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 Коваленко Ярослава Сергійовича
(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 бюро перекладів компанії "InText" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі."
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Бешта Д.О.			
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 ступеня
бакалавр

студента Коваленко Я. С. **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 бюро перекладів компанії "InText" 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	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	17.05.2023
Розробка апаратноїчастини	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 компонентасистеми	Виконується детальна розробка компонента системи	27.05.2023

Завдання видано доц. Бешта Д.О.

Дата видачі 19.12.2022

Дата подання до екзаменаційної комісії .06.2023

Прийнято до виконання Коваленко Я. С.

РЕФЕРАТ

Пояснювальна записка: 79 с.,28 рис.,12 табл.,2 додатки, 6 джерел.

Об’єкт розробки: комп’ютерна система бюро перекладів «Intext» з опрацюванням побудови, налаштування та безпеки корпоративної мережі

Мета: створення комп’ютерної системи бюро перекладів «Intext»

Розроблена комп'ютерна система з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову систем контролю та редагування для бюро перекладів «Intext» 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 наводяться у пояснювальній записці або додатках.

CISCO PACKET TRACER, CISCO, МАРШРУТИЗАТОР, КОМУТАТОР, NAT, VPN, DHCP, ACL, IOT, VLAN, ETHERNET, DNS, HTTP

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КС – Комп'ютерна система.

ПК – Персональний комп'ютер.

ПЗ – Програмне забезпечення.

NAT – Network Address Translation – перетворення мережевих адрес з приватної у публічну.

VPN – Virtual Private Network – віртуальна приватна мережа

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

ACL – Access Control List – список контролю доступу.

DHCP – Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла

IoT – Internet of Things – Інтернет речей

RFID – Radio Frequency Identification – радіочастотна ідентифікація

DNS – Domain Name System – Система доменних імен

HTTP – HyperText Transfer Protocol – протокол передачі гіпертекстових документів

ВСТУП

У сучасному світі, де глобалізація та міжнародний спілкування стають дедалі більш важливими, послуги бюро перекладів стають необхідним елементом успішної бізнес-комунікації. Однак, для ефективного функціонування бюро перекладів і забезпечення якісного та швидкого перекладу, необхідна надійна та безпечна комп'ютерна система, яка може забезпечити ефективне опрацювання та збереження великої кількості інформації.

Ця дипломна робота присвячена розгляду комп'ютерної системи бюро перекладів компанії "InText" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі. Корпоративна мережа відіграє вирішальну роль у забезпеченні зв'язку між різними відділами компанії, а також у забезпеченні безпеки та конфіденційності важливої інформації.

У цій дипломній роботі буде розглянуто такі основні аспекти як:

- побудови комп'ютерної системи бюро перекладів;
- вибір технологій, архітектури мережі та розгортання комп'ютерних ресурсів;
- налаштування мережевих протоколів;
- забезпечення безпеки мережі;
- захисту від несанкціонованого доступу;

Результати цієї дипломної роботи допоможуть компанії "InText" впровадити надійну та безпечну комп'ютерну систему, що сприятиме покращенню ефективності та якості перекладу, а також забезпечить збереження та конфіденційність важливої інформації.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умови застосування КС

Галузь бюро перекладів є важливою і необхідною складовою сучасного світу, де мовна різноманітність і культурна взаємодія стають все більш важливими. Бюро перекладів забезпечують професійні послуги перекладу між різними мовами для клієнтів з різних сфер діяльності.

Одна з ключових характеристик галузі бюро перекладів - це висока якість перекладу. Професійні перекладачі, які працюють у бюро перекладів, володіють не лише майстерністю у власній мові, але й глибоким розумінням культур, з яких походять джерелові тексти. Вони здатні передати нюанси мови, стилю, тону і контексту оригіналу, забезпечуючи максимальну точність та вірність перекладу.

Інша важлива характеристика - це широкий спектр послуг. Бюро перекладів пропонують переклади не лише письмових текстів, але й усних перекладів, локалізацію програмного забезпечення, веб-сторінок та інших мультимедійних матеріалів. Вони можуть також забезпечити послуги редакції, коректури та ревізії текстів для забезпечення їх якості і граматичної правильності.

Гнучкість і швидкість - ще одна характеристика галузі бюро перекладів. Бюро перекладів здатні пристосовуватися до вимог клієнтів та надавати послуги в короткі терміни. Вони забезпечують відповідність графікам та термінам проектів, що є важливим для багатьох клієнтів, особливо в умовах швидкого розвитку технологій та комунікацій.

Конфіденційність і безпека є ключовими принципами роботи бюро перекладів. Клієнти можуть мати впевненість, що їхні дані та конфіденційна інформація залишаються в безпеці та не підлягають розголошенню. Бюро перекладів дотримуються етичних стандартів та використовують захисні технології для забезпечення безпеки даних.

Бюро перекладів повинно мати надійну комп'ютерну мережу, яка забезпечує стабільне і швидке з'єднання між різними комп'ютерами та пристроями в офісі. Це включає належне налаштування мережних пристроїв,

таких як маршрутизатори та комутатори. Також важливо мати швидке і стабільне з'єднання з Інтернетом. Важливо забезпечити захист даних. Це може включати використання шифрування даних, захищених мережевих з'єднань, а також наявність фаєрволів та інших заходів безпеки для запобігання несанкціонованому доступу до конфіденційної інформації. Важливою частиною є збереження текстових даних є. Важливо мати систему резервного копіювання даних, щоб у разі випадкового видалення, помилкової редагування або виходу з ладу обладнання можна було відновити важливі тексти. У бюро перекладів є спільна мережа для кількох перекладачів, важливо встановити контроль доступу та автентифікацію.

1.2 Характеристика і структура об’єкта впровадження

1.2.1 Характеристика об’єкта впровадження

InText - це бюро перекладів зі штаб-квартирою в Дніпрі, Україна. Компанія спеціалізується на наданні послуг перекладу для бізнесу та інших клієнтів з усього світу.

Компанія пропонує послуги перекладу текстів різних форматів та мов. Вона має широкий досвід в перекладі технічних документів, літературних творів, медичних даних, юридичних документів, веб-сайтів та багатьох інших типів документів.

InText працює з багатьма мовами, включаючи англійську, французьку, німецьку, іспанську, італійську, польську, українську та багато інших. Компанія має висококваліфікованих перекладачів, які мають багатий досвід роботи в цій галузі. Вони використовують сучасні інструменти та технології, щоб забезпечити високу якість перекладу та точність передачі інформації між мовами.

Крім основної послуги перекладу текстів, InText надає додаткові послуги, які допомагають клієнтам удосконалити свої продукти та послуги на міжнародному ринку.

Один з таких додаткових сервісів - локалізація веб-сайтів та програмного забезпечення. Локалізація допомагає компаніям адаптувати свої продукти та

послуги для різних культур та мов. Це дозволяє підвищити ефективність маркетингових кампаній та збільшити продажі.

Крім того, InText надає послуги з редагування та корегування текстів, що допомагає забезпечити високу якість перекладу та зробити текст більш зрозумілим та зрідненим для аудиторії.

Інші можливості InText включають консультації щодо міжнародного бізнесу та культурних особливостей, а також навчання мовам для бізнесу.

Загалом, InText - це компанія, яка допомагає клієнтам з усього світу успішно просуватися на міжнародному ринку, забезпечуючи високоякісний переклад та інші послуги, що допомагають розширювати їхні можливості та залучати нових клієнтів.

InText має декілька досягнень, які підтверджують її професійність та якість роботи:

- Сертифікат ISO 17100:2015. Цей сертифікат підтверджує, що InText відповідає стандартам якості та процедурам, які рекомендує міжнародна організація зі стандартизації. Зокрема, цей стандарт вимагає від компанії використовувати лише професійних перекладачів та проводити відповідний контроль якості перекладу.
- Нагороди на конкурсах. Компанія InText неодноразово отримувала нагороди на різних конкурсах та форумах. Наприклад, в 2018 році вона отримала нагороду "Краще бюро перекладів" на Ukrainian Outsourcing Forum.
- Професійний підхід. Компанія InText прагне забезпечити якісний та професійний підхід до кожного проекту. Кожен перекладач, який працює в компанії, має професійну підготовку та досвід у відповідній галузі.
- Використання технологій. Компанія InText використовує різноманітні технології, щоб забезпечити якісний та швидкий переклад текстів. Наприклад, вона використовує перекладацькі

платформи та CAT-інструменти, які допомагають зберігати консистентність перекладів та зменшувати час на проект.

Загалом, компанія InText має високі стандарти якості та професіоналізму у своїй роботі, що дозволяє їй забезпечувати задоволення потреб клієнтів та досягати успіху в своїй галузі.

1.2.2 Організаційна структура підприємства

Структура управління у бюро перекладів InText заснована на тісному співробітництві між керівництвом компанії та перекладацькою командою.

На вершині структури знаходиться засновник компанії, який також є генеральним директором. Він відповідає за стратегічне планування, прийняття стратегічних рішень та загальне керівництво компанією. Також йому підпорядковується IT відділ, а йому у свою чергу відділ технічної підтримки.

Під керівництвом генерального директора працює команда професійних менеджерів проектів, які відповідають за взаємодію з клієнтами, прийом та оцінку проектів, розподіл завдань між перекладачами та контроль якості перекладів.

Після прийому проекту менеджери проектів передають його до команди перекладачів та реакторів. Команда перекладачів складається з професійних перекладачів, які мають відповідний досвід та знання у відповідній галузі. Кожен проект підтримується кваліфікованим редактором, який контролює якість перекладу та дотримання стандартів.

У компанії також є відділ маркетингу та продажу, який відповідає за залучення нових клієнтів та розвиток бізнесу компанії.

Така структура управління дозволяє компанії InText ефективно керувати своїми проектами та забезпечувати якісні переклади для своїх клієнтів.

Схему організаційної структури підприємства наведено на рисунку 1.1.

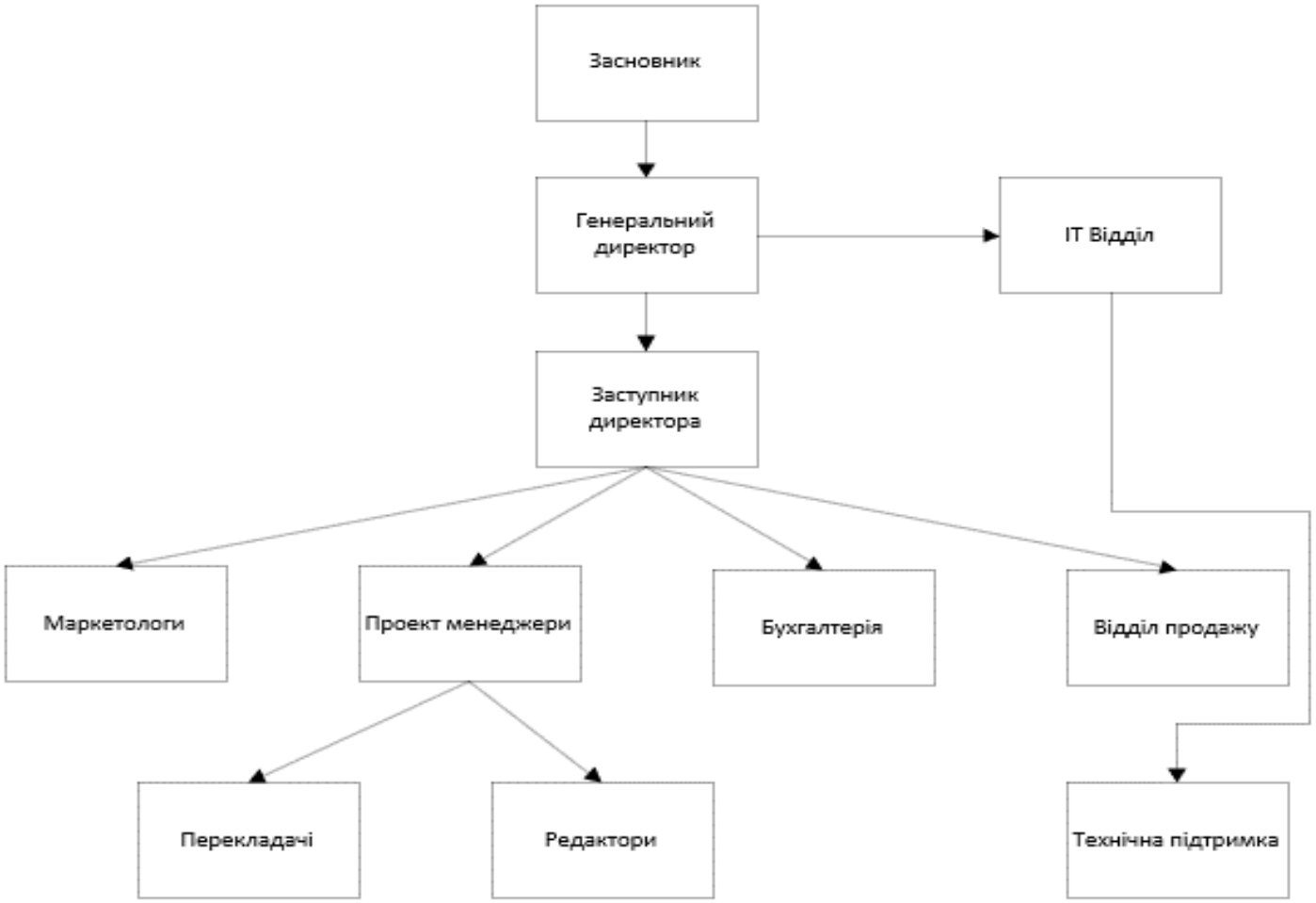

Рисунок 1.1 – Організаційна структура підприємства

1.2.3 Розміщення структурних підрозділів підприємства

Топологія бюро перекладів InText складається з двох поверхів офісного будинку на правому березі міста Дніпро, та знаходиться за адресую проспект Пушкіна, 49, м. Дніпро, Дніпропетровська область, 49000(рис. 1.2)

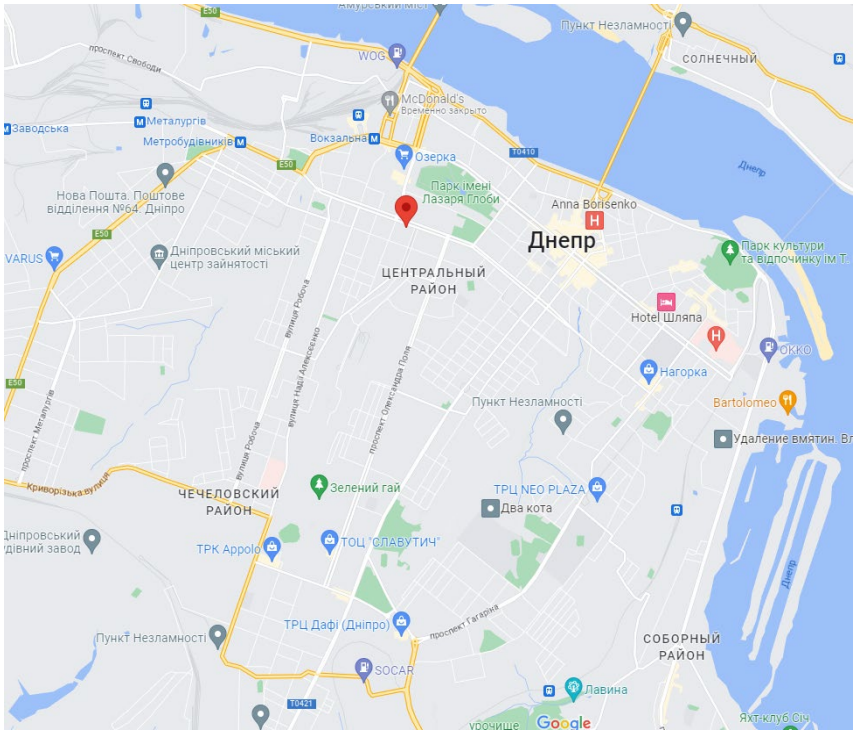

Рисунок 1.2 – Георозміщення офісу бюро перекладів «InText»

Бюро перекладів InText орендує 5 та 6 поверхи у 7 поверховій офісній будівлі

Структурна схема 5 поверху включає у себе схему серверної, відділу з перекладачами, бухгалтерів та менеджерів проектів(рис.1.3)

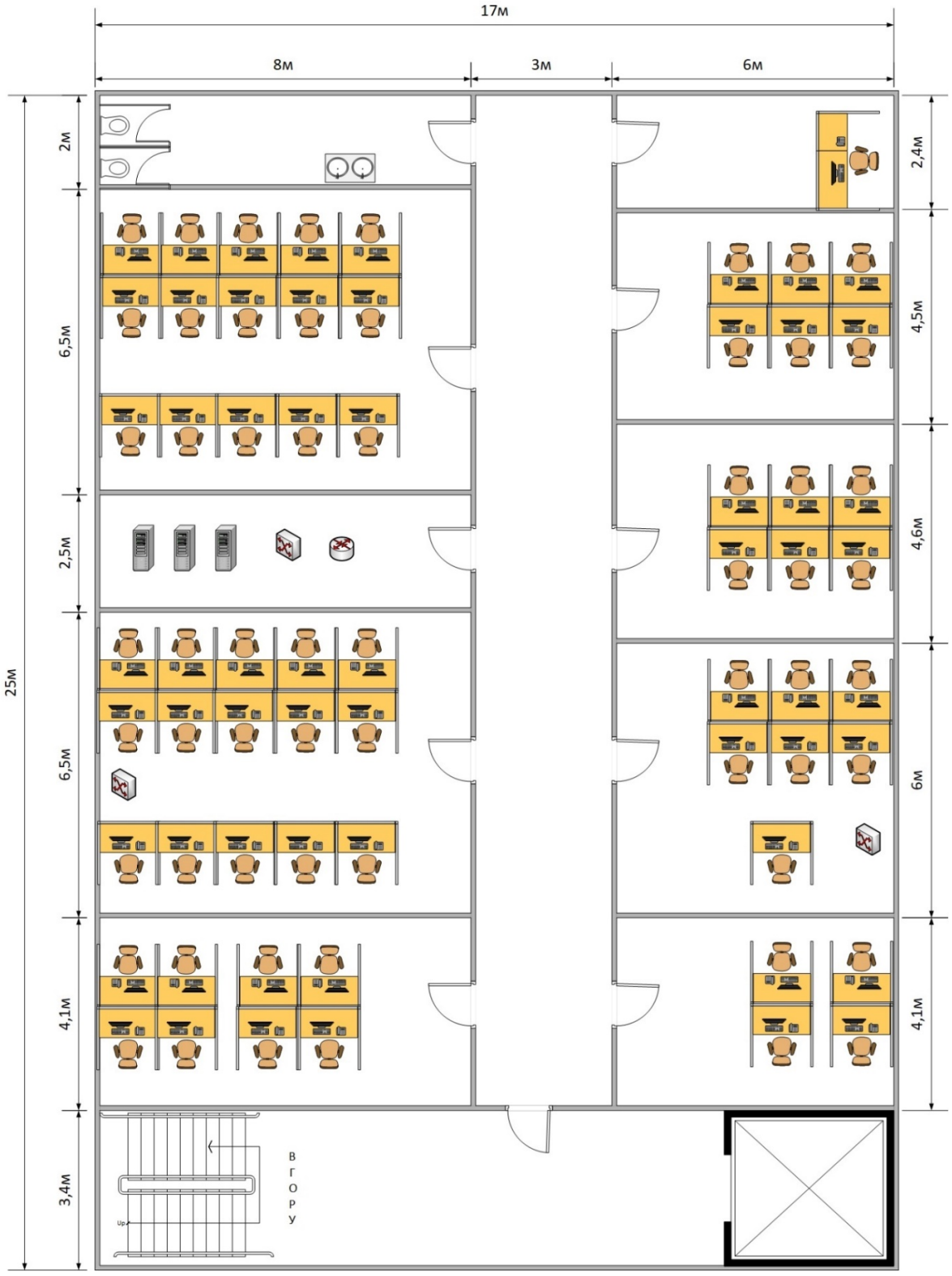

Рисунок 1.3 – Структурна схема 5 поверху

Структурна схема 6 поверху включає у себе схему кімнати керівництва, бухгалтерію, IT відділу, відділу продажу та маркетингу(рис.1.4)

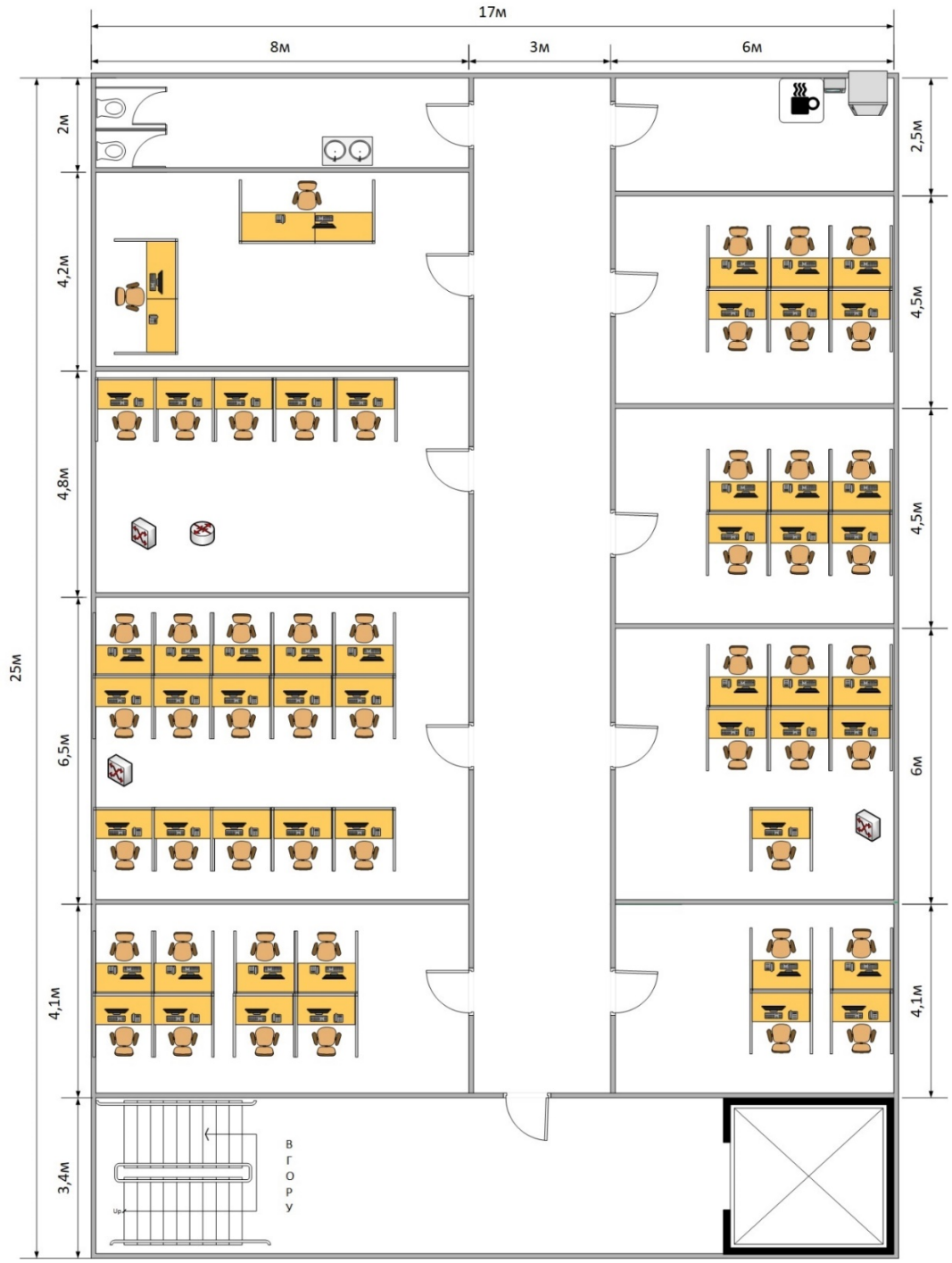

Рисунок 1.4 – Структурна схема 6 поверху

1.3 Принципи та технічні способи інформаційного забезпечення об’єкта впровадження

Бюро перекладів широко використовують інформаційні технології для забезпечення ефективної та швидкої роботи. Нижче описано деякі принципи та технічні способи , які використовуються для інформаційного забезпечення:

1. Конфіденційність: Застосування шифрування та аутентифікації для забезпечення захисту конфіденційної інформації. Наприклад, використання SSL / TLS для шифрування передачі даних через мережу.
2. Забезпечення цілісності даних: Цілісність даних є важливою для бюро перекладів, оскільки будь-які зміни в тексті можуть вплинути на точність перекладу. Технічні методи, такі як контрольна сума (checksum) або хеш-функції, можуть використовуватися для виявлення будь-яких змін або пошкоджень даних під час передачі або зберігання.
3. Забезпечення доступності: Бюро перекладів повинно мати технічні засоби для забезпечення доступності даних та послуг для своїх клієнтів. Це може включати використання високошвидкісних мереж та потужних серверів, щоб забезпечити швидкий доступ до перекладів і мовних ресурсів.
4. Автентифікація та авторизація: Використання методів перевірки ідентичності користувачів та надання прав доступу до різних ресурсів відповідно до їхніх повноважень. Наприклад, використання системи управління ідентифікацією та доступом (IAM).
5. Управління базами даних: Бюро перекладів може використовувати бази даних для зберігання та керування перекладами, лексикою, глосаріями та іншою мовною інформацією. Ефективне управління базами даних допомагає забезпечити швидкий доступ до необхідної інформації та організувати робочий процес перекладу.
6. Резервне копіювання та відновлення: Регулярне створення резервних копій даних та можливість їх відновлення у випадку втрати або пошкодження. Наприклад, використання системи автоматичного резервного копіювання і відновлення.
7. Моніторинг та аудит: Використання систем моніторингу та аудиту для виявлення і відстеження подій, помилок та зловживань у системі. Наприклад, використання системи журналювання подій та моніторингу мережі.

8. Інтеграція технологій: Бюро перекладів повинно забезпечити інтеграцію різних технологій та програмних рішень для оптимізації робочих процесів та підвищення продуктивності. Наприклад, інтеграція систем управління базами даних, електронної пошти, проектного управління, спеціалізованого перекладацького ПО та інших рішень може допомогти автоматизувати рутинні завдання та поліпшити ефективність роботи.
9. Масштабованість: Бюро перекладів повинно мати гнучку та масштабовану IT-інфраструктуру, яка може зростати разом із збільшенням обсягу роботи, клієнтів або персоналу. Це може включати використання хмарних рішень, віртуалізацію серверів, резервне забезпечення ресурсів та інші методи масштабування системи.

Ці принципи та технічні способи допомагають бюро перекладів забезпечити високу якість перекладів, збереження даних та захист інформації своїх клієнтів.

1.4 Аналітичний огляд існуючих способів та відомих рішень обробки та передачі інформації

Аналітичний огляд існуючих способів обробки та передачі інформації у бюро перекладів включає в себе розгляд різних методів та технологій, що застосовуються в цій галузі. Ось кілька способів обробки та передачі інформації у бюро перекладів:

1. Комп'ютерні програми для перекладу: Використання спеціалізованих комп'ютерних програм, таких як машинний переклад або перекладацькі платформи, може значно спростити та прискорити процес перекладу. Ці програми використовуються для автоматичного перекладу текстів, створення глосаріїв, керування перекладами та спільної роботи перекладачів.

   Наприклад: SDL Trados Studio: Популярне програмне забезпечення для професійного перекладу, яке включає інструменти для керування глосаріями, попереднього перекладу та підтримки спільної роботи перекладачів.

Memsource: Хмарна платформа для керування перекладами, яка забезпечує автоматичний переклад, спільну роботу та управління проектами.

2. Хмарні технології: Багато бюро перекладів використовують хмарні технології для збереження та обробки даних. Це дозволяє зберігати переклади, глосарії та інші мовні ресурси в хмарних сховищах, що забезпечує доступ до них з різних пристроїв та місць розташування.
3. Комунікаційні системи: У бюро перекладів використовуються різні комунікаційні системи для зв'язку між перекладачами, клієнтами та менеджерами проектів. Це можуть бути електронна пошта, чат-програми, спеціалізовані платформи для спільної роботи тощо. Ці системи дозволяють швидко та ефективно обмінюватися інформацією та файлами.

Наприклад: Slack: Платформа для комунікації та спільної роботи, яка дозволяє перекладачам, клієнтам та менеджерам проектів обмінюватися повідомленнями, файлами та звітами.

Microsoft Teams: Інструмент для комунікації та спільної роботи, який надає можливості зв'язку через чат, аудіо та відеозв'язок для перекладачів та інших учасників проектів.

4. Системи керування проектами: Управління перекладацькими проектами є важливою складовою роботи бюро перекладів. Використання спеціалізованих систем керування проектами допомагає відстежувати стан проектів, призначати завдання перекладачам, контролювати терміни виконання та забезпечувати ефективну комунікацію.

Наприклад: Trello: Популярна онлайн-платформа для керування завданнями та проектами, яка дозволяє організовувати та відстежувати прогрес перекладів.

Basecamp: Інструмент для управління проектами, який дозволяє створювати завдання, встановлювати терміни та спілкуватися з командою перекладачів та клієнтами.

5. Електронний документообіг: Замість традиційного паперового документообігу, бюро перекладів можуть використовувати електронні системи для обміну документами, підписів та затверджень. Це спрощує та прискорює процес обробки та передачі документів у віртуальному середовищі.

   Наприклад: Adobe Sign: Сервіс електронного підпису, який дозволяє перекладачам та клієнтам підписувати та затверджувати документи в електронному форматі.

   DocuSign: Інший популярний сервіс електронного підпису, який дозволяє зручно обробляти та передавати документи в бюро перекладів.

Це лише декілька прикладів існуючих способів обробки та передачі інформації у бюро перекладів. Вибір конкретних методів залежить від потреб та можливостей кожного окремого бюро перекладів.

1.5 Постановка завдання та мета роботи

Завданням кваліфікаційної роботи є розробка комп'ютерної системи бюро перекладів "InText" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Для вирішення поставленої мети в роботі слід виконати наступні завдання:

- проаналізувати об’єкт впровадження;
- розробити структуру КС;
- вибрати мережеву архітектуру для корпоративної мережі бюро перекладів "InText";
- проаналізувати інтенсивність трафіку;
- розробити фізичну та логічну топології мережі;
- виконати конфігурування компонентів системи;
- розробити IoT систему для забезпечення безпеки офісу, обладнаного камерами та іншими датчиками

Результуюча мережа має бути надійною, масштабованою, гнучкою, безпечною та швидкою.

1.6 Визначення можливих напрямків рішення поставлених завдань

Зважаючи на потреби та вимоги бюро перекладів "InText" щодо побудови, налаштування та безпеки корпоративної мережі, можливі такі напрямки рішення:

Планування і архітектура мережі: Розробимо оптимальну фізичну і логічну структуру мережі, враховуючи розташування приміщень, потреби в підключеннях, зони покриття Wi-Fi, маршрутизацію та сегментування мережі. Будемо використовувати топологію Зірка задля кращої масштабованості мережі

Вибір обладнання: Використаємо надійне і сучасне мережеве обладнання від компанії Cisco. Розглянемо можливість використання промислових стандартів і протоколів, які підтримують безпеку та швидкість передачі даних.

Забезпечення безпеки мережі: Розробимо комплексну стратегію безпеки, яка включатиме захист від зовнішніх загроз, перехоплення даних та несанкціонованого доступу. Використаємо NAT, віртуальні приватні мережі (VPN), шифрування трафіку та системи виявлення вторгнень.

Моніторинг системи: Використаємо моніторингові системи, які дозволять відстежувати стан мережі, моніторити навантаження та виявляти проблеми в реальному часі.

Кабельна інфраструктура: Запроектуємо кабельну інфраструктуру для забезпечення надійного зв'язку між різними пристроями та приміщеннями бюро перекладів. Розглянемо використання крученої пари стандарту 5E, розподільних панелей, роз'ємів Ethernet та інших необхідних компонентів.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до системи бюро перекладів

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури та функціонування системи

Основні вимоги до структури і функціонування системи бюро перекладів «InText» можна сформулювати наступним чином:

- Безпека: мережа повинна бути забезпечена надійними методами захисту від несанкціонованого доступу та злому.
- Швидкість: мережа повинна забезпечувати швидкий доступ до даних та інформації для працівників компанії, які займаються перекладами.
- Безперебійність: мережа повинна працювати без перебоїв, щоб забезпечити безперервну роботу компанії та уникнути втрати даних.
- Скалабельність: мережа повинна бути здатна збільшуватись у міру зростання компанії та збільшення обсягів даних.
- Легкість управління: мережа повинна мати просту та зрозумілу структуру управління, щоб працівники компанії могли швидко і ефективно вирішувати завдання, пов'язані з мережею.
- Резервне копіювання: мережа повинна мати систему резервного копіювання, щоб у разі виникнення непередбачуваних ситуацій забезпечити можливість відновлення даних.
- Підтримка: мережа повинна мати систему технічної підтримки, яка забезпечує надійність та якість роботи мережі, а також допомагає вирішувати технічні проблеми.
- Сумісність: мережа повинна бути сумісна з різноманітним програмним та апаратним забезпеченням, яке використовується в компанії.
- Мобільність: мережа повинна бути здатною працювати на різних пристроях та підключатися до різних мереж.

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

- Швидкість передачі даних: Забезпечення швидкості передачі даних 100 мбіт/с для ефективної передачі великих обсягів даних.
- Надійність: Міцне та стабільне з'єднання без втрати даних або перебоїв у зв'язку.
- Низька затримка: Мінімізація часу передачі даних між компонентами системи для швидкої реакції та покращення продуктивності.

- Сумісність: Здатність працювати з різними протоколами та стандартами зв'язку для забезпечення сумісності між компонентами системи.
- Простота керування та налаштування: Забезпечення зручного та легкого керування засобами зв'язку, а також швидкої настройки та конфігурації.

2.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами, вимоги до її сумісності, у тому числі вказівки про способи обміну інформацією

- Сумісність форматів документів: система повинна підтримувати основні формати документів, використовувані в галузі перекладу, наприклад, DOCX, XLSX, PDF і т. д.
- Інтеграція з платформами перекладу: система повинна бути здатною інтегруватися з платформами перекладу, що дозволить зручно обмінюватися завданнями, документами та іншою інформацією з партнерами або підрядними перекладачами.
- Електронна пошта та файловий обмін: система повинна підтримувати обмін інформацією через електронну пошту та файловий обмін, щоб забезпечити зручний спосіб передачі документів і повідомлень.
- API і сервіси веб-сервісів: система повинна мати документоване API і можливості веб-сервісів для інтеграції з іншими системами, наприклад, CRM, управління проектами або системами спільної роботи.
- Системи управління завданнями: система повинна мати функціонал для ефективного управління завданнями, включаючи призначення, відстеження стану, пріоритетів та звітності.

2.1.1.4 Вимоги до режимів функціонування системи

Надійність: стабільна та безперебійна робота системи 24/7.

Швидкодія: висока швидкість обробки та відгуку.

Масштабованість: здатність системи масштабуватися залежно від потреб користувачей.

Автоматизація: мінімізація ручної роботи та оптимізація процесів налаштування та обробки даних.

Зручність інтерфейсу: інтуїтивний та зручний інтерфейс для користувачів.

Безпека: захист даних та системи від несанкціонованого доступу за допомогою VPN та NAT.

2.1.1.5 Вимоги до діагностування системи

- Моніторинг: Наявність засобів для постійного моніторингу стану мережі, включаючи пропускну здатність, завантаження, пінгу та інші параметри.
- Виявлення проблем: Система повинна виявляти та реєструвати проблеми, такі як переривання з'єднання, недоступність пристроїв, помилки передачі даних тощо.
- Аналіз трафіку: Можливість аналізувати трафік мережі для виявлення аномальних або ненормальних патернів, атак або інших проблем.
- Система сповіщень: Наявність механізму сповіщення про виявлені проблеми або несправності, щоб оператори або адміністратори могли своєчасно реагувати на них.
- Логування: Зберігання журналів подій та дій, що стосуються мережі, для аналізу та відновлення історії подій.
- Діагностичні інструменти: Наявність спеціальних інструментів та програмних засобів для діагностики, виявлення та усунення проблем в мережі.
- Віддалений доступ: Можливість здійснювати діагностику та вирішення проблем віддалено, без необхідності фізичного присутності на місці за допомогою RDP або SSL.
- Тестування: Можливість проводити тестування мережі для виявлення проблем, перевірки пропускної здатності та інших характеристик.
- Швидке виявлення та усунення несправностей: Система повинна забезпечувати швидке виявлення та усунення несправностей в мережі у продовж години з мінімальним впливом на роботу користувачів.
- Підтримка протоколів діагностики: Сумісність з різними протоколами діагностики, такими як ICMP, SNMP, syslog тощо, для отримання інформації про стан мережевих пристроїв та послуг.

2.1.1.6 Перспективи розвитку системи

1. Збільшення швидкості передачі даних до 1 Гбіт/с.
2. Використання нових технологій, таких як 5G та IoT.
3. Покращення безпеки мережі.
4. Розширення пропускної здатності.
5. Вдосконалення мережевого управління.
6. Підтримка мобільності та бездротових технологій Wifi 6.
7. Інтеграція хмарних сервісів.
8. Використання віртуалізації мережі.

2.1.1.7 Вимоги до показників призначення

Основними показниками призначення бюро перекладів є:

- Швидкість та продуктивність системи. Перекладацька компанія повинна мати можливість швидко та ефективно обробляти великий обсяг інформації, що надходить щоденно. Тому комп'ютерна система повинна мати достатню швидкість та продуктивність, щоб забезпечувати швидке оброблення даних.
- Надійність та безпека даних. У перекладацькій компанії зберігається велика кількість конфіденційної інформації. Тому важливо, щоб комп'ютерна система була надійною та забезпечувала безпеку даних. Для цього необхідно встановити ефективні засоби захисту даних та забезпечити резервне копіювання даних та їх шифрування.
- Інтеграція з іншими програмами та системами. У перекладацькій компанії можуть використовуватися різні програми та системи для різних завдань. Тому важливо, щоб комп'ютерна система була здатна інтегруватися з іншими програмами та системами.
- Підтримка міжнародних мов. Оскільки перекладацька компанія працює з багатьма мовами, важливо мати комп'ютерну систему, яка підтримує всі мови, з якими працює компанія.

2.1.1.8 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

Вимоги до експлуатації, технічного обслуговування, ремонту та зберігання компонентів системи комп'ютерної мережі бюро перекладів включають в себе наступні пункти:

1. Інструкції з експлуатації: Кожен компонент системи мережі повинен мати інструкції з експлуатації, в яких має бути детально описано правила та рекомендації щодо користування та зберігання обладнання.
2. Регулярне технічне обслуговування: Обладнання повинно проходити технічне обслуговування 2 рази на рік, щоб забезпечити його надійну та безперебійну роботу. Це включає в себе перевірку на віруси та інші загрози за допомогою антивіруса Symantech Endpoint Protection, оновлення програмного забезпечення, заміну деталей, які вийшли з ладу, тощо.
3. Ремонт та заміна компонентів: У разі поломки компонентів системи мережі, їх можна ремонтувати або міняти. Ремонт повинен проводитись фахівцем, який має відповідні знання та досвід у цій області. Можливе залучання фахівців з інших компаній. Якщо компонент не може бути відремонтований, його потрібно замінити на новий.
4. Зберігання компонентів: Компоненти системи мережі повинні зберігатись в спеціальних умовах, щоб забезпечити їхню безпеку та надійність. Це включає в себе зберігання в сухому та прохолодному місці (17-25^{o}C), захист від пилу та інших забруднень, а також відповідне упакування та маркування.
5. Запобігання несанкціонованому доступу: Компоненти системи мережі мають бути захищені від несанкціонованого доступу з боку зовнішніх користувачів за допомогою VPN з'єднання .
6. Резервне копіювання даних: Для запобігання втрати важливих даних, компанія повинна мати резервні копії всієї інформації, яка зберігається на серверах мережі. Копії даних мають зберігатись в іншому місці, щоб у разі виникнення аварійної ситуації збережені дані не постраждали.

7. Оновлення програмного забезпечення: Для забезпечення найвищої продуктивності та безпеки системи мережі, необхідно регулярно оновлювати програмне забезпечення на всіх комп'ютерах та серверах.
8. Використання ліцензійного програмного забезпечення: Усе програмне забезпечення, яке використовується в системі мережі, має бути ліцензійним. Використання піратського програмного забезпечення може призвести до серйозних правових проблем.
9. Організація кабельних систем: Кабелі, які використовуються для підключення компонентів мережі, мають бути організовані та позначені, щоб у разі потреби їх можна було легко знайти та замінити.
10. Електропостачання: Бюро перекладів повинно бути забезпечено стабільним та безперебійним електропостачанням для роботи локальної комп'ютерної мережі. Це може включати встановлення резервних джерел живлення (UPS) для серверів, мережевого обладнання та користувацьких ПК та генератору потужністю 15 кВт для запобігання втрат даних під час перерв у роботі електромережі.

2.1.1.8.1 Умови і режим експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) системи з заданими технічними показниками

- Робочі години: Система повинна бути доступна для використання 24 години на добу, 7 днів на тиждень.
- Час відновлення після збоїв: Система повинна мати можливість відновлюватися протягом 1 години після виявлення збою.
- Швидкість обробки даних: Система повинна мати можливість обробляти принаймні 1000 операцій на секунду.
- Завантаження мережі: Мережа повинна мати достатню пропускну здатність для передачі даних обсягом 100 Мбіт на секунду.
- Обсяг зберігання: Система повинна мати можливість зберігати не менше 10 терабайт даних.

- Періодичність планових технічних перевірок: Технічне обслуговування системи повинно проводитися щоквартально.
- Ремонтні роботи: Система повинна мати можливість виконувати ремонтні роботи протягом 48 годин після виявлення несправності.
- Заміна зношених елементів і компонентів: Зношені елементи і компоненти повинні бути замінені протягом 24 годин після виявлення їхнього зносу або несправності.

2.1.1.8.2 Вимоги до параметрів мереж енергопостачання

Стабільність напруги:

- Допустимі відхилення напруги від номінального значення: ±10%

Частота:

- Допустимі відхилення частоти від номінального значення: ±0.2 Гц.
- Максимальний допустимий розмах зміни частоти: 49.8 Гц - 50.2 Гц.

Мережева заземлення:

- Вимоги до опору заземлення: менше 4 Ом для систем з номінальною напругою до 1 кВ і менше 1 Ом для систем з номінальною напругою понад 1 кВ.

Резервне живлення:

- Наявність безперебійного живлення (UPS) з часом автономної роботи не менше 1 години для забезпечення роботи серверів та мережевого обладнання, та 15 хвилин безперебійної роботи користувацьких ПК під час вимкнення основного живлення.
- Наявність генератору резервного живлення потужністю 15 кВт з можливістю автоматичного переключення при відмові основного живлення.

Захист від перенапруг і електромагнітних перешкод:

- Вимоги до захисту від перенапруг відповідно до національних стандартів та рекомендацій, наприклад, захист від блискавки, перенапругові розрядники тощо.

- Вимоги до захисту від електромагнітних перешкод, наприклад, застосування екранованих кабелів, фільтрів для спрямовування та поглинання шумів.

2.1.1.8.3 Вимоги до кількості кваліфікації обслуговуючого персоналу

Кількість IT-спеціалістів: Рекомендується мати команду IT-спеціалістів у складі 10-15 осіб які працюють в IT відділі компанії. Це включає системних адміністраторів, мережевих інженерів, розробників програмного забезпечення та технічну підтримку.

Кваліфікація IT-спеціалістів: Вимагається наявність вищої освіти в галузі інформаційних технологій, комп'ютерних наук або суміжних спеціальностей. Також, відповідно до специфіки роботи, важливими навичками є досвід роботи з комп'ютерними системами, знання мережевих протоколів, баз даних, безпеки і захисту даних.

Режим роботи: Комп'ютерна система повинна працювати безперервно, тому вимагається наявність IT-спеціалістів у режимі 24/7. Рекомендується розподілити робочий час між спеціалістами, включаючи зміни, вихідні та святкові дні, для забезпечення неперервної підтримки системи.

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

Склад запасних виробів і приладів: Включає необхідні запасні частини, компоненти та прилади для обслуговування комп'ютерної мережі. Наприклад, це можуть бути мережеві комутатори, маршрутизатори, сервери, мережеві кабелі, резервні блоки живлення, модулі пам'яті, жорсткі диски тощо.

Кількість запасних виробів і приладів: 1 додатковий комутатор, кабелі живлення, Ethernet кабелі та HDMI кабелі у кількості 10-20 штук, 5 комп'ютерів або ноутбуків.

Розміщення: Визначення місця для зберігання запасних виробів і приладів, яке забезпечує зручний доступ та захист від небезпек. Це може бути окремий серверний приміщення або шафа замкнутого типу. Важливо забезпечити належні

умови зберігання, уникати пилу, вологості вище 60%, екстремальних температур та ударів.

Умови збереження: Застосування заходів для збереження запасних виробів і приладів у належному стані. Це включає використання антистатичних упаковок для електронних компонентів, позначення та маркування комплектів, регулярну перевірку стану запасних компонентів і заміну старих або пошкоджених елементів.

2.1.1.8.5 Вимоги до регламенту обслуговування

Регулярність обслуговування: Для серверів та ПК раз на рік

Перевірка та діагностика: Вимоги до проведення перевірки та діагностики комп'ютерної системи з метою виявлення потенційних проблем, помилок або несправностей. Це може включати перевірку жорсткого диска, пам'яті, перевірку наявності вірусів, аналіз роботи компонентів тощо.

Заплановане технічне обслуговування: Встановлення регламентованого графіка технічного обслуговування компонентів комп'ютерної системи:

- Щотижнева перевірка наявності та оновлення антивірусного програмного забезпечення.
- Щомісячне проведення повного сканування жорсткого диска на наявність вірусів.
- Щорічна перевірка та очищення системних блоків від пилу.
- заміна термопаст на процесорах та графічних картках кожні 3 роки.
- Щоквартальне резервне копіювання даних та їх зберігання в окремому місці.
- Оновлення операційної системи та програмного забезпечення наявних комп'ютерів за потребою.
- Ведення журналу обслуговування, включаючи дати проведення процедур, виявлені проблеми та виконані дії.

Збереження документації: Вимоги до збереження документації про обслуговування комп'ютерної системи, включаючи журнали обслуговування, довідники, інструкції, сертифікати тощо.

2.1.1.9 Вимоги до патентної чистоти

Для забезпечення патентної чистоти комп'ютерної системи бюро перекладів можна вживати наступні заходи:

- Вжити заходів до уникнення порушення патентних прав шляхом придбання ліцензій на використання програмного забезпечення або технологій.
- Провести ретельну перевірку нових технологій і програм перед їх використанням, щоб переконатися, що вони не порушують патентних прав інших компаній або фізичних осіб.
- Укладати угоди про нерозголошення зі співробітниками, підрядниками та іншими сторонами, які мають доступ до конфіденційної інформації компанії.

2.1.2 Додаткові вимоги

2.1.2.1.1 Вимоги до активного обладнання (функціонування, кількість портів та їх запас, технічні вимоги)

Функціональні вимоги до обладнання:

- Підтримка мережевих протоколів, таких як Ethernet, TCP/IP, VLAN, VPN.
- Забезпечення необхідної швидкості передачі даних, наприклад, Gigabit Ethernet, 10 Gigabit Ethernet або вище.
- Функції маршрутизації та комутації для забезпечення ефективного руху даних в мережі.
- Підтримка безпеки мережі, таких функцій як файрвол, виявлення вторгнень (IDS/IPS), VPN-з'єднання.

Кількість портів та їх запас:

- Забезпечити наявність комутатора з мінімум 24 портами для підключення комп'ютерів та пристроїв в бюро перекладів.
- Рекомендується мати щонайменше 15% запасу вільних портів на комутаторі для майбутнього розширення.

Технічні вимоги до обладнання:

- Розміри обладнання можуть бути різними залежно від типу пристрою. Наприклад, сервери можуть мати стандартні розміри, такі як 1U (висота 1,75 дюйма) або 2U, а комутатори можуть мати розмір 19 дюймів для розміщення в стандартних стійках.
- Вимоги до живлення, наприклад, підтримка вхідного напруги, резервні джерела живлення (UPS), можливість гарячої заміни живлення.
- Вимоги до охолодження, такі як вентиляція, вентилятори, розташування обладнання у відповідних умовах температури від 14°C до 25°C.
- Розміри та стандарти монтажу, щоб забезпечити відповідну установку та розміщення обладнання в шафі або на стіні.

2.1.2.1.2 Вимоги до кабель-каналів, інформаційних та електричних розеток

Вимоги до кабель-каналів:

- Матеріал: Кабель-канали повинні бути виготовлені з вогнестійкого матеріалу, яким може бути сталь, алюміній або пластик. Матеріал повинен мати достатню міцність та стійкість до зовнішніх впливів.
- Розмір: Розмір кабель-каналів повинен відповідати кількості та діаметру кабелів, які будуть прокладені. Для кабелів з великим діаметром можуть використовуватися кабель-канали шириною 4-6 дюймів (100-150 мм).
- Комплектуючі: Кабель-канали повинні мати вбудовані комплектуючі для фіксації кабелів та їх організації. Це можуть бути монтажні стяжки, рейки, утримувачі кабелів тощо.
- Монтаж: Вимоги до монтажу кабель-каналів включають правильне закріплення до стін або стель, використання необхідних кріпильних елементів та дотримання встановлених проміжків між кабель-каналами.

Вимоги до інформаційних та електричних розеток

- Електробезпека: Розетки повинні відповідати стандартам електробезпеки, таким як IEC 60884-1, що визначає параметри для безпечної експлуатації, наприклад, мінімальну відстань між контактами і ступінь ізоляції.

- Стандарти розеток: В Україні використовуються розетки стандарту типу C (розетки з контактами типу "штепсель") та стандарту типу F (розетки з контактами типу "шуко").
- Напруга та струм: Вимоги до розеток передбачають підтримку певної напруги та струму. В Україні зазвичай використовується напруга 230 В та струм до 16 А.
- Водонепроникність: Для вологих середовищ або зовнішнього використання, розетки повинні мати високий рівень захисту від вологи та пилу, що відповідає стандарту IP44.

2.1.2.1.3 Вимоги до комунікаційного обладнання і його розташування

1. Розташування у приміщенні: Комунікаційне обладнання повинно бути розміщене в спеціально призначених приміщеннях, які забезпечують належні умови для функціонування та безпеки обладнання. Це може бути окрема серверна кімната або спеціально обладнаний простір з контрольованими параметрами, такими як температура, вологість та захист від пилу.
2. Тип шаф: Комунікаційне обладнання може бути розміщене у спеціальних комунікаційних шафах або стійках. Шафи повинні відповідати стандартам і вимогам щодо розмірів, міцності та безпеки. Наприклад, шафи можуть мати стандартні розміри 19 дюймів (48.26 см) для монтажу обладнання зі стандартною шириною.
3. Тип підводу кабельних трас: Кабельні траси для підводу комунікаційних кабелів повинні відповідати стандартам і вимогам щодо монтажу та безпеки. Це можуть бути металеві кабельні лотки, канали або гофровані труби, які забезпечують правильну фіксацію та захист кабелів.
4. Розташування обладнання усередині шафи: Комунікаційне обладнання повинно бути належно організоване та закріплене всередині шафи. Це може включати встановлення стандартних 19-дюймових кронштейнів для монтажу обладнання, використання горизонтальних і вертикальних кабельних органайзерів для розташування кабелів та елементів керування,

а також застосування вентиляційних пристроїв для забезпечення належної температури усередині шафи.

2.1.2.1.4 Вимоги до однорідності

1. Тип кабелів: Для забезпечення однорідності комунікаційної системи, рекомендується використовувати однаковий тип кабелів на всіх рівнях і підрозділах мережі. Наприклад, можна використовувати стандартні категорії кабелів, такі як Cat5e, Cat6 або Cat6a, для передачі даних.
2. Роз'єми: Важливо використовувати однакові роз'єми на всіх кінцях кабелів для забезпечення сумісності та зручності підключення. Наприклад, RJ-45 роз'єми часто використовуються для Ethernet-з'єднань.
3. Магістралі: Для забезпечення однорідності і спрощення конфігурації мережі рекомендується використовувати однакові типи магістралей на різних рівнях комунікаційної інфраструктури. Наприклад, можна використовувати однакові типи магістралей, такі як Ethernet або оптоволоконні з'єднання, для передачі даних між різними пристроями.
4. Протоколи і стандарти: Для забезпечення однорідності і сумісності обладнання рекомендується використовувати однакові протоколи і стандарти на всіх рівнях мережі. Наприклад, можна використовувати стандартні протоколи TCP/IP для мережевого зв'язку.

Застосування вимог до однорідності сприяє спрощенню управління, обслуговуванню і розширенню комунікаційної системи, а також забезпечує сумісність і синхронізацію пристроїв у мережі.

2.1.2.1.5 Вимоги до резервування

1. Регулярність резервного копіювання: Резервні копії даних повинні бути створювані регулярно згідно з встановленим графіком. Частота резервного копіювання залежить від критичності даних. Для критичних даних це кожен день.
2. Зберігання резервних копій: Резервні копії даних повинні зберігатися в безпечному місці, віддаленому від основного місця зберігання даних. Це

може бути офісна схованка, віддалений серверний центр або хмарне сховище.

3. Перевірка цілісності даних: Після створення резервних копій необхідно перевіряти їх цілісність, щоб переконатися, що дані успішно скопійовані та не пошкоджені. Це можна зробити за допомогою валідації хеш-сум або інших методів перевірки цілісності даних.
4. Тестування процесу відновлення: Регулярно проводьте тести відновлення, щоб переконатися в ефективності процесу відновлення даних. Це допоможе виявити можливі проблеми та вдосконалити процес резервного копіювання і відновлення.
5. Документація та плани відновлення: Важливо мати документовані плани відновлення даних, які включають процедури відновлення, контактну інформацію та іншу важливу документацію. Це допоможе забезпечити швидке та ефективне відновлення даних у разі втрати.

2.1.3 Вимоги до налаштувань та функцій, виконуваних системою

Мережа повинна бути поділена на 5 підмереж (Додаток А), які підключені між собою за допомогою портів GigabitEthernet та FastEthernet. Під'єднання кабелями за допомогою цих портів забезпечують швидкий та стабільний зв'язок з комутаторами та маршрутизаторами до яких вони підключені.

Основні вимоги до функцій комп'ютерної системи бюро перекладів можуть бути наступними:

- Забезпечення надійного та швидкого доступу до перекладацьких ресурсів та інформації за допомогою TFTP серверу.
- Збереження, організація та захист перекладацьких даних та документів шляхом використання відповідних систем зберігання та резервного копіювання.
- Контроль та аналіз використання ресурсів комп'ютерної системи для ефективного управління проектами та завданнями з перекладу.

- Забезпечення безпеки мережі та даних, включаючи захист від несанкціонованого доступу, вірусів та інших загроз за допомогою антивірусів та VPN з'єднання.
- Підтримка комунікаційних сервісів, таких як електронна пошта, відеоконференції та обмін файлами для зручного спілкування з клієнтами та співробітниками.
- Автоматизований контроль безпеки та ризиків згідно з внутрішніми та зовнішніми вимогами.
- Резервне копіювання та відновлення даних для запобігання втраті важливої перекладацької інформації у випадку непередбачених ситуацій.є
- Безпека офісу завдяки впровадженій IoT системи яка вмикає сирену при виявленні вогню у офісі або вмикає сирену та камери при застосування неідентифікованої карти доступу.

Основні вимоги до налаштувань підсистеми компанії:

- виконати налаштування адресації всіх пристроїв;
- виконати налаштування динамічного призначення адрес вузлам за допомогою DHCP;
- виконати налаштування аутентифікації на маршрутизаторах використовуючи службу AAA по протоколу Radius;
- виконати налаштування DNS та HTTP серверів для забезпечення функціюваня сайту компанії за доменою адресою 123.dnipro.ua;
- використати протокол маршрутизації OSPF;
- призначити на кожному мережевому пристрої ім’я, створити користувача, доменне ім’я, встановити паролі до режиму EXEC та ліній console та vty. Використовувати протокол SSH для віддаленного з’єднанні з пристроями;
- для відділу керівництва, маркетингу, відділу продаж та бухгалтерії виконати поділення на підмережі VLAN таким чином: VLAN 16 для керівництва,VLAN 26 для бухгалтерії таVLAN 36 для відділу продаж та маркетингу;

- на маршрутизаторах виконати налаштування NAT та VPN використовуючи протокол IPsec. Також додати ACL списки доступу;
-

2.1.4 Вимоги до видів забезпечення

2.1.4.1 Вимоги до інформаційного забезпечення

Вимоги до складу, структури і способів організації даних у Системі:

- Система повинна мати структуровану базу даних, де розміщені перекладацькі проекти, власні термінологічні бази, клієнтські дані та інша важлива інформація.

  Наприклад: Використання реляційної бази даних, де кожен перекладацький проект представлений окремим записом зі збереженими текстами, статусами та іншими відомостями.

Вимоги до інформаційного обміну між компонентами Системи:

- Система повинна забезпечувати ефективний обмін даними між різними компонентами, такими як додатки для управління проектами, системи перекладу та редактування, електронна пошта тощо.

  Наприклад: Автоматичний обмін текстовими файлами між системою управління проектами та системою перекладу для передачі завдань перекладачам та отримання готових перекладів.

Вимоги до інформаційної сумісності із суміжними Системами:

- Система повинна бути сумісною з іншими системами, які використовуються в бюро перекладів, наприклад, системами управління клієнтами або системами фінансового обліку.
- Приклад: Інтеграція системи бюро перекладів з системою управління клієнтами для автоматичного обміну даними про клієнтів, проекти та фінансову інформацію.

Вимоги до застосування Систем керування базами даних:

- Система повинна використовувати сучасні системи керування базами даних (СКБД) для забезпечення ефективного зберігання, організації та доступу до даних.

Наприклад: Використання СКБД, таких як MySQL або PostgreSQL, для зберігання та керування даними бюро перекладів.

Вимоги до структури процесу збору, обробки, передачі даних у Системі і представлення даних:

- Система повинна мати чітку структуру для збору, обробки та передачі даних між різними етапами перекладу та редактування. Дані повинні бути представлені зрозуміло та зручно для користувачів.

Наприклад: Використання розширених форматів файлів, таких як XML або JSON, для зберігання даних про проекти, відстеження стану та представлення результатів перекладу.

Вимоги до контролю, збереження і відновлення даних:

- Система повинна мати механізми контролю цілісності даних, забезпечення резервного копіювання та можливості відновлення даних в разі втрати або пошкодження.

Наприклад: Автоматичне резервне копіювання бази даних на регулярній основі та забезпечення можливості відновлення збережених копій в разі потреби.

2.1.4.2 Вимоги до лінгвістичного забезпечення

Застосування мов програмування високого рівня: Система бюро перекладів повинна використовувати мови програмування, які дозволяють зручно та ефективно розробляти функціонал, взаємодіяти з базами даних та іншими компонентами системи. Наприклад, мови програмування такі як Python, Java, C# можуть бути використані для розробки лінгвістичної функціональності.

Мови взаємодії користувачів і технічних засобів: Система повинна підтримувати мови взаємодії, що зрозумілі користувачам та сприяють зручній навігації та використанню функцій. Наприклад, веб-інтерфейс системи може мати підтримку мов, що дозволяють користувачам вибирати бажану мову

взаємодії. Необхідно виконати переклад сайту компанії англійською, французькою, німецькою, китайською, іспанською, української та італійською мовами.

Кодування і декодування даних: Система повинна мати підтримку різних стандартів кодування та декодування даних, зокрема для обробки текстових даних різних мов та символьних наборів. Наприклад, Unicode та UTF-8 може використовуватися для забезпечення міжнародної підтримки символів і мов.

Мови маніпулювання даними: Система повинна мати можливість маніпулювати лінгвістичними даними, зокрема для пошуку, сортування, фільтрації та інших операцій з даними. Наприклад, SQL може використовуватися для виконання запитів до бази даних з перекладами.

Способи організації діалогу: Система повинна мати механізми для організації діалогу з користувачами, такі як діалогові вікна, панелі інструментів, кнопки тощо. Наприклад, інтерфейс системи може містити кнопки для виклику функцій перекладу або відображення результатів.

2.1.4.3 Вимоги до технічного забезпечення

Усі комп’ютери або ноутбуки повинні відповідати нижче зазначеними характеристиками:

- Процесор Intel Core I5 не нижче 6 покоління;
- Оперативна пам'ять обсягом не менше 8 ГБ для перекладачів, і не менше 16 ГБ для проект менеджерів
- Використання дискретних відеоадаптерів не нижче GTX 1050 необхідно тільки для працівників пов’язаних з Autodesk AutoCAD.
- 1 або 2 додаткових монітора з діагоналлю не менше 21 дюйму
- Для проект менеджерів повинні бути встановлені веб камери великої роздільної здатності

Усі комутатори повинні мати не менше 24 портів

Маршрутизатори повинні мати порти які підтримують швидкість до 1Гб\с

2.1.4.4 Вимоги до організаційного забезпечення

Бюро перекладів повинно мати відділи замовлень, координації проектів, перекладу, редагування та контролю якості. Кожен підрозділ має свої визначені функції і відповідальності. Наприклад, відділ замовлень приймає замовлення від клієнтів і забезпечує встановлення термінів виконання завдань, а відділ перекладу займається безпосереднім перекладом текстів.

Забезпечення створення цілісної системи управління проектами, яка включає в себе розподіл завдань, встановлення пріоритетів, контроль виконання та звітність. Регулярні наради з персоналом для обговорення поточних проектів, вирішення проблем та планування подальших кроків.

Встановлення політики безпеки інформації, яка передбачає обов'язкове навчання персоналу з питань конфіденційності, безпеки даних та процедур захисту інформації. Встановлення обмеженого доступу до важливих систем та даних, використання ідентифікаторів і паролів для авторизації персоналу.

2.1.4.5 Вимоги методичного забезпечення

При проєктуванні системи повинні використовувати та спиратись на наступні стандарти:

ISO/IEC 11801: Цей стандарт визначає вимоги до структурированих кабельних систем (Structured Cabling Systems), які використовуються для передачі даних у мережах. Він встановлює стандарти для кабельних з'єднань, роз'ємів та категорій кабелів.

ISO/IEC 27001: Цей стандарт визначає вимоги до систем управління інформаційною безпекою. Він встановлює принципи та процедури для захисту інформації в комп'ютерних мережах, включаючи керування ризиками, фізичну безпеку, доступ до інформації та інші аспекти безпеки.

ISO/IEC 27031: Цей стандарт надає рекомендації щодо управління контингентністю бізнесу та відновлення роботи в комп'ютерних мережах. Він визначає принципи та процедури для планування, реалізації та відновлення діяльності мережі після аварійних ситуацій.

ISO/IEC 19770: Цей стандарт визначає вимоги до управління програмним забезпеченням та активами програмного забезпечення в комп'ютерних мережах. Він встановлює принципи та процеси для ідентифікації, вимірювання, керування та звітності про використання програмного забезпечення.

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

Зважаючи на визначену організаційну структуру підприємства (рисунок 1.1) та технічні вимоги до системи, потрібно розробити структурну схему комплексу технічних засобів комп'ютерної системи спираючись на загальну архітектуру та структуру мережі.

З метою врахування структурної схеми підприємства та вимог замовника, мережу необхідно розділити на підмережі. Для забезпечення пересилання трафіку між маршрутизаторами буде використано протокол маршрутизації OSPF. Структурна схема зображена на рисунку 2.1.

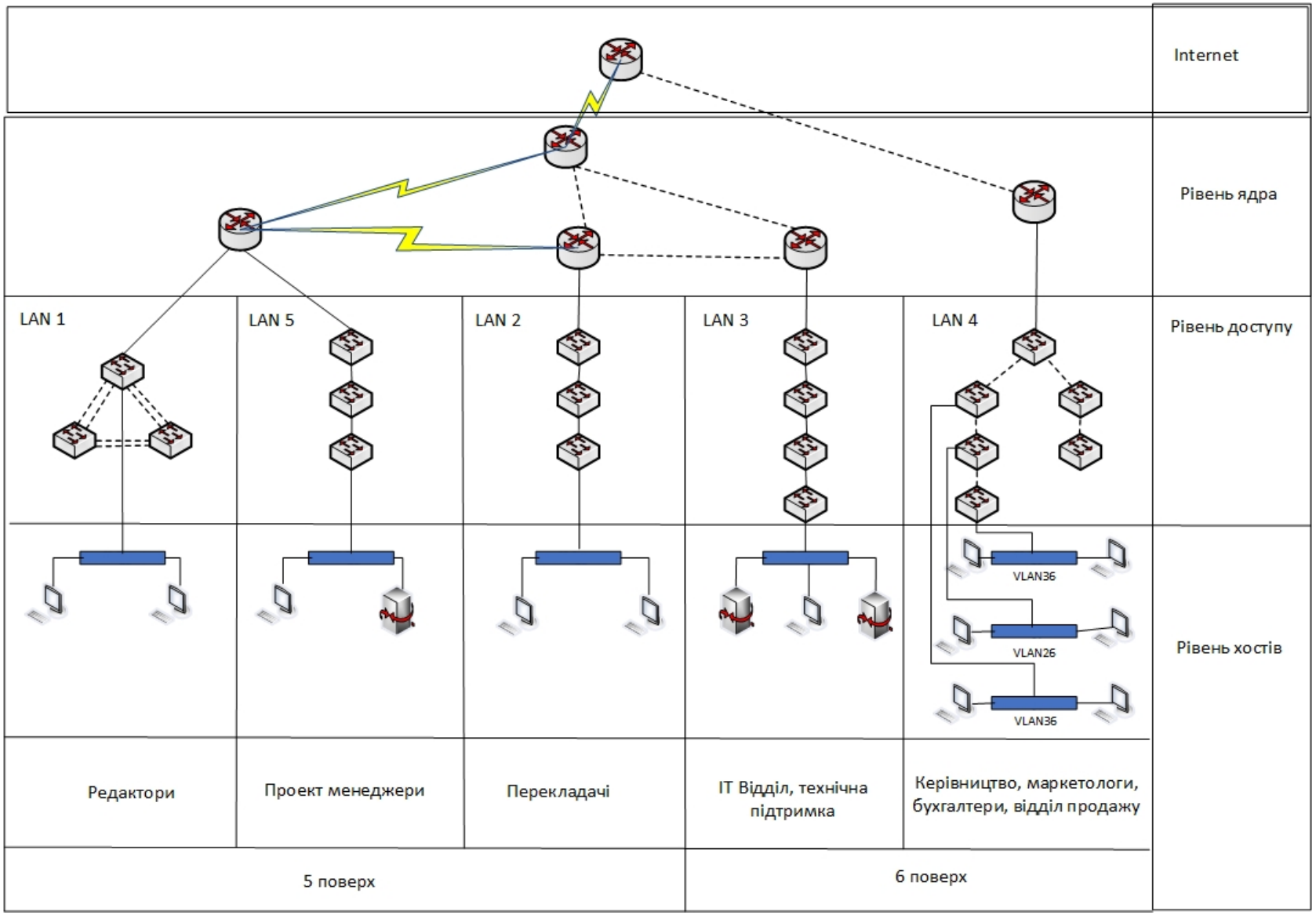

Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної системи

2.2.2 Розробка специфікації апаратних засобів комп’ютерної системи

Бюро перекладів «InText» орендує два поверхи офісної будівлі.

Враховуючи розроблену структурну схему комплексу технічних засобів комп'ютерної системи, необхідно розробити специфікацію для апаратних засобів системи.

LAN1 налічує 63 вузли. Враховуючи необхідний запас у 15% резервних портів, необхідно обрати 3 комутатора по 24 порти. Відповідно загальна кількість портів буде становити 72 шт.

LAN2 та LAN5 налічують 67 вузлів відповідно. Враховуючи необхідний запас у 15% резервних портів, необхідно обрати 3 комутатора по 24 порти. Задля економії коштів компанії було обрано 3, а не 4 комутатори. Відповідно загальна кількість портів буде становити 72 шт.

LAN3 налічує 88 вузлів. Враховуючи необхідний запас у 15% резервних портів, необхідно обрати 4 комутатора по 24 порти. Відповідно загальна кількість портів буде становити 96 шт.

LAN4 налічує 94 вузли. Враховуючи необхідний запас у 15% резервних портів, необхідно обрати 5 комутаторів по 24 порти. Відповідно загальна кількість портів буде становити 120 шт.

Для забезпечення зв'язку між комп'ютерами в офісній мережі були використані маршрутизатор серії 2911 та комутатори 2960-24TT зі стандартними портами FastEthernet та GigabitEthernet. В цьому випадку не було необхідності використовувати будь-які технології для покращення зв'язку в мережі. Сервера 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: 1x10/100 Fast Ethernet,

Компьютери було підібрано ARTLINE Business B29 v33 з процесором Intel Core i5-11400, оперативною пам’яттю 16 ГБ, SSD накопичувачем обсягом 512 ГБ та встановленою Windows 11.

Сервери та мережеве обладнання підібрано однакового виробника Cisco, завдяки цьому не повинні виникати проблем з сумісністю обладнання.

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

Таблиця 2.1 – Використані пристрої при побудові корпоративної мережі бюро перекладів «InText»

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: 3 integrated GigabitEthernet 4x EHWIC slots 2x onboard DSP slots 1x ISM slot 512 - 2048 MB DRAM 256 MB Compact Flash	Cisco 2900	од	5	За структурною схемою: Router0-5 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: 24x 10/100 Ethernet Ports 2x 1GSFP amd RJ-45 combo uplinks	Cisco 2960-24PS	од	19	Детальні характеристики: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html
3	Комп’ютер моделі B29 v33 Процесор Intel Core i5-11400 ОЗУ 16 ГБ Накопичувач SSD 512 ГБ	ARTLINE Business	од	379	Детальні характеристики: https://hard.rozetka.com.ua/artline_b29v33/p299437908/characteristics/

	ПЗ Windows 11				
4	Сервер C220 M3: Процесор: 2 шт x Intel Xeon E5-2650L v2. ОЗУ: 16 GB DDR3. RAID-контролер: Cisco UCS RAID SAS 2008M-8i Mezzanine Card UCSC-RAID-11-C220 74-10149-01. Мережеві порти: 2x 10/100/1000 Ethernet	Cisco UCS	од	3	https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m3-lff-specsheet.pdf

Для об’єднання усіх цих пристроїв в одну мережу і підтримання сайту бюро перекладів необхідні потужні сервери. Один з них забезпечує DNS зв’язок. Інші два – HTTP-сервер та TFTP-сервер. Порти між маршрутизаторами використовуються Serial, а між маршрутизаторами та комп’ютерами використовується порти FastEthernet або GigabitEthernet.

Також на комутаторах використовується система VLAN.

Розглянемо вибір структурованої кабельної мережі на прикладі 5 поверху. Бюро займає 5 та 6 поверх офісної будівлі. Складемо план розміщення вузлів комп'ютерної системи та спроектуємо схему кабельних мереж як показано на рисунку 2.3.

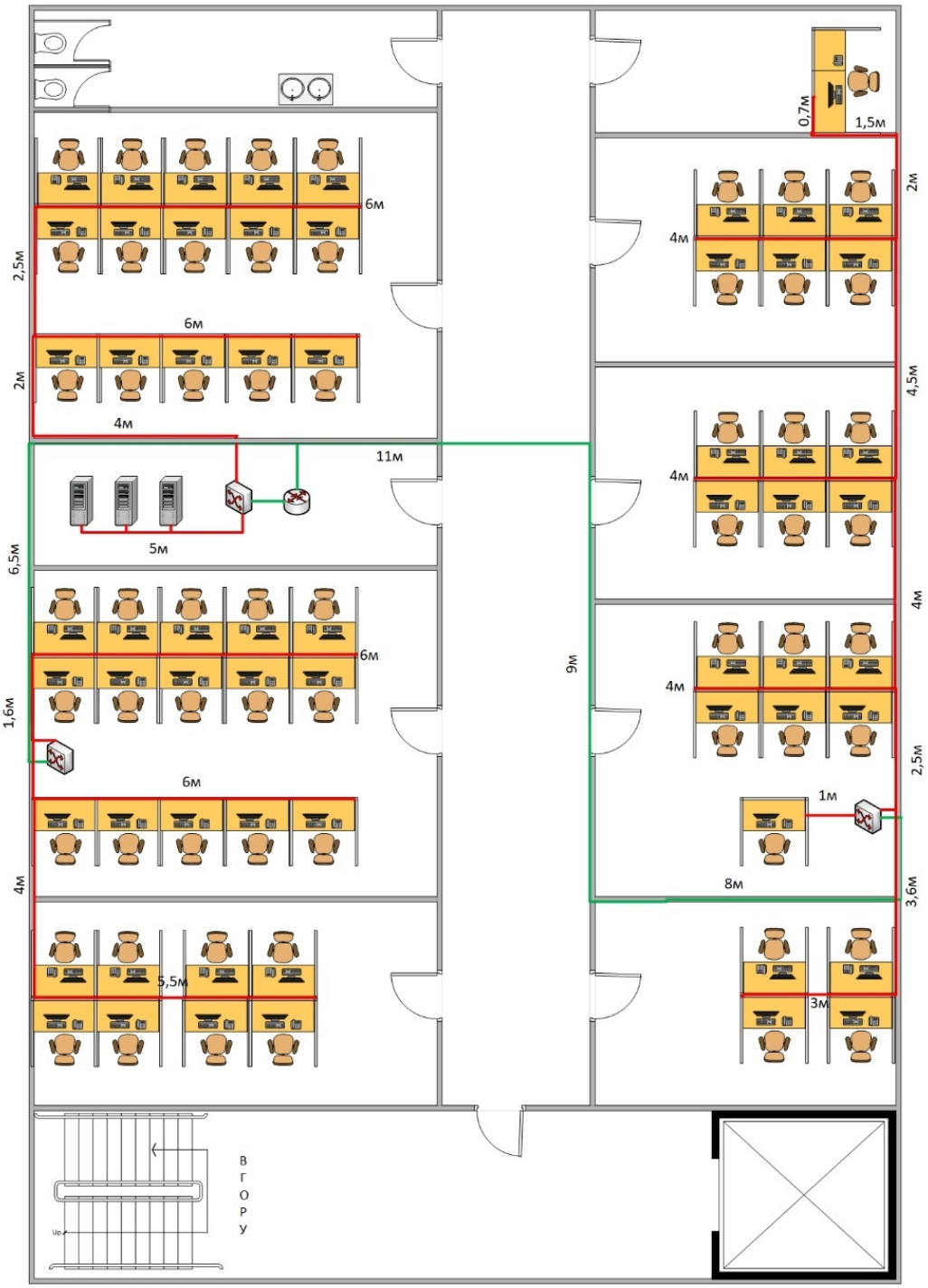

Рисунок 2.2 – Схема кабельної мережі 5 поверху

Для 5 поверху була розроблена схема кабельної мережі з використанням кабель каналів у стінах та розеток RJ-45.

Складемо специфікацію СКМ (таблиця 2.2)

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	Розетка комп'ютерна RJ45 UTP кат. 5E подвійна	Schneider	од	100	LAN1, LAN2, LAN5,
2	Розетка із заземленням подвійна	Schneider	од	120	LAN1, LAN2, LAN5,
3	LAN-кабель U/UTP кат 5E	Vinga	м	150	LAN1, LAN2, LAN5,
4	Кабель живлення ПВС 3х0,75	GAL-KAT	м	150	LAN1, LAN2, LAN5,
5	Кабельний канал пластиковий 30х25	Simon	м	130	LAN1, LAN2, LAN5,

2.2.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Найбільша мережа це LAN4 яка знаходиться на 6 поверсі. В неї входить 94 ПК. Вихідний трафік маршрутизується в лінію з пропускною здатністю у 1000 Мбіт на секунду.

Для того, щоб уникнути перенавантаження маршрутизатора, швидкість находження пакетів до нього повинна буде менше швидкості їх відправлення.

Для розрахунків візьмемо максимальний розмір навантаження пакетів у канальному рівні моделі OSI.

$$\mu_{вих} = \frac{1000000000}{650 \times 8} = 192\ 300 \frac{пакетів}{с} \qquad (2.1)$$

В середньому кожне джерело виробляє 52 пакетів на секунду. Виходячи з цього, максимальна кількість пристроїв, які можуть бути під'єднані до маршрутизатора розраховується наступним чином:

$$N=\frac{192300}{52}=3698 \text{ пристроїв} \quad (2.2)$$

Це підходить для підмережі на 94 ПК та залишає великі можливості для масштабування.

Кожен зі 94 ПК надсилає потік з інтенсивністю 52 кадрів/с.

Виходячи з цього, інтенсивність вихідного трафіку дорівнюватиме:

$$\lambda=94*52=4888 \text{ кадрів/с} \quad (2.3)$$

Коефіцієнт затримки розраховується наступним чином:

$$\rho = \frac{\lambda}{\mu_{вих}} = 4888/192300 = 0.025 \quad (2.4)$$

Коефіцієнт зайнятості маршрутизатора розраховується наступним чином:

$$\frac{\rho}{1-\rho}=\frac{0.025}{1-0.025}=0.025 \quad (2.5)$$

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

$$T=\frac{1}{\mu-\lambda}=\frac{1}{192300-4888}=5.33 \text{ мкс} \quad (2.6)$$

Середня довжина черги дорівнює:

$$L_{чер}=\frac{\rho^2}{1-\rho}=\frac{0.025^2}{1-0.025}=0.0006 \quad (2.7)$$

Середній час перебування пакета в черзі дорівнює:

$$T_{очікування}=\frac{L_{чер}}{\lambda}=\frac{0.0006}{4888}=122 \text{ нс} \quad (2.8)$$

Пропускну здатність каналу виведемо з наступної формули:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l} \quad (2.9)$$

Звідси отримуємо:

$$b=\lambda\times l=4888\times 650\times 8=25417600 \text{ біт/с} = 25{,}4176 \text{ Мбіт/с} \quad (2.10)$$

Це повністю задовольняє пропускну здатність нашого вихідного каналу в 1000 Мбіт/с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок адресації корпоративної мережі

В кваліфікаційній роботі необхідно змоделювати КС згідно заданої структури (рисунок 2.1).

Кожній підмережі має бути надана мережна адреса за принципом 10.23.36.0/22 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
6	10.23.36.0	63	67	88	94	67

Необхідно організувати 5 підмереж с загальною кількістю користувачів у 379 штуки.

Застосуємо метод VLSM, який дозволяє виділити мережу розміру у ступінь двійки. Також слід ураховувати те, що перша та остання адреси мережі зайняті, а тому у мережі з 128 адрес, тільки 126 є корисними.

Враховуючи необхідну кількість пристроїв у кожній підмережі, поділимо діапазон таким чином: 5x128

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

10.23.00100100.|00000000

Першу мережу візмемо LAN_4 як саму велику. Вона налічує 94 користувача.

Мінімальний блок адрес для такої кількості користувачів містить 128 адрес, дві з яких виділені.

Для розрахунку виділяємо блок в 128 адрес:
10.23.00100101.01111111

Отримуємо адресу 10.23.00100101.01111111 - 10.23.36.127 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.36.127 та діапазоном доступних адрес 10.23.36.1 – 10.23.36.126.

Наступну мережу оберемо LAN_3, так як вона наступна по кількості користувачів і налічує 88 користувачів. Мінімальний блок адрес для такої кількості користувачів містить також 128 адрес, дві з яких виділені.

Для розрахунку виділяємо ще блок в 128 адрес:

10.23.00100100.11111111

Отримуємо адресу 10.23.00100100.11111111 – 10.23.36.255 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.36.255 та діапазоном доступних адрес 10.23.36.129-10.23.36.254.

Наступною мережою по кількості візьмемо LAN_5, яка налічує 67 користувачів. Мінімальний блок адрес для такої кількості користувачів містить також 128 адрес, дві з яких виділені.

Додамо 1 біт до попередньої мережі та додамо ще блок з 128 адрес

10.23.00100101.01111111

Отримуємо адресу 10.23.00100101.01111111 - 10.23.37.127 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.37.127 та діапазоном доступних адрес 10.23.37.1 – 10.23.37.126.

Наступною мережою візьмемо LAN_2, яка налічує також 67 користувачів. Мінімальний блок адрес для такої кількості користувачів містить також 128 адрес, дві з яких виділені.

Для розрахунку виділяємо ще блок в 128 адрес:

10.23.00100101.11111111

Отримуємо адресу 10.23.00100100.11111111 – 10.23.37.255 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.37.255 та діапазоном доступних адрес 10.23.37.129-10.23.37.254.

Останньою мережою візьмемо LAN_1, вона налічує 63 користувача. Мінімальний блок адрес для такої кількості користувачів містить також 128 адрес, дві з яких виділені.

Для розрахунку виділяємо ще блок в 128 адрес:

10.23.00100110.01111111

Отримуємо адресу 10.23.00100110.01111111 - 10.23.38.127 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.38.127 та діапазоном доступних адрес 10.23.38.1 – 10.23.38.126.

Адресація з врахуванням вимог до мережі і представлена у вигляді таблиці 3.2.

Таблиця 3.2 – Схема адресації мережі

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
LAN1	63	126	10.23.38.0	/25	10.23.38.1 - 10.23.38.126	10.23.38.127
LAN2	67	126	10.23.37.128	/25	10.23.37.129 - 10.23.37.254	10.23.37.255
LAN3	88	126	10.23.36.128	/25	10.23.36.129 - 10.23.36.254	10.23.36.255
LAN4	94	126	10.23.36.0	/25	10.23.36.1 - 10.23.36.126	10.23.36.127
LAN5	67	126	10.23.37.0	/25	10.23.37.1 - 10.23.37.126	10.23.37.127

Схема адресації каналів між маршрутизаторами з діапазону 10.1.6.0/24 представлена у таблиці 3.3.

Таблиця 3.3 – Підмережі каналів WAN між маршрутизаторами

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
WAN1	2	2	10.1.6.0	/30	10.1.6.1 - 10.1.6.2	10.1.6.3
WAN2	2	2	10.1.6.4	/30	10.1.6.5 - 10.1.6.6	10.1.6.7
WAN3	2	2	10.1.6.8	/30	10.1.6.9 - 10.1.6.10	10.1.6.11
WAN4	2	2	10.1.6.12	/30	10.1.6.13 - 10.1.6.14	10.1.6.15
WAN5	2	2	10.1.6.16	/30	10.1.6.17 - 10.1.6.18	10.1.6.19

3.2 Розрахунок адресації пристроїв

У таблиці 3.4 наведена адресація всіх маршрутизаторів мережі з дотриманням всіх необхідних вимог.

Таблиця 3.4 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска
Kovalenko_Router_0	Gig0/1.36	10.23.36.1	255.255.255.224
	Gig0/1.26	10.23.36.33	255.255.255.224
	Gig0/1.16	10.23.36.65	255.255.255.224
	Gig0/1.99	10.23.36.97	255.255.255.240
	Gig0/0	64.100.13.2	255.255.255.252
	Gig0/1	10.23.36.1	255.255.255.128
Kovalenko_Router_1	Gig0/0	10.1.6.13	255.255.255.252
	Gig0/1	10.1.6.10	255.255.255.252
	Gig0/2	10.23.37.129	255.255.255.128
	Se0/3/0	10.1.6.6	255.255.255.252
Kovalenko_Router_2	Gig0/0	10.23.38.1	255.255.255.128
	Gig0/1	10.23.37.1	255.255.255.128
	Se0/3/0	10.1.6.2	255.255.255.252
	Se0/3/1	10.1.6.5	255.255.255.252
Kovalenko_Router_3	Gig0/0	10.1.6.17	255.255.255.252
	Gig0/1	10.1.6.9	255.255.255.252
	Se0/3/0	10.1.6.1	255.255.255.252
	Se0/3/1	209.165.202.1	255.255.255.252
Kovalenko_Router_4	Gig0/0	10.1.6.18	255.255.255.252
	Gig0/1	10.1.6.14	255.255.255.252
	Gig0/2	10.23.36.129	255.255.255.128
Kovalenko_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	209.165.202.2	255.255.255.252

Адреси в підмережах, що привласнюються інтерфейсам комутаторів, написані у таблиці 3.5.

Таблиця 3.5 – IP-адреси комутаторів в підмережах відділів

Підмережа	Пристрій	IP-адреса SVI інтерфейсу	Маска підмережі	Адреса шлюзу
LAN1	Kovalenko_Switch_0	10.23.38.2	255.255.255.128	10.23.38.1
	Kovalenko_Switch_1	10.23.38.3		
	Kovalenko_Switch_2	10.23.38.4		
LAN2	Kovalenko_Switch_8	10.23.37.130	255.255.255.128	10.23.37.129

Підмережа	Пристрій	IP-адреса SVI інтерфейсу	Маска підмережі	Адреса шлюзу
	Kovalenko_Switch_7	10.23.37.131		
	Kovalenko_Switch_6	10.23.37.132		
LAN3	Kovalenko_Switch_12	10.23.36.130	255.255.255.128	10.23.36.129
	Kovalenko_Switch_13	10.23.36.131		
	Kovalenko_Switch_14	10.23.36.132		
	Kovalenko_Switch_15	10.23.36.133		
LAN4	Kovalenko_Switch_4	10.23.36.2	255.255.255.128	10.23.36.1
	Kovalenko_Switch_3	10.23.36.3		
	Kovalenko_Switch_16	10.23.36.4		
	Kovalenko_Switch_17	10.23.36.5		
	Kovalenko_Switch_5	10.23.36.6		
	Kovalenko_Switch_18	10.23.36.7		
LAN5	Kovalenko_Switch_9	10.23.37.2	255.255.255.128	10.23.37.1
	Kovalenko_Switch_11	10.23.37.3		
	Kovalenko_Switch_10	10.23.37.4		

3.3 Налаштування моделі комп’ютерної системи корпоративної мережі

На рисунку 3.1 зображена топологічна схема корпоративної мережі. Топологічна схема включає в себе головний та віддалений офіс, мережу провайдера. Мережа зв’язана між собою за допомогою кабелів SerialEthernet та GigabitEthernet.

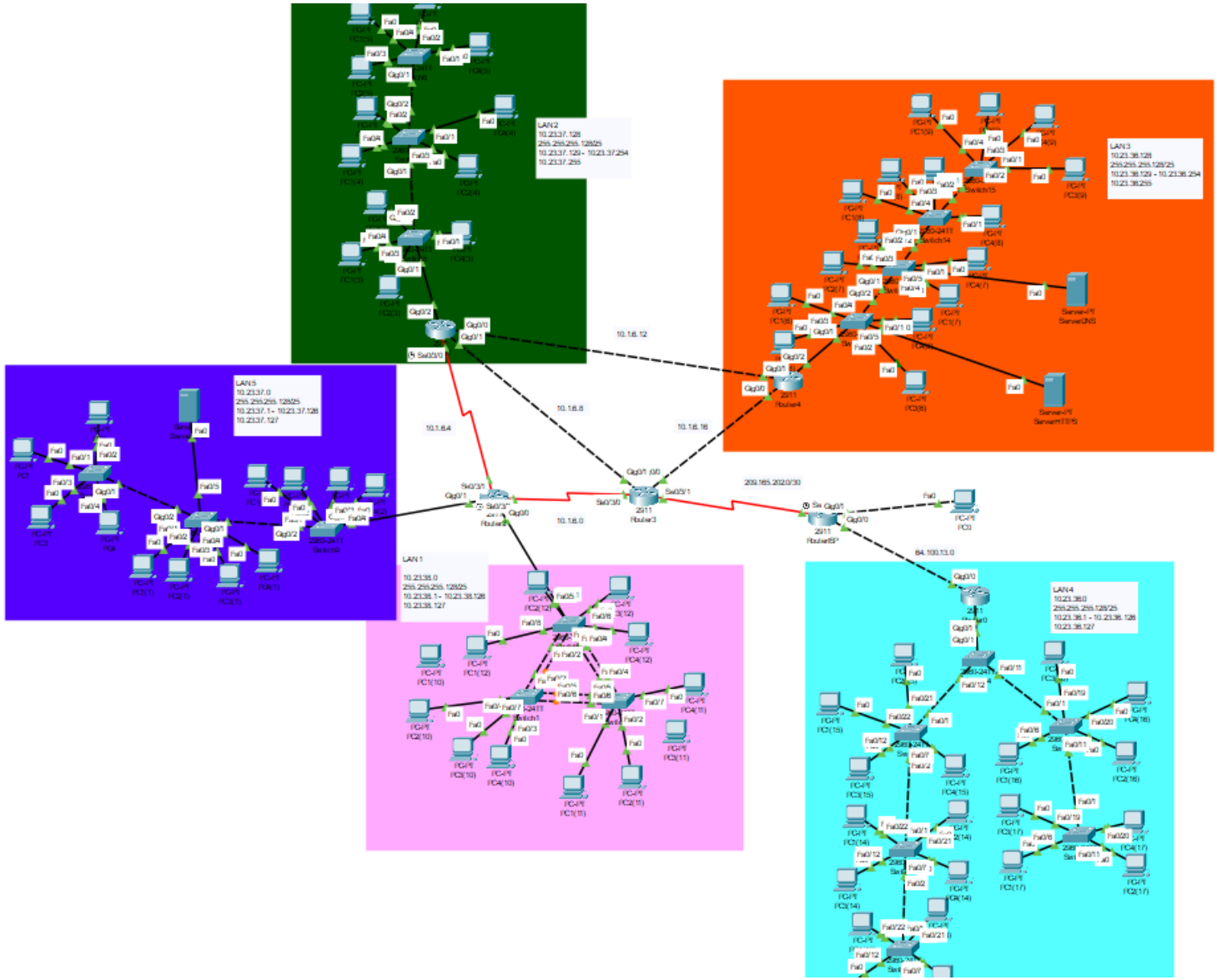

Рисунок 3.1 – Топологічна схема КМ бюро перекладів «InText»

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

Щоб захистити мережеві пристрої від несанкціонованого доступу виконаємо базова нелаштування пристроїв. За приклад візьмемо Kovalenko_Router_0:

Перейдемо до привілейованого режиму:

Enable

Перейдемо до режиму глобальної конфігурації:

Conf t

Змінемо назву маршрутизатору:

Hostname Kovalenko_Router_0

Встановимо пароль на вхід для консолі:

Line console 0

Password cisco

Login

Встановимо пароль для ліній vty:

Line vty 0 15

Password cisco

Login

Встановимо пароль для привілейованого режиму та увімкнемо його шифрування:

Enable secret class

Service password-encryption

Встановимо банер MOTD:

Banner motd 'Kovalenko_Router_0'

Встановиме доменне ім'я:

ip domain-name Kovalenko_Router_0

Згенеруємо пари ключів для встановлення зв'язку протоколом SSH:

Crypto key generate rsa

1024

Username 123191_Kovalenko password admincisco

Line vty 0 15

Увімкнемо доступ до консолі через SSH:

Transport input ssh

Login local

Збережемо налаштування:

copy running-config startup-config

За для збільшення пропускної здатності мережі LAN1, необхідно об'єднати фізичні лінії комутаторів. Технологія EtherChannel дозволяє збільшити пропускну можливість. Нижче наведено приклад налаштування Kovalenko_Switch_0

Виберемо діапазон портів:

interface range fa0/3-4

Обє'днаємо порти у групу:

channel-group 1 mode active

interface port-channel 1

Увімкнемо режим trunk:

switchport mode trunk

Дозволимо усім vlan передавати трафік:

switchport trunk allowed vlan all

Повторимо налаштування для 2 групи:

interface range fa0/5-6

channel-group 2 mode active

interface port-channel 2

switchport mode trunk

switchport trunk allowed vlan all

З рисунку 3.2 видно, що агрегація каналів успішно налаштована та працює:

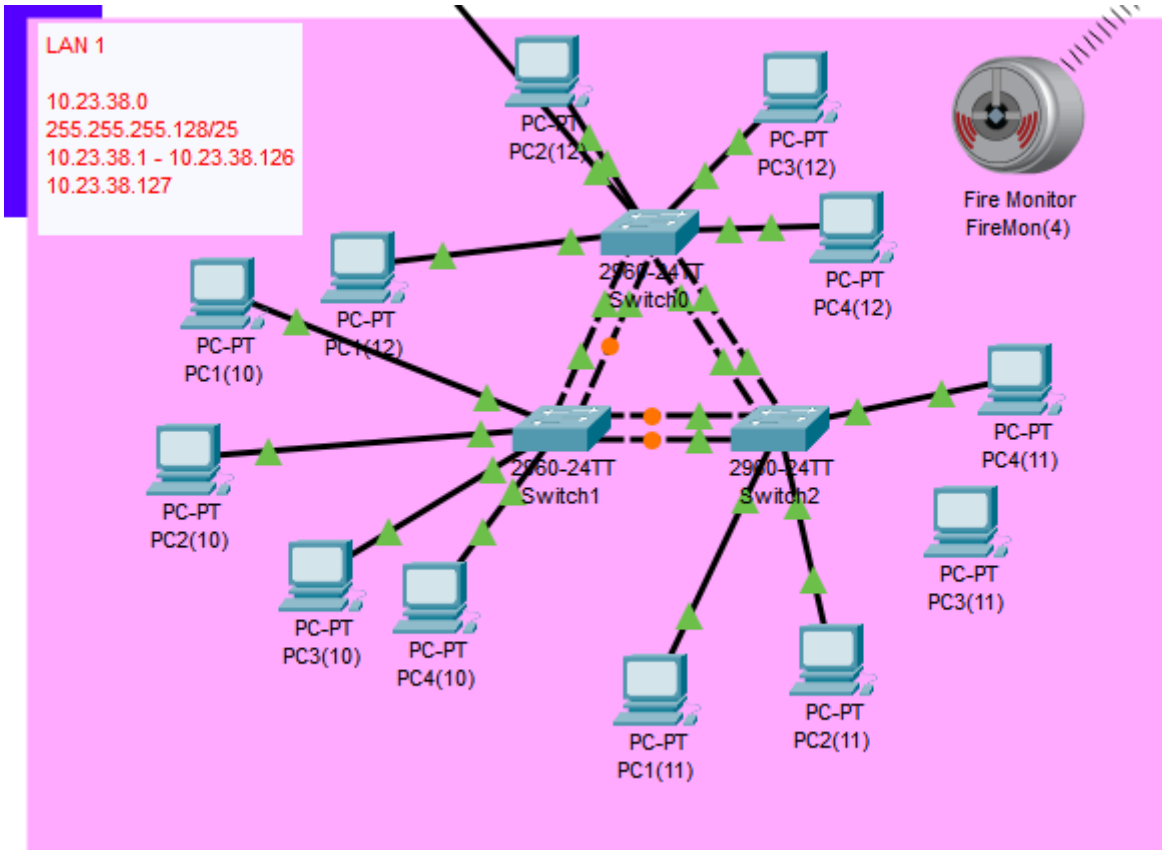

Рисунок 3.2 – Агрегація каналів комутаторів

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Щоб користувачі з різних підмереж могли взаємодіяти один з одним, налаштуємо протокол динамічної маршрутизації OSPF. Цей протокол підтримується великою кількістю пристроїв та швидко працює у великих мережах, що нам і необхідно.

Нижче наведено приклад налаштування протоколу OSPF для маршрутизатора Kovalenko_Router_2:

Увімкнемо протокол OSPF:

router ospf 1

Налаштуємо пасивні інтерфейси:

passive-interface default

no passive-interface Gig0/1

no passive-interface Gig0/0

no passive-interface Serial0/3/0

no passive-interface Serial0/3/1

Оголосимо необхідні мережі:

network 10.1.6.0 0.0.0.3 area 0

network 10.1.6.4 0.0.0.3 area 0

network 10.23.37.0 0.0.0.127 area 0

network 10.23.38.0 0.0.0.127 area 0

На маршрутизаторі який під'єднан безпосередньо до маршрутизатору провайдера (Kovalenko_Router_3) налаштуємо статичний маршрут за замовчуванням:

ip route 0.0.0.0 0.0.0.0 209.165.202.1

Додамо ще один статичний маршрут, щоб забезпечити доступ до мережі ISP з локальної мережі:

ip route 209.165.201.0 255.255.255.240 209.165.202.2

Також налаштуємо службу AAA на всіх марщрутизаторах мережі. За допомогою даною служби з'являється можливість перевіряти ідентичність користувача за допомогою аутентифікації до того, як надати йому дсотуп до налаштування мережевого обладнання.

Нижче наведено приклад налаштування AAA на маршрутизаторі:

Створюємо нову AAA модель:

aaa new-model

Призначаємо адреси Radius серверу:

radius-server host 64.100.13.2 auth-port 1645 key radius123

Налаштуємо аутентифікацію до консолі:

aaa authentication login CONSOLE group radius local

line console 0

login authentication CONSOLE

Створимо локальну базу користувачів:

aaa authentication login default local

Створимо користувача:

username Kovalenko_Router_0 password admin123

line vty 0 15

login authentication default

Також необхідно налаштувати службу AAA безпосередньо на сервері. Для цього використаємо DNS-сервер компанії задля збереження коштів. Налаштування серверу зображено на рисунку 3.4.

На рисунку 3.3 зображена перевірка роботи аутентифікації за допомогою служби AAA:

```
User Access Verification

Username: Kovalenko_Router_0
Password:
Kovalenko_Router_0>
```

Рисунок 3.3 – Аутентифікація за допомогою служби AAA

Також необхідно налаштувати службу AAA безпосередньо на сервері. Використаємо вже становлений сервер DNS. Налаштування зображено на рисунку 3.4

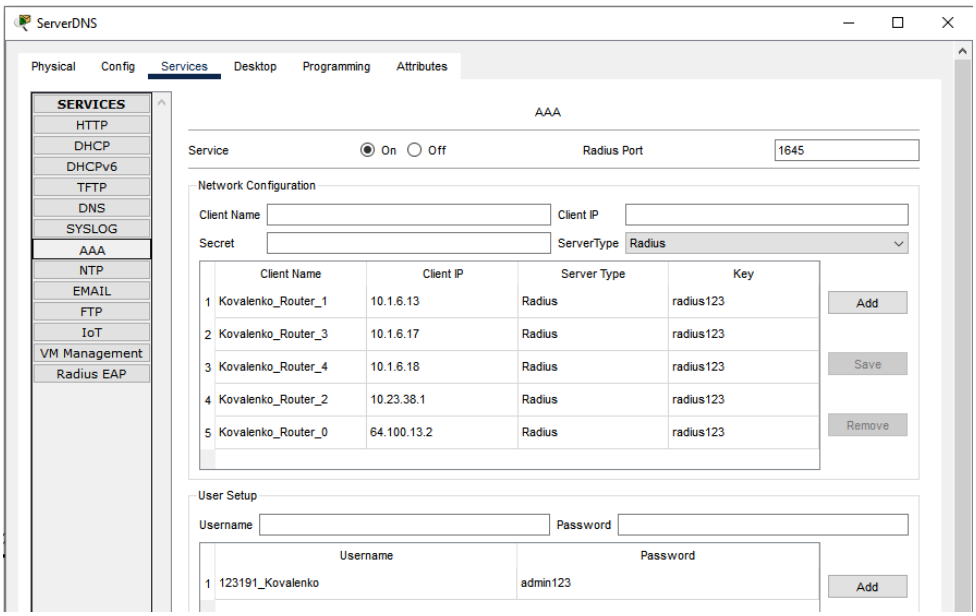

Рисунок 3.4 – Налаштування служби AAA

3.4.3 Налаштування роботи Інтернет

Для налаштування роботи Інтернету, необхідно на пограничному маршрутизаторі налаштувати NAT. Пул адрес задіяний для трансляції становить: 209.165.200.5 по 209.165.200.30.

Щоб забезпечити роботу NAT, необхідно створити список ACL. В цьому списку необхідно дозволити прохід трафіку з локальних підмереж у Інтеренет. Також у цьому списку необхідно заборонити прохід трафіку з локальних мереж у віддалену мережу LAN4.

Нижче наведено налаштування NAT та ACL списків:

Створимо список:

ip access-list extended NAT6

Заблокуємо трафік з локальної мережі у віддаленкїу:

deny ip 10.23.38.0 0.0.0.127 10.23.36.0 0.0.0.127

deny ip 10.23.37.128 0.0.0.127 10.23.36.0 0.0.0.127

deny ip 10.23.36.128 0.0.0.127 10.23.36.0 0.0.0.127

deny ip 10.23.37.0 0.0.0.127 10.23.36.0 0.0.0.127

deny ip 10.1.6.0 0.0.0.255 10.23.36.0 0.0.0.127

Дозволимо трафік з локальних мереж:

permit ip 10.23.38.0 0.0.0.127 any

permit ip 10.23.37.128 0.0.0.127 any

permit ip 10.23.36.128 0.0.0.127 any

permit ip 10.23.37.0 0.0.0.127 any

permit ip 10.1.6.0 0.0.0.255 any

Створимо NAT пул:

ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224

Увімкнемо трансляцію відповідно до ACL списку:

ip nat inside source list NAT6 pool Internet

Налаштуємо зовнішній порт:

interface Serial0/3/1

ip nat outside

Налаштуємо внутрішній порт:

interface Serial0/3/0

ip nat inside //налаштування внутрішнього порту

Перевіримо роботу NAT. Надішлемо ICMP пакет з мережі LAN5 до ПК провайдеру. На рисунку 3.5 показано успішне виконання трансляції локальної мережі у глобальну мережу.

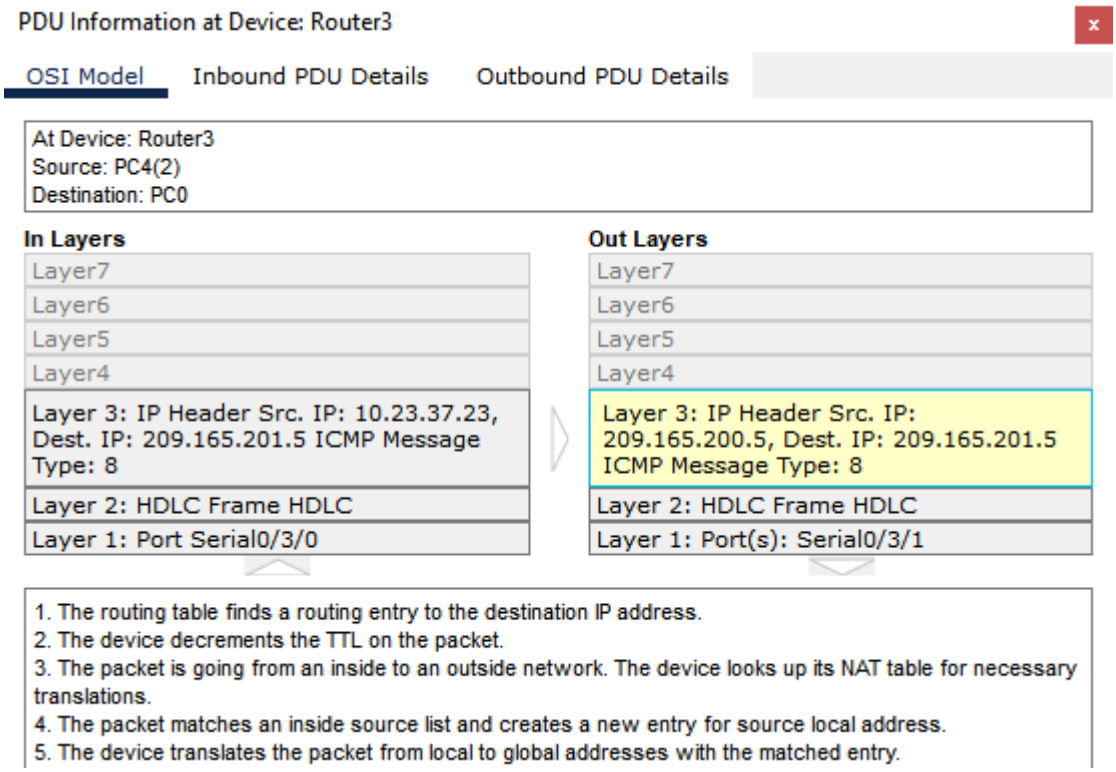

Рисунок 3.5 – Пакет з LAN5 під час трансляції NAT

Далі налаштуємо VPN для зв'язку між основною та віддаленою мережами. За основу візьмемо IPsec. Для цього необхідно створити новий ACL список для керування трафіком. Нижче наведено налаштування ACL списку на роутері Kovalenko_Router_3:

Створимо новий список:

ip access-list extended VPN6

Дозволимо трафік з основної мережі у віддалену:

permit ip 10.23.38.0 0.0.0.127 10.23.36.0 0.0.0.127

permit ip 10.23.37.128 0.0.0.127 10.23.36.0 0.0.0.127

permit ip 10.23.36.128 0.0.0.127 10.23.36.0 0.0.0.127

permit ip 10.23.37.0 0.0.0.127 10.23.36.0 0.0.0.127

permit ip 10.1.6.0 0.0.0.255 10.23.36.0 0.0.0.127

Після створення ACL списку необхідно налаштувати сам VPN. Нижче наведено команди для його налаштування:

Активуємо модуль securityk9 та перезавантажуємо його:

license boot module c2900 technology-package securityk9

Створюємо політику ISAKMP 10 та налаштовуємо її:

crypto isakmp policy 10

encr 3des

hash md5

authentication pre-share

group 2

Створюємо ключ cisco та вказуємо адресу адресу зовнішнього інтерфейсу маршрутизатора віддаленої мережі LAN4:

crypto isakmp key cisco address 209.165.202.1

Створюємо набор перетворень:

crypto ipsec transform-set TS esp-3des esp-md5-hmac

Створюємо крипто-зіставлення

crypto map MAP 10 ipsec-isakmp

set peer 209.165.202.1

set transform-set TS

match address VPN6

Вмикаємо крипто-зіставлення на зовнішньому інтерфейсі маршрутизатора:

interface Gig0/0

crypto map MAP

Виконаємо аналогічні налаштування на маршрутизаторі у відаленій мережі LAN4

Пакет який відправдяється з підмережі LAN5 у віддалену підмережу LAN4 шифрується пограничним маршрутизатором Kovalenko_Router_3 протоколом IPsec та пересилає його на маршрутизатор провайдеру. Це показано на рисунку 3.6

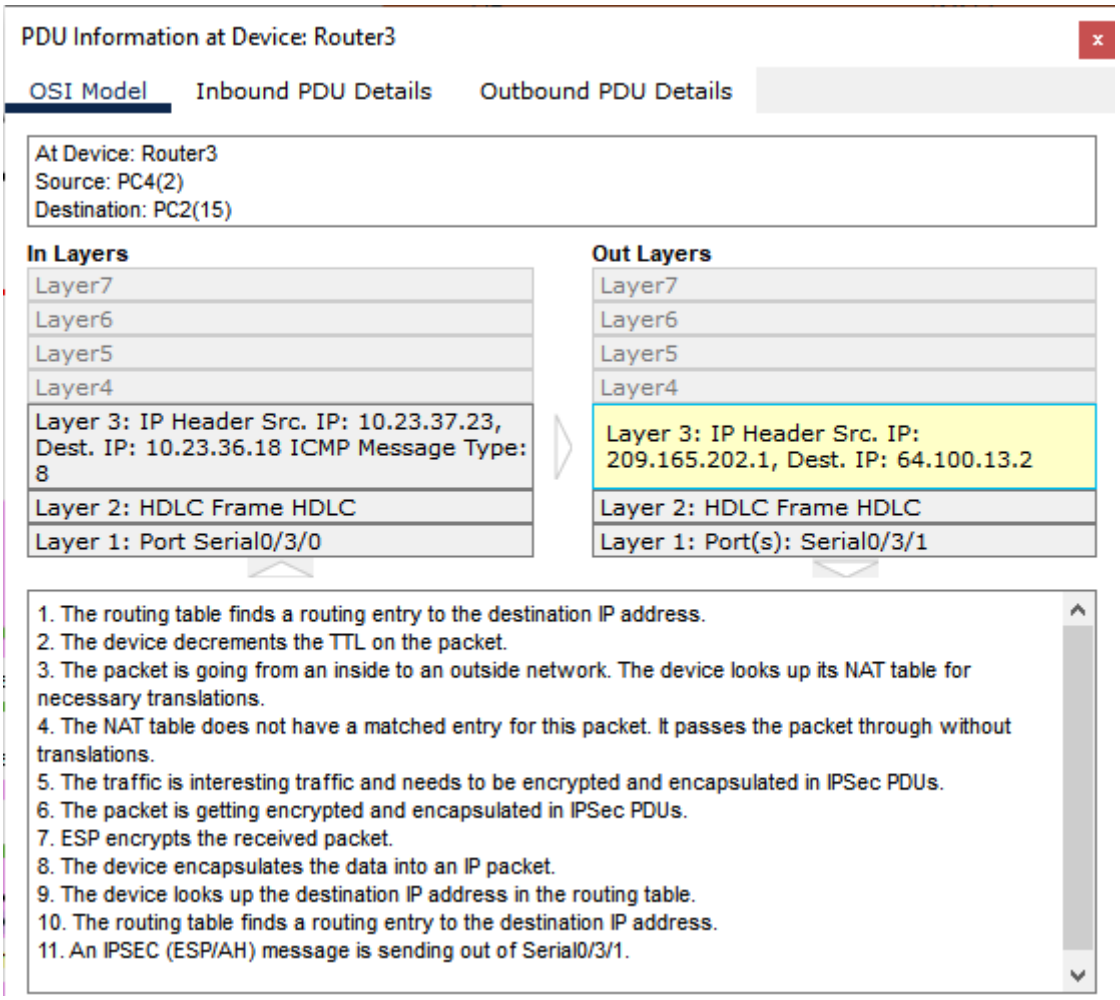

Рисунок 3.6 – Шифрування пакету на пограничному маршрутизаторі

Також налаштуємо HTTP сервер так, щоб на вузлах при вводі у рядок браузеру http://123.dnipro.ua або http://209.165.200.4 відкривався веб-сайт з відомостями про кваліфікаційну роботу, її тему та завдання.

Налаштуємо статичну трансляцію на Kovalenko_Router_3, де локальна адреса серверу буде транслюватись як 209.165.200.4. Також на сервері DNS необхідно створити доменне ім'я 123.dnipro.ua з прив'язкою до глобальної адреси HTTP серверу.

Команда для налаштування статичної трансляції:

ip nat inside source static 10.23.36.144 209.165.200.4

Налашутвання доменного імені на DNS сервері показано на рисунку 3.7.

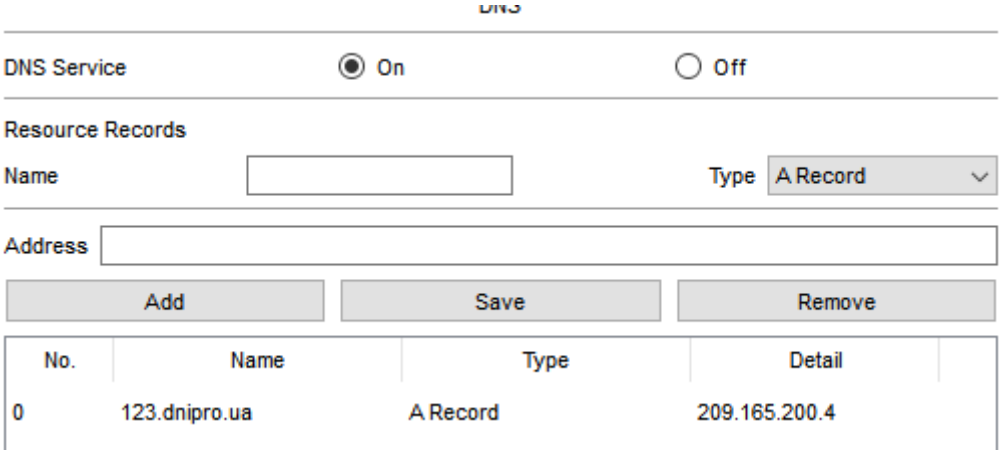

Рисунок 3.7 – Налаштування доменного імені на DNS-сервері

Перевіримо доступ до веб-сайту. Для цього необхідно з веб-браузеру будь-якого комп'ютеру зайти за доменним ім'ям 123.dnipro.ua. Результат показанона рисунку 3.8.

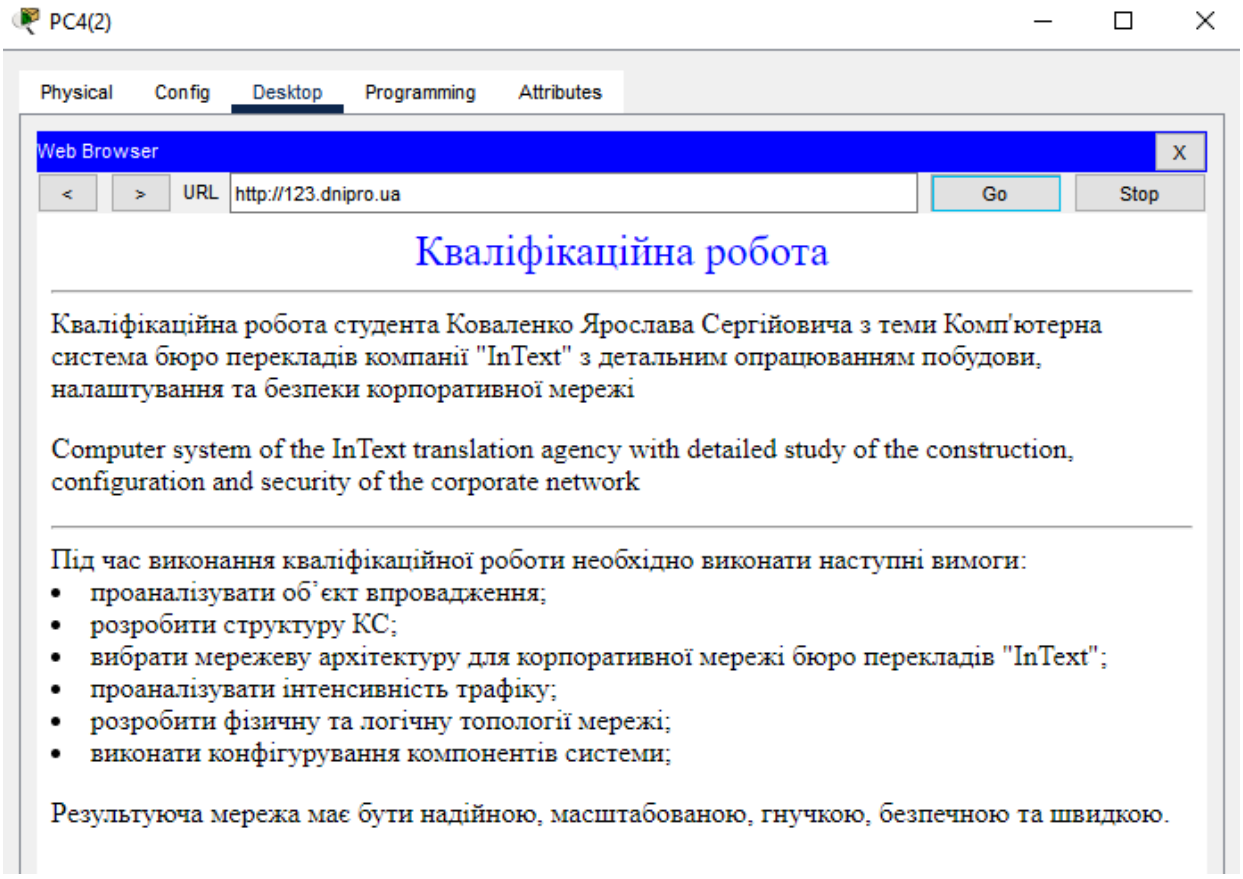

Рисунок 3.8 – Відображення вебсайту з браузеру ПК

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Комплекс заходів для захисту інформації в комп'ютерній системі включає в себе різноманітні методи та технології. Одним з найважливіших аспектів є аутентифікація користувачів, яка забезпечує перевірку їх ідентичності та доступ до системи лише після підтвердження правильності даних. Для забезпечення конфіденційності даних використовується шифрування, що дозволяє захистити інформацію від несанкціонованого доступу шляхом перетворення її у незрозумілий для сторонніх вид.

Окрім цього, важливим компонентом є використання антивірусного програмного забезпечення, яке виявляє та нейтралізує шкідливі програми та загрози, що можуть пошкодити систему або викрасти дані. Фізична безпека також має велике значення, оскільки контроль доступу до приміщення, де знаходяться сервери та інші пристрої, забезпечує захист від фізичних атак та незаконного доступу до обладнання.

Комплексне застосування цих методів та технологій дозволяє створити надійний рівень захисту інформації в комп'ютерній системі, забезпечуючи конфіденційність, цілісність та доступність даних для авторизованих користувачів.

3.5.2 Налаштування віртуальних мереж VLAN

У мережі LAN4 виконаємо розділення робітників на 3 групи за допомогою технології віртуаьних локальних мереж VLAN. Ця технологія дозволяє заощадити на покупці нових маршрутизаторів шляхом створення нових віртуальних мереж.

У таблиці 3.6 вказано нумерації створених VLAN та їх призначення:

Таблиця 3.6 – Нумерація створених VLAN та їх призначення

Номер VLAN	Ім’я VLAN	Примітка
16	VLAN16	Керівництво
26	VLAN26	Маркетологи
36	VLAN36	Відділ продажу та бухгалтерія
1	Default	Не використовується
99	Management	Для керування пристроями
100	Native	Власна

Адресацію віртуальних мереж VLAN наведено у таблиці 3.7.

Таблиця 3.7 – Схема адресації VLAN

Назва підмережі	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
VLAN16	30	30	10.23.36.64	/27	10.23.36.65 - 10.23.36.94	10.23.36.95
VLAN26	30	30	10.23.36.32	/27	10.23.36.33 - 10.23.36.62	10.23.36.63
VLAN36	30	30	10.23.36.0	/27	10.23.36.1 - 10.23.36.30	10.23.36.31
Management	14	14	10.23.36.96	/28	10.23.36.97 - 10.23.36.110	10.23.36.111
Native	6	6	10.23.36.112	/29	10.23.36.113 - 10.23.36.118	10.23.36.119

У таблиці 3.8 наведено розподіл портів комутаторів для мереж VLAN

Таблиця 3.8 – Розподіл портів комутаторів

Назва підмережі	VLAN	Розподіл портів
VLAN16	16	Fa0/5-Fa0/9
VLAN26	26	Fa0/10-Fa0/14
VLAN36	36	Fa0/15-Fa0/24

У таблиці 3.9 наведено адресацію портів пристроїв у мережі LAN5.

Таблиця 3.9 – Адресація портів пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN
Kovalenko_Switch_3	SVI	10.23.36.3	/27	10.23.36.1	99
Kovalenko_Switch_4	SVI	10.23.36.2	/27	10.23.36.1	99
Kovalenko_Switch_5	SVI	10.23.36.6	/27	10.23.36.1	99
Kovalenko_Switch_16	SVI	10.23.36.4	/27	10.23.36.1	99
Kovalenko_Switch_17	SVI	10.23.36.5	/27	10.23.36.1	99
Kovalenko_Switch_18	SVI	10.23.36.7	/27	10.23.36.1	99
Kovalenko_Router_0	G0/1.16	10.23.36.65	/27	-	16
	G0/1.26	10.23.36.33	/27	-	26
	G0/1.36	10.23.36.1	/27	-	36
	G0/1.99	10.23.36.97	/28	-	99

Виконаємо налаштування VLAN на комутаторах

Виберемо діпазон портів:

int range fa0/15-24

Налаштуємо режим access:

switchport mode access

Призначимо VLAN36 на порті:

switchport access vlan 36

Повторимо налаштування для VLAN26 та VLAN16:

int range fa0/10-14

switchport mode access

switchport access vlan 26

int range fa0/5-9

switchport mode access

switchport access vlan 16

Налаштуємо режим trunk для портів:

int range fa0/11-12

switchport mode trunk

Призначимо native vlan:

switchport trunk native vlan 100

Встановимо VLAN яким дозволено передавати трафік через trunk канал:

switchport trunk allowed vlan 36,26,16,99-100

Перевіримо розподіл портів за допомогою команди show vlan (рисунок 3.9)

```
show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Gig0/1, Gig0/2
16   VLAN0016                         active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9
26   VLAN0026                         active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14
36   VLAN0036                         active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.9 – Призначені vlan інтерфейсам комутатора

Налаштуємо суб інтерфейс на маршрутизаторі:

Створення суб інтерфейсу:

Int g0/1.16

Encapsulation dot1Q 16

Призначення адреси:

Ip address 10.23.36.65 255.255.255.224

Int g0/1.26

Encapsulation dot1Q 26

Ip address 10.23.36.33 255.255.255.224

Int g0/1.36

Encapsulation dot1Q 36

Ip address 10.23.36.1 255.255.255.224

Int g0/1.99

Encapsulation dot1Q 99

Ip address 10.23.36.97 255.255.255.240

3.5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

В мережах VLAN адресація вузлів повинна виконуватися за допомогою динамічного розподілення адрес за протоколом DHCP. Налаштуємо маршрутизатор у якості DHCP серверу:

Виключимо перші 5 адрес призначених для мережевого обладнання:

Ip dhcp excluded-address 10.23.36.1 10.23.36.5

Створимо пул:

Ip dhcp pool VLAN-36

Призначемо мережу:

Network 10.23.36.0 255.255.255.224

Призначимо шлюз за замовчування:

Default-router 10.23.36.1

Та DNS сервер:

Dns-server 10.23.36.143

Проведемо аналогічні налаштування та створимо пул VLAN-16 та VLAN-26.

Перевіримо роботу протоколу DHCP(рисунок 3.10).

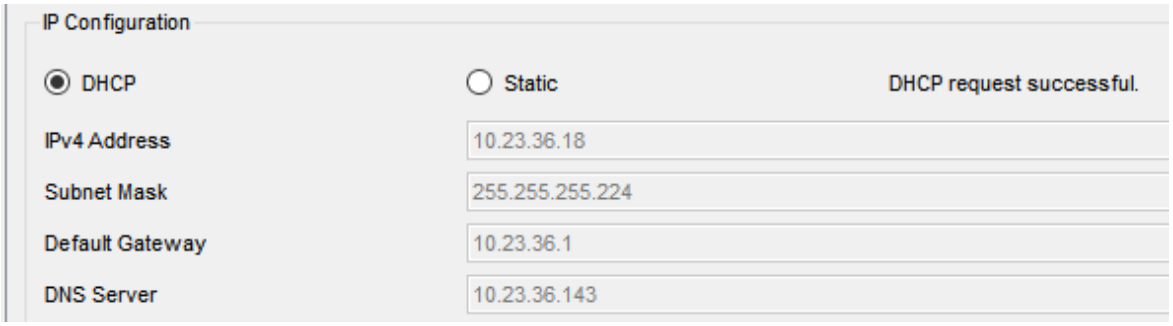

Рисунок 3.10 – Отримання адреси за протоколом DHCP

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента системи

IoT (Internet of Things) означає "Інтернет речей" і відноситься до концепції, в якій фізичні об'єкти, такі як пристрої, сенсори та інші "речі", з'єднані між собою та з Інтернетом, щоб обмінюватися даними та взаємодіяти один з одним. Ідея полягає в тому, що ці речі мають вбудовану електроніку, сенсори, програмне забезпечення та здатність передавати та отримувати дані через мережу Інтернет. За допомогою IoT, різні фізичні об'єкти можуть бути підключені до мережі та взаємодіяти між собою та з людьми.

Згідно вимог замовника, необхідно впровадити IoT-систему безпеки офісу яка буде спостерігати та контролювати бюро перекладів «InText».

Система складається з наступних пристроїв: камери спостереження, датчики вогню, сирени та RFID зчитувачі з електронними картками для дверей. Також додано термостат, кондиціонер та батарею для контролювання температури в приміщенні.

Необхідні функції виконувані системою:

- При спрацюванні невідомої картки, вмикається сирена та відеокамери.
- При спрацюванні датчика вогню повина вмикатися сирена.
- Двері повинні відкриватися тільки з ідентифікованими RFID картками доступу
- Сирена вимикається після повернення всіх показників у норму
- Підтримка діапазону температур від 22°C до 26 °C

Зв'язок між реалізовано за допомогою HomeGateway, який виконую роль серверу Інтернету речей. Всі пристрої підключаються за допомогою Wi-fi стандарту IEEE 802.11.

4.2 Налаштування обладнання та сервісів системи IoT

Для розміщення та підключення пристроїв будемо використовувати середовище Cisco Packet Tracer. Розташуємо необхідне обладнання та підключемо його до HomeGateway. Створимо мережу SSID 123191_Kovalenko з

протоколом безпеки WPA2-PSK та паролем Cisco123. Топологічну схему КМ з розміщеними пристроями IoT показано на рисунку 4.1

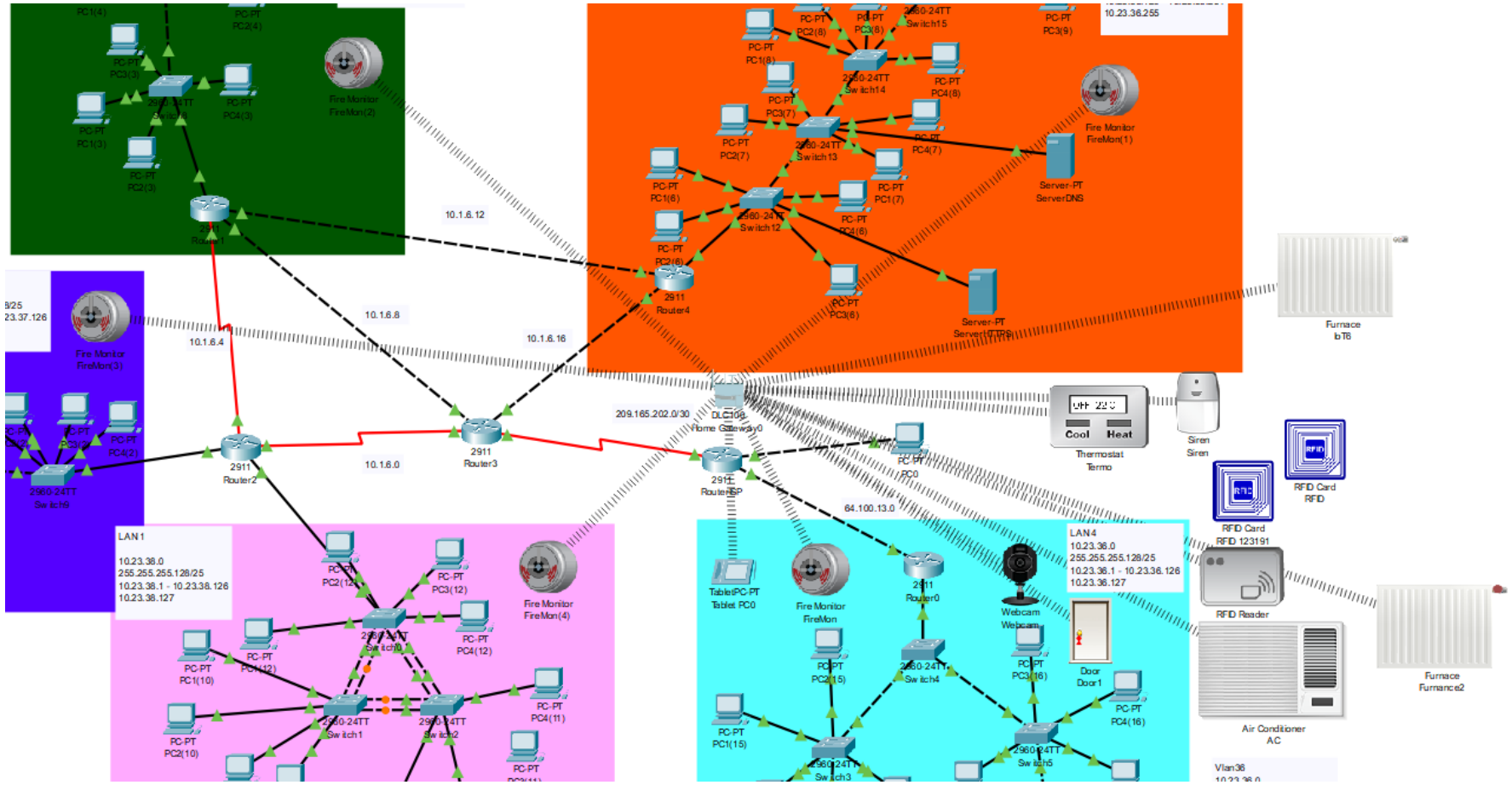

Рисунок 4.1 – Топологічна схема КМ бюро перекладів «InText» з IoT системою безпеки

У процесі налаштування IoT системи використовувся планшет який був підключен до тієї ж мережі що і інші пристрої.

Необхідно на всіх пристроях ввімкнути динамічне отримання адрес, а також обрати HomeGateway як IoT сервер (рисунок 4.2).

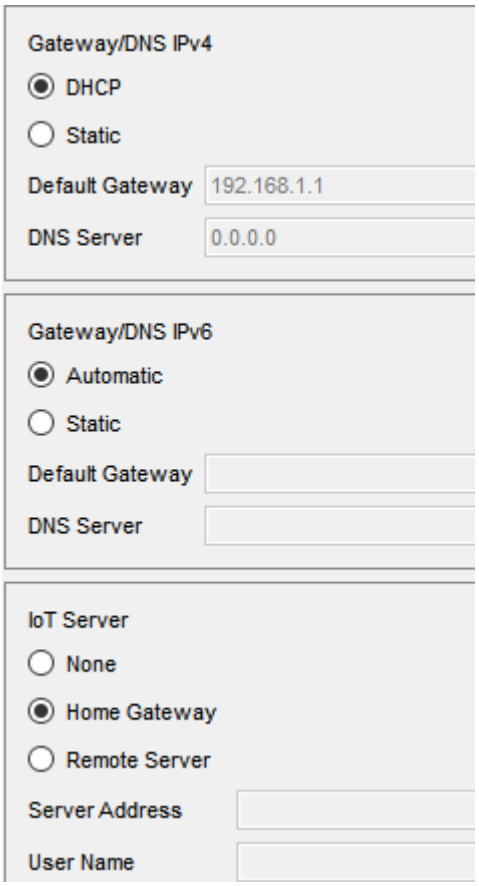

Рисунок 4.2 – Конфігурація усіх пристроїв

Після налаштування усіх пристроїв їх перелік можливо побачити на головній сторінці IoT монитора на планшеті. Перелік усіх пристроїв показано на рисунку 4.3.

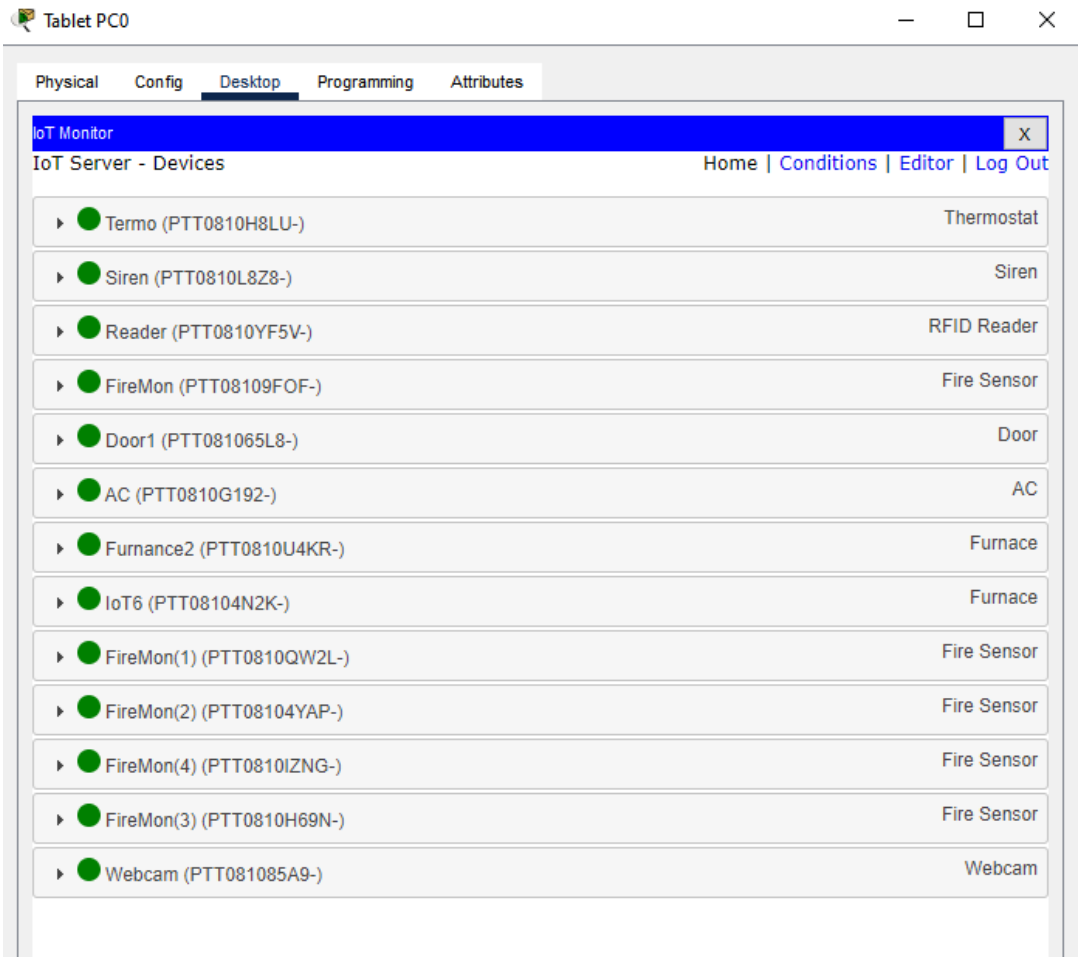

Рисунок 4.3 – Перелік усіх пристроїв

Виконаємо налаштування роботи сирени та камер під час активації дверей невідомою RFID карткою (рисунок 4.4).

Рисунок 4.4 – Сценарій для спрацювння сирени та камери

Далі налаштуємо спрацювання сирени та відмикання дверей від спрацювання датчику вогню (рисунок 4.5).

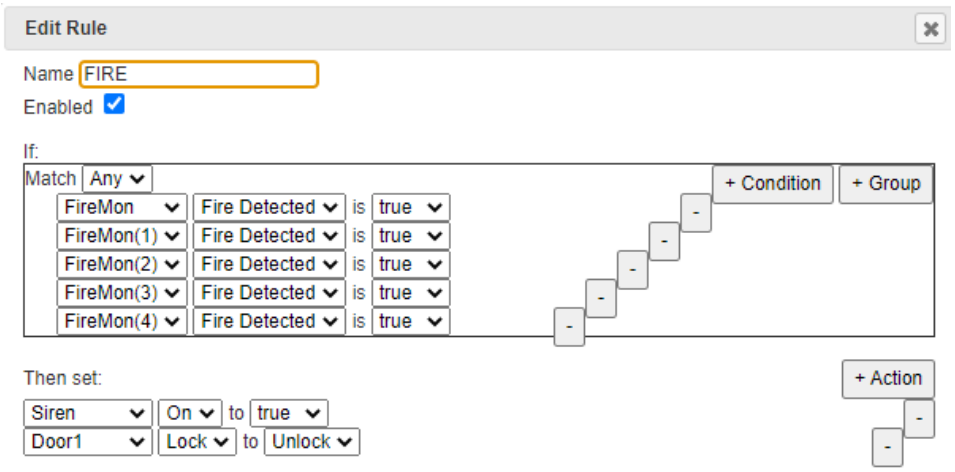

Рисунок 4.5 – Сценарій для спрацювання датчика вогню

Наступним кроком налаштуємо відмикання та замикання дверей RFID карткою доступу (рисунок 4.6-7).

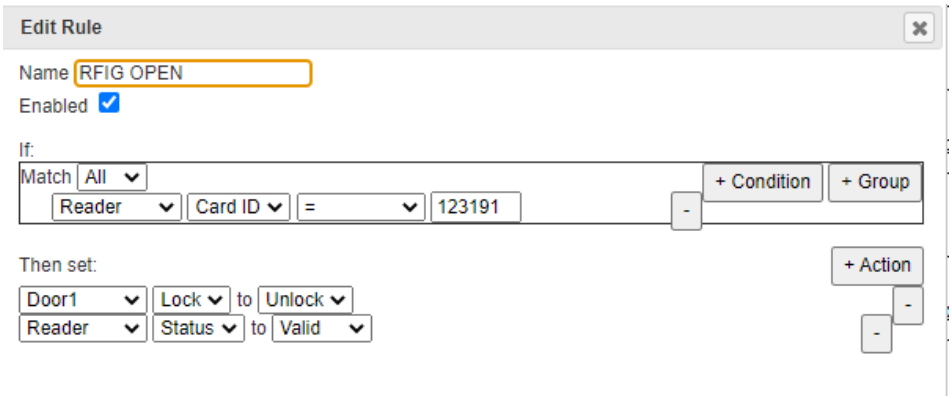

Рисунок 4.6 – Сценарій для відмикання дверей

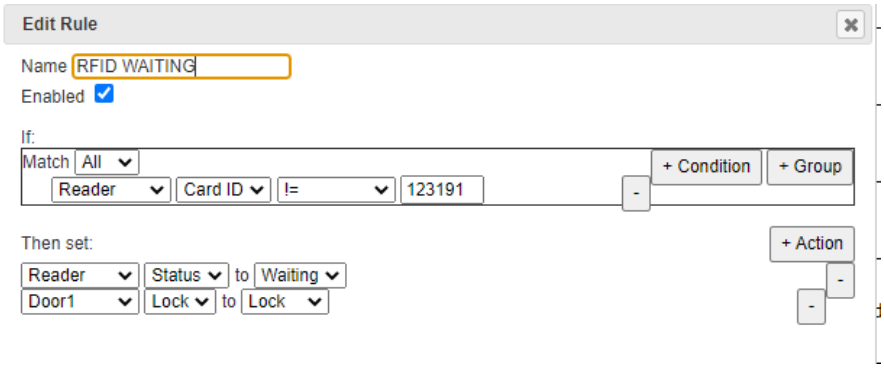

Рисунок 4.7 – Сценарій для замикання дверей у режимі очікування

Налаштуємо вимикання камери та сирени у режимі очікування (рисунок 4.8)

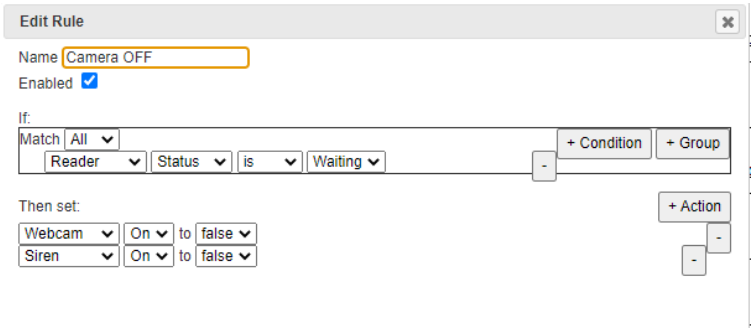

Рисунок 4.8 – Сценарій для вимикання камери та сирени у режимі очікування

Також налаштуємо роботу системи підтримки температури у діапазоні від 22°C до 26°C.

Налаштуємо ввімкнення кондиціонеру за умови температури вище 26°C (рисунок 4.9). Також налаштуємо вимкнення кондиціонеру після охолодження офісу до 24°C (рисунок 4.10).

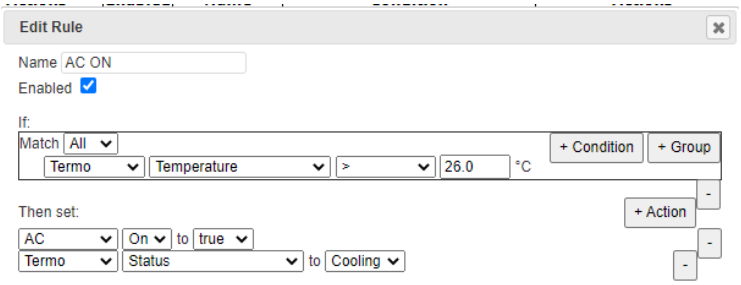

Рисунок 4.9 – Сценарій для ввімкнення кондиціонера

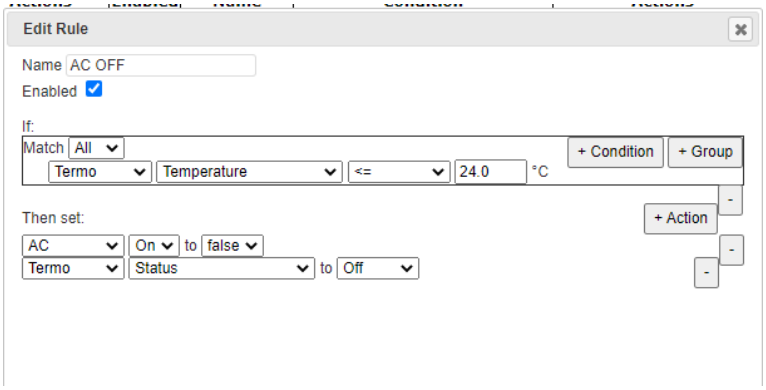

Рисунок 4.10 – Сценарій для вимкнення кондиціонера

Налаштуємо ввімкнення обігрівача за умови температури нижче 22°C (рисунок 4.11). Також налаштуємо вимкнення кондиціонеру після обігріву офісу до 22°C (рисунок 4.12).

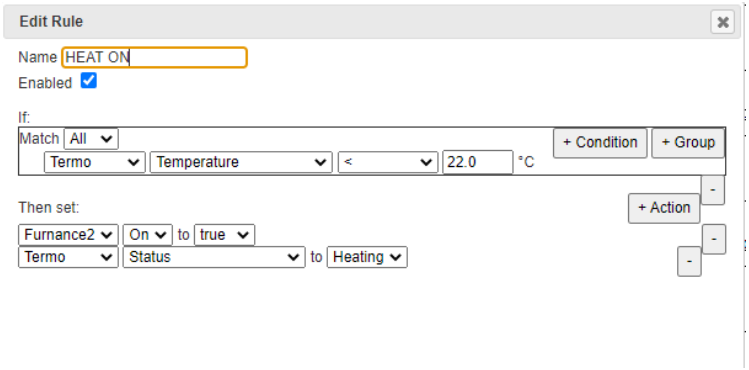

Рисунок 4.11 – Сценарій для ввімкнення обігрівача

Рисунок 4.12 – Сценарій для вимкнення обігрівача

Повний перелік усіх налаштованих та створених сценаріїв наведено на рисунку 4.13.

IoT Monitor

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	RFIG OPEN	Reader Card ID = 123191	Set Door1 Lock to Unlock Set Reader Status to Valid
Edit Remove	Yes	AC ON	Termo Temperature > 26.0 °C	Set AC On to true Set Termo Status to Cooling
Edit Remove	Yes	AC OFF	Termo Temperature <= 24.0 °C	Set AC On to false Set Termo Status to Off
Edit Remove	Yes	HEAT ON	Termo Temperature < 22.0 °C	Set Furnance2 On to true Set Termo Status to Heating
Edit Remove	Yes	HEAT OFF	Termo Temperature >= 22.0 °C	Set Furnance2 On to false Set Termo Status to Off
Edit Remove	Yes	HEAT TEST	Termo Temperature < 30.0 °C	Set IoT6 On to false
Edit Remove	Yes	Camera OFF	Reader Status is Waiting	Set Webcam On to false Set Siren On to false
Edit Remove	Yes	SIREN	Reader Status is Invalid	Set Webcam On to true Set Siren On to true
Edit Remove	Yes	RFID INVALID	Match all: • Reader Card ID != 123191 • Reader Card ID != 0	Set Reader Status to Invalid
Edit Remove	Yes	RFID WAITING	Reader Card ID != 123191	Set Reader Status to Waiting Set Door1 Lock to Lock
Edit Remove	Yes	FIRE	Match any: • FireMon Fire Detected is true • FireMon(1) Fire Detected is true • FireMon(2) Fire Detected is true • FireMon(3) Fire Detected is true • FireMon(4) Fire Detected is true	Set Siren On to true Set Door1 Lock to Unlock

Рисунок 4.13 – Перелік сценаріїв на сервері HomeGateway

Висновки

У цій кваліфікаційній роботі були розглянуті основні аспекти побудови, налаштування та безпеки комп'ютерної системи бюро перекладів компанії "InText". Здійснено аналіз технологій, архітектури мережі та розгортання комп'ютерних ресурсів, що дозволило визначити оптимальні рішення для компанії. Моделювання мережі було здійснено у середовищі Cisco Packet Tracer.

У процесі проектування було налаштовано здійснено налаштування всіх необхідних параметрів мережевого обладнання. Було налаштовано динамічну маршрутизацію за протоколом OSPF, застосовано динамічне призначення IP адрес за допомогою протоколу DHCP. Доступ до Інтернету було забезпечено за допомогою динамічного NAT. Також було застосовано VPN з'єднання для забезпечення захищеного зв'язку між головною мережею та віддаленою, а також налаштовано ACL списки. У віддаленій мережі було використано технологію VLAN. В одній з головних мереж за допомогою технології EtherChannel було налаштовано об'єднання фізичних ліній комутаторів за для підвищення стабільності та швидкості роботи мережі. Також було розроблено та реалізовано безпеку офісу з використанням IoT.

Усе налаштування та проектування системи було виконано згідно до вимог та теми кваліфікаційної роботи. Під час виконання кваліфікаційної роботи всі цілі роботи було виконано. Кваліфікаційна робота виконана та оформлена згідно всіх стандартів та методичних вказівок.

Перелік посилань

1. Бюро перекладів InText – [Електронний ресурс] – https://intext.eu/
2. Інтернет-магазин Hotline – [Електронний ресурс] – https://hotline.ua/
3. Налаштування мережі VPN – [Електронний ресурс] – https://cisco.nitaet.com/ccna-4-cn-u/course/module7/7.1.2.4/7.1.2.4.html
4. ISO 17100:2015 “Вимоги до основних процесів, ресурсів та інших аспектів, необхідних для надання якісних послуг перекладу, які відповідають специфікаціям.”
5. ISO/IEC 27001: “Системи менеджменту інформаційної безпеки”
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

Схема загальної архітектури мережі підприємства

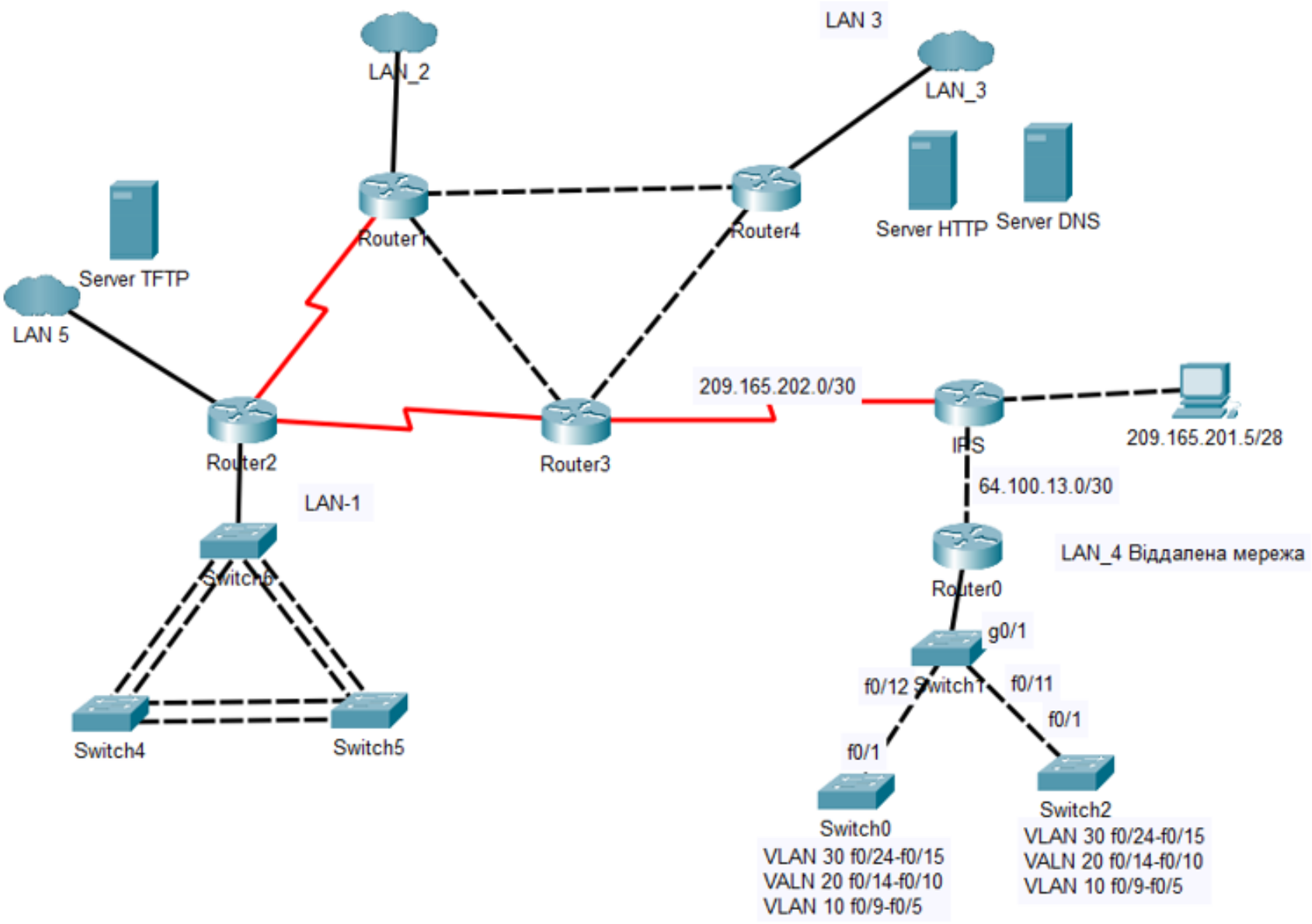

Рисунок А.1 – Схема загальної архітектури мережі підприємства

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
804.02070743.23006-01 12 01
Листів 12

2023

АНОТАЦІЯ

Даний документ містить ПЗ налаштувань маршрутизаторів Cisco для структурної схеми моделі комп’ютерної системи.

Тексти програм реалізовані на мові конфігураційних скриптів для мережного обладнання Cisco.

Середовище розробки та налагодження скриптів – пакет моделювання мереж «Cisco Packet Tracer» версії 8.2.1 в середовищі операційної системи Windows 10 Pro.

ЗМІСТ

1. Скрипт налаштування Router3

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Kovalenko_Router_3 // Зміна назви маршрутизатора
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1 //зашифрований пароль до привілейованого режиму
!
aaa new-model //увімкнення служби AAA
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
no ip cef
no ipv6 cef
!
username 123191_Kovalenko password 7 082048430017061E010803
username Kovalenko_Router_3 password 7 082048430017544541 //налаштування логіну та паролю у локальній базі даних AAA
!
license udi pid CISCO2911/K9 sn FTX1524885M-
license boot module c2900 technology-package securityk9 //Увімкнення модулю безпеки securityk9
!
crypto isakmp policy 10 //створення криптографічної політики
encr 3des //вибір алгоритму шифрування
hash md5 //вибір алгоритму створення геш-суми
authentication pre-share //вибір методу автентифікації пірів
group 2
!
crypto isakmp key cisco address 64.100.13.2 //створення ключа для взаємодії з обраним партнером
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp //створення криптографічного зіставлення
set peer 64.100.13.2
set transform-set TS
match address VPN6
!
ip domain-name Kovalenko_Router_3 //визначення доменного ім’я маршрутизатора
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0 //налаштування портів
ip address 10.1.6.17 255.255.255.252
ip nat inside //визначення напрямку роботи NAT
```

```
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.1.6.9 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 10.1.6.1 255.255.255.252
ip nat inside
!
interface Serial0/3/1
ip address 209.165.202.1 255.255.255.252
ip nat outside
crypto map MAP
!
interface Vlan1
no ip address
shutdown
!
router ospf 1 //увімкнення протоколу маршрутизації OSPF
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
network 10.1.16.0 0.0.0.3 area 0
network 10.1.16.16 0.0.0.3 area 0
network 10.1.16.8 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
network 10.1.6.0 0.0.0.3 area 0
network 10.1.6.16 0.0.0.3 area 0
network 10.1.6.4 0.0.0.3 area 0
network 10.1.6.8 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 //створення пулу
адрес для NAT
ip nat inside source list NAT6 pool Internet
ip nat inside source static 10.23.36.144 209.165.200.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
```

```
ip route 209.165.201.0 255.255.255.240 209.165.202.2
ip route 209.165.202.0 255.255.255.252 Serial0/3/1
!
ip flow-export version 9
!
!
ip access-list extended VPN6 //створення списку доступу VPN6
permit ip 10.23.38.0 0.0.0.127 10.23.36.0 0.0.0.127
permit ip 10.23.37.128 0.0.0.127 10.23.36.0 0.0.0.127
permit ip 10.23.36.128 0.0.0.127 10.23.36.0 0.0.0.127
permit ip 10.23.37.0 0.0.0.127 10.23.36.0 0.0.0.127
permit ip 10.1.6.0 0.0.0.255 10.23.36.0 0.0.0.127
ip access-list extended NAT6
deny ip 10.23.38.0 0.0.0.127 10.23.36.0 0.0.0.127
deny ip 10.23.37.128 0.0.0.127 10.23.36.0 0.0.0.127
deny ip 10.23.36.128 0.0.0.127 10.23.36.0 0.0.0.127
deny ip 10.23.37.0 0.0.0.127 10.23.36.0 0.0.0.127
deny ip 10.1.6.0 0.0.0.255 10.23.36.0 0.0.0.127
permit ip 10.23.38.0 0.0.0.127 any
permit ip 10.23.37.128 0.0.0.127 any
permit ip 10.23.36.128 0.0.0.127 any
permit ip 10.23.37.0 0.0.0.127 any
permit ip 10.1.6.0 0.0.0.255 any
!
banner motd ^CKovalenko_Router_3^C //створення банеру MOTD
!
radius server 10.1.6.17
address ipv4 10.1.6.17 auth-port 1645
key radius123
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16 //встановлення паролю для ліній vty
login authentication default
transport input ssh //увімкнення доступу до консолі через 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 Kovalenko_Router_0
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip dhcp excluded-address 10.23.36.1 10.23.36.10 //виключення IP адрес з DHCP
ip dhcp excluded-address 10.23.36.1 10.23.36.5
ip dhcp excluded-address 10.23.36.33 10.23.36.38
ip dhcp excluded-address 10.23.36.65 10.23.36.70
!
ip dhcp pool VLAN-36 //створення DHCP пулу для VLAN-36
network 10.23.36.0 255.255.255.224
default-router 10.23.36.1
dns-server 10.23.36.143
ip dhcp pool VLAN-26//створення DHCP пулу дляVLAN-26
network 10.23.36.32 255.255.255.224
default-router 10.23.36.33
dns-server 10.23.36.143
ip dhcp pool VLAN-16//створення DHCP пулу для VLAN-16
network 10.23.36.64 255.255.255.224
default-router 10.23.36.65
dns-server 10.23.36.143
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
ip cef
no ipv6 cef
!
username 123191_Kovalenko password 7 082048430017061E010803
username Kovalenko_Router_0 password 7 082048430017544541
!
license udi pid CISCO2911/K9 sn FTX152424RJ-
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 209.165.202.1
!
```

```
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 209.165.202.1
set transform-set TS
match address VPN6
!
ip domain-name Kovalenko_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
no ip address
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1.16 //налаштування суб інтерфейсів
encapsulation dot1Q 16
ip address 10.23.36.65 255.255.255.224
ip nat inside
!
interface GigabitEthernet0/1.26
encapsulation dot1Q 26
ip address 10.23.36.33 255.255.255.224
ip nat inside
!
interface GigabitEthernet0/1.36
encapsulation dot1Q 36
ip address 10.23.36.1 255.255.255.224
ip nat inside
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 10.23.36.97 255.255.255.240
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
```

```
interface Vlan1
no ip address
shutdown
!
ip nat pool Internet 209.165.203.5 209.165.203.30 netmask 255.255.255.224
ip nat inside source list NAT6 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 flow-export version 9
!
ip access-list extended VPN6
permit ip 10.23.36.0 0.0.0.127 10.23.38.0 0.0.0.127
permit ip 10.23.36.0 0.0.0.127 10.23.37.128 0.0.0.127
permit ip 10.23.36.0 0.0.0.127 10.23.36.128 0.0.0.127
permit ip 10.23.36.0 0.0.0.127 10.23.37.0 0.0.0.127
permit ip 10.23.36.0 0.0.0.127 10.1.6.0 0.0.0.255
ip access-list extended NAT6
deny ip 10.23.36.0 0.0.0.127 10.23.38.0 0.0.0.127
deny ip 10.23.36.0 0.0.0.127 10.23.37.128 0.0.0.127
deny ip 10.23.36.0 0.0.0.127 10.23.36.128 0.0.0.127
deny ip 10.23.36.0 0.0.0.127 10.23.37.0 0.0.0.127
deny ip 10.23.36.0 0.0.0.127 10.1.6.0 0.0.0.255
permit ip 10.23.36.0 0.0.0.127 any
!
banner motd ^CKovalenko_Router_0^C
!
radius server 64.100.13.2
address ipv4 64.100.13.2 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
```

3. Скрипт налаштування Switch3:

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Kovalenko_Switch_3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip domain-name Kovalenko_Switch_3
!
username 123191_Kovalenko privilege 1 password 7 082048430017061E010803
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1 //налаштування портів комутатора
switchport trunk native vlan 100
switchport trunk allowed vlan 16,26,36,99-100 //налаштування доступу між VLAN
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport trunk allowed vlan 16,26,36,99-100
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 100
switchport trunk allowed vlan 16,26,36,99-100
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 100
switchport trunk allowed vlan 16,26,36,99-100
switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 16
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 16
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 16
switchport mode access
!
interface FastEthernet0/8
```

```
switchport access vlan 16
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 16
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 26
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 26
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 26
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 26
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 26
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 36
switchport mode access
```

```
!
interface FastEthernet0/21
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 36
switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 10.23.36.3 255.255.255.128 //налаштування SVI-адреси комутатора
!
ip default-gateway 10.23.36.1
!
banner motd ^CKovalenko_Switch_3^C
!
line con 0
password 7 0822455D0A16
login
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
!
end
```