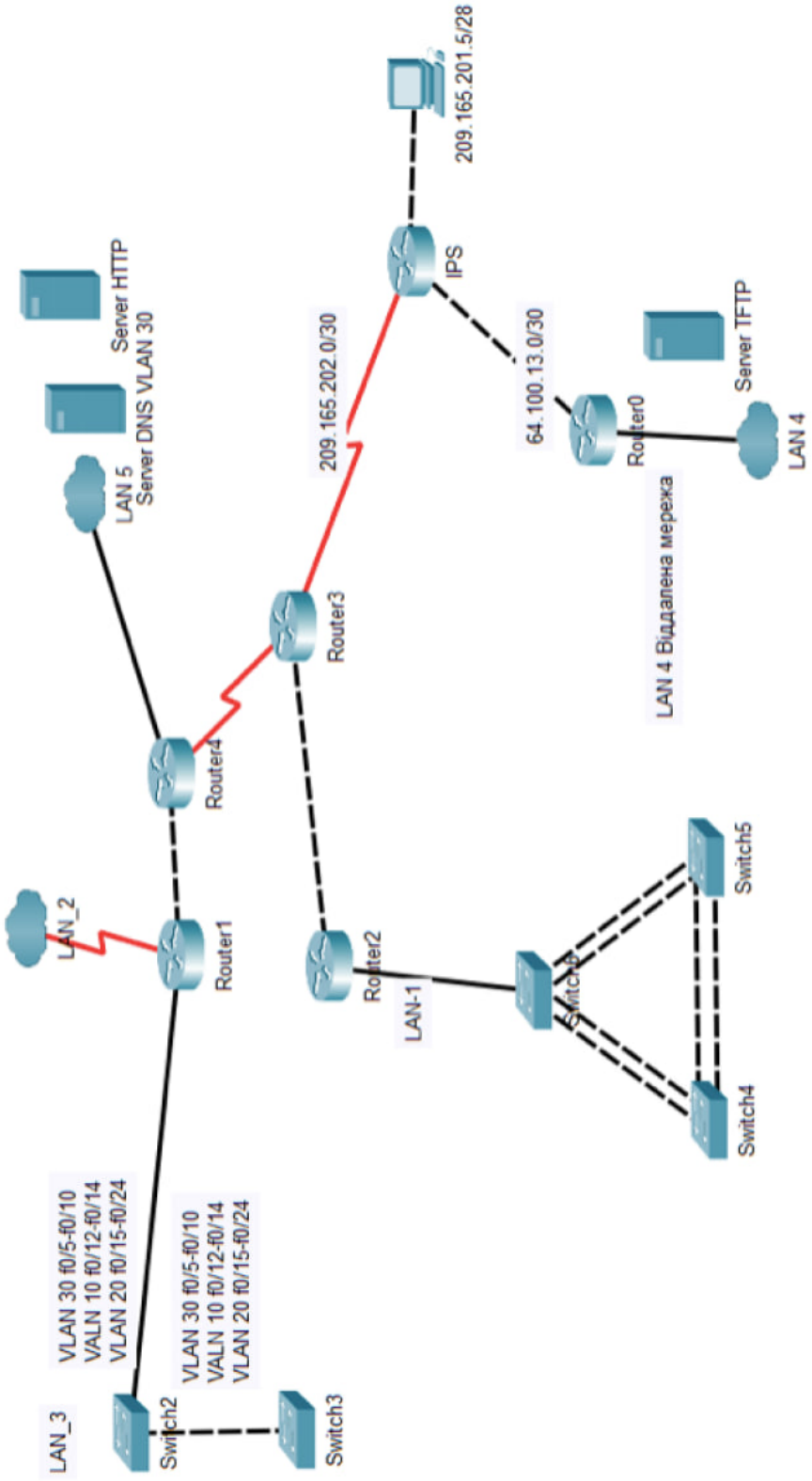


Рисунок А.1 – Загальна архітектура мережі підприємства «Steko»

# Додаток Б

## Тексти програм налаштування мережі комп’ютерної системи

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

# ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23002-01 12 01

Листів 12

2023

# АНОТАЦІЯ

Цей документ містить програмне забезпечення маршрутизаторів виробництва Cisco, яке призначене для структурної схеми моделі комп'ютерної мережі.

Тексти програм реалізовані за допомогою мови конфігураційних скриптів, спеціально розробленої для налаштування мережного обладнання Cisco.

Для розробки та налагодження цих скриптів використовується пакет моделювання мереж "Cisco Packet Tracer", який працює в операційній системі Windows 10.

# ЗМІСТ

1. Скрипт налаштування Router3:

```
Current configuration : 3028 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Vakhrushev_Router_3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
!
!
!
!
!
!
no ip cef
```

```
no ipv6 cef
!
!
!
username 123191_Vakhrushev password 7 082048430017061E010803
username Vakhrushev_Router_3 password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX152468T3-
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 VPN2
!
```

```
!
!
!
ip domain-name Vakhrushev_Router_3
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 10.1.2.5 255.255.255.252
 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 209.165.202.2 255.255.255.252
 ip nat outside
 crypto map MAP
!
interface Serial0/3/1
 ip address 10.1.2.1 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.2.4 0.0.0.3 area 0
 network 10.1.2.0 0.0.0.3 area 0
 network 209.165.202.0 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT2 pool Internet
ip nat inside source static 10.23.20.10 209.165.200.4
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 VPN2
 permit ip 10.23.21.0 0.0.0.127 10.23.21.128 0.0.0.31
 permit ip 10.23.21.160 0.0.0.31 10.23.21.128 0.0.0.31
 permit ip 10.23.20.128 0.0.0.127 10.23.21.128 0.0.0.31
 permit ip 10.23.20.0 0.0.0.127 10.23.21.128 0.0.0.31
ip access-list extended NAT2
 deny ip 10.23.21.0 0.0.0.127 10.23.21.128 0.0.0.31
 deny ip 10.23.21.160 0.0.0.31 10.23.21.128 0.0.0.31
 deny ip 10.23.20.128 0.0.0.127 10.23.21.128 0.0.0.31
 deny ip 10.23.20.0 0.0.0.127 10.23.21.128 0.0.0.31
 permit ip 10.23.21.0 0.0.0.127 any
 permit ip 10.23.21.160 0.0.0.31 any
 permit ip 10.23.20.128 0.0.0.127 any
 permit ip 10.23.20.0 0.0.0.127 any
 permit ip 10.1.2.0 0.0.0.255 any
!
banner motd ^CVakhrushev_ Router_3^C
!
radius server 10.23.20.12
 address ipv4 10.23.20.12 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 Switch2:

```
Current configuration : 1174 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
```

```
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
```

```
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 10.23.21.162 255.255.255.224
!
ip default-gateway 10.23.21.161
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```