Міністерство освіті 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 Нечепоренка Романа Геннадійовича
(ПІБ)

академічної групи 123-20-2
(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 ІТ-компанії ТОВ "ІНФОТЕХ" м. Київ 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. Шедловський І.А.			
спеціальної частини	доц. Шедловський І.А.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"15" квітня 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Нечепоренка Р. Г. **академічної групи** 123-20-2
спеціальності 123 «Комп'ютерна інженерія»
за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
на тему "Комп'ютерна система ІТ-компанії ТОВ "ІНФОТЕХ" м. Київ з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"
затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	**Зміст**	**Термін виконання**
Стан питання і постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2024
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2024
Розробка корпоративної мереж	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2024
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2024

Завдання видано _____ доц. Шедловський І.А.
(підпис керівника) (прізвище, ініціали)

Дата видачі 15.04.2024
Дата подання до екзаменаційної комісії 14.06.2024
Прийнято до виконання _____ Нечепоренко Р.Г.

РЕФЕРАТ

Пояснювальна записка: 71 с., 50 рис., 10 табл., 10 джерел, 1 додаток.

КОМП'ЮТЕРНА СИСТЕМА, МЕРЕЖА, ПІДПРИЄМСТВО, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, МОДЕЛЬ, БЕЗПЕКА, СЕРВІСИ.

Об'єкт розробки: корпоративна мережа, що забезпечує функціонування підприємства ТОВ “ІНФОТЕХ”.

Мета: створення комп'ютерної системи для підприємства із застосуванням сучасних технологій та комп'ютерних мереж.

Розроблені технічні вимоги для корпоративної мережі та інформаційної системи підприємства.

Виконано аналіз сучасного мережеві технологій, на основі якого було підібрано технічні засоби комп'ютерної мережі.

Розроблено схему адресації пристроїв інформаційної системи та виконано налаштування мережевих сервісів та засобів безпеки.

Виконано моделювання комп'ютерної мережі у середовищі Cisco Packet Tracer, де, за допомогою симуляції, було підтверджено коректність розрахунків та працездатність мережі.

Робота виконано згідно до вимог і завдання.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІТ - інформаційні технології;

ТОВ - товариство з обмеженою відповідальністю;

ПЗ - програмне забезпечення;

ТЗ - технічні засоби;

ЛОМ - локальна обчислювальна мережа;

АРМ - автоматизоване робоче місце;

ЦОД - центр обробки даних;

ПК - персональний комп’ютер;

ОС - операційна система;

ДБЖ - джерело безперебійного живлення;

КС - комп’ютерна система;

ВСТУП

Товариство з обмеженою відповідальністю «Інфотех» є компанією з надання послуг в ІТ-сфері.

У Європі та Україні спостерігається стрімкий розвиток індустрії ІТ-послуг. Європейські країни активно інвестують у технологічні стартапи та дослідження, що сприяє створенню нових інновацій та ринкових можливостей.

Україна, з своєю висококваліфікованою робочою силою та конкурентоспроможними цінами на послуги, стала ключовим гравцем у сфері ІТ. Компанії, як «Інфотех», є прикладом успішної української ініціативи, яка допомагає формувати нову картину розвитку технологій в регіоні.

«Інфотех» знаходиться у стадії стрімкого розвитку, нещодавно залучивши фінансування від інвесторів.

Компанія спеціалізується у наданні ІТ-послуг, а зокрема:

– Розробка програмного забезпечення: компанія «Інфотех» вирізняється високоякісною розробкою програмного забезпечення, яке відповідає конкретним потребам клієнтів. Завдяки команді досвідчених розробників, вони вивчають та аналізують вимоги проекту, вибирають оптимальні технології та створюють продукти, які відзначаються високою ефективністю, надійністю та масштабованістю.
– Інтеграція технологій: «Інфотех» роботу з інтеграції технологій, допомагаючи підприємствам оптимально використовувати сучасні інновації у своїх бізнес-процесах. Це включає в себе злагоджену роботу з різними технологічними рішеннями та їх інтеграцію в єдину, підтримувану і ефективну бізнес-екосистему.
– Консалтинг та стратегічна підтримка: компанія надає консультативні послуги з ІТ-стратегій, допомагаючи клієнтам визначити та реалізувати їхні корпоративні цілі в контексті інформаційних технологій. Це включає в себе аналіз бізнес-процесів, розробку

стратегій цифрової трансформації та впровадження оптимальних IT-рішень.

- Кібербезпека та захист даних: безпека є пріоритетом для «Інфотех» Компанія розробляє та впроваджує комплексні заходи з кібербезпеки для захисту інформації та даних клієнтів. Це включає в себе моніторинг, виявлення та реагування на потенційні загрози, а також регулярне оновлення систем безпеки.
- Технічна підтримка та обслуговування: компанія забезпечує технічну підтримку та обслуговування розроблених інформаційних систем. Це включає в себе регулярне оновлення програмного забезпечення, вирішення технічних проблем, а також надання консультацій та підтримки для оптимальної експлуатації систем.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

На протязі початку 2020-х років ринок IT-послуг свідчив про значущий ріст, відтінюючися активністю та динамічністю. За звітами на той період, глобальний обсяг цього ринку, відповідно до Gartner, перевищив 1,2 трильйона доларів США у 2021 році.

Однією з ключових тенденцій було активне впровадження цифрової трансформації підприємств, що викликало збільшений попит на розробку програмного забезпечення, інтеграцію технологій та аналітичні рішення. Компанії стрімко вкладали в інновації, прагнучи адаптуватися до зростаючих вимог цифрової економіки.

Хмарні технології також відзначилися значним зростанням популярності. Підприємства все частіше обирали облачні рішення для зберігання та обробки даних, що сприяло зростанню обсягу послуг у цьому напрямку. Безпека даних та захист від кіберзагроз стали однією з ключових пріоритетних областей. Збільшений попит на послуги кібербезпеки відображав важливість встановлення ефективних заходів безпеки та захисту важливих інформаційних ресурсів.

Новаторські технології, такі як штучний інтелект, продовжували інтегруватися в бізнес-процеси. Впровадження інтелектуальних рішень дозволяло підприємствам автоматизувати процеси та отримувати цінні інсайти з великих обсягів даних.

У Європі спостерігався стійкий попит на IT-послуги, особливо у контексті цифрової трансформації та змін в бізнес-моделях. Декілька країн, таких як Німеччина, Велика Британія, та Франція, визначались високим рівнем інвестицій у технології. Обсяг ринку IT-послуг у Європі досягав значущих масштабів, враховуючи ростові тенденції у сфері розробки програмного забезпечення, кібербезпеки та хмарних технологій.

Україна зберігала свою позицію серед провідних країн у сфері IT-аутсорсингу. За рахунок висококваліфікованої робочої сили та конкурентних цін, українські IT-компанії залучали велику кількість проектів з Заходу.

Розробка програмного забезпечення, тестування, технічна підтримка, та аутсорсинг IT-інфраструктури входять в основні напрями діяльності.

Європейські та українські компанії активно взаємодіяли у сфері IT-послуг, забезпечуючи ефективне та інноваційне впровадження технологій. Тренди розвитку цих ринків визначається такими факторами, як цифрова трансформація, кібербезпека, інтеграція новітніх технологій, та постійний попит на високофахові IT-послуги.

1.1 Сфера та умови застосування комп'ютерної системи

У кваліфікаційній роботі головним суб'єктом виступає компанія «Інфотех», що спеціалізується у наданні IT-послуг на українському та європейських ринках.

Основним напрямком роботи підприємства є розробка WEB-застосунків та іншого прикладного ПЗ на замовлення, тобто аутсорсинг. Також компанія займається консалтингом у сфері хмарних рішень.

Аутсорсинг (англ. outsourcing) - це процес залучення сторонніх компаній з метою передачі їм відповідальності за розробку програмного забезпечення. Це дозволяє компаніям-замовникам отримувати доступ до глибоких знань та експертизи висококваліфікованих фахівців без необхідності формувати великі внутрішні команди. Це дозволяє суттєво зменшити витрати на заробітну плату та інфраструктуру, одночасно забезпечуючи високий рівень технічної компетентності.

Іншою перевагою аутсорсингу є гнучкість - підприємства можуть миттєво масштабувати або зменшувати обсяги робіт в залежності від потреб та етапів проекту, що надає їм можливість більш точно реагувати на зміни в ринкових умовах.

Крім того, аутсорсинг розробки ПЗ розширює географію доступних талантів. Компанії можуть співпрацювати із експертами з усього світу, використовуючи різноманітні культури та перспективи для збагачення своїх проектів. Це сприяє різноманітності інновацій та сприяє кращим рішенням.

Однак важливо зазначити, що успішний аутсорсинг вимагає ефективного управління комунікаціями та контролю над процесами. Правильно вибрані партнери та встановлені чіткі системи спілкування можуть максимізувати переваги аутсорсингу, роблячи його важливою ланкою в стратегічному розвитку компаній.

1.2 Характеристика і структура об'єкта впровадження

Головний офіс компанії «Інфотех» розташовується у м. Київ за адресою вул. Дегтярівська 15.

На підприємстві знаходяться наступні приміщення:

- Кабінет директора
- Переговорні кімнати
- Зона розробників та тестувальників
- Зона спеціалістів з підтримки клієнтів
- Кімната бухгалтерії
- Серверна кімната
- Санвузол
- Кухня
- Кімната зберігання

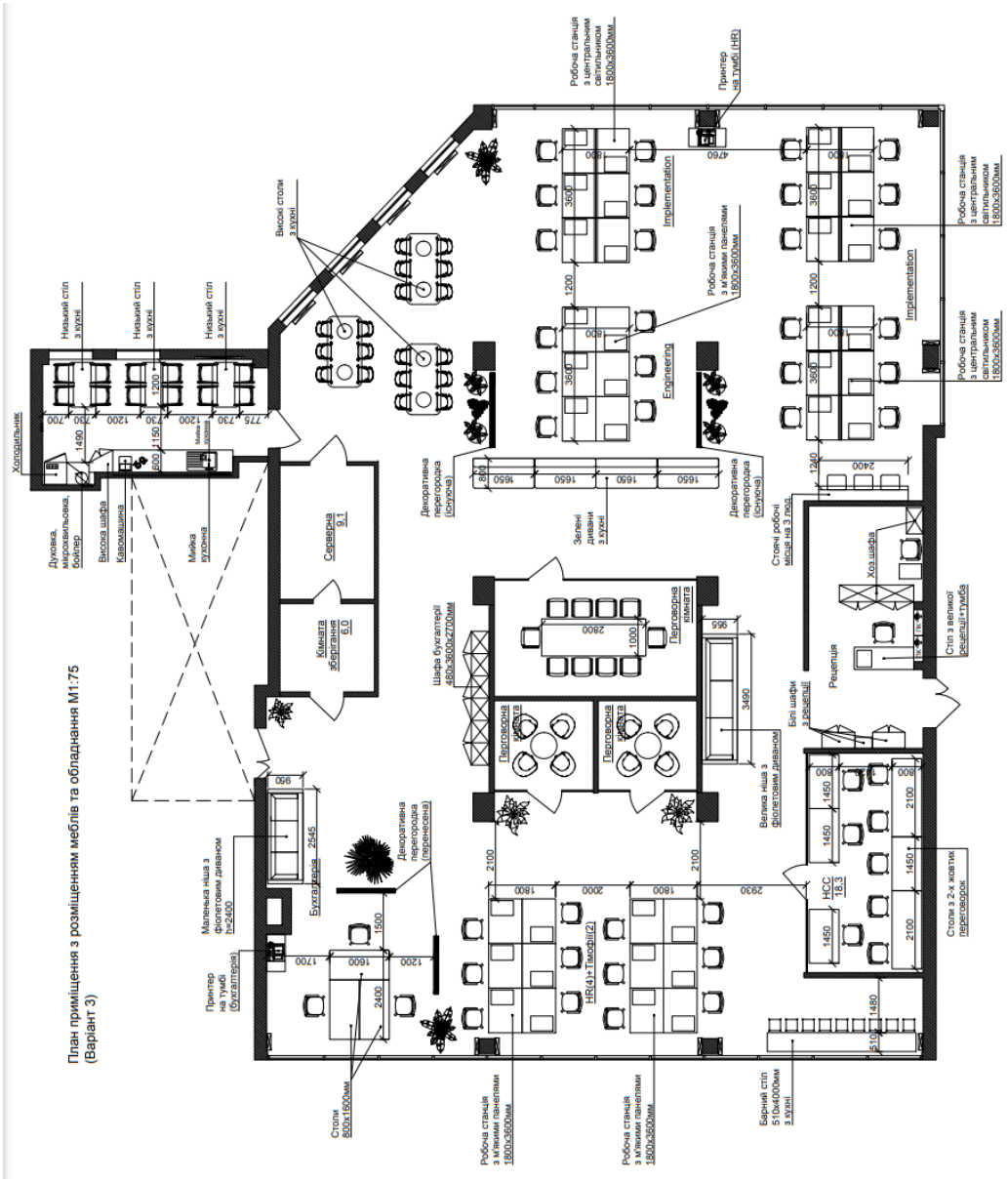

Рисунок 1.1 – План офісного приміщення

1.2.1 Структура і особливості підприємства

Робочий час компанії - з понеділка по п'ятницю з дев'ятої ранку до шостої години вечора, вихідні - субота та неділя.

Формат роботи компанії - робота з офісу. В залежності від навантаження дозволяється робота віддалено, але не більше двох днів на тиждень.

Штат співробітників складається з 80 чоловік:

Таблиця 1.1 – Організаційна структура підприємства

Назва структурного підрозділу	Чисельність
Виконавчий директор (CEO)	1
Керівник відділу розробки (CTO)	1
Розробники ПЗ	25
Тестувальники ПЗ	14
Системні адміністратори	4
Бухгалтери	3
Юристи	5
Менеджери з продажів	12
Спеціалісти з підтримки клієнтів	15

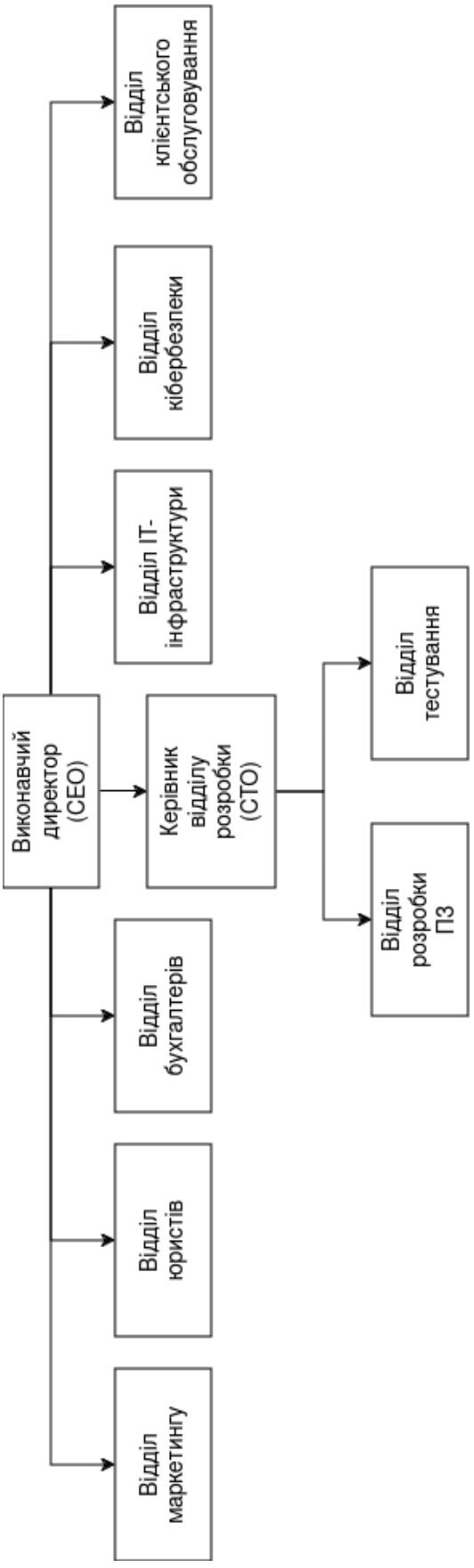

Рисунок 1.2 – Схема організаційної структури підприємства

1.2.2 Технології збору та передачі інформації

Підприємство надає ІТ-послуги клієнтам у різних сферах діяльності, що потребує надійного зберігання та захисту клієнтських даних. Штат співробітників поділений на ряд чітко структурованих відділів з різними обов'язками та задачами, тому не менш важливим фактором є право доступу до різних даних підприємства.

Основна частина даних зберігається на серверах підприємства в електронному вигляді. Документи, які цього потребують (договори, бухгалтерська звітність тощо), можуть додатково зберігатись у паперовому вигляді у спеціально виділених для цього приміщеннях: кімната директора, кімната бухгалтерії, переговорні кімнати тощо.

Таблиця 1.2 – Визначення доступу до інформації

Тип даних	Формат зберігання	Особи, що мають доступ	Де зберігається
1	2	3	4
Інформація про підприємство, кількість робітників та систему оплати праці	Паперовий, в електронному вигляді	Директор, юристи, бухгалтерія	Кабінет директора, сервери підприємства
Трудові договори	Паперовий, в електронному вигляді	Директор, юристи, бухгалтерія	Кабінет директора, сервери підприємства
Бухгалтерська звітність	Паперовий, в електронному вигляді	Директор, юристи, бухгалтерія	Бухгалтерія, сервери підприємства
Договори з клієнтами	Паперовий, в електронному вигляді	Директор, юристи, бухгалтерія	Кабінет директора, сервери підприємства

База даних клієнтів	Паперовий, в електронному вигляді	Директор, юристи, бухгалтерія, відділ продажів	Кабінет директора, сервери підприємства
Проекти замовників	В електронному вигляді	Директор, Технічний директор (CTO), менеджери проектів, розробники, тестувальники, замовник	Сервери підприємства
Документація комп'ютерної мережі	Паперовий, в електронному вигляді	Директор, системні адміністратори, спеціалісти з кібербезпеки	Серверна, сервери підприємства
Вихідний код	В електронному вигляді	Технічний директор (CTO), розробники, тестувальники	Сервери підприємства

У компанії «Інфотех» інформація передається різними шляхами, що відповідають її структурі та функціональним потребам. Співробітники різних відділів зазвичай використовують електронну пошту для офіційного спілкування та звернень, а також Slack для швидкого обговорення проекту та розв'язання питань в реальному часі. Також у компанії використовується PM-система Notion для планування завдань та відстеження їх виконання, і для координування робочого процесу в цілому.

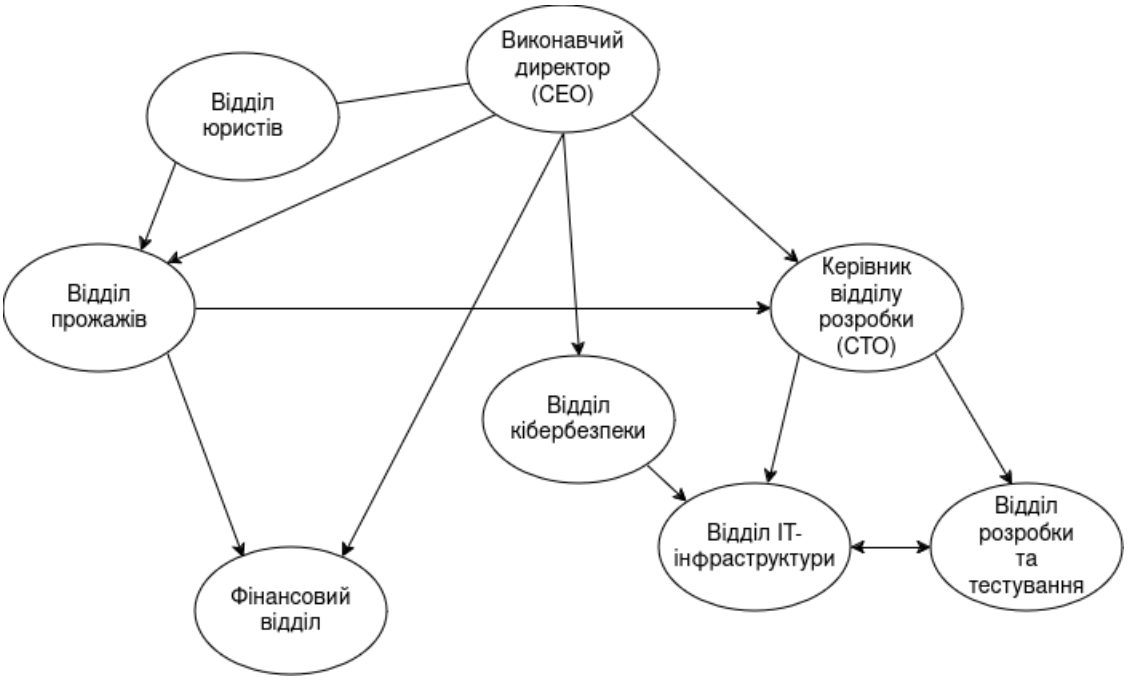

Рисунок 1.3 – Основні напрямки комунікації у компанії

Основною діяльністю компанії є надання послуг з розробки ПЗ та консультацій щодо хмарних рішень. Кожному співробітнику виділяється власне робоче місце, що включає в себе ПК з встановленим ПЗ необхідним для виконання поставлених задач. У роботі компанії використовується ряд прикладних програм, як з відкритим кодом і дозволом на вільне використання, так і ПЗ з комерційними ліцензіями.

Таблиця 1.3 – Використовуване програмне забезпечення

Назва та версія	Де встановлено	Тип ліцензії
1	2	3
GNU/Linux Ubuntu 22.04 (Caddy, OpenSSH, PostgreSQL)	Web-сервер, DNS-Server	GNU GPL
GNU/Linux Ubuntu 22.04 (ATFTP)	TFTP-сервер	GNU GPL
Fedora Workstation 39	ПК1-46	MIT
Mozilla Firefox v120	ПК1-46	MPL v2.0

Mozilla Thunderbird v115	ПК1-46	MPL v2.0
LibreOffice 7.6	ПК1-46	MPL v2.0
GCC, Python 3.11	ПК1-31	GNU GPL, PSF
Oracle VirtualBox	ПК1-31	MIT

1.3 Завдання і мета роботи

Мета кваліфікаційної роботи - проектування комп'ютерної мережі підприємства задля забезпечення функціонування комп'ютерної системи в цілому.

За завданням необхідно визначити список апаратного та програмного забезпечення комп'ютерної мережі. Враховуючи стрімкий розвиток компанії, необхідно приділити увагу вибору сучасних рішень, які можуть забезпечити швидку та надійну передачу інформації між користувачами мережі. Політика компанії вимагає надійного захисту конфіденційних даних від несанкціонованого доступу, а також, при виборі апаратних засобів та ПЗ має бути приділена увага їх ліцензії та вимогам на користування у комерційній діяльності.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до Системи

2.1.1 Вимоги до Системи в цілому

Комп’ютерна система (КС) призначена для забезпечення роботи підприємства ТОВ «Інфотех».

Система, що розробляється, складається з двох підсистем - корпоративна мережа підприємства та система Інтернету речей.

Корпоративна мережа має наступне призначення:

- Забезпечення передачі інформації між структурними підрозділами підприємства
- Забезпечення робочих місць для розробки програмного забезпечення;
- Забезпечення надійного зберігання даних підприємства (дані про договори з клієнтами, дані про трудові договори, фінансові операції тощо);

Структурно корпоративна мережа поділена на 5 підмереж:

- Відділ IT-інфраструктури (LAN 1) - 4 вузла;
- Відділ маркетингу (LAN 2) - 12 вузлів;
- Відділ розробки ПЗ (LAN 3) - 39 вузлів;
- Відділ бухгалтерії та юристів (LAN 4) - 8 вузлів;
- Відділ підтримки клієнтів (LAN 5) - 15 вузлів;

Система Інтернету виконує наступні функції:

- Автоматичне регулювання температури в офісному приміщенні;
- Автоматичне вмикання освітлення в офісному приміщенні;
- Контроль доступу до серверної кімнати за допомогою RFID-карток;

Окремим функціональним компонентом КС є серверна кімната, в якій знаходяться сервери підприємства. На серверах підприємства налаштована робота наступних служб:

- Для доступу до інформаційних ресурсів підприємства (документація, вихідний код програм) налаштований HTTP-сервер;
- Налаштована служба DNS, яка містить записи для внутрішніх серверів КМ;
- Налаштований IoT-сервер, що виконує роль контролера розумних пристроїв датчиків;

Усі компоненти КС повинні бути пов’язані між собою задля забезпечення стабільної роботи підприємства.

2.1.1.1 Вимоги до характеристик взаємозв'язків із суміжними системами

Для доступу до системи Інтернет на маршрутизаторах КМ має бути налаштована трансляція IP-адрес NAT. Додатково на маршрутизаторах повинні бути налаштовані списки доступ, що обмежують вхідний трафік до мережі ззовні.

2.1.1.2 Вимоги до експлуатації

Необхідно забезпечити роботу Системи з понеділка по п’ятницю з 08:00 до 19:00. Окремо, роботу серверної кімнати забезпечити безперервно 7 днів на тиждень 24 години на добу.

Робочий день усіх відділів підприємства триває з 09:00 до 18:00 з понеділка по п’ятницю. Вихідні дні – субота та неділя. Робота системи повинна передбачати можливе відхилення від графіку, але не більше ніж на ±1 годину. Співробітникам з відділу розробки та тестування ПЗ дозволяється працювати віддалено.

2.1.1.3 Вимоги до персоналу, що обслуговує систему

Персонал, що займається налаштуванням та обслуговуванням комп’ютерної системи повинен мати відповідні сертифікати, свідоцтва та допуски. Для обслуговування основної та віддаленої мережі потрібно 4

спеціалісти зі встановлення та налаштування мережевого обладнання. Кожен спеціаліст повинен мати вищу освіту ступеня бакалавра у відповідній галузі знань. Персонал, що обслуговує систему, займає посади системних адміністраторів.

2.1.1.4 Вимоги до регламенту обслуговування

Обслуговування Системи має проводити авторизований персонал. При обслуговуванні окремих компонентів необхідно забезпечити роботу решти Системи. Персонал, що обслуговує Систему, знаходиться безпосередньо на робочому місці та виконує задачі з налагодження та ремонту Системи. Планове обслуговування Системи проводиться не частіше ніж 1 раз на 6 місяців. Оновлення АРМ співробітників на більш сучасне обладнання проводиться 1 раз на 3 роки. Оновлення мережевого обладнання, ДБЖ та резервних джерел живлення, розумних пристроїв виконується згідно з гарантійними термінами, зазначеними виробником.

2.1.1.5 Вимоги до надійності

Необхідно забезпечити безвідмовність Системи на протязі 10 тисяч годин. Час відновлення працездатності серверної кімнати при відмовах не має перевищувати 2 години, крім випадків несправності мережевого або серверного обладнання.

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

Запасне обладнання та розхідні матеріали, що використовуються на підприємстві або необхідні для ремонту компонентів Системи зберігаються у серверній кімнати в головному офісі підприємства. Приміщення серверної кімнати має відповідати наступним показникам:

- Площа приміщення: не більше, ніж 15 м^2;
- Вологість повітря має бути в межах від 40 до 60%;

- Температура повітря: від 20 °С до 24 °С;

2.1.1.7 Вимоги до безпеки

Основні вимоги до пожежної безпеки на підприємстві включають:

- Меблі та обладнання мають розміщуватися так, щоб забезпечити евакуаційний прохід до виходу з приміщення;
- Документи, папір та інші горючі матеріали слід зберігати на відстані від електрощитів, електрокабелів, проводів – не менше 1,0 м, від світильника – 0,5 м від приладів опалення – 0,25 м;
- Засоби протипожежного захисту слід утримувати у справному стані. Всі працівники в офісі зобов`язані вміти користуватися наявними вогнегасниками, іншими первинними засобами пожежогасіння та внутрішніми пожежними кранами, знати місця їх розташування. Відстань від найвіддаленішого місця офісу до вогнегасника не повинна перевищувати 20 м;

У службових приміщеннях забороняється:

- облаштовувати тимчасові електромережі;
- застосовувати саморобні некалібровані плавкі вставки в запобіжниках і саморобні подовжувачі, які не відповідають вимогам Правил улаштування електроустановок, прокладати електричні проводи безпосередньо по горючій основі, експлуатувати світильники зі знятими ковпаками (розсіювачами);
- використовувати вимикачі та штепсельні розетки для розвішування на них одягу або інших предметів, обгортати електролампи й світильники папером, заклеювати ділянки електропроводки горючою тканиною, папером; [6]

2.1.1.8 Вимоги до захисту інформації від несанкціонованого доступу

Доступ до кожного ресурсу у мережі має бути персоналізований та розмежований. Порядок створення та використання інформаційних ресурсів

визначається окремими положеннями та розпорядженнями керівництва компанії. Відповідальним за всі питання щодо розміщення ресурсів у мережі та надання доступу до них співробітникам є відділ IT-інфраструктури та відділ кібербезпеки. Доступ до консолі налаштування мережевих пристроїв має бути захищений паролем. АРМ співробітників мають бути захищені паролем з довжиною не менше 8 символів. Паролі необхідно оновлювати не рідше ніж раз на 3 місяці. На мережевому обладнанні застосувати реєстрацію дій користувачів за допомогою служби AAA. Пропуск до серверної кімнати має здійснюватись за допомогою RFID-карток.

2.1.1.9 Вимоги до параметрів мереж електропостачання

Для нормального функціонування Системи необхідно забезпечити постачання та наявність стабільної напруги ~230 В (± 10%) з частотою 50 Гц.

На підприємстві має бути застосована схема заземлення TN-S.

Додатково забезпечити безперебійне живлення серверної кімнати з використанням таких резервних джерел живлення, як генератори та/або зарядні станції.

2.1.1.10 Вимоги до патентної чистоти

Використані у інформаційній системі апаратні засоби та пристрої, програмне забезпечення та прикладні програми мають бути сертифіковані та ліцензовані для використання на території України.

2.1.1.11 Вимоги до однорідності

Для нормальної роботи Системи, вона має відповідати наступним вимогам до однорідності:

- Використання мережевого обладнання виробника Cisco;
- Використання UTP-кабеля категорії 5e;
- Використання конекторів типу RJ-45 для підключення мережевих кабелів;
- Використання стандартних протоколів мережі: TCP/IP, Wi-Fi;

2.1.1.12 Вимоги до показників призначення

Параметри Системи мають відповідати наступним показникам:

- КМ може бути розширена до кількості вузлів, вказаної у перспективах модернізації Системи
- Корпоративна мережа складається з 4 підмереж та 1 віддаленої мережі;
- Використаний блок IP-адрес у КМ: 10.25.96.0/22;
- Використаний блок IP-адрес для міжмаршрутизаторних каналів: 10.1.12.0/24;
- Середня довжина повідомлення: 650 байт;
- Середня інтенсивність кадрів складає 110 кадрів/с;
- Максимальна допустима затримка пакетів на фізичних каналах ≤ 6 мс;
- Перші доступні IP-адреси мереж призначаються інтерфейсам маршрутизаторів;
- Серверам призначається перша доступна адреса у мережі + 9 + №, де № - номер варіанта;
- HTTP-серверну призначена зовнішня адреса 209.165.200.4;
- Доступ до привілейованого режиму у Cisco IOS - *class*;
- Налаштування шифрування паролів;
- На мережевому обладнанні налаштований баннер MOTD;
- Між комутаторами підмережі LAN 1 налаштована агрегація портів;
- Налаштування віртуальних мереж VLAN у підмережі LAN 5;

2.1.1.13 Перпективи розвитку, модернізації Системи

Межею модернізації Системи щодо масштабованості КМ є загальна кількість хостів не більше 499. Максимально допустимий розмір кожної з підмереж складає: LAN 1 - 48 вузлів; LAN 2 - 103 вузлів; LAN 3 - 214 вузлів; LAN 4 - 15 вузлів; LAN 5 - 119 вузлів;

2.1.2 Вимоги до видів забезпечення

2.1.2.1 Вимоги до лінгвістичного забезпечення

Основною мовою комунікації співробітників та ведення документації є українська. Мова інтерфейсів робочих пристроїв може бути або англійська, або українська. Коментарі до вихідного коду програм мають бути виключно

2.1.2.2 Вимоги до технічого забезпечення

При проектування корпоративної мережі необхідно обрати мережеві пристрої від виробника Cisco.

Обрані комутатори мають підтримувати можливість налаштування VLAN та агрегації портів PAgP.

Обрані маршрутизатори мають підтримувати протокол динамічної маршрутизації EIGRP, NAT, службу DHCP та VPN.

Сервери корпоративної мережі повинні відповідати наступним характеристикам:

- Процесором з 4 фізичними ядрами та тактовою частотою не нижче 2 Ггц;
- Об'єм оперативної пам'яті - не нижче 8 гб;
- Об'єм накопичувача SSD - не нижче 256 гб;
- Операційною системою Ubuntu або Fedora;

Робочі місця на підприємстві повинні відповідати наступним характеристикам;

- Процесором з 4 фізичними ядрами та тактовою частотою не нижче 2 Ггц;
- Об'єм оперативної пам'яті - не нижче 16 гб;
- Об'єм накопичувача SSD - не нижче 512 гб;
- Однією з наступних операційних систем: Windows 10, Windows 11, Ubuntu або Fedora;

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Специфікація апаратного обладнання системи

Для забезпечення роботи комп'ютерної системи було обрано низьку мережевих пристроїв від виробника Cisco.

В якості маршрутизаторів було обрано модель Cisco 2911. Дана модель має пропускну спроможність 1000 Мбіт/с та підтримку гігабітних Ethernet-портів з роз’ємом RJ-45. Також є можливість встановлення модулів розширення з Serial-портами. Виходячи з вимог до фізичного рівня обладнання, ця модель дозволить з’єднати маршрутизатори між собою двома Serial-кабелями та пропускна спроможність пристрою повністю покриє розраховані значення щодо трафіку мережі. Загалом необхідно встановити 5 маршрутизаторів щоби забезпечити роботу мережі основного офісу та віддаленої мережі.

Рисунок 2.1 – Зовнішній вигляд маршрутизатора Cisco 4331

В якості комутатора було обрано модель Cisco 2960. Ця модель має 48 Ethernet-портів з роз’ємом RJ-45. Додатково, комутатори цієї моделі дозволяють виконати налаштування безпеки, зазначені у технічних вимогах. Загалом на усі

підмережі корпоративної підмережі встановлено 9 комутаторів даної моделі, що є достатнім для підключення усіх кінцевих пристроїв мережі.

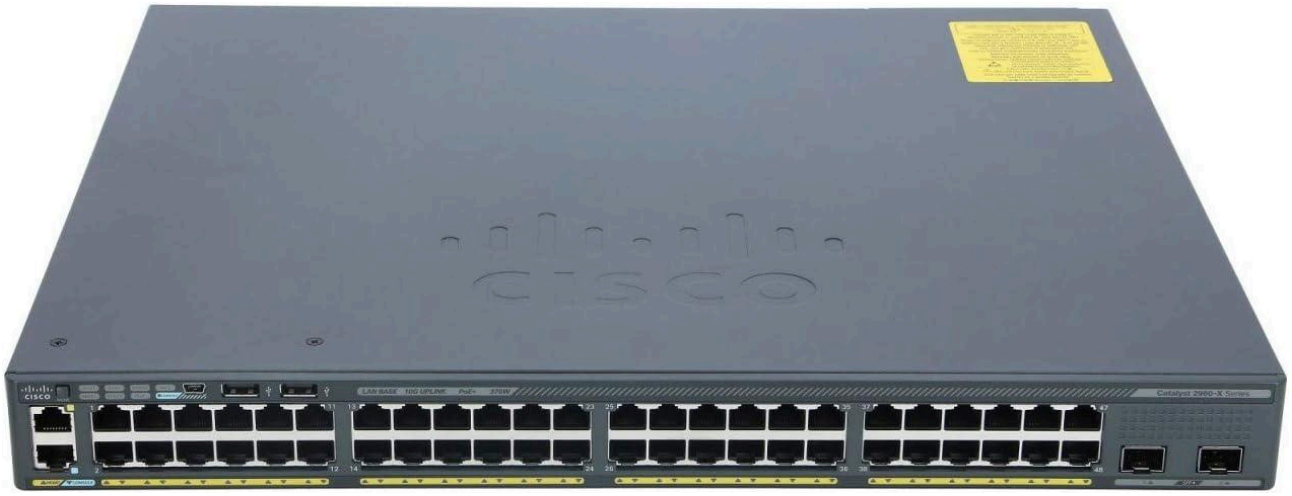

Рисунок 2.2 – Зовнішній вигляд комутатора Cisco 2960

В якості бездротової точки доступу Wi-Fi для пристроїв системи Інтернету речей було обрано точку доступу Cisco Catalyst 9136. Дана модель може працювати на двох діапазонах 2.4 ГГц і 5 ГГц та має 2 Ethernet порти для більш надійного з’єднання на фізичному рівні.

Для забезпечення резервного живлення серверної кімнати було встановлено ДБЖ Logic Power LPY-B-PSW-6000VA+ з правильною синусоїдою, генератор з номінальною потужністю 5 кВт та 2 зарядні станції потужністю 2 кВт за ємністю 2 кВт/год кожна. При середньому споживанні серверної (2 серверів та мережевих пристроїв) у 1 кВт, даного обладнання має вистачити на 8 годин безперебійної роботи.

У таблиці 2.2 наведено специфікацію обраного мережевого та технічного обладнання, що використовується у корпоративній мережі.

Таблиця 2.2 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка позначення документа, опитувального листа	Одиниці виміру	Кількість
1	2	3	4	5

1	Cisco 2911 w/3 GE,4 EHWIC, 2 DSP, 1 SM, 256MB CF, 512MB DRAM, IPB	Маршрутизатор	шт.	6
2	Cisco 2960-24TT Layer 2 - 24 x 10/100 Ports - 2 x 1000BT	Комутатор	шт.	9
3	Кабель UTP кат. 5e, оболонка FR-ПВХ (IEC 332.1); діаметр провідника з ізоляцією < 0,001 м; діаметр кабелю < 0,005 м. Бухта 305м.		од.	2
4	ДБЖ Logic Power LPY-B-PSW-6000VA; Pure Sine;	ДБЖ	шт.	1
5	Зарядна станція Jackery Explorer 2000 Pro 2kW; Pure Sine Wave 230V		шт.	2
6	Генератор Honda EU70IS 5 kW		шт.	1
7	Cisco Catalyst 9136 2.4 GHz + 5 GHz 2 Ethernet ports	Точка доступу	шт.	1
8	Intel Xeon E3-1275v5; 1 x 8 Gb DDR4; 2 x SSD SATA 480 Gb;	TFTP Server, HTTP Server, DNS Server	шт.	3
9	Intel Core i3 12100F 3.3 GHz; 1 x 8Gb DDR4;	ПК2	шт.	37

	1 x SSD SATA 480 Gb;			
10	Intel Core i5 12400F 2.5 GHz; 2 x 16Gb DDR4; 1 x SSD NVMe 1Tb;	ПК1	шт.	43
11	Принтер Canon MF 2401; 600x600 DPI;	Принтер	шт.	2

На рисунку 2.3 наведено структурну схему обладнання Системи.

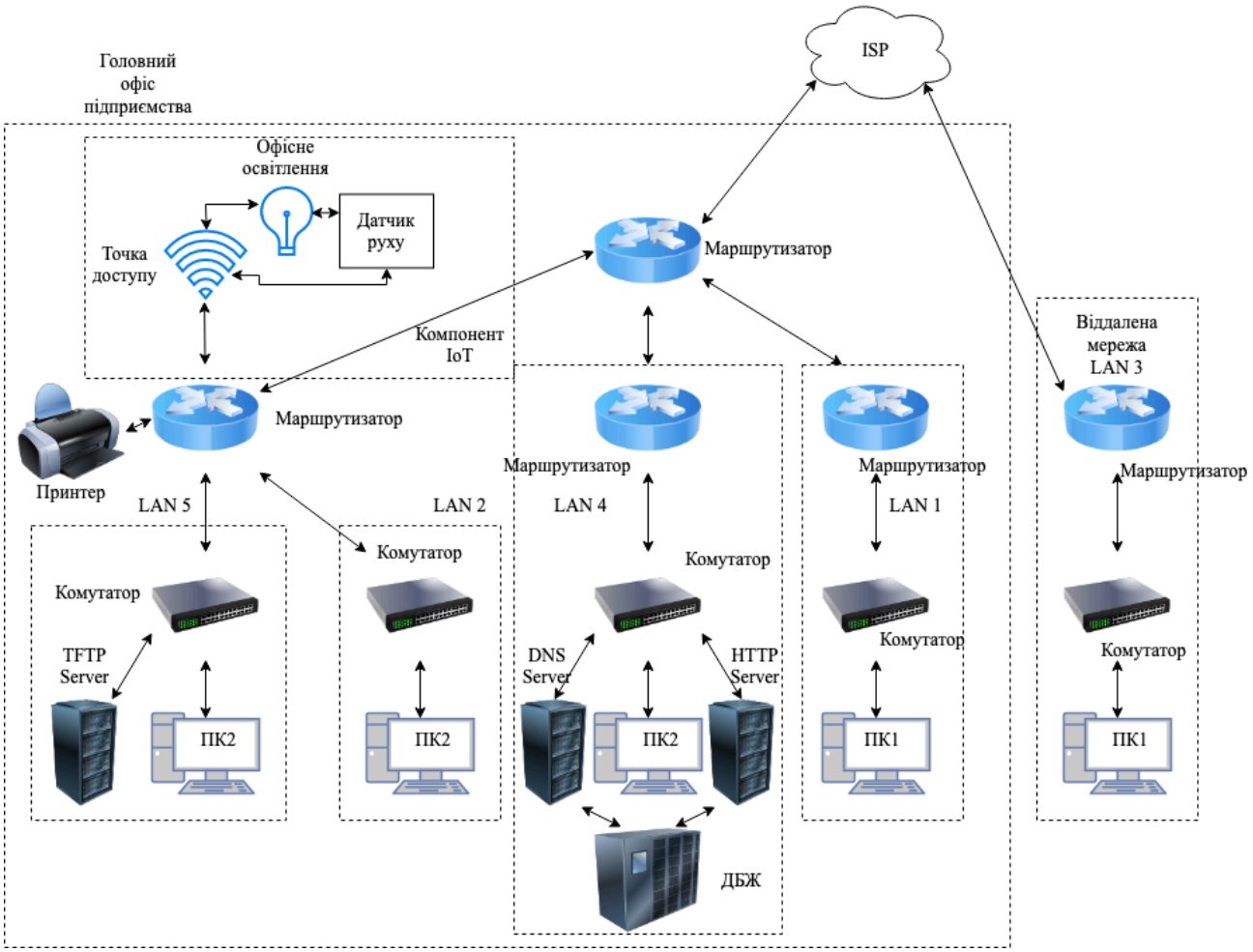

Рисунок 2.3 – Структурна схема обладнання

2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі

Для розрахунку інтенсивності вихідного трафіку та перевірки пропускної здатності каналів зв'язку береться найбільша локальна підмережа. В комп'ютерній мережі підприємства ТОВ “ІНФОТЕХ” встановлений маршрутизатор Cisco 2911 та комутатор Cisco 2960, що об'єднують ПК, сервери та інші мережеві пристрої в офісі компанії. Вихідний трафік подається на маршрутизатор Cisco 2911 з пропускною спроможністю у 1000 Мбіт/с. Щоби запобігти перенасичення комутатора рівня доступу, швидкість надходження пакетів має бути нижчою за швидкість відправлення. Для розрахунку припустимо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку $\mu = 110$ (кадрів/с), а середня довжина повідомлення складає 650 байтів.

Розрахуємо пропускну здатність мережі на рівні доступу за наступною формулою:

$$\text{Рр.р} = \mu \times l \times N \times 8$$

де l - середня довжина повідомлення, N - кількість вузлів.

$$\text{Рр.р} = 110 \times 650 \times 214 \times 8 = 122.4\ (\text{Мбіт/с})$$

Отримані результати після розрахунку не перевищують параметри мережі, а отже перевантажень на обраному обладнанні не буде.

Комутатор направляє трафік на маршрутизатор через лінію з пропускною здатністю у 1000 Мбіт/с.

Максимальне допустиме навантаження на комутатор можна розрахувати за наступною формулою:

$$\mu_{вих} = \frac{1000\ (\text{Мбіт/с})}{l \times 8}$$

Таким чином загальне навантаження на комутатор не повинно перевищувати

$$\mu_{вих} = \frac{1000\,000\,000}{650 \times 8} = 192307\ (\text{пакетів/с})$$

Оскільки кожен вузол в мережі в середньому виробляє 110 пакетів/с, то максимальна допустима кількість приєднаних вузлів до комутатора рівня доступу складає:

$$N = \frac{192307}{110} = 1748$$

що задовольняє вимоги нашої мережі, яка складається з 499 хостів.

Кожен з 499 хостів генерує вихідний трафік з інтенсивністю у 110 пакетів/с. Таким чином, загальна інтенсивність вихідного трафіку складає:

$$\lambda = N \times \mu = 499 \times 110 = 54890\ (\text{пакетів/с})$$

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу, що впливає на час знаходження у черзі визначається за формулою:

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{54890}{192307} = 0.28$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \frac{\rho}{1-\rho} = \frac{0.28}{1-0.28} = 0.39$$

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

$$T = \frac{1}{\mu_{вих} - \lambda} = \frac{1}{192307 - 54890} = 7.3 \times 10^{-6}(\text{с})$$

Середня довжина черги складає:

$$L_{черг} = \frac{\rho^2}{1-\rho} = 0.1$$

Ці значення можуть стати у нагоді при налаштуванні черг пакетів на мережевому обладнанні. У нашому випадку в середньому на обслуговуванні в

черзі знаходиться лише частка 1 пакету. Це значення є умовним, але воно свідчить про доволі великий запас продуктивності у системі.

Середній час перебування пакета у черзі складає:

$$T_{\text{оч}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0.1}{54890} = 1.98\text{мс}$$

Це значення є меншим за задане число у 6мс, а отже задовольняє технічним вимогам.

На останок, розрахуємо пропускну здатність каналу за формулою:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l}$$

$$b = \lambda \times l = 54890 \times 650 \times 8 = 285\ \text{Мбіт/с}$$

що задовольняє пропускній здатності вихідного каналу на обраному обладнанні у 1000 Мбіт/с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

При проектуванні корпоративної мережі ТОВ “ІНФОТЕХ” було враховано всі вимоги до мережі: виділений блок IP-адрес, кількість підмереж та кількість вузлів у підмережах. Додатково було приділено увагу наступним критеріям: мінімальна витрата адрес та найкраща сумаризація. Розрахунок схеми адресації мережі було зроблено за допомогою технологій CIDR та VLSM з використанням адресного простіру 10.25.96.0/22. [1] У таблиці 3.1 наведено кількість підмереж з кількістю вузлів в кожній з них.

Таблиця 3.1 – Кількість вузлів у підмережах

LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
48	103	214	15	119

Схему адресації корпоративної мережі отриманої в результаті проведених розрахунків наведено у таблиці 3.2. [8][9][10]

Таблиця 3.2 – Схема адресації мережі

Назва підмережі	Кількість вузлів	Адреса	Десяткова маска	Діапазон доступних адрес
LAN 3	214	10.25.96.0	255.255.255.0	10.25.96.1 - 10.25.96.254
LAN 5	119	10.25.97.0	255.255.255.128	10.25.97.1 - 10.25.97.126
LAN 2	103	10.25.97.128	255.255.255.128	10.25.97.129 - 10.25.97.254
LAN 1	48	10.25.98.0	255.255.255.192	10.25.98.1 - 10.25.98.62
LAN 4	15	10.25.98.64	255.255.255.224	10.25.98.65 - 10.25.98.94

VLAN22	30	10.25.97.0	255.255.255.224	10.25.97.1 - 10.25.97.31
VLAN32	30	10.25.97.32	255.255.255.224	10.25.97.3 - 10.25.97.62
VLAN42	30	10.25.97.64	255.255.255.224	10.25.97.65 - 10.25.97.94
VLAN99	30	10.25.97.96	255.255.255.224	10.25.97.97 - 10.25.97.126

В обраному блоці IP-адрес доступно 1022 адрес, а загальна кількість хостів в корпоративній мережі - 499, що складає 48% доступних адрес. Таким чином виконана вимога до мінімальної витрати адрес.

Адресація мережевих інтерфейсів вузлів мережі наведена у таблиці 3.3 [7]

Таблиця 3.3 – Схема адресації пристроїв мережі

Ім’я пристрою	Інтер-фейс	IP-адреса	Мас-ка	Шлюз	VLAN	Інтер-фейс підклю-ченого при-строю
LAN 1						
Necheporenko_R2	G0/0	10.25.98.1	/25	-	-	G0/1
	S0/1/0	209.165.202.2	/30			
	S0/0/0	10.1.12.10	/30			
	S0/0/1	10.1.12.14	/30			
PC1/1-9	NIC	10.25.98.2 - 10.25.98.10	/25	10.25.98.1	-	F0/10-12
LAN 2						
Necheporenko_R1	G0/0	10.25.97.129	/25	-	-	G0/0
PC2/1-3	NIC	10.25.97.130 -	/25	10.25.97.129	-	F0/1-3

		10.25.97.132				
Server-IoT	NIC	10.25.97.140	/25	10.25.97.129	-	F0/11
Tablet-IoT	Wireless	10.25.97.141	/25	10.25.97.129	-	-
LAN 3						
Necheporenko_R5	G0/0	10.25.96.1	/24	-	-	G0/1
PC3/1-3	NIC	10.25.96.2 - 10.25.96.4	/24	10.25.96.1	-	F0/1-3
LAN 4						
Necheporenko_R3	G0/1	10.25.98.65	/27	-	???	G0/1
	G0/0	10.1.12.18	/30	-	-	G0/0
HTTP-Server	NIC	10.25.98.86	/27	10.25.98.65	-	F0/4
DNS-Server	NIC	10.25.98.87	/27	10.25.98.65	-	F0/5
PC4/1-3	NIC	10.25.98.88 - 10.25.98.90	/27	10.25.98.65	-	F0/1-3
LAN 5						
Necheporenko_R1	G0/1.22	10.25.97.1	/27	-	22	G0/1
	G0/1.32	10.25.97.33	/27	-	32	G0/1
	G0/1.42	10.25.97.65	/27	-	42	G0/1
	G0/1.99	10.25.97.97	/27	-	99	G0/1
	S0/0/0	10.1.12.2	/30	-	-	S0/0/0
	S0/0/1	10.1.12.6	/30	-	-	S0/0/1
Necheporenko_SW5_1	VLAN 99	10.25.97.98	/27	10.25.97.97	99	G0/1
Necheporenko_SW5_2	VLAN 99	10.25.97.99	/27	10.25.97.97	99	G0/1
Necheporenko	VLAN	10.25.97.100	/27	10.25.97.97	99	G0/1

_SW5_3	99					
TFTP-Server	NIC	10.25.97.22	/27	10.25.97.1	22	F0/6
PC5/2, PC5/5	NIC	DHCP	/27	10.25.97.1	22	F0/6-11
PC5/4, PC5/7	NIC	DHCP	/27	10.25.97.33	32	F0/12-14
PC5/1, PC5/3, PC5/6	NIC	DHCP	/27	10.25.97.65	42	F0/15-24
ISP						
Necheporenko_ISP	G0/1	209.165.201.1	/28	-	-	NIC
	G0/0	64.100.13.1	/30	-	-	G0/1
	S0/0/0	209.165.202.1	/30	-	-	S0/1/0
PC-ISP	NIC	209.165.201.5	/28	209.165.201.1	-	G0/1

3.2 Розробка логічної схеми корпоративної мережі

Логічна схема корпоративної мережі підприємства ТОВ «Інфотех» створена на основі організаційної структури та технічних вимог наведена на рисунку 3.1. Топологія КМ об'єднує 5 підмереж. Архітектура комп'ютерної мережі заснована на топології «ієрархічна зірка».

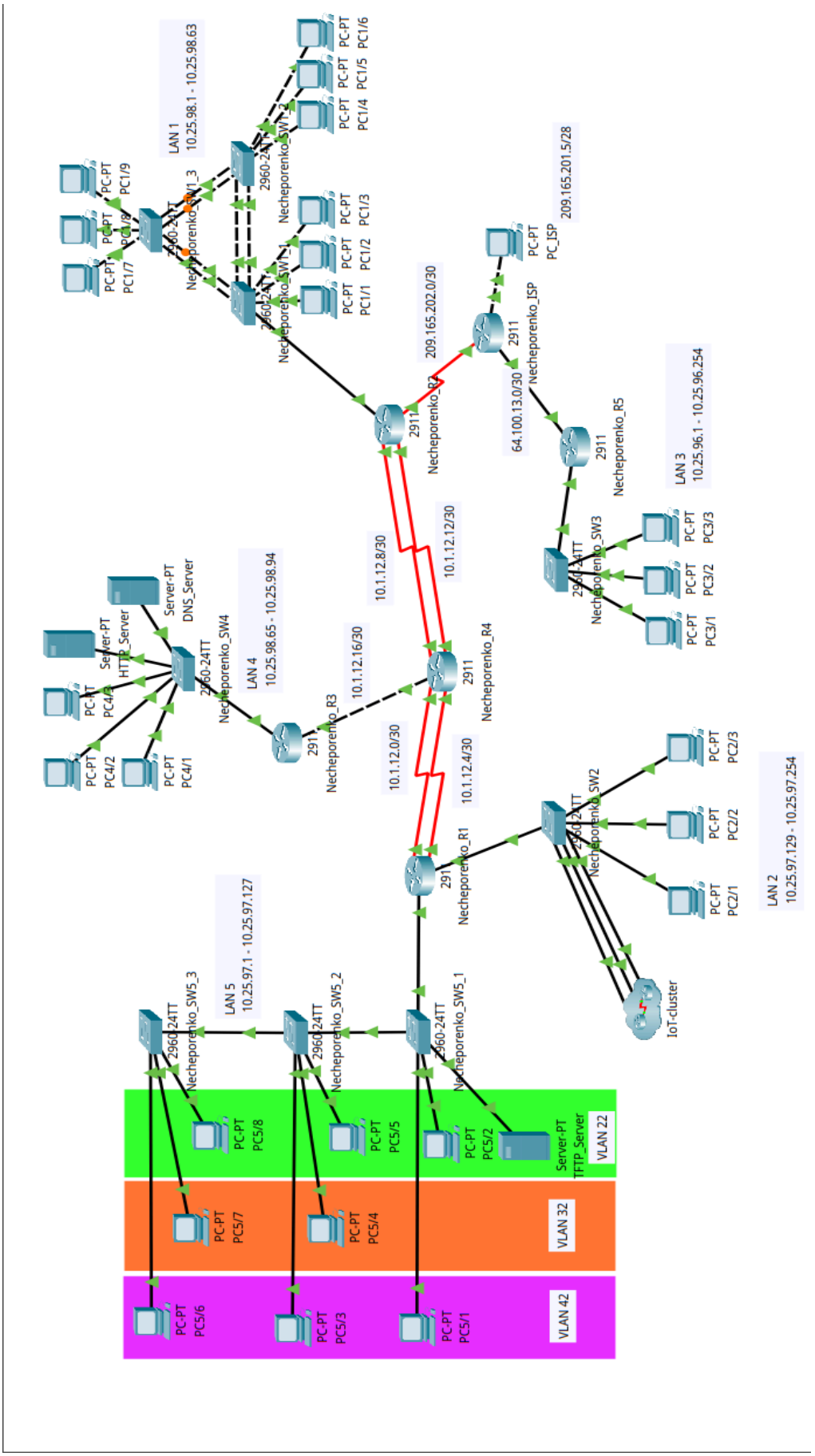

Рисунок 3.1 – Логічна схема корпоративної мережі

3.3 Налаштування моделі комп'ютерної системи

3.3.1 Базове налаштування конфігурації пристроїв

Згідно технічним вимогам до комп'ютерної системи було виконано базове налаштування всіх мережевих пристроїв. Розроблено базову конфігурацію пристроїв мережі, а саме:

- Назначено назви пристроям;
- Застовано паролі для привілейованого режиму, консолі і vty;
- Застовано шифрування до паролів; \item Встановлено баннер MOTD;
- На лініях vty назначено використання протоколу SSH;
- Створено користувачів на всіх мережевих пристроях;
- Задано доменне ім'я пристрою;
- Для шифрування даних створено ключ RSA завдовжки 1024 біт;
- Задано IP-адреси на інтерфейсах пристроїв згідно розрахунків;
- На DCE-інтерфейсах маршрутизаторів призначено значення тактової частоти 128000;

```
Router(config)#hostname Necheporenko_R1
Necheporenko_R1(config)#service password-encryption
Necheporenko_R1(config)#enable secret class
Necheporenko_R1(config)#line console 0
Necheporenko_R1(config-line)#password cisco
Necheporenko_R1(config-line)#login
Necheporenko_R1(config-line)#exit
Necheporenko_R1(config)#line vty 0 15
Necheporenko_R1(config-line)#password cisco
Necheporenko_R1(config-line)#login local
Necheporenko_R1(config-line)#transport input ssh
Necheporenko_R1(config-line)#exit
Necheporenko_R1(config)#banner motd #123-20 Necheporenko. Password-protected access#
Necheporenko_R1(config)#username 12320_Necheporenko password cisco
Necheporenko_R1(config)#ip domain-name Necheporenko_R1
Necheporenko_R1(config)#crypto key generate rsa
The name for the keys will be: Necheporenko_R1.Necheporenko_R1
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

Necheporenko_R1(config)#
```

Рисунок 3.2 – Базове налаштування маршрутизатора Necheporenko_R1

Згідно з таблицею 3.3 виконано налаштування адресації на інтерфейсах мережевих пристроїв.

3.3.2 Налаштування маршрутизаторів

3.3.2.1 Налаштування Serial-інтерфейсів

Згідно технічних вимог на Serial інтерфейсах маршрутизаторів задано пропускну спроможність у 128 Кб/с та значення тактової частоти 128000.

```
Necheporenko_R1(config)#interface Serial0/0/0
Necheporenko_R1(config-if)#bandwidth 128
Necheporenko_R1(config-if)#clock rate 128000
Necheporenko_R1(config-if)#no sh
Necheporenko_R1(config-if)#exit
Necheporenko_R1(config)#interface Serial0/0/1
Necheporenko_R1(config-if)#bandwidth 128
Necheporenko_R1(config-if)#clock rate 128000
Necheporenko_R1(config-if)#no sh
Necheporenko_R1(config-if)#exit
Necheporenko_R1(config)#
```

Рисунок 3.3 – Налаштування пропускної спроможності Serial-інтерфейсів

3.3.2.2 Налаштування маршрутизації

Налаштування динамічної маршрутизації у комп'ютерній мережі підприємства ТОВ «Інфотех» було виконано з використанням протоколу EIGRP. Протокол EIGRP є пропрієтарним протоколом маршрутизації розроблений компанією Cisco. Він оснований на попередніх, застарілих протоколах RIP (Routing Information Protocol) і IGRP (Interior Gateway Routing Protocol). Ці протоколи також використовували векторну маршрутизацію, проте мали певні обмеження, які були вирішені у EIGRP, а саме:

- DUAL (Diffusing Update ALgorithm) - ключова відмінність EIGRP від RIP і IGRP. DUAL дозволяє швидко відновлювати роботу маршрутизації в разі зміни топології мережі, забезпечуючи швидке виявлення найкращих шляхів до всіх мережевих сегментів;
- Мінімальне використання пропускної здатності мережі: EIGRP передає лише необхідну інформацію про маршрути, що робить його менш

витратним у використанні пропускної здатності мережі в порівнянні з іншими протоколами.

– Підтримка для VLSM і CIDR: У відміну від RIP, який працює тільки з класовими мережами, і безкласну міждоменну маршрутизацію (CIDR).

Для кожного маршрутизатора оголошені безпосередньо підключені мережі та відключено поширення оновлень правил маршрутизації на інтерфейси в локальній мережі.

```
Necheporenko_R1(config)#router eigrp 12
Necheporenko_R1(config-router)#no auto-summary
Necheporenko_R1(config-router)#redistribute static
Necheporenko_R1(config-router)#network 10.25.97.128 0.0.0.127
Necheporenko_R1(config-router)#network 10.0.12.0 0.0.0.3
Necheporenko_R1(config-router)#network 10.0.12.4 0.0.0.3
Necheporenko_R1(config-router)#end
```

Рисунок 3.4 – Налаштування правил EIGRP на маршрутизаторі Necheporenko_R1

На рисунку 3.4 наведено приклад налаштування динамічної маршрутизації EIGRP. За допомогою команд Cisco IOS було задано адресу прилягаючої мережі LAN 2 та між-маршрутизаторні мережі.

```
Necheporenko_R4(config)#router eigrp 12
Necheporenko_R4(config-router)#network 10.0.12.0 0.0.0.3
Necheporenko_R4(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 12: Neighbor 10.0.12.2 (Serial0/0/0) is up: new adjacency

Necheporenko_R4(config-router)#network 10.0.12.4 0.0.0.3
Necheporenko_R4(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 12: Neighbor 10.0.12.6 (Serial0/0/1) is up: new adjacency

Necheporenko_R4(config-router)#no auto-summary
Necheporenko_R4(config-router)#redist static
Necheporenko_R4(config-router)#end
Necheporenko_R4#
```

Рисунок 3.5 – Налаштування правил EIGRP на маршрутизаторі Necheporenko_R4

На рисунку 3.5 можна побачити, що при налаштуванні підключених мереж маршрутизатор автоматично отримує інформацію про підключеного до

нього сусіда. На маршрутизаторі Necheporenko_R2, що безпосередньо підключений до інтернет провайдера (ISP) задано маршрут за замовчуванням 209.165.202.1, який розповсюджується через оновлення маршрутизації EIGRP.

```
Necheporenko_R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
Necheporenko_R2(config)#exit
```

Рисунок 3.6 – Налаштування маршруту за замовчуванням до ISP

Перевірити таблицю маршрутизації на роутері в Cisco IOS можна за допомогою команди *show ip route* в привілейованому режимі.

```
Necheporenko_R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.12.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 20 subnets, 5 masks
C       10.0.12.0/30 is directly connected, Serial0/0/0
L       10.0.12.2/32 is directly connected, Serial0/0/0
C       10.0.12.4/30 is directly connected, Serial0/0/1
L       10.0.12.6/32 is directly connected, Serial0/0/1
D       10.0.12.8/30 [90/21024000] via 10.0.12.1, 01:46:37, Serial0/0/0
                     [90/21024000] via 10.0.12.5, 00:11:32, Serial0/0/1
D       10.0.12.12/30 [90/21024000] via 10.0.12.1, 01:46:35, Serial0/0/0
                      [90/21024000] via 10.0.12.5, 00:11:32, Serial0/0/1
D       10.0.12.16/30 [90/20512256] via 10.0.12.1, 01:46:37, Serial0/0/0
                      [90/20512256] via 10.0.12.5, 00:11:32, Serial0/0/1
D       10.25.96.0/24 [90/21536512] via 10.0.12.1, 01:43:35, Serial0/0/0
                      [90/21536512] via 10.0.12.5, 00:11:32, Serial0/0/1
C       10.25.97.0/27 is directly connected, GigabitEthernet0/1.22
L       10.25.97.1/32 is directly connected, GigabitEthernet0/1.22
C       10.25.97.32/27 is directly connected, GigabitEthernet0/1.32
L       10.25.97.33/32 is directly connected, GigabitEthernet0/1.32
C       10.25.97.64/27 is directly connected, GigabitEthernet0/1.42
L       10.25.97.65/32 is directly connected, GigabitEthernet0/1.42
C       10.25.97.96/27 is directly connected, GigabitEthernet0/1.99
L       10.25.97.97/32 is directly connected, GigabitEthernet0/1.99
C       10.25.97.128/25 is directly connected, GigabitEthernet0/0
L       10.25.97.129/32 is directly connected, GigabitEthernet0/0
D       10.25.98.0/25 [90/21024256] via 10.0.12.1, 01:46:37, Serial0/0/0
                      [90/21024256] via 10.0.12.5, 00:11:32, Serial0/0/1
D       10.25.98.64/27 [90/20512512] via 10.0.12.1, 01:46:37, Serial0/0/0
                       [90/20512512] via 10.0.12.5, 00:11:32, Serial0/0/1
     64.0.0.0/30 is subnetted, 1 subnets
D       64.100.13.0/30 [90/21536256] via 10.0.12.1, 01:43:36, Serial0/0/0
                       [90/21536256] via 10.0.12.5, 00:11:32, Serial0/0/1
     209.165.202.0/30 is subnetted, 1 subnets
D       209.165.202.0/30 [90/21536000] via 10.0.12.1, 01:46:37, Serial0/0/0
                         [90/21536000] via 10.0.12.5, 00:11:32, Serial0/0/1
D*EX 0.0.0.0/0 [170/26144000] via 10.0.12.1, 01:26:36, Serial0/0/0
               [170/26144000] via 10.0.12.5, 00:11:32, Serial0/0/1

Necheporenko_R1#
```

Рисунок 3.7 – Таблиця маршрутизації

Виходячи з отриманої таблиці маршрутизації, шлях до усіх підмереж КС присутній у таблиці. З цього можна зробити висновок, що топологія мережі сходиться, і, відповідно, між будь-якими підмережами можна відправляти повідомлення, і вони будуть доставлені.

3.3.3 Налаштування роботи Інтернет

3.3.3.1 Налаштування мереж VLAN

VLAN (Virtual Local Area Network) — це логічна підмережа, яка згруповує набір пристроїв у одну чи більше логічних мереж, незалежно від їх фізичного розташування. VLAN дозволяє створювати ізольовані мережеві сегменти в межах одного фізичного комутатора або між кількома комутаторами, що забезпечує підвищену гнучкість, безпеку та управління трафіком у мережі. Згідно з технічними вимогами, КС ТОВ «Інфотех», у локальній мережі LAN 5 було створено 3 віртуальні підмережі VLAN для різних груп користувачів та дві службові VLAN.

Таблиця 3.4 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
1	default	Не використовується
22	Accounting	Для бухгалтерії
32	Resources	Для відділу кадрів
42	Guest	Для гостей
99	Management	Для управління пристроями
100	Native	Власна мережа

Додатково виконано наступні налаштування:

- Налаштовано транкові порти і порти доступу;
- Вимкнено усі невикористані фізичні порти комутаторів;
- Тільки двом унікальним пристроям був дозволений доступ до порту;

– MAC-адреси пристроїв розпізнаються динамічно і додаються до поточної конфігурації;

```
Necheporenko_SW5_1(config)#vlan 22
Necheporenko_SW5_1(config-vlan)#name Accounting
Necheporenko_SW5_1(config-vlan)#vlan 32
Necheporenko_SW5_1(config-vlan)#name Resources
Necheporenko_SW5_1(config-vlan)#vlan 42
Necheporenko_SW5_1(config-vlan)#name Guest
Necheporenko_SW5_1(config-vlan)#vlan 99
Necheporenko_SW5_1(config-vlan)#name Management
Necheporenko_SW5_1(config-vlan)#vlan 100
Necheporenko_SW5_1(config-vlan)#name Native
Necheporenko_SW5_1(config-vlan)#end
```

Рисунок 3.8 – створення груп VLAN

```
Necheporenko_SW5_2(config)#int r f0/6-11
Necheporenko_SW5_2(config-if-range)#switch mode access
Necheporenko_SW5_2(config-if-range)#switch access vlan 22
Necheporenko_SW5_2(config-if-range)#no sh
Necheporenko_SW5_2(config-if-range)#exit
Necheporenko_SW5_2(config)#int r f0/12-14
Necheporenko_SW5_2(config-if-range)#switch mode access
Necheporenko_SW5_2(config-if-range)#switch access vlan 32
Necheporenko_SW5_2(config-if-range)#no sh
Necheporenko_SW5_2(config-if-range)#exit
Necheporenko_SW5_2(config)#int r f0/15-24
Necheporenko_SW5_2(config-if-range)#switch mode access
Necheporenko_SW5_2(config-if-range)#switch access vlan 42
Necheporenko_SW5_2(config-if-range)#no sh
Necheporenko_SW5_2(config-if-range)#exit
Necheporenko_SW5_2(config)#
```

Рисунок 3.9 – Переведення портів у режим доступу

```
Necheporenko_SW5_1(config)#int g0/1
Necheporenko_SW5_1(config-if)#switchport mode trunk

Necheporenko_SW5_1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Necheporenko_SW5_1(config-if)#switchport trunk native vlan 100
Necheporenko_SW5_1(config-if)#switchport trunk allowed vlan 22,32,42,99-100
Necheporenko_SW5_1(config-if)#no sh
Necheporenko_SW5_1(config-if)#exit
Necheporenko_SW5_1(config)#
```

Рисунок 3.10 – Налаштування транку

```
Necheporenko_SW5_1(config)#int vlan 99
Necheporenko_SW5_1(config-if)#description LAN5
Necheporenko_SW5_1(config-if)#ip addr 10.25.97.98 255.255.255.224
Necheporenko_SW5_1(config-if)#no sh
Necheporenko_SW5_1(config-if)#ip default-gateway 10.25.97.97
Necheporenko_SW5_1(config)#
```

Рисунок 3.11 – Налаштування інтерфейсу VLAN 99

```
Necheporenko_SW5_1(config)#int r f0/6-11
Necheporenko_SW5_1(config-if-range)#switchport port-sec
Necheporenko_SW5_1(config-if-range)#switchport port-sec max 2
Necheporenko_SW5_1(config-if-range)#switchport port-sec mac-addr sticky
Necheporenko_SW5_1(config-if-range)#
```

Рисунок 3.12 – Налаштування безпеки фізичних портів

Маршрутизація трафіку між мережами VLAN здійснюється за допомогою маршрутизатора, відповідно кожна мережа має бути підключена до окремого інтерфейсу. Оскільки виділення окремих фізичних портів під кожну VLAN є неефективним, на одному фізичному інтерфейсі маршрутизатора можна створити логічні під-інтерфейси. Налаштування маршрутизації на під-інтерфейсах виконується з використанням технології 802.1Q інкапсуляції. Під кожну VLAN створюється окремий під-інтерфейс, який має свою IP-адресу.

На рисунку 3.13 наведено приклад налаштування логічних інтерфейсів з використанням 802.1Q інкапсуляції на маршрутизаторі.

```
Necheporenko_R1(config-subif)#encapsulation dot1Q 22
Necheporenko_R1(config-subif)#no sh
Necheporenko_R1(config-subif)#ip addr 10.25.97.1 255.255.255.224
Necheporenko_R1(config-subif)#int g0/1.32
Necheporenko_R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.32, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.32, changed state to up

Necheporenko_R1(config-subif)#encap dot1Q 32
Necheporenko_R1(config-subif)#ip addr 10.25.97.33 255.255.255.224
Necheporenko_R1(config-subif)#no sh
Necheporenko_R1(config-subif)#int g0/1.42
Necheporenko_R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.42, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.42, changed state to up

Necheporenko_R1(config-subif)#encap dot1Q 42
Necheporenko_R1(config-subif)#ip addr 10.25.97.65 255.255.255.224
Necheporenko_R1(config-subif)#no sh
Necheporenko_R1(config-subif)#int g0/1.99
Necheporenko_R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up

Necheporenko_R1(config-subif)#encap dot1Q 99
Necheporenko_R1(config-subif)#ip addr 10.25.97.97 255.255.255.224
Necheporenko_R1(config-subif)#no sh
Necheporenko_R1(config-subif)#
```

Рисунок 3.13 – Налаштування інкапсуляція dot1Q

Адресацію для хостів у VLAN було налаштовано службу DHCP на маршрутизаторі Necheporenko_R1. TFTP-серверу було окремо задано статичну адресу 10.25.97.22.

Для кожної підмережі VLAN створено свій DHCP пул, з яких виключено перші 10 адрес в мережі. Додатково виключено статичну адресу TFTP-серверу.

```
Necheporenko_R1(config)#ip dhcp excluded-address 10.25.97.1 10.25.97.10
Necheporenko_R1(config)#ip dhcp excluded-address 10.25.97.33 10.25.97.43
Necheporenko_R1(config)#ip dhcp excluded-address 10.25.97.65 10.25.97.75
Necheporenko_R1(config)#ip dhcp excluded-address 10.25.97.22
```

Рисунок 3.14 – Виключення адрес з DHCP-пулів

```
Necheporenko_R1(config)#ip dhcp pool poolvlan22
Necheporenko_R1(dhcp-config)#network 10.25.97.0 255.255.255.224
Necheporenko_R1(dhcp-config)#default-router 10.25.97.1
Necheporenko_R1(dhcp-config)#dns-server 10.25.98.87
Necheporenko_R1(dhcp-config)#exit
```

Рисунок 3.15 – Створення пулу DHCP

Перевірка призначених IP-адрес хостам у мережі за допомогою протоколу DHCP здійснюється командою *show ip dhcp binding* у привілейованому режимі.

```
Necheporenko_R1#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.25.97.12      000A.F3D4.6318           --                     Automatic
10.25.97.13      00E0.F991.BEEE           --                     Automatic
10.25.97.11      0060.3E20.5452           --                     Automatic
10.25.97.44      0060.3EA2.9801           --                     Automatic
10.25.97.45      0002.1796.2446           --                     Automatic
10.25.97.77      000C.8503.74E7           --                     Automatic
10.25.97.78      0001.C989.3034           --                     Automatic
10.25.97.76      0006.2A07.3A4D           --                     Automatic
Necheporenko_R1#
```

Рисунок 3.16 – Перевірка роботи служби DHCP

3.3.3.2 Налаштування агрегування портів PAgP

Port Aggregation Protocol (PAgP) - протокол агрегування каналів; пропрієтарний протокол компанії Cisco Systems, що служить для автоматизації агрегування фізичних Ethernet-портів комутатора в один логічний. Таке об'єднання дозволяє збільшувати пропускну здатність і надійність каналу. Агрегування каналів може бути налаштоване між двома комутаторами, комутатором і маршрутизатором, між комутатором і хостом.

У локальній мережі LAN 3 було налаштовано агрегацію Ethernet-портів між трьома комутаторами. На рисунку 3.17 наведено схему логічної топології підмережі з налаштованою агрегацією фізичних каналів комутаторів.

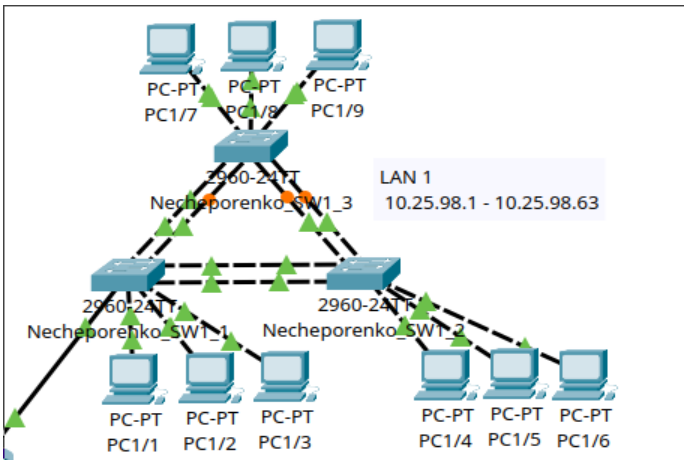

Рисунок 3.17 – Топологія з агрегацією фізичних каналів

Налаштування агрегації каналів виконується на групі інтерфейсів за допомогою команд *channel-protocol pagp* та *channel-group N mode*. За допомогою першої команди задається протокол агрегації: в нашому випадку це PAgP, також можна обрати LACP. Друга команда об'єднує декілька інтерфейсів в 1 групу. Один об'єднаний логічний інтерфейс може бути в активному (desirable) або пасивному (auto) режимі. Для утворення агрегованого каналу між комутаторами один з логічних портів має бути активним, а інший - пасивним. Це є необхідною умовою утворення каналу.

На рисунку 3.18 наведено приклад налаштування агрегації портів на одному з комутаторів.

```
Necheporenko_SW1_3(config)#int r f0/1-2
Necheporenko_SW1_3(config-if-range)#channel-proto pagp
Necheporenko_SW1_3(config-if-range)#channel-group 1 mode auto
Necheporenko_SW1_3(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

Рисунок 3.18 – Налаштування об'єднаних портів

На рисунку 3.19 наведено результат налаштування агрегації каналів PAgP на одному з комутаторів мережі.

```
Necheporenko_SW1_1#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

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

1      Po1(SU)           PAgP   Fa0/1(P) Fa0/2(P)
2      Po2(SD)           PAgP   Fa0/3(I) Fa0/4(I)
Necheporenko_SW1_1#
```

Рисунок 3.19 – Перевірка налаштування агрегації каналів

3.3.3.3 Налаштування NAT

NAT (Network Address Translation) — це метод, що широко використовується в комп'ютерних мережах для зменшення кількості необхідних IP-адрес та підвищення рівня безпеки мережі. Основна функція NAT полягає в тому, щоб дозволити маршрутизатору змінювати IP-адреси вихідних пакетів даних, що надсилаються з приватної мережі в публічну мережу Інтернет. Це дає змогу використовувати одну або кілька публічних IP-адрес для великої кількості пристроїв, що мають приватні IP-адреси всередині локальної мережі.

NAT також забезпечує захист внутрішніх IP-адрес мережі, роблячи їх невидимими для зовнішнього світу. Це підвищує рівень безпеки, оскільки зовнішні користувачі не можуть безпосередньо взаємодіяти з пристроями всередині мережі, що має приватні IP-адреси. Така ізоляція захищає внутрішні ресурси від потенційних загроз ззовні.

Відповідно до технічних вимог КС, на прикордонному маршрутизаторі задано наступні налаштування NAT:

- Створено список доступу з номером 12;
- Створено пул NAT з назвою Internet;
- Пул адрес з 209.165.200.5 по 209.165.200.30;
- Присвоєно статичну зовнішню адресу 209.165.200.4 HTTP-серверу;
- Присвоєно доменне ім'я 123.dnipro.ua зовнішній адресі Web-серверу;

На рисунку 3.20 наведено команди, використані для налаштування NAT на маршрутизаторі Necheporenko_R3.

```
Necheporenko_R2(config)#access-list 12 permit 10.25.96.0 0.0.3.255
Necheporenko_R2(config)#ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
Necheporenko_R2(config)#ip nat inside source li
Necheporenko_R2(config)#ip nat inside source list 12 pool Internet
Necheporenko_R2(config)#ip nat inside source static 10.25.98.86 209.165.200.4
Necheporenko_R2(config)#int s0/1/0
Necheporenko_R2(config-if)#ip nat outside
Necheporenko_R2(config-if)#int s0/0/0
Necheporenko_R2(config-if)#exit
Necheporenko_R2(config)#int s0/0/0
Necheporenko_R2(config-if)#ip nat inside
Necheporenko_R2(config-if)#exit
Necheporenko_R2(config)#int s0/0/1
Necheporenko_R2(config-if)#ip nat inside
Necheporenko_R2(config-if)#exit
Necheporenko_R2(config)#
```

Рисунок 3.20 – Налаштування NAT

На DNS-сервері створено запис типу A, який призначає доменне ім'я 123.dnipro.ua зовнішній адресі Web-серверу.

No.	Name	Type	Detail
0	123.dnipro.ua	A Record	209.165.200.4

Рисунок 3.21 – Налаштування записів DNS

На домашній сторінці HTTP-серверу розміщено відомості про тему та завдання на кваліфікаційну роботу. На рисунку 3.22 показано роботу HTTP-серверу та коректне відображення Web-сторінки з хоста віддаленої мережі по доменному імені.

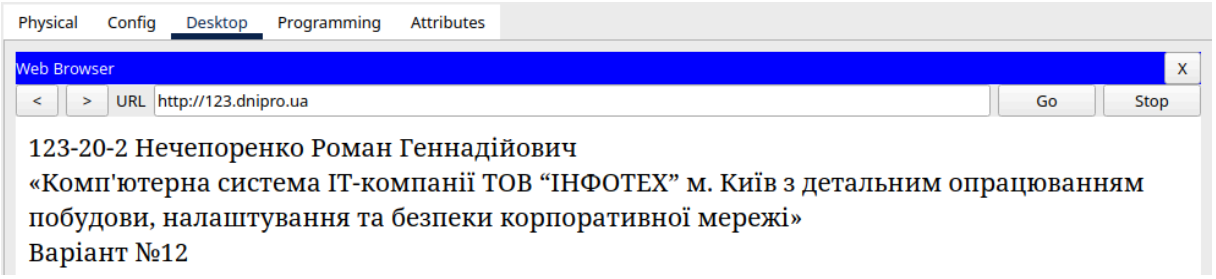

Рисунок 3.22 – Перевірка роботи HTTP-серверу

На рисунку 3.23 наведено таблицю підміни адрес NAT.

```
Necheporenko_R2#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.4     10.25.98.86        ---                ---
tcp 209.165.200.4:80   10.25.98.86:80     10.25.96.4:1025    10.25.96.4:1025
tcp 209.165.200.4:80   10.25.98.86:80     209.165.200.5:1025 209.165.200.5:1025
tcp 209.165.200.5:1025 10.25.97.132:1025  209.165.200.4:80   209.165.200.4:80

Necheporenko_R2#
```

Рисунок 3.23 – Таблиця адрес NAT

3.3.3.4 Налаштування маршрутизаторів на підтримку служби AAA

Cisco AAA (Authentication, Authorization, and Accounting) — це концепція та набір технологій, які використовуються для управління доступом до мережевих ресурсів, забезпечення безпеки та моніторингу активності користувачів. AAA є основоположною частиною мережевої безпеки і допомагає

гарантувати, що лише авторизовані користувачі мають доступ до відповідних ресурсів, а також, що їхні дії ретельно відстежуються.

Усі маршрутизатори у комп'ютерній мережі було налаштовано на підтримку служби AAA з наступною конфігурацією:

– Для доступу до ліній VTY використовується локальна база користувачів;
– Для доступу до консолі використовується RADIUS-сервер або, у випадку відсутності, локальна база користувачів;
– Ключове слово RADIUS-серверу: *radius123*;
– В якості облікового запису користувачів використано ім’я пристрою з паролем *admin123*;

На рисунку 3.24 наведено приклад налаштування служби AAA на маршрутизаторі Necheporenko_R4.

```
Necheporenko_R3(config)#aaa new-model
Necheporenko_R3(config)#aaa authentication login default local
Necheporenko_R3(config)#aaa authentication login Login group radius local
Necheporenko_R3(config)#line vty 0 4
Necheporenko_R3(config-line)#login authentication default
Necheporenko_R3(config-line)#exit
Necheporenko_R3(config)#line console 0
Necheporenko_R3(config-line)#login authentication Login
Necheporenko_R3(config-line)#exit
Necheporenko_R3(config)#radius-server key radius123
Necheporenko_R3(config)#radius-server host 10.25.98.87 auth-port 1645
Necheporenko_R3(config)#
```

Рисунок 3.24 – Налаштування маршрутизатора на підтримку служби AAA

У якості RADIUS-серверу було обрано DNS-сервер з мережі LAN 4, де знаходяться сервери підприємства. На рисунках 3.25 та 3.26 наведено налаштовані параметри RADIUS-серверу.

	Client Name	Client IP	Server Type	Key
1	Necheporenko_...	10.25.98.65	Radius	radius123

Рисунок 3.25 – Налаштування клієнтів служби AAA

	Username	Password
1	Necheporenko_R1	admin123
2	Necheporenko_R3	admin123
3	Necheporenko_R4	admin123

Рисунок 3.26 – Налаштування користувачів служби AAA

На рисунку 3.27 показано успішну авторизацію на маршрутизаторі Necheporenko_R3 за допомогою серверу AAA з обліковим записом *Necheporenko_R3* та паролем *admin123*. Після успішної авторизації в консолі можна побачити раніше встановлене банерне повідомлення.

```
123-20 Necheporenko. Password-protected access

User Access Verification

Username: Necheporenko_R3
Password:
Necheporenko_R3>en
Password:
Necheporenko R3#
```

Рисунок 3.27 – Авторизація через службу AAA

3.3.3.5 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec

Згідно з технічними вимогами до КС, між підмережами LAN 1 та віддаленою мережею LAN 3 було налаштовано віртуальну приватну мережу site-to-site VPN з використанням IPsec.

Першим чином, на маршрутизаторах Necheporenko_R2 (LAN 1) та Necheporenko_R5 (LAN 3) було налаштовано списки доступів з номером 100, які дозволяють вхідний трафік лише від адрес цих двох підмереж.

```
Necheporenko_R2(config)#access-list 100 permit ip 10.25.98.0 0.0.0.63 10.25.96.0 0.0.0.255
Necheporenko_R2(config)#
```

Рисунок 3.28 – Налаштування списку доступу для VPN

Наступним кроком було налаштовано параметри шифрування. В якості алгоритму шифрування було використано AES-256, а ключ - *cisco*. Аналогічні налаштування виконуються на обох маршрутизаторах.

```
Necheporenko_R2(config)#crypto isakmp policy 12
Necheporenko_R2(config-isakmp)#encryption aes 256
Necheporenko_R2(config-isakmp)#authentication pre-share
Necheporenko_R2(config-isakmp)#group 2
Necheporenko_R2(config-isakmp)#exit
Necheporenko_R2(config)#crypto isakmp key cisco address 64.100.13.2
Necheporenko_R2(config)#
```

Рисунок 3.29 – Налаштування параметрів шифрування VPN

Останнім кроком є налаштування IPsec.

```
Necheporenko_R2(config)#crypto ipsec transform-set VPN esp-aes 256 esp-sha-hmac
Necheporenko_R2(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Necheporenko_R2(config-crypto-map)#set peer 64.100.13.2
Necheporenko_R2(config-crypto-map)#set transform-set VPN
Necheporenko_R2(config-crypto-map)#match address 100
Necheporenko_R2(config-crypto-map)#exit
Necheporenko_R2(config)#int s0/1/0
Necheporenko_R2(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Necheporenko_R2(config-if)#
```

Рисунок 3.30 – Налаштування IPsec

Після налаштування перевіримо стан IPsec на маршрутизаторі Necheporenko_R2 командою *show crypto ipsec sa*.

```
Necheporenko_R2#sh crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: VPN-MAP, local addr 10.25.98.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.25.98.0/255.255.255.192/0/0)
   remote  ident (addr/mask/prot/port): (10.25.96.0/255.255.255.0/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.25.98.1, remote crypto endpt.:64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

Necheporenko_R2#
```

Рисунок 3.31 – Перевірка стану IPsec

3.3.4 Перевірка роботи комп'ютерної системи

Процес перевірки налаштування спроектованої корпоративної мережі заключається у перевірці роботи налаштованих служб та способів доступу. Перевіримо можливість підключення з хоста PC2/1 до маршрутизатора Necheporenko_R1 через SSH.

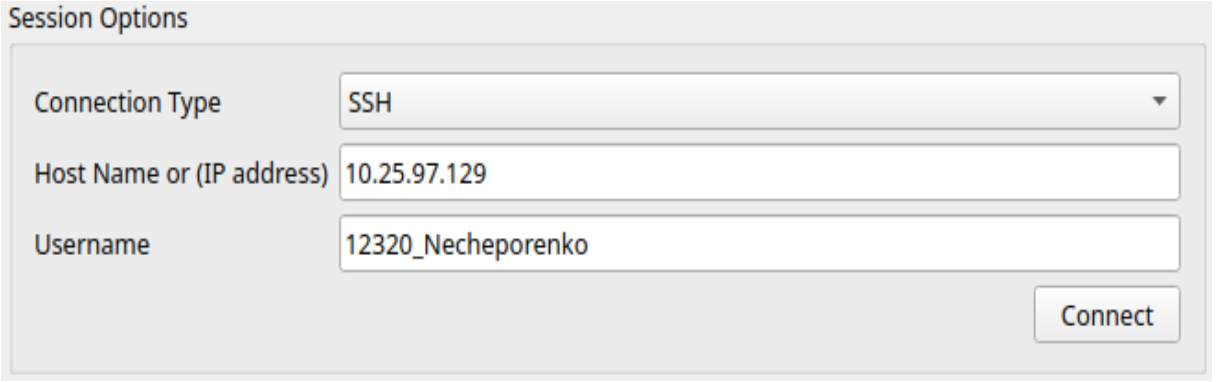

Рисунок 3.32 – Підключення за допомогою SSH клієнту

На рисунку 3.33 можна побачити, що після введення вірного паролю користувача ми отримали змогу зайти до привілейованого режиму Cisco IOS через SSH-з'єднання.

Рисунок 3.33 – Встановлення SSH-з'єднання

На рисунку 3.34 показано перевірку DNS-запису для доменного імені *123.dnipro.ua*, що призначений до зовнішньої адреси HTTP-серверу.

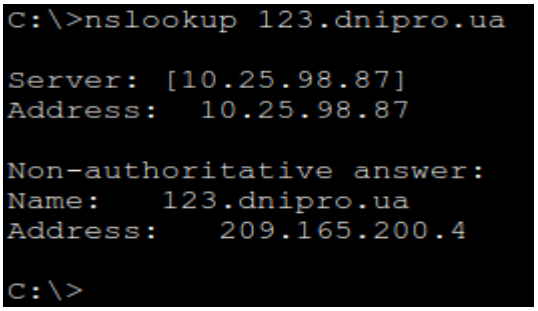

Рисунок 3.34 – Перевірка DNS-записів

За допомогою команди *ping* перевіримо зв’язок між хостами LAN 1 та LAN 3, між якими створено віртуальну приватну мережу.

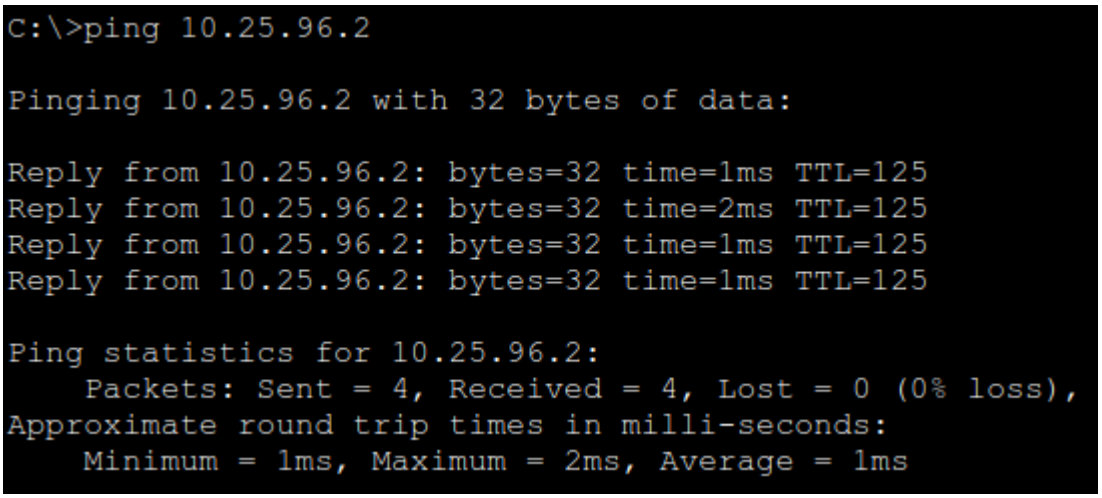

Рисунок 3.35 – Перевірка зв’язку між хостами через VPN

4 РОЗРОБКА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ

У офісі підприємства ТОВ «Інфотех» налаштовано систему Інтернету речей, що включає в себе комплекс розумних пристроїв та датчиків, які дозволяють автоматизувати певні процеси. Обмін даними та доступ до мережі забезпечується через бездротове з'єднання Wi-Fi. Управління та адміністрування пристроїв системи IoT здійснюється через веб-інтерфейс IoT-серверу.

4.1 Налаштування компонентів системи IoT

Система інтернету речей у мережі підприємства ТОВ «Інфотех» складається з наступних пристроїв та датчиків: датчик температури, датчик руху, лампи освітлення (4шт.), 2 кондиціонери та RFID-зчитувач для керування відкриванням дверей у серверну кімнату. Для зв'язку пристроїв встановлення бездротову точку доступу. Додатково для керування IoT-пристроями встановлено IoT-сервер та планшет, для віддаленого доступу до веб-інтерфейсу серверу.

Розумні пристрої системи Інтернету речей комунікують між собою по бездротовій технології Wi-Fi через спеціально налаштовану бездротову точку доступу, що знаходиться у мережі LAN 2.

Налаштування бездротової мережі на точці доступу наведено на рисунку 4.1.

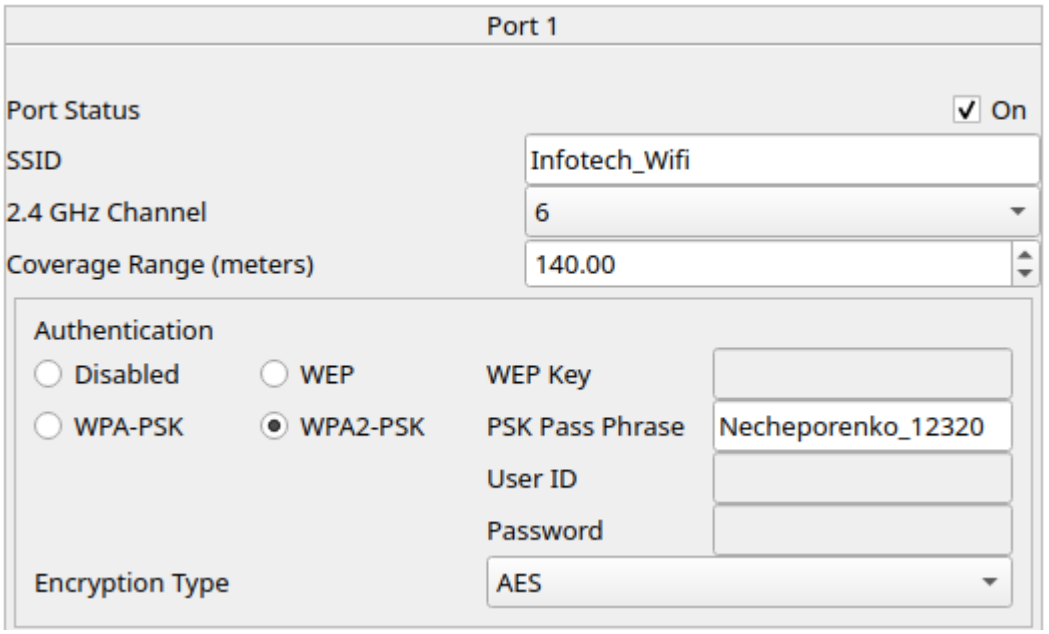

Рисунок 4.1 – Налаштування бездротової мережі

Для керування розумними пристроями та датчиками налаштовано IoT-сервер з IP-адресою 10.25.97.140. Через веб-інтерфейс серверу можна переглядати список підключених IoT-пристроїв, а також віддалено керувати ними або моніторити їхній стан та показники.

Для віддаленого керування IoT-пристроями через IoT-сервер у серверній кімнаті було встановлено планшет. Через веб-інтерфейс було створено користувача з ім’ям *admin* та паролем *admin12320*.

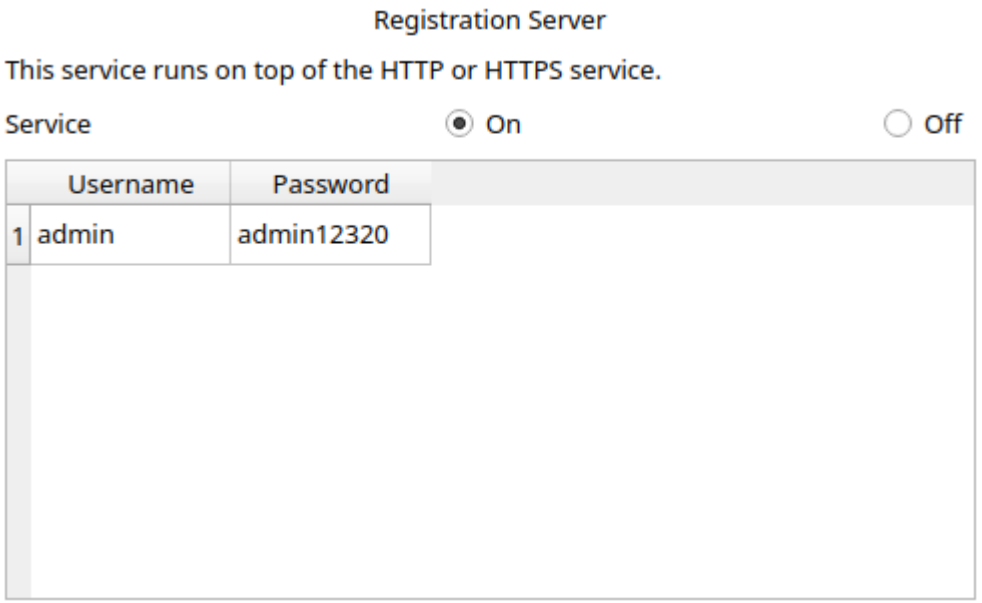

Рисунок 4.2 – База користувачів інтерфейсу IoT-пристроями

На кожному пристрої системи IoT були виконані базові налаштування мережі. Кожному з них задано статичну IP-адресу, параметри для підключення до бездротової мережі через точку доступу та параметри для підключення до IoT-серверу.

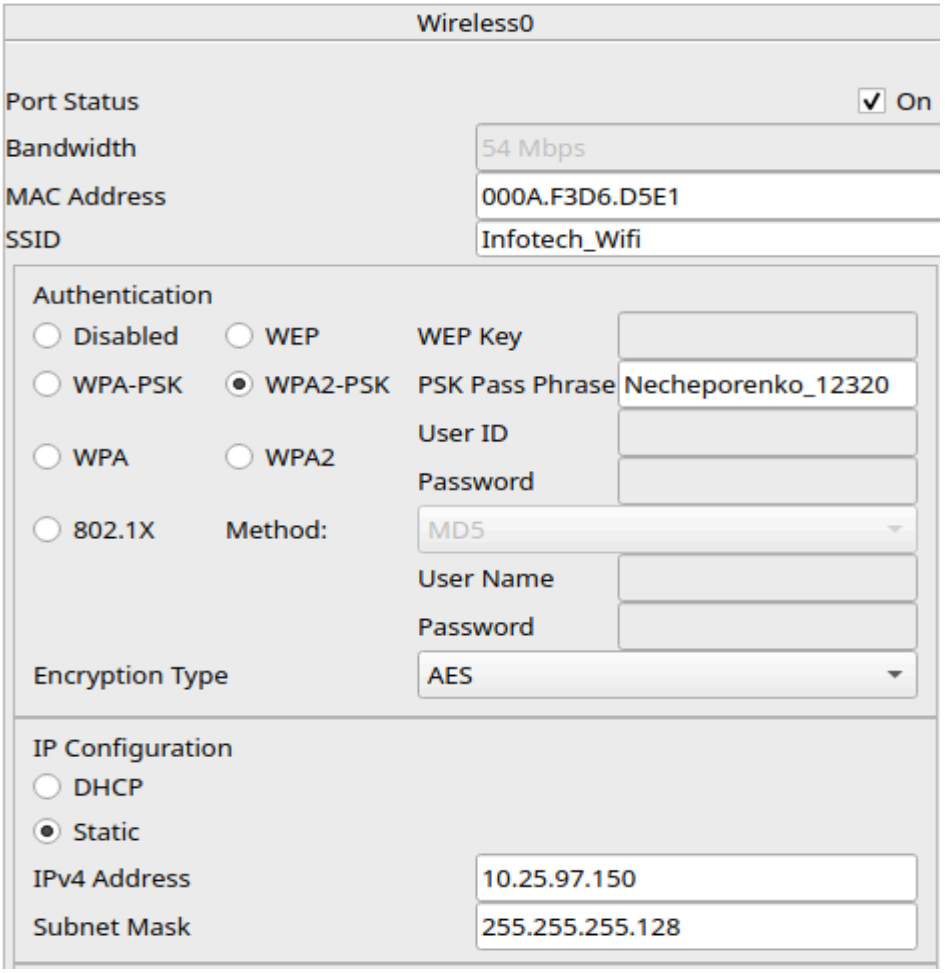

Рисунок 4.3 – Налаштування підключення до бездротової мережі

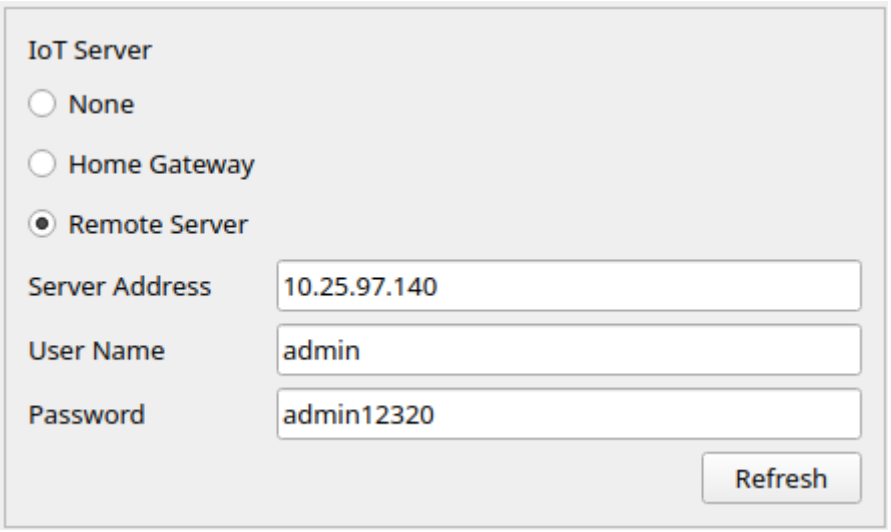

Рисунок 4.4 – Налаштування підключення до IoT-серверу

На рисунку 4.5 наведені список пристроїв, підключених до IoT-сервера, який можна переглянути підключившись до веб-інтерфейсу сервера.

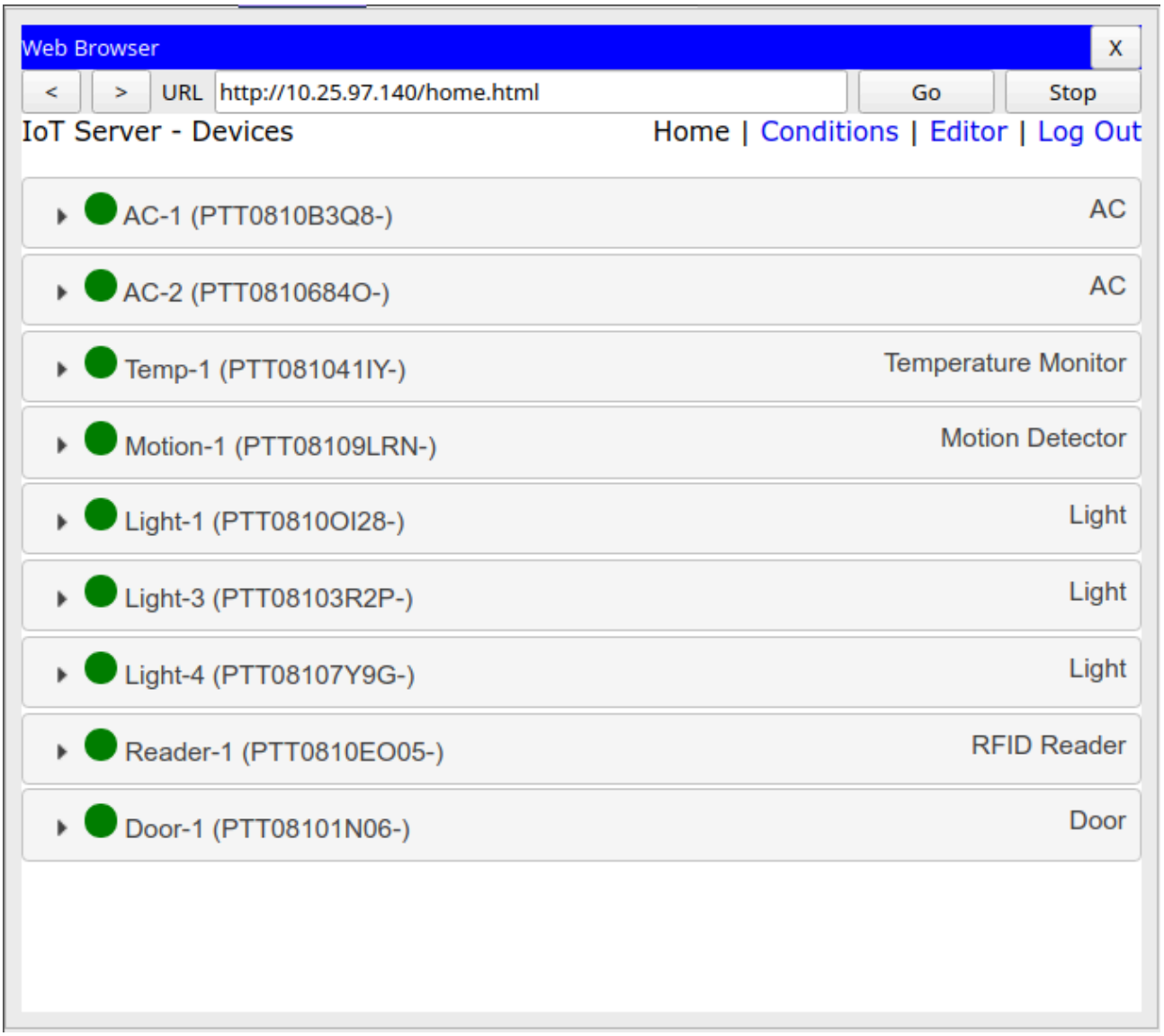

Рисунок 4.5 – Підключені IoT-пристрої

Через веб-інтерфейс IoT-серверу налаштовано наступні сценарії керування розумними пристроями:

– При температурі вище 26 градусів вмикаються два кондиціонери, а при падінні температури нижче 21 градуса - автоматично вимикаються;
– При виявленні руху біля вхідної двері в офіс у приміщенні автоматично вмикається освітлення;
– Доступ до серверної кімнати забезпечується через зчитування RFID-міток;

Налаштування сценаріїв керування IoT-пристроїв виконується через веб-інтерфейс IoT-сервера у вкладці Conditions. На даній вкладці є можливість задання умов, в яких можна використовувати параметри пристроїв та датчиків та логічні операції над ними. При істинному значенні такої умови, можна задати дію або зміну стану того чи іншого параметру IoT-пристрою.

Для автоматичного включення та виключення кондиціонерів у приміщенні було створено 2 умови, які засновуються на поточному значенні температури на термометрі Temp-1: при падінні температури нижче 21 градуса вмикаються кондиціонери AC-1 та AC-2, а при значенні датчику вище 26 - вимикаються.

Для автоматичного освітлення приміщення створено 2 умови, які базуються на значенні датчику руху Motion-1: при наявності руху, ліхтарі Light-1-4 автоматично включаються, а при відсутності - вимикаються.

Для доступу до серверної кімнати по RFID-мітках було налаштовано RDIF-зчитувач, який контролює відчинення двері у кімнату. Двері відкриваються тільки при зчитуванні картки з ID від 1 до 100. Для відтворення цього сценарію було створено 2 умови.

Усі сценарії керування пристроями Інтернету речей з відповідними логічними умовами наведені на рисунку 4.6.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	AC_On	Temp-1 Temperature > 26.0 °C	Set AC-1 On to true Set AC-2 On to true
Edit Remove	Yes	AC_Off	Temp-1 Temperature < 21.0 °C	Set AC-1 On to false Set AC-2 On to false
Edit Remove	Yes	Lights_On	Motion-1 On is true	Set Light-1 Status to On Set Light-2 Status to On Set Light-3 Status to On Set Light-4 Status to On
Edit Remove	Yes	Lights_Off	Motion-1 On is false	Set Light-1 Status to Off Set Light-2 Status to Off Set Light-3 Status to Off Set Light-4 Status to Off
Edit Remove	Yes	Door_Unlock	Reader-1 Card ID is between 1 and 100	Set Door-1 Lock to Unlock
Edit Remove	Yes	Door_Lock	Match any: • Reader-1 Card ID < 1 • Reader-1 Card ID > 100	Set Door-1 Lock to Lock

Рисунок 4.6 – Умови сценаріїв керування IoT-пристроями

Для зручності підключення до IoT-сервера для налаштувань пристроїв на планшеті Tablet-IoT було задано адресу DNS-серверу, на якому у свою чергу було налаштовано A-запис з доменним ім’ям *iot.infotech.ua*, що посилається на адресу IoT-серверу.

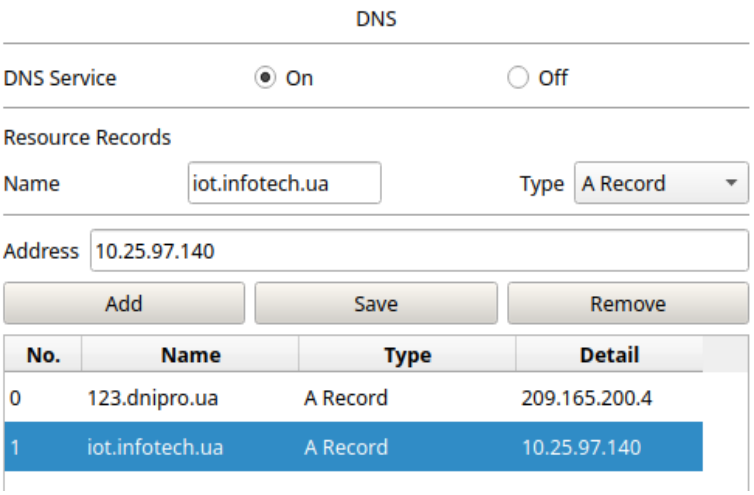

Рисунок 4.7 – Створення DNS-запису для IoT-серверу

На рисунку 4.8 наведено результат завантаження веб-інтерфейсу IoT-серверу при підключенні до заданого доменного імені.

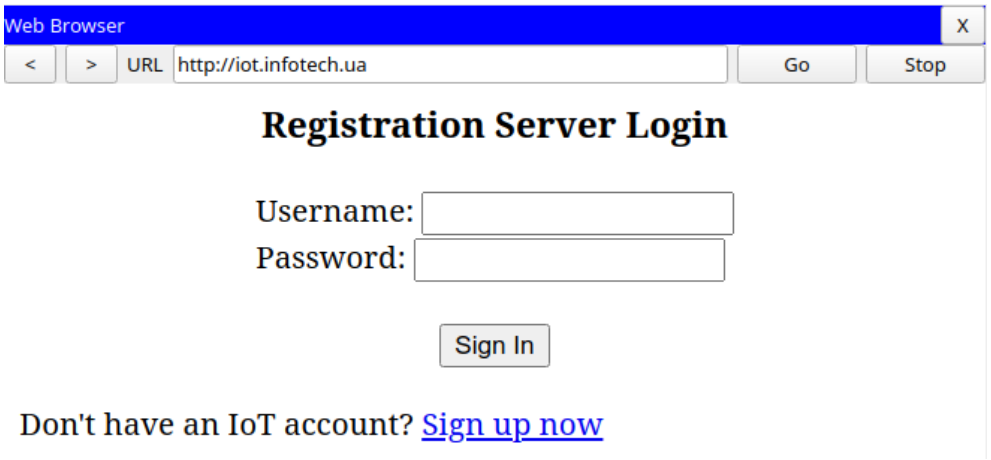

Рисунок 4.8 – Підключення до IoT-серверу через доменне ім’я

ВИСНОВКИ

У кваліфікаційній роботі бакалавра був розроблений проект корпоративної мережі підприємства ТОВ «ІНФОТЕХ», основуючись на аналізі вимог та завдань. У відповідності з архітектурою мережі та виконуваними функціями вузлів мережі було підібрано мережеві пристрої фірми Cisco, що задовольняють технічним вимогам мережі.

У роботі була розроблена мережева модель, що задовольняє всі вимоги та потреби підприємства щодо передачі та зберігання інформації. Розроблено схему адресації вузлів у мережі, а також виконано налаштування мережевих пристроїв, згідно технічним вимогам підприємства. Виконано перевірку комп'ютерної мережі у середовищі Cisco Packet Tracer.

ПЕРЕЛІК ПОСИЛАНЬ

1. Цвіркун Л.І. 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», 2024. - 63 с.
2. Навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Київ, 2020. – 336 с.
3. Жуков, І. А. Комп’ютерні мережі і технології : навч. посіб. для вузів [Текст] / І. А. Жуков, В. О. Гуменюк, І. Є. Альтман. – К. : НАУ, 2004. – 276 с.
4. Журавська І. М. Проектування та монтаж локальних комп’ютерних мереж [Навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.
5. Комп’ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с.
6. Жидецький, В. Ц. Охорона праці користувачів комп’ютерів [Текст] / В. Ц. Жидецький. – Львів : Афіша, 2000. – 176 с.
7. VLSM Calculator [Електронний ресурс]. Режим доступу : URL: https://vlsmcalc.vercel.app
8. RFC 1517. Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR) [Електронний ресурс]. – Режим доступу : URL : www.ietf.org/rfc/rfc1517.txt
9. RFC 1918. Address Allocation for Private Internets [Електронний ресурс]. – Режим доступу : URL : www.rfc-editor.org/rfc/rfc1918.txt
10. RFC 3330. Special-Use IPv4 Addresses [Електронний ресурс]. - Режим доступу : URL : www.rfc-editor.org/rfc/rfc3330.txt

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ

Текст програми
04.02070743.24012-01 12 01

Листів Х

2024

АНОТАЦІЯ

Дана програма містить частину налаштувань мережевого обладнання за допомогою Cisco IOS для компонентів корпоративної мережі підприємства ТОВ «ІНФОТЕХ». Програма призначення для налаштування протоколу динамічної маршрутизації, роботи сервісів AAA та DHCP, налаштування інтерфейсів пристроїв та налаштування роботи Internet.

ЗМІСТ

```
!
version 15.1
no service timestamps log datetime
msec
no service timestamps debug datetime
msec
service password-encryption
! hostname Necheporenko_R4
!
!
!
enable secret 5
$1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
aaa new-model
!
aaa authentication login Login group
radius local
aaa authentication login default local
!
!
!
!
!
!
!
ip cef no ipv6 cef
!
!
!
username 12320_Necheporenko
password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn
FTX152441N8-
!
!
!
!
!
!
!
!
ip domain-name Necheporenko_R4
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface GigabitEthernet0/0
```

```
ip address 10.0.12.17 255.255.255.252
duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 bandwidth 128
 ip address 10.0.12.1 255.255.255.252 !
interface Serial0/0/1
 bandwidth 128
 ip address 10.0.12.5 255.255.255.252 !
interface Serial0/1/0
 bandwidth 128
 ip address 10.0.12.9 255.255.255.252 !
interface Serial0/1/1
 bandwidth 128
 ip address 10.0.12.13 255.255.255.252
!
 interface Vlan1
 no ip address
 shutdown
!
router eigrp 12
 redistribute static
 network 10.0.12.0 0.0.0.3
 network 10.0.12.4 0.0.0.3
 network 10.0.12.16 0.0.0.3
 network 10.0.12.8 0.0.0.3
 network 10.0.12.12 0.0.0.3
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
!
!
banner motd #123-20 Necheporenko.
Password-protected access#
!
radius server 10.25.98.87
 address ipv4 10.25.98.87 auth-port
1645
!
line con 0
 password 7 0822455D0A16
 login authentication Login
!
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
```

```
!
version 15.0
no service timestamps log datetime
msec
no service timestamps debug datetime
msec
service password-encryption
!
hostname Necheporenko_SW4
!
enable secret 5
$1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
ip domain-name Necheporenko_SW4
!
username 12320_Necheporenko
privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
```

```
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #123-20 Necheporenko.
Password-protected access#
!
!
!
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
```