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

Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавр

студента Байдака Леоніда Васильовича
(ПІБ)
академічної групи 123-16-1
(шифр)
галузь знань: 123 «Комп'ютерна інженерія»

напрям підготовки: 123 «Комп'ютерна інженерія»

на тему «Комп'ютерна система аутсорсингового приватного підприємства "ThinkServe" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»

(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
розділів:				
Розробка апаратної частини	доц. Ткаченко С.М.			
визначення моделі обєкта	ас. Панферова Я.В.			
Економічний розділ	ст. викл. Яремчук І.О			
Охорона праці	доц. Іконніков М.Ю			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних систем
та технологій
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

«_____»_____2020року

ЗАВДАННЯ
на кваліфікаційну роботу
бакалавра

студенту Байдаку Л.В. **академічної групи** 123-16-1
(прізвище та ініціали) (шифр)

галузь знань: 123 «Комп'ютерна інженерія»

напрям підготовки: 123 «Комп'ютерна інженерія»
(офіційна назва)

на тему «Комп'ютерна система аутсорсингового приватного підприємства "ThinkServe" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 21.05.2020 р. №771-л

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи	18.05.2020
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи	25.05.2020
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи з опрацюванням побудови і захисту інформації та налаштуванням корпоративної мережі	01.06.2020
Економічна частина	Економічно обґрунтувати доцільність витрат на створення та дослідження системи	08.06.2020
Охорона праці	Розробити організаційно-технічні заходи, щодо реалізації правил безпеки при експлуатації системи	15.06.2020

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

Дата видачі 27.01.2020

Дата подання до екзаменаційної комісії 16.06.2020

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

РЕФЕРАТ

Пояснювальна записка: 68 с., 17 рис., 11 табл., 1 додаток., 10 джерел.

Об’єкт дослідження: комп’ютерна система аутсорсингового приватного підприємства “ThinkServe” з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета проекту: розробка локальної мережі для приватного аутсорсингового підприємства.

Розроблена комп'ютерна система з запасом потужності, можливістю гнучкого горизонтального та вертикального розвитку. Система орієнтована для використання в компанії, котра займається аутсорсингом.

Завдяки виконанню роботи було досліджено сучасні тенденції в проектуванні комп’ютерних мереж, враховані вимоги до претендентів на робочі місця за спеціальностями “System administrator”, “DevOps engineer”.

Необхідність розробленої системи обумовлена вимогами замовника до гнучкої, розширюваної, безпечної та стійкої до зовнішніх загроз мережі.

Систему було побудовано з використанням мережевого обладнання Cisco – одного зі світових лідерів у галузі розробки та забезпечення комп'ютерних систем.

Розроблена мережа була імплементована у вигляді моделі з використанням програмного забезпечення “Cisco Packet Tracer”.

Розраховано річний економічний ефект та термін окупності при введенні в експлуатацію розробленої системи управління та режимів роботи. Розглянуто комплекс питань що до охорони праці.

СИСТЕМА, МЕРЕЖА, АУТСОРСИНГ, CISCO, ПІДПРИЄМСТВО

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНІ І ТЕРМІНІВ

ПЗ — програмне забезпечення;

AI — Artificial Intelligence;

ОС — операційна система;

IT — Information technology;

КР — кваліфікаційна робота;

ПК — персональний комп’ютер;

UI — User Interface;

ВСТУП

Зараз відбувається так звана «Четверта промислова революція» — поняття, що означає розвиток і злиття автоматизованого виробництва, обміну даних і виробничих технологій в єдину саморегульовану систему, з мінімальним або взагалі відсутнім втручанням людини у виробничий процес.

Термін був визначений як «збірне поняття для технологій і концепцій організації ланцюжка створення додаткової вартості» із використанням кіберфізичних систем, Інтернету речей, Інтернету послуг, Розумних заводів. Фаза промислової революції, яка характеризується злиттям технологій, що розмиває межі між фізичною, цифровою та біологічною сферами[1]. Завдяки цьому має місце бурхливий розвиток майже всіх аспектів промисловості, зокрема – ІТ-галузі. Щодня створюються нові робочі місця, з’являються та зникають стартапи, технології. Мережні технології – не виключення. Навпаки, цей напрям має чи не найстрімкіший розвиток.

Створення комп'ютерних мереж було обумовлено прагненням до економії ресурсів. Правильно спроектована комп'ютерна мережа повинна забезпечувати – колективне опрацювання даних користувачами, комп'ютери яких під'єднані до мережі, та обмін даними між цими користувачами; спільне використання програм; спільне використання принтерів, модемів та інших периферійних пристроїв.

Перед сучасним комп’ютерним інженером стоїть нелегка задача – як розробити гнучку, розширювану, безпечну та стійку до зовнішнього випливу систему? Які обрати технології та апаратне забезпечення? Чи є доцільним слідування новітнім тенденціям, або ж краще опиратись на перевірені рішення? Ці та інші питання постають перед спеціалістами під час розробки комп’ютерної мережі.

В ході роботи була розроблена та змодельована комп’ютерна системи для підприємства, котре займається розробкою програмного забезпечення в якості

підрядника. Створено топологія локальної мережі, враховано можливість виходу в Інтернет, опираючись на вимоги замовника щодо масштабу мережі та перспективи її подальшого розширення і розвитку.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Галузь промисловості

Основним напрямом української IT-галузі станом на 2020 рік є аутсорсингова розробка програмного забезпечення. Роль аутсорсингових постачальників у сфері високих технологій перейшла від ручної праці до верхніх рішень щодо архітектури програмного забезпечення та розробки продукту повного циклу.

Станом на 2019 рік кількість зайнятих спеціалістів в українському IT досягла позначки 190 тисяч, що складає приблизно $4,7 млрд . Україна є лідером серед країн — аутсорсерів в Європі. На думку українських фахівців, 90% наших IT-спеціалістів працюють саме на засадах аутсорсингу, а не як розробники власних IT-продуктів, себто близько 171 тисячі працівників. За статистикою 94% клієнтів повністю задоволені рівнем українського сервісу, тоді як в кращих іноземних компаній цей показник становить лише 84%. Це пояснюється, зокрема, тим, що 72% українських провайдерів активно займаються інноваціями. За даними Gartner, Україна посідає 1-ше місце у Східній Європі за співвідношенням “ціна — якість”.

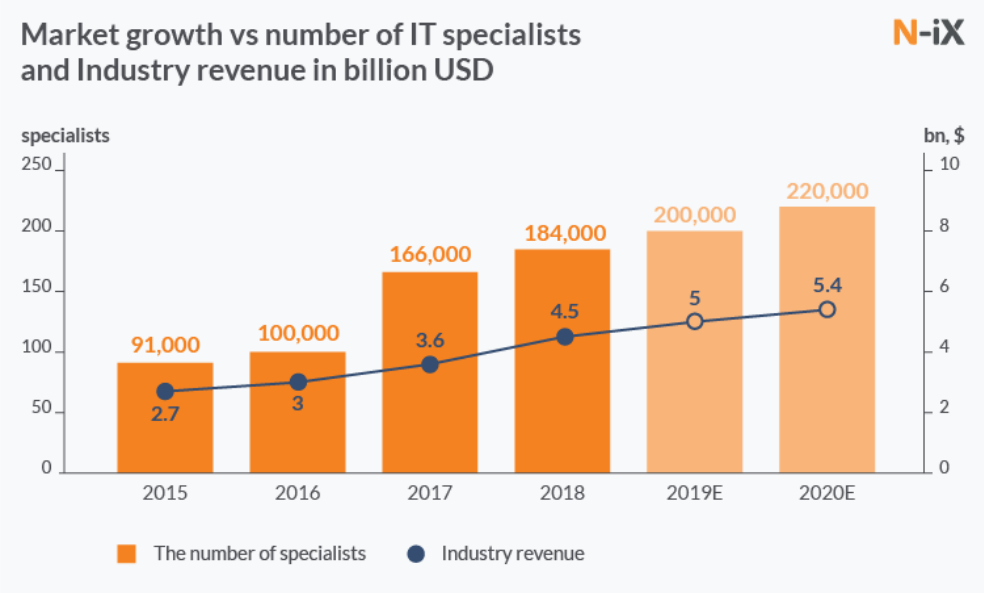

Рисунок 1.1 – Український IT-ринок станом на 2020 рік[2].

Найбільшими IT-компаніями в Україні, котрі займаються здебільшого аутсорсинговою розробкою є SoftServe, Epam-Ukraine, GlobalLogic, Luxoft, Ciklum. В місті Дніпро присутні як окремі департаменти цих гігантів (наприклад, три відділення SoftServe, офіси Epam та Luxoft), так і локальні IT-компанії - Yalantis, Cleveroad, LANARS, Giraffe та інші.

Звісно, теперішня епідеміологічна ситуація, викликана вірусом COVID-19, та криза, спричинена нею, призупинила бурхливий розвиток українського аутсорсингу. Згідно кризовій аналітиці DOU, «у травні опубліковано 3500 вакансій на jobs.dou.ua. Це на 17% більше, ніж у квітні, але на 21% менше, ніж у березні 2020-го. Якщо порівнювати з минулим роком, то цього травня розміщено на третину менше позицій, ніж торік. Ця різниця приблизно така сама, як у квітні. А позитивна динаміка травня до квітня спостерігалася і в попередні роки. Ринок усе ще тримається на рівні 2017 року.[3]»

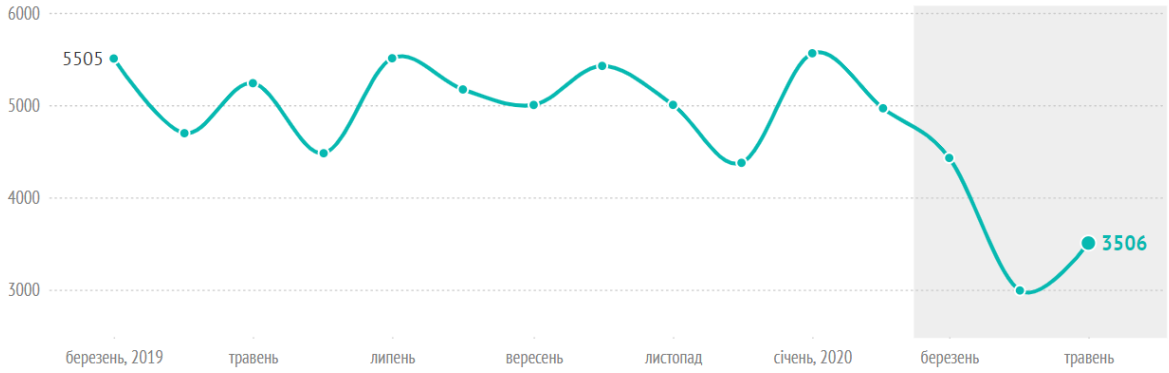

Рисунок 1.2 – Загальна кількість вакансій на jobs.dou.ua з березня 2019-го по травень 2020-го [3].

Але все-ж напрям IT-аутсорсингу залишається найбільш перспективним в галузі.

1.2 Стан питання і постановка завдання

Приватне підприємство “ThinkServe” є аутсорсинговою компанією, котра займається господарською діяльністю в сфері розробки програмного забезпечення. На підприємстві базується декілька підрозділів, а саме: Менеджмент, Web-UI розробка (за допомогою мови програмування JS, а також окремих фреймворків — Vue та React), Ентерпрайз розробка на Java, Artificial Intelligence розробка, IT – Академія, Бухгалтерія, відділ HR.

Першочерговими замовниками є продуктові компанії зі Сполучених Штатів Америки. Після обговорення деталей між замовником та менеджментом, проект потрапляє до відповідального Program Manager. У підпорядкуванні Program Manager є декілька команд розробників спеціалізованого профілю, кожна з власним Project Manager-ом. Така організація процесу розробки дозволяє забезпечити декілька вагомих переваг. По-перше — гнучкість(тобто можливість пристосуватись до динамічних умов ринку). По друге — синегрію між різними командами, що дозволяє розподілити функціональні обов’язки. По-третє — мінімізація ризиків для клієнта, котрому гарантується виконання поставленої задачі у визначений термін. Загальноприйнятим стандартом в компанії є використання методології гнучкої розробки Scrum, тому в кожній команді є свій Scrum-master. Всі можливі правки та побажання представника замовника надходять до відповідального менеджера. Задля запровадження ефективної взаємодії, слід забезпечити спілкування пристроїв один з одним.

Human Resources відділ займається пошуком працівників, організацією необхідних співбесід, як-то технічна співбесіда чи інтерв’ю для визначення рівня володіння англійською мовою.

Також в компанії базується IT-Академія, котра дозволяє формувати кваліфіковані робочі кадри, замість того щоб приваблювати їх іззовні. Основна частина людей, котрі проходять навчання в IT-Академії, являє собою студентів ВНЗ технічних спеціальностей.

Через велику кількість роботи і продукуючих даних було прийнято рішення відмовитися від хмарного зберігання даних. Замість цього краще використати 6 серверів: по одному серверу на відділ Ентерпрайз-Java, Web-UI, AI розробки, один сервер для молодих спеціалістів, які будуть проходити стажування в IT – Академії, один сервер для менеджменту, HR та бухгалтерії, один спільний DNS сервер. Задля більшої безпеки потрібно використані ACL списки, щоб кожний відділ мав доступ тільки до свого серверу. Все це надасть підприємству більш оперативний прийом замовлень, підвищення продуктивності праці за рахунок більш ефективної взаємодії співробітників, скорочення ризиків витоку приватної інформації.

Згідно з всіма перерахованими задачами і умовами роботи, компанії “ThinkServe” необхідно орендувати 8 офісних приміщень: 7 офісів і 1 підвальне приміщення, де буде знаходитися серверна кімната.

В побудові мережі було вирішено використовувати обладнання Cisco. Головними аргументами такого рішення були надійність та відмовостійкість обладнання данного виробника.

Для вирішення поставлених завдань потрібно вирішити, який протокол динамічної маршрутизації буде використано, які відділи мають бути захищені та яким способом, як буде організовано роботу з провайдером.

Для маршрутизації буде використано пропрієтарний протокол EIGRP – вдосконалений дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco. Цей протокол простий в налаштуванні і показує швидку роботу на малих мережах, тому він ідеально підходить для даного підприємства.

Серверна кімната повинна бути захищенною від несанкціонованого доступу за допомогою технології ACL (Access Control List) — це набір текстових виразів, які щось дозволяють, або щось забороняють. Зазвичай ACL

дозволяє або забороняє IP-пакети, але крім усього іншого він може заглядати всередину IP-пакета, переглядати тип пакету, TCP і UDP порти.

Відділи Менеджменту, Бухгалтерії, HR будуть розташовані в сусідніх кімнатах і їхнє зростання не буде значним, тому на ці 3 відділи буде доцільним використання одного комутатора з підключеною технологією VLAN (Virtual Local Area Network) – логічна («віртуальна») локальна комп'ютерна мережа, представляє собою групу хостів із загальним набором вимог, які взаємодіють так, як якщо б вони були підключені до широкомовного домену, незалежно від їх фізичного місцезнаходження. Також на цьому комутаторі буде підключена технологія DHCP для коректного розподілу IP – адрес в мережах VLAN. DHCP – мережевий протокол, що дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP / IP.

Кожен виділений сектор являє собою open space офіс приблизно на 20 робочих місць.

ОРГАНІЗАЙЦІНА СТРУКТУРА «ThinkServeInc.»

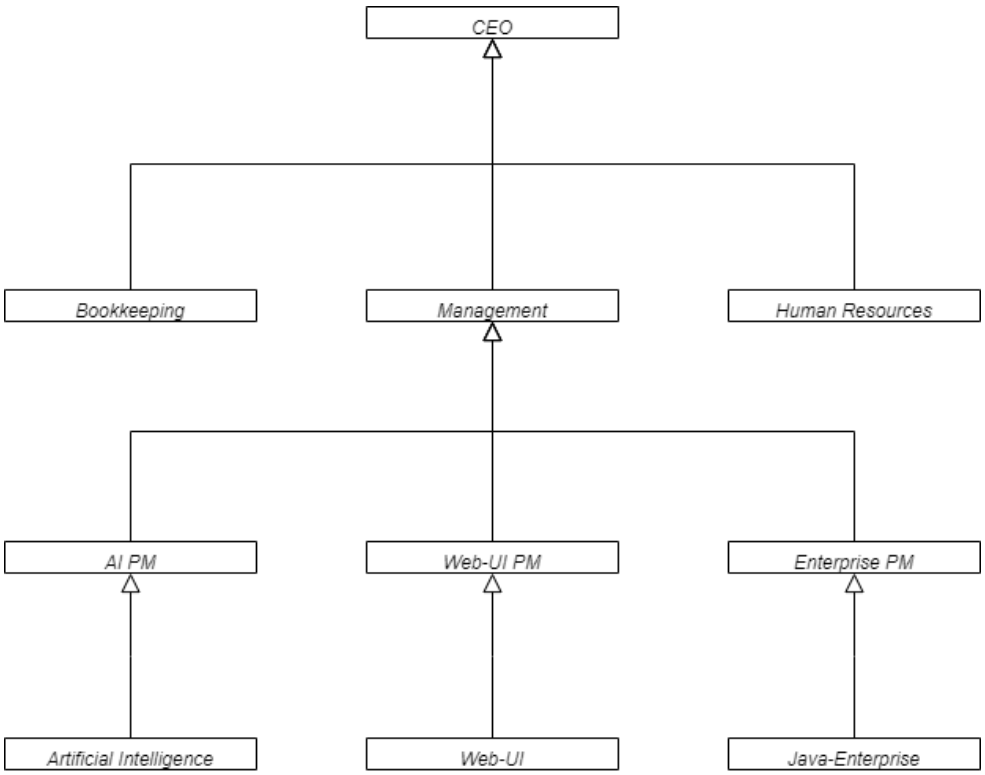

Рисунок 1.3 – Структурна схема підприємства

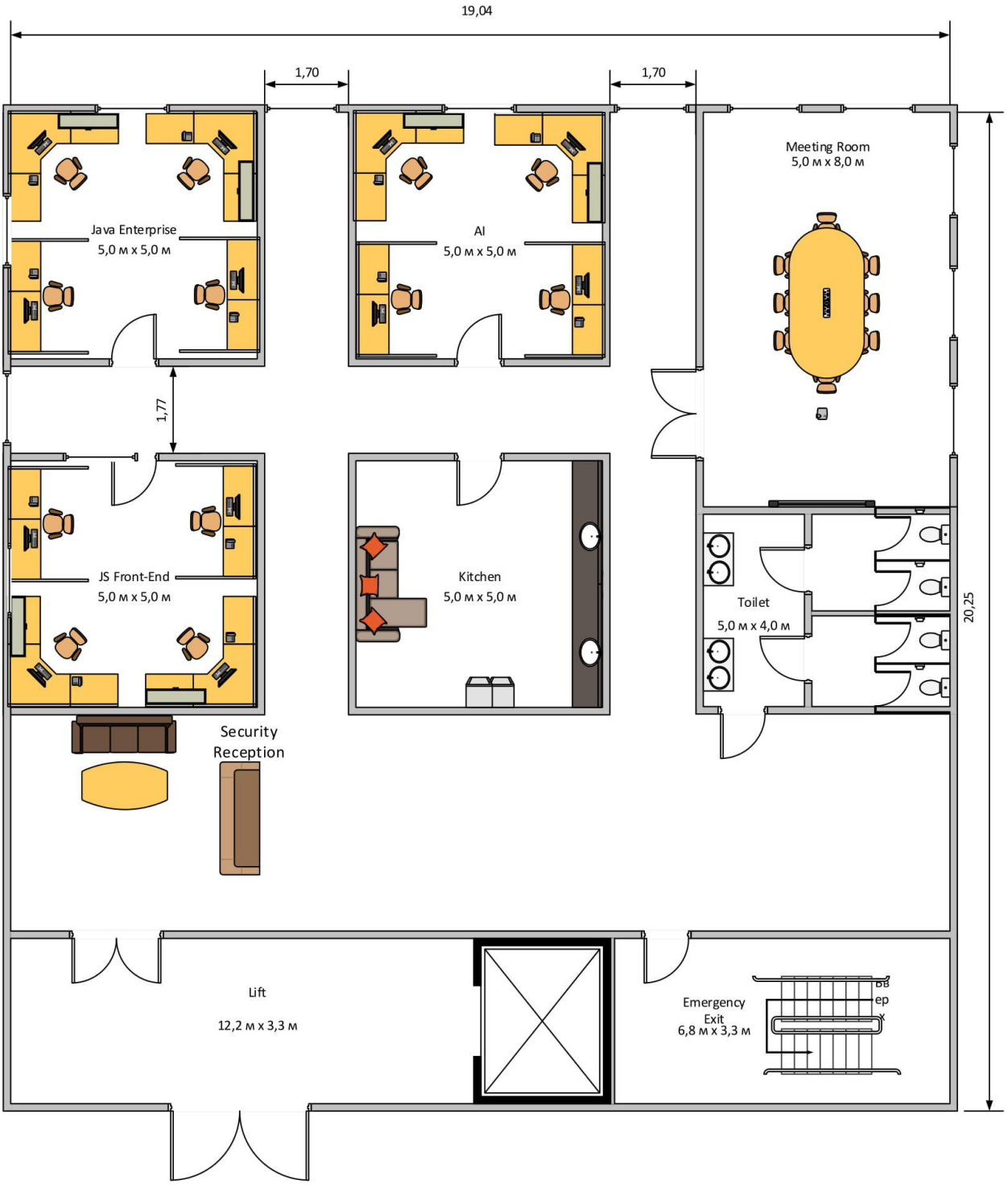

Рисунок 1.4 – План першого поверху

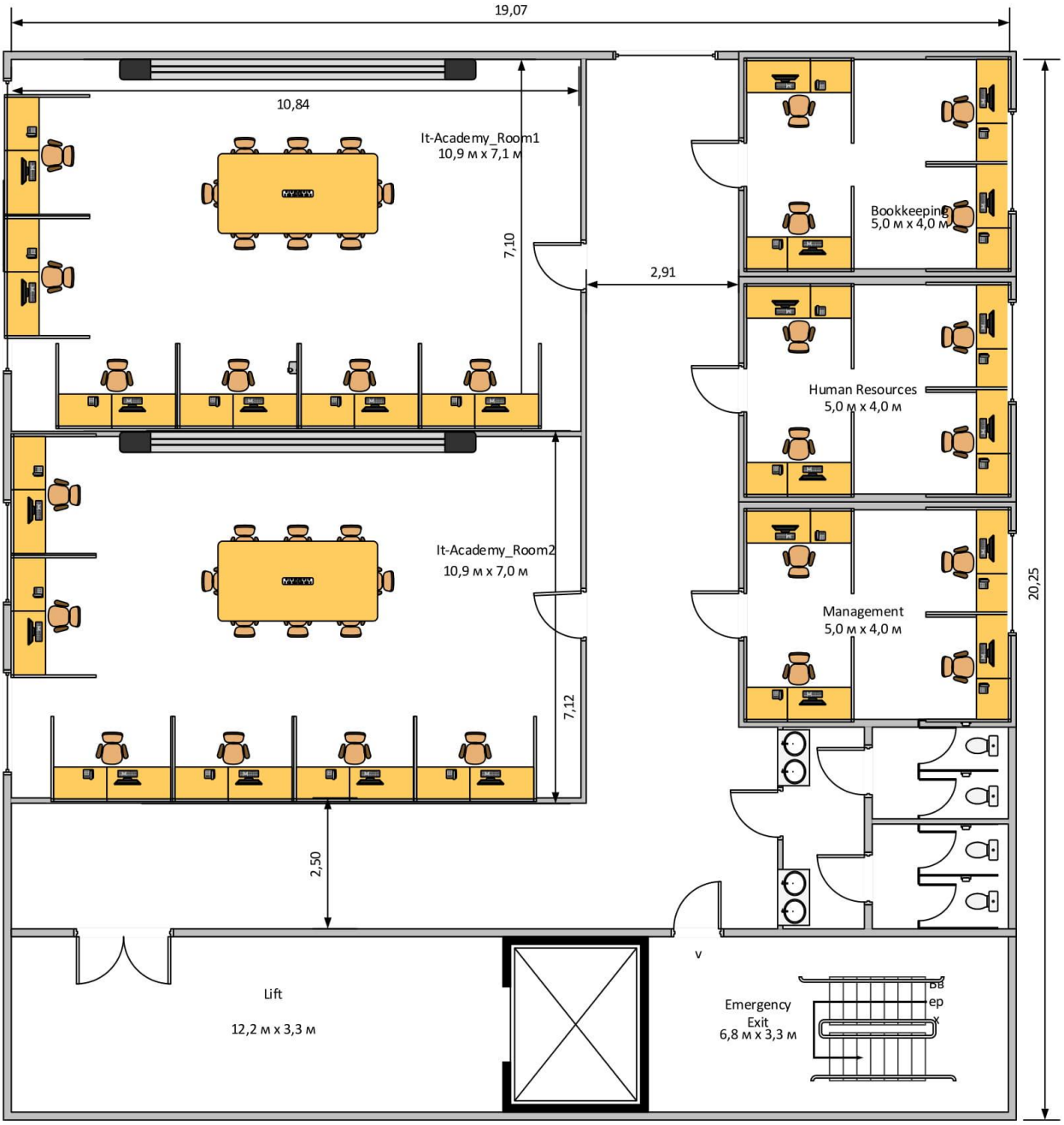

Рисунок 1.5 – План другого поверху

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Вимоги до системи в цілому

2.1.1 Вимоги до структури і функціонування мережі

В рамках створення комп'ютерної мережі для аутсорсингової компанії, повинні бути розроблені наступні ключові підсистеми:

- підсистема відділу менеджмента;
- підсистема HR відділу;
- підсистема відділу Web-UI;
- підсистема Java-enterprise;
- підсистема відділу AI.
- підсистема IT-Академії;

Підсистема менеджменту призначена для створення взаємодії з замовником, розподілу ресурсів.

Підсистема HR-відділу створена для управління працівниками, їх наймом.

Підсистема відділу Java-enterprise призначена для розробки великих enterprise проектів.

Підсистема Web-UI відділу призначена для розробки front-end частини застосунків.

Підсистема відділу Artificial Intelligence створена для проектів створених на основі Machine Learning.

Підсистема IT-Академії призначена для створення повноцінних робочих кадрів.

Система повинна мати ієрархічну структуру управління. Зокрема дирекція має доступ до всіх ресурсів системи, а підпорядковані системи мають повний доступ до ресурсів, необхідних для роботи безпосередньо в конкретному відділі. Доступ до створюваних підсистем мережі користувачами повинен отримуватись з автоматизованих робочих місць на базі персональних комп'ютерів, ноутбуків або мобільних пристроїв, підключених до мережі.

Передача інформації між компонентами системи має виконуватись стандартними протоколами на рівні програмного забезпечення або на рівні платформи. Зв'язок між системами реалізований у вигляді передачі інформації через локальну мережу, засоби телефонного зв'язку та електронну пошту.

Безперервне повноцінне функціонування відповідно до заявленого фунціоналу. Серверні програмно-технічні засоби повинно функціонувати у цілодобовому режимі із заздалегідь визначеними періодами регламентного обслуговування, без необхідності зупинки її роботи для проведення планового регламентного технічного обслуговування під час робочого дня.

Експлуатація повинна передбачати такі режими:

- Основний режим – режим штатного функціонування всіх програмних компонентів за своїм призначенням.
- Нештатний режим – режим нештатного функціонування всіх програмних модулів / компонентів, наприклад, недоступність даних серверу.
- Режим адміністрування – режим здійснення централізованого автоматизованого налагоджування та автоматизованого оновлення програмних модулів / компонентів.
- Режим регламентного обслуговування – режим регламентного технічного обслуговування та відновлення працездатності технічних засобів програмних модулів / компонентів .

При розробці системи передбачена можливість її подальшої модернізації та масштабування при мінімальних затратах часу у випадку необхідності додавання нових користувачів системи в конкретну підсистему; прискорення роботи системи шляхом нарощування обчислювальних потужностей у разі збільшення навантаження. Нові робочі місця ЛВС повинні бути інтегровані в існуючу мережу і максимально використовувати наявні, власні, орендовані ресурси.

2.1.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує мережу і режиму його роботи.

Запропоновані рішення створення системи будуть вимагати не менш ніж 2-х фахівців з певною роллю та відповідним рівнем підготовки, які повинні забезпечувати:

- безперервне супроводження на всіх стадіях експлуатації та підтримки;
- необхідний режим роботи мережі за призначенням в повному обсязі;
- централізований контроль працездатності мережі;
- усунення відмов роботи мережі та її компонентів;
- адміністрування (оперативне налагодження під час експлуатації) роботи мережі;
- своєчасне централізоване застосування оновлень програмного забезпечення.

2.1.3 Вимоги до показників призначення

Мережа в цілому повинна відповідати категорії не нижче 5Е, всі комплектуючі (кабель, розетки, комутаційні панелі, з'єднувальні шнури) повинні відповідати категорії не нижче 5Е. Інформаційна кабельна підсистема

повинна будуватися відповідно до вимог стандарту ISO / IEC 11801 Class D, категорія 5E. Для створення мережі необхідно використовувати тільки високоякісні компоненти, які пройшли стовідсоткове тестування відповідно до вимог ISO 9001 (ГОСТ 40.9001-88).

2.1.4 Вимоги до надійності

Збереження працездатності повинно забезпечуватись надійністю роботи при відмові одного або декількох компонентів за рахунок їх резервування. При цьому повинна вимагатися мінімальна увага з боку адміністратора щодо реакції на усунення наслідків відмов компонентів. Збереження даних повинно забезпечуватись програмно-апаратними засобами та механізмами обміну інформації.

Надійність повинна бути забезпечена за наступними напрямками:

- забезпечення працездатності;
- збереження даних.

Надійність повинна забезпечуватись за рахунок:

- використання сучасних технологій розробки та забезпеченням якісного тестування;
- резервуванням компонентів та їх елементів;
- режиму автоматичного аналізу поточного стану (в реальному стані) та відновлення працездатності у відповідності до регламенту відновлювальних робіт;
- організації систематичного резервного копіювання та архівного збереження інформації;
- апаратно-програмним захистом роботи від стороннього несанкціонованого програмно-апаратного втручання;

- оперативністю заміни програмно-технічних засобів, що вийшли з ладу;
- сумісністю технічних засобів та програмного забезпечення.

2.1.5 Вимоги безпеки

Під час монтажу та експлуатації ліній мережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією . Усі кабелі обов'язково закриваються пластиковими коробами, а мережеве обладнання встановлюється у виключно відведеному для нього місці.

Забороняється працювати з обладнанням особі, яка не вивчила правила безпеки, встановлені на даному об'єкті. Перед початком монтажу апаратури технічне приміщення повинно бути повністю підготовлено до роботи, звільнено від залишків будівельних матеріалів, повинно бути перевірено захисне заземлення. Виправлення пошкоджень, установку і заміну блоків і плат, заміну запобіжників дозволяється проводити тільки при повному знятті напруги. Під час роботи обладнання забороняється доступ до внутрішніх частин обладнання, розташованим під захисними накладками, які знімаються за допомогою інструментів.

2.1.6 Вимоги до ергономіки та технічної естетики

Інтерфейс системи повинен бути зручним та інтуїтивно зрозумілим користувачам. Форми внесення інформації повинні мати підказки щодо обов’язковості заповнення полів та щодо формату їх заповнення. Інтерфейс системи повинен бути орієнтований на використання клавіатури та маніпулятора «миша» (з можливістю використання тільки клавіатури, для пришвидшення введення інформації) з мінімізацією кількості дій для виконання простих операцій.

Взаємодія користувача з системою повинна виконуватись українською мовою, за винятком системних повідомлень, що не підлягають перекладу.

Кольорове оформлення інтерфейсу повинне бути виконане в єдиному строгому стилі. Сигналізація про помилки або помилкові дії повинна супроводжуватися підказкою про подальші дії.

2.1.7 Вимоги до захисту інформації від несанкціонованого доступу

Забезпечення цілісності загальнодоступної інформації вимагає застосування технологій, що забезпечують реалізацію контрольованого і санкціонованого доступу до інформації та заборону неконтрольованої й несанкціонованої її модифікації, що повинно вирішуватися на рівні операційної системи сервера, системи управління баз даних та розроблюваного програмного забезпечення.

Повинна здійснюватися фільтрація на мережевому рівні, фільтрація пакетів службових повідомлень, фільтрація з урахуванням вхідного та вихідного інтерфейсу. За допомогою апаратних та/або програмних (pf, ipfw, iptables) міжмережевих екранів забезпечити фільтрацію вхідних інформаційних потоків.

Привілеї для користувачів при доступі до файлів та папок (директорій) серверу застосувань повинні виставлятися за критерієм мінімально необхідних.

Користувачам повинна бути реалізована форма входу виключно із використанням модулю автентифікації користувачів за допомогою пари логін/пароль.

Контроль цілісності основних файлів повинен здійснюватися на рівні операційної системи та системи управління базами даних.

Робочі станції повинні передбачати автоматичний вихід користувача з системи, якщо користувач не виконував жодних дій протягом 15 хвилин.

З метою безпеки всі файли, що відносяться до системи, повинні зберігатися в спеціальній структурі каталогів на рівні операційної системи і бути захищені.

Повинні бути заблоковані несанкціоновані завантаження файлових об’єктів на сервер застосувань. Користувачам дозволено завантажувати тільки документи, необхідні для надання адміністративних послуг. Файли повинні завантажуватись до спеціально призначеної для цього директорії, запуск сценаріїв та скриптів з якої повинен бути заборонений.

Система повинна контролювати одержувану інформацію на предмет відсутності шкідливого для неї або інших користувачів системи програмного коду і керуючих послідовностей.

При розробці системи повинні бути визначені можливі типи помилок і механізми обробки аварійних ситуацій. При виникненні помилок або аварійних ситуацій, система повинна видавати користувачам повідомлення про це, не вказуючи при цьому жодних додаткових даних.

В мережі повинно бути забезпечено реєстрацію всіх подій, які мають безпосереднє відношення до безпеки і зберігати їх в окремо виділеній базі даних.

Певні типи помилок повинні реєструватися в журналах збоїв. Склад реєстрованих помилок повинен бути визначений на стадії технічного проектування. Атакож мережа повинна передбачати можливість резервного копіювання та відновлення системних та користувацьких даних.

2.1.8 Вимоги до патентної чистоти

Патентна чистота мережі повинна бути забезпечена розробником і повинна гарантуватися фірмами виробниками програмних та апаратних засобів.

2.1.9 Вимоги до стандартизації й уніфікації

Стандартизація та уніфікація функцій мережі повинна бути забезпечена за рахунок використання сучасних засобів які підтримують єдину технологію проектування та розробки комплексної мережі. Обладнання повинно підбиратися раціонально, виходячи з необхідної структури та місткості мережі.

2.1.10 Вимоги до забезпечення збереження інформації у випадку аварійних ситуацій

Забезпечення збереження інформації у випадку аварійних ситуацій повинно передбачатись архітектурою системи. Система повинна передбачати обов’язкове створення резервних копій баз даних, файлів налаштувань, тощо. Відновлення інформації у випадку аварій повинно виконуватись за допомогою наперед передбачених сценаріїв адміністратором системи за мінімально можливий термін.

2.1.11 Додаткові вимоги

2.1.11.1 Загальні вимоги до інформаційної кабельної підсистеми.

Інформаційна кабельна підсистема призначена для передачі інформації між локальними пристроями автоматизованих робочих місць (комп'ютери, активне обладнання, багатофункціональними пристроями). Кількість автоматизованих робочих місць може бути змінено Підрядником по погодженням із замовником на етапі проектування локальної обчислювальної мережі.

Всі порти RJ-45 розташовані на робочих місцях, а також на комутаційной панелі в комутаційній шафі повинні бути підписані таким чином, що б їх можна було однозначно ідентифікувати. Маркування повинно бути виконане друкарським способом або за допомогою лазерного принтера.

Технологія прокладки кабелю повинна забезпечувати збереження естетичного вигляду приміщень після виконання монтажних робіт.

2.1.11.2 Вимоги до кабель-каналів, інформаційних та електричних розеток

Для реалізації проекту виконавець самостійно вибирає виробника кабельної системи. Тип і розмір кабель каналу для горизонтальної кабельної підсистеми повинен бути однаковий у всіх приміщеннях.

Прокладання електричних кабелів здійснити в металевих лотках при прокладці кабельних трас приховано за фальшпотолком або в кабельних каналах при відкритому прокладанні. У робочих кабінетах монтаж повинен бути виконаний в окремих секціях пластикових кабельних каналів.

Інформаційна кабельна підсистема призначена для передачі інформації між пристроями наступних систем:

- локальна обчислювальна мережа;
- система телефонії.

Основні вимоги до кабель-каналів:

- легкий монтаж;
- можливість швидкого доступу до несправної проводки;
- за рахунок подвійного замку кришка щільно з'єднується з кабель каналом;
- стійкість до впливу сонячних променів і різних ушкоджень;
- стійкість до вогню;
- забезпечення додаткової ізоляції;
- висока якість і естетичний зовнішній вигляд.

Всі розетки зовнішні, без прихованого монтажу, встановлюються в спеціальному місці для цегляних або порожніх стін в залежності від структури стіни.

2.1.11.3 Вимоги до електроживлення і заземлення

Система електроживлення робочих місць призначена для підключення комп'ютерної техніки на робочих місцях СКС до електричної мережі 220В, 50Гц. Кожне робоче місце має оснащуватися двома електричними розетками 220В, 50Гц з заземлюючим контактом. Комп'ютерні розетки повинні відрізнятися за кольором від побутових або мати відповідну маркування.

Система електроживлення повинна бути виконана по 5-ти провідний схемою (TN-C-S) в магістральної частини і по 3-провідній схемі в груповій частині.

Повинно бути передбачено рівномірний розподіл навантажень по фазах.

Передбачити підключення джерела безперебійного живлення, що забезпечує електроживлення мережевого і серверного (при наявності вільного місця) обладнання, розміщується в комутаційній шафі, окремою лінією харчування і від окремого автоматичного вимикача. Для зручності підключення активного і телекомунікаційного обладнання в шафі необхідно передбачити електричні панелі, що підключаються до ДБЖ, з кількістю розеток, достатнім для підключення встановлюваного в шафі обладнання і з запасом на розвиток.

2.1.11.4 Вимоги до однорідності

Застосувати уніфіковані типи кабелів і роз'ємів в рамках робочих місць, горизонтальної підсистеми, підсистем внутрішніх магістралей, а також розподільних вузлів, незалежно від типів підключення абонентського обладнання та активного обладнання різних підсистем.

2.2 Вимоги до функцій (задач), виконуваним мережою

Підсистема менеджментового відділу буде виконувати наступні функції:

- аналіз ринкових ситуацій;
- вивченням тенденцій розвитку ринку;
- пошук релевантних замовлень;
- вивченням попиту;
- координацією дій підрозділів розробки;

Для даної підсистеми необхідно забезпечити доступ в Інтернет для пошуку необхідної для коректної роботи інформації. Також робітники даної підсистеми повинні мати доступ до інформації про поточних клієнтів. Необхідно дозволити звертатись до підсистем відділу Java-enterprise, Web-UI та AI для координації їх роботи.

Підсистеми Java-enterprise, Web-UI та AI займаються розробкою відповідного ПЗ.

Підсистема IT-Академії має виконувати наступне:

- підготовка конкурентноспроможних робочих кадрів;
- перекваліфікація або підвищення кваліфікації працівників;
- сертефікація за міжнародними стандартами;

2.3 Вимоги до видів забезпечення

2.3.1 Вимоги до інформаційного забезпечення

Дані повинні знаходитись у структурованому вигляді. Структура даних повинна задавати строгі правила зберігання інформації для точної ідентифікації її в мережі. Організація даних повинна забезпечувати:

- мінімальну надмірність інформації та максимальну швидкість роботи з нею;
- багаторазове використання даних у різних ділових процесах;
- забезпечення фізичної та логічної цілісності даних;
- мінімізація надмірності даних, що зберігаються;
- стандартизація представлення даних;
- достовірність та актуальність даних.
-

2.3.2 Вимоги до лінгвістичного забезпечення

Інтерфейс користувачів ІС повинен бути виконаний англійською мовою.

2.3.3 Вимоги до організаційного забезпечення

Для розробки будуть забезпечені наступні умови:

- набувачем буде надано постачальнику необхідні для розробки мережі матеріали, інтерфейси взаємодії з іншими системами, що використовуються при роботі.
- набувачем буде забезпечено функціонування існуючого програмно-технічного комплексу, на якому Постачальник розгортатиме компоненти мережі

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМПЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Обстеження об’єкту розробки та аналіз способів доступу до інфраструктури мережі

Приватне підприємство має два відділення – основний офіс та IT-Академія. Для доступу до корпоративної мережі віддаленого необхідно впровадити технологію VPN (site to site) — спосіб реалізації технології OpenVPN, призначений для створення захищеного віртуального тунелю між декількома приватними мережами.

Всього в корпоративній мережі будуть знаходитися 4 маршрутизатори, до яких будуть під’єднуватися комутатори в залежності від кількості користувачів в мережах.

В компанії є відділ Керування, в який входить 3 підрозділи. Для цієї мережі буде доцільним використання технології VLAN, адже це сприяє скороченню широкомовного трафіку між всіма користувачами мережі, зменшує кошторис на впровадження апаратного забезпечення та надає більше безпеки цій підсистемі.

3.2 Розробка специфікації апаратних засобів комп’ютерної системи

Специфікація обладнання наведена в таблиці 3.1. В випадку з даною мережею доцільно використати активне обладнання компанії Cisco.

Таблиця 3.1 − Специфікація обладнання

№	Тип, найменування	Технічна характеристика	Кількість
1	Маршрутизатор Cisco 2901	Керування: Web-інтерфейс, SNMP Базові можливості: DHCP-сервер Перенаправлення портів Клонування MAC-адреса Підтримка VPN Безпека: Фільтрація MAC-адрес Захист від DoS-атак Фільтрація web-трафіка Інтерфейс: WAN: 2 x 10/100/1000 RJ-45	4
2	Комутатор Cisco Catalyst WS-C2960-24TT	Керований комутатор з 24 фіксованими 10/100 Fast Ethernet портами та 2 аплінками 10/100/1000 Gigabit Ethernet, встановлене ПЗ - LAN Base. Можливості: Підключення: Fast Ethernet і Gigabit Ethernet 24 портами Живлення пристроїв по витій парі: конфігурації з 24 портами з повною підтримкою PoE і 24 портами Інтегровані функції безпеки, включаючи контроль доступу в мережу Розширені можливості управління якістю обслуговування (QoS) і забезпечення відмовостійкості Інтелектуальні сервіси на кордоні мережі	6
3	Серверне обладнання Cisco UCS C220 M4S	Модель процесора Intel Xeon E5-2620 Частота процесора 3.2 GHz Кількість ядер 6 Об’єм оперативної пам’ятї 8 Gb Інтерфейс SAS, SATA	2
4	Моноблок для персоналу Apple iMac 27" Retina 5K	Процессор: шестиядерний Intel Core i7 (3.7 - 4.6 ГГц) Об’єм оперативної пам’яті: 16 ГБ Об’єм накопичувача: 512 ГБ SSD Тип оперативної пам’яті:DDR4-2400 МГц Графічний адаптер: дискретний, AMD Radeon Pro 580x, 8 ГБ виділенною відеопам’яттю GDDR5	70

3.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Вихідний трафік найбільшої мережі розробниуів маршрутизується в лінію GigabitEthernet з пропускною здатністю 100Мбіт/с. Для того, щоб маршрутизатор не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Таким чином, загальне навантаження не повинно перевищувати μ вих = 100000000/(650*8) = 19230пакетів/с

Оскільки кожне джерело виробляє в середньому 160 пакетів/с, то ми обмежені приєднанням до маршрутизатора максимум:

N=192300/110=174 джерел.

Що задовольняє нашу мережу на 510 робочих станцій та персональних телефонів. Кожен з 510 робочих станції посилає потік заявок з інтенсивністю 160 кадрів/с. Інтенсивність вихідного трафіку:

λ= 80*110=8800(пакетів/с)

Коефіцієнт затримки:

$$\boldsymbol{\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{8800}{19230} = 0,46}$$

Коефіцієнт зайнятості маршрутизатора:

$$\boldsymbol{\frac{\rho}{1-\rho} = \frac{0,46}{1-0,46} = 0,85}$$

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

$$\text{T} = \boldsymbol{\frac{1}{(\mu - \lambda)} = \frac{1}{19230 - 8800} = 0,96}\text{мкс}$$

Це значення менше необхідного значення ≤6 мс, що задовольняє вимогам.

Середня довжина черги:

$$\boldsymbol{\mathcal{L}_{\text{чер}} = \frac{\rho^2}{1-\rho} = \frac{0,46^2}{1-0,46} = 0,39}$$

Середній час перебування пакета в черзі

$$\mathrm{T_{оч}} = \frac{\boldsymbol{\mathcal{L}_{\text{чер}}}}{\boldsymbol{\lambda}} = \frac{\boldsymbol{0,39}}{\boldsymbol{8800}} = \boldsymbol{0,44}\ \text{мкс}$$

Пропускну здатність каналу:

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

$$\boldsymbol{b = \lambda * l = 8800 * 650 * 8 = 45760000}\ \frac{\text{біт}}{\text{с}} = \boldsymbol{45,76}\text{Мбіт/с}$$

Що задовольняє пропускній здатності вихідного каналу в 100Мбіт/с.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

4.1 Розрахунок схеми адресації корпоративної мережі

Згідно варіанту було обрано мережу 192.168.16.0/24 (255.255.255.0.)

Дану мережу необхідно поділити на 6 підмереж: Enterprise, IT-Academy, Head-Department, Servers, Web-UI, AI. В свою чергу підмережа Head-Department буде поділена на 3 сегмента VLAN.

Найбільшою буде мережа Head-Department. Для неї виділимо розмір у 80 (126) хостів.

Для IT-Academy виділимо розмір 67(126) адрес для можливості виходу в інтернет гостям компанії. Кількість персоналу в мережі Web-UI невелика, тому необхідний розмір складає 30(30) вільних адресів. AI буде достатньо 75(126) адрес. Для Java-Enterprise буде достатньо 35(62) доступних адреси. Скористаємося технологією VLSM для поділу мережі на підмережі. Почнемо з найбільшої з підмереж.

Таблиця 4.1 – Виділений блок адрес для компанії «ThinkServeInc.»

№	Адреса мережі	IT-Academy	Head-Department	Web-UI	AI	Enterprise	Server_room
12	192.168.16.0/24	67	80	30	75	35	30

1. Необхідний розмір IT-Academy – 67

Розмір, який можна виділити – 126 ($2^7 – 2 = 126$). Від цього ще віднімається 2, бо перша адреса, адреса підмережі, остання – адреса широкомовного повідомлення. 2^7 – означає, що у нас є 7 кінцевих біт для адресації вузлів в підмережі, а 23 перших біта – це адреса мережі.

Адреса – 192.168.16.1|0000000 /25

Маска – 255.255.255.1| 0000000 (/25)

Адреса мережі – 192.168.16.128 /25

Для розрахунку широкомовної адреси необхідно нулі в правій частині замінити на одиниці.

Широкомовна адреса – 192.168.16.255

Діапазон допустимих адрес – 192.168.16.129– 192.168.16.254

2. Необхідний розмір Head-Department – 80

Виділений розмір – 2^7 - 2 = 126.

Адреса мережі – 192.128.18.128/25

Маска – 255.255.255.128

Широкомовна адреса – 192.128.18.255

Діапазон допустимих адрес – 192.128.18.129 - 192.128.18.254

3. Необхідний розмір Web-UI – 30

Виділений розмір – 2^5 - 2 = 30.

Адреса мережі – 192.168.17.224/27

Маска мережі – 255.255.255.224

Широкомовна адреса – 192.168.17.255

Діапазон допустимих адрес – 192.168.17.225 - 192.168.17.254

4. Необхідний розмір Artificial Intelligence – 75

Виділений розмір – 2^7 - 2 = 126.

Адреса мережі –192.168.19.128/25

Маска мережі – 255.255.255.128

Широкомовна адреса –192.168.19.255

Діапазон допустимих адрес – 192.168.19.129- 192.168.19.255

5. Необхідний розмір Enterprise – 35

   Виділений розмір – 2^6 - 2 = 62.

   Адреса мережі – 192.168.23.192 /26

   Маска мережі – 255.255.255.192

   Широкомовна адреса – 192.168.23.255

   Діапазон допустимих адрес – 192.168.23.193 - 192.168.23.254

За такою схемою розмежування адрес досягається максимальна ефективність пулу адрес — мінімум невикористаних адрес в кожній підмережі. Для проектування Системи будуть використані адреси, наведені в таблиці 4.2

Таблиця 4.2 – Схема адресації мережі

Назва підмережі	**Розмір**	**Виді-й розмір**	**Адреса**	**Маска**	**Діапазон доступних адрес**	**Широкомовна адреса**
IT-Academy	67	126	192.168.16.128	/25	192.168.16.129-192.168.16.254	192.168.16.255
Head-Department	80	126	192.168.18.128	/25	192.168.18.129-192.168.18.254	192.168.18.255
Web-UI	30	30	192.168.17.225	/27	192.168.17.225-192.168.17.254	192.168.17.255
AI	75	126	192.168.19.128	/25	192.168.19.129-192.168.19.254	192.168.19.255
Java-Enterprise	35	62	192.168.23.192	/26	192.168.23.193-192.168.23.254	192.168.23.255

Адресацію каналів між маршрутизаторами корпоративної мережі буде здійснена з мережі 10.0.2.0/30 та розбита за допомогою технології VLSM

Таблиця 4.3 – Підмережа каналів WAN між маршрутизаторами

Назва підмережі	Розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
WAN_1	2	10.0.2.0	/30	10.0.2.1 - 10.0.2.2	10.0.2.3
WAN_2	2	10.0.2.4	/30	10.0.2.5 - 10.0.2.6	10.0.2.7
WAN_3	2	10.0.2.8	/30	10.0.2.9 - 10.0.2.10	10.0.2.11

Продовження таблиці 4.3

Назва підмережі	Розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
Provider_1	30	209.165.200.0	/27	209.165.200.1 - 209.165.200.30	209.165.200.31
Provider_2	30	64.100.13.0	/27	64.100.13.1 - 64.100.13.30	64.100.13.31

4.2 Розрахунок схеми адресації пристроїв пристроїв корпоративної мережі

В таблиці 4.4 наведена адресація інтерфейсів та підінтерфейсів маршрутизаторів, створена на основі таблиць адресації мереж. За правилом, їм видаються перші можливі адреси в мережі.

Далі розрахуємо адреси SVI інтерфейсів комутаторів в мережах. За правилом, їм привласнюються другі можливі адреси в мережі.

Таблиця 4.4 – IP-адреси пристроїв в підмережах відділів.

Пристрій	Інтерфейс	IP-адреса	Маска	LAN
Baidak_Router_1	Se0/0/1	10.0.2.5	255.255.255.252(/30)	10.0.2.4
	Se0/1/1	10.0.2.9	255.255.255.252(/30)	10.0.2.8
	Gig0/0	192.168.17.225	255.255.255.224(/27)	192.168.17.224
	Gig0/1	192.168.23.193	255.255.255.192(/26)	192.168.23.192
Baidak_Router_2	Se0/1/0	62.100.23.2	255.255.255.224(/27)	62.100.23.0
	Gig0/0	192.168.16.129	255.255.255.224(/25)	192.168.16.128
Baidak_Router_3	Se0/1/0	10.0.2.1	255.255.255.252(/30)	10.0.2.0
	Se0/1/1	10.0.2.6	255.255.255.252(/30)	10.0.2.4
	Gig0/0.12	192.168.18.161	255.255.255.224(/25)	192.168.18.160
	Gig0/0.22	192.168.18.193	255.255.255.224(/25)	192.168.18.192
	Gig0/0.32	192.168.18.225	255.255.255.224(/25)	192.168.18.224
	Gig0/0.100	192.168.18.129	255.255.255.224(/25)	192.168.18.128
Baidak_Router_4	Se0/0/1	10.1.2.2	255.255.255.252(/30)	10.1.2.0
	Se0/1/0	10.1.2.10	255.255.255.252(/30)	10.1.2.8
	Se0/1/1	10.1.2.17	255.255.255.252(/30)	10.1.2.16
	Gig0/0	192.168.19.129	255.255.255.128(/25)	192.168.19.128
	Gig0/1	192.168.19.193	255.255.255.192(/26)	192.168.19.192

Продовження таблиці 4.4

Пристрій	Інтерфейс	IP-адреса	Маска	LAN
ISP	Se0/1/0	64.0.13.1	255.255.255.224(/27)	64.0.13.0
	Se0/1/1	10.1.2.18	255.255.255.252(/30)	10.1.2.16
	Gig0/0	209.165.200.1	255.255.255.0(/24)	209.165.200.0

4.3 Налаштування моделі комп'ютерної системи корпоративної мережі

На рисунку 4.1 зображена топологічна схема корпоративної мережі, виконана та протестована в симуляторі Packet Tracer. Система складається з таких підмереж:

- IT-Academy
- Head-Department
- Web-UI
- Artificial Intelligence
- Enterprise
- Servers

Для маршрутизації використовується протокол EIGRP з номером 1. Маршрутизатори в мережі під'єднані до Serial портів, комутатори — до GigabitEthernet.

На рисунку 4.1 наведено топологічну схему корпоративної мережі підприємства, де блакитним кольором виділено підмережу Head-Department, зеленим – Web-UI, синім – Java-Enterprise, помаранчевим – Artificial Intelligence, жовтим – IT-Academy, а пурпурним виділено серверну.

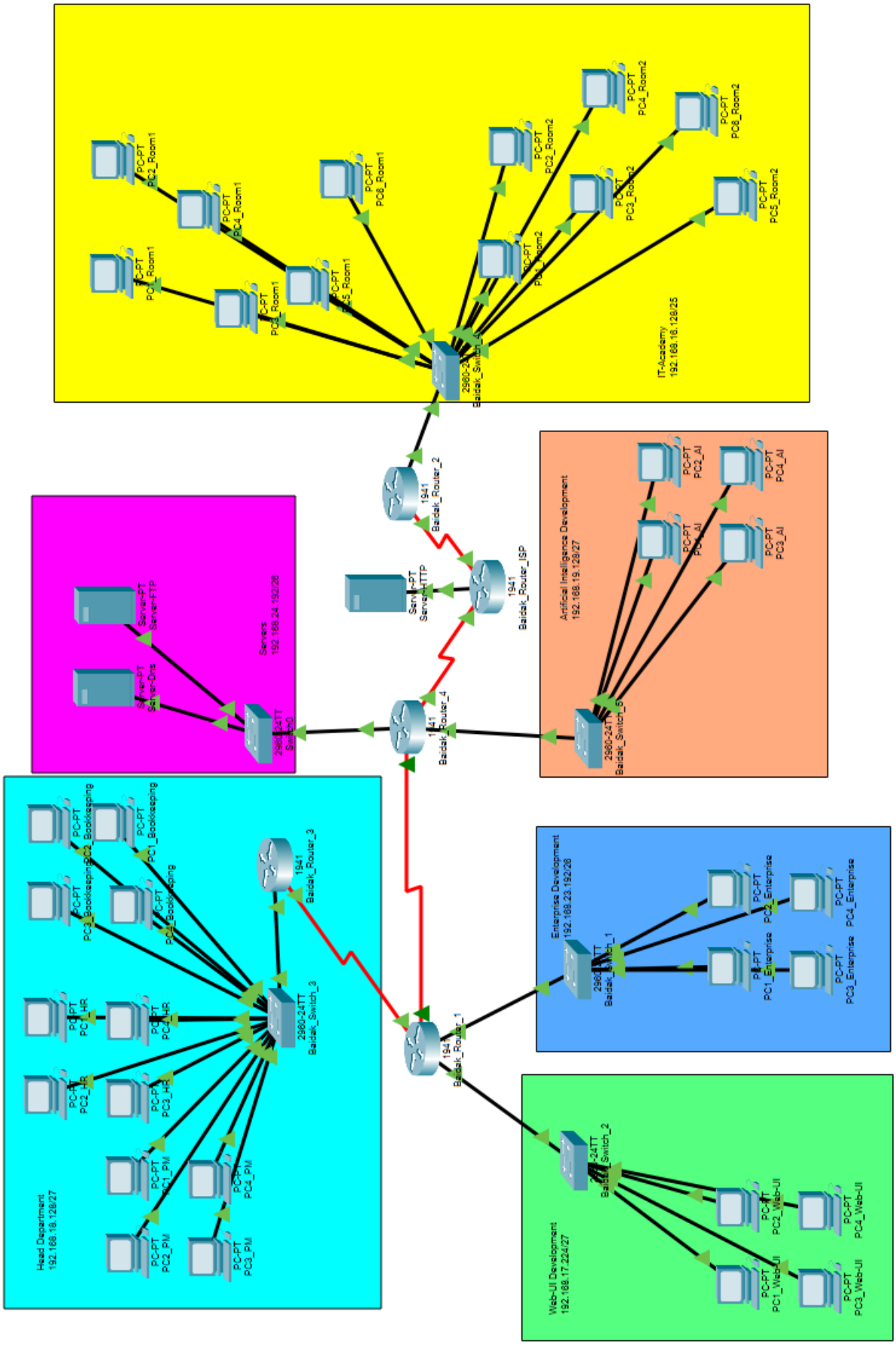

Рисунок 4.1 – Топологічна схема корпоративної мережі компанії

4.4 Налаштування та перевірка роботи корпоративної мережі

4.4.1 Базове налаштування конфігурації пристроїв

Для забезпечення безпеки мережного обладнання від несанкціонованого доступу потрібно виконати базове налаштування. Для прикладу наведена базова конфігурація маршрутизатора Baidak_Switch_3 на рисунку 4.2.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Baidak_Router_3
Baidak_Router_3(config)#ip domain-name Baidak_Router_3
Baidak_Router_3(config)#crypto key generate rsa
The name for the keys will be: Baidak_Router_3.Baidak_Router_3
Choose the size of the key modulus in the range of 360 to 2048 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]

Baidak_Router_3(config)#ip ssh version 2
*Бер 1 0:1:35.783: %SSH-5-ENABLED: SSH 1.99 has been enabled
Baidak_Router_3(config)#service password-encryption
Baidak_Router_3(config)#username 123161_Baidak password admincisco
Baidak_Router_3(config)#line vty 0 15
Baidak_Router_3(config-line)#transport input ssh
Baidak_Router_3(config-line)#logging synchronous
Baidak_Router_3(config-line)#exec-timeout 60 0
Baidak_Router_3(config-line)#exit
Baidak_Router_3(config)#line console 0
Baidak_Router_3(config-line)#password cisco
Baidak_Router_3(config-line)#exit
Baidak_Router_3(config)#enable secret class
Baidak_Router_3(config)#do write
Building configuration...
[OK]
Baidak_Router_3(config)#
```

Рисунок 4.2 – Типове базове налаштування роутера

4.4.2 Налаштування маршрутизаторів корпоративної мережі

На роутерах необхідно налаштупати динамічну маршрутизацію за протоколом EIGRP за номером 1, щоб вони могли обмінюватися пакетами з сусідніми маршрутизаторами.

Для прикладу буде розглянуто налаштування Baidak_Router_3, наведене на рисунку 4.3.

```
Baidak_Router_3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Baidak_Router_3(config)#router eigrp 1
Baidak_Router_3(config-router)#network 192.168.18.160
Baidak_Router_3(config-router)#network 192.168.18.192
Baidak_Router_3(config-router)#network 192.168.18.224
Baidak_Router_3(config-router)#network 192.168.18.128
Baidak_Router_3(config-router)#network 10.1.2.0
Baidak_Router_3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.2.5 (Serial0/1/1) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.2.2 (Serial0/1/0) is up: new adjacency
network 10.1.2.4
Baidak_Router_3(config-router)#passive-interface g0/0
Baidak_Router_3(config-router)#passive-interface g0/0.12
Baidak_Router_3(config-router)#passive-interface g0/0.22
Baidak_Router_3(config-router)#passive-interface g0/0.32
Baidak_Router_3(config-router)#passive-interface g0/0.99
%Invalid interface type and number
Baidak_Router_3(config-router)#passive-interface g0/0.100
Baidak_Router_3(config-router)#do write
Building configuration...
[OK]
Baidak Router 3(config-router)#
```

Рисунок 4.3 – Налаштування протоколу динамічної маршрутизації EIGRP

На інтерфейсі роутера, до якого буде підключено мережу Head-Department необхідно створити підінтерфейси відповідно до створених VLAN-ів та оголосити підтримку стандарту з відповідним номером VLAN-у.

На рисунку 4.4 показано налаштування протоколу DHCP.

```
Baidak_Router_3(config)#no ip dhcp pool poolvlan12
Baidak_Router_3(config)#no ip dhcp pool poolvlan22
Baidak_Router_3(config)#no ip dhcp pool poolvlan32
Baidak_Router_3(config)#do show ip dhcp pool
Baidak_Router_3(config)#ip dhcp pool poolvlan12
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#no ip dhcp pool poolvlan12
Baidak_Router_3(config)#ip dhcp excluded-address 192.168.18.161 192.168.18.170
Baidak_Router_3(config)#ip dhcp excluded-address 192.168.18.193 192.168.18.202
Baidak_Router_3(config)#ip dhcp excluded-address 192.168.18.225 192.168.18.234
Baidak_Router_3(config)#ip dhcp pool poolvlan12
Baidak_Router_3(dhcp-config)#network 192.168.18.160 255.255.255.224
Baidak_Router_3(dhcp-config)#default-router 192.168.18.161
Baidak_Router_3(dhcp-config)#dns-server 192.168.24.254
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#ip dhcp pool poolvlan22
Baidak_Router_3(dhcp-config)#network 192.168.18.192 255.255.255.224
Baidak_Router_3(dhcp-config)#default-router 192.168.18.193
Baidak_Router_3(dhcp-config)#dns-server 192.168.24.254
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#ip dhcp pool poolvlan32
Baidak_Router_3(dhcp-config)#network 192.168.18.224 255.255.255.224
Baidak_Router_3(dhcp-config)#default-router 192.168.18.225
Baidak_Router_3(dhcp-config)#dns-server 192.168.24.254
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#do write
Building configuration...
[OK]
Baidak_Router_3(config)#
```

Рисунок 4.4 – Налаштування протоколу DHCP

На граничному маршрутизаторі *Baidak_Router_4* необхідно налаштувати статичний маршрут за змовчуванням і виконати його розповсюдження через оновлення маршрутизації:

Baidak_Router_4(config)# ip route 0.0.0.0 0.0.0.0 10.1.2.18

Baidak_Router_4(config)# redistribute static

Додаємо статичний маршрут так, щоб був доступ з локальної мережі до провайдера ISP:

Baidak_Router_4 (config)# ip route 209.165.200.0 255.255.255.240 209.165.200.1

- Задаємо пропускну спроможність та тактову частоту на serial-інтерфейсах:

Baidak_Router_4 (config)#interface Serial0/0/1

Baidak_Router_4 (config-if)# bandwidth 128

Baidak_Router_4 (config-if)# clock rate 128000

- Налаштовуємо всі маршрутизатори на підтримку служби AAA таким чином:

Baidak_Router_4 (config)#aaa new-model // Вмикаємо службу

Baidak_Router_4 (config)#radius-server host 192.168.24.253 auth-port 1645 key radius123 // вказуємо AAA Radius сервер

Для доступу до консолі створюємо аутентифікацію на основі протоколу RADIUS і якщо з ним немає зв’язку − локальну базу даних:

Baidak_Router_4 (config)#aaa authentication login RADIUS_LIST group radius local

Baidak_Router_4 (config)#line console 0

Baidak_Router_4 (config-line)#login authentication RADIUS_LIST

Baidak_Router_4 (config-line)#exit

Для перевірки підключень до VTY ліній на маршрутизаторі створимо локальну базу даних користувачів:

Baidak_Router_4 (config)#aaa authentication login default local

Baidak_Router_4 (config)#line vty 0 15

Baidak_Router_4 (config)#username Baidak_Router_4 password admin123

Baidak_Router_4 (config-line)#login authentication default

4.4.3 Налаштування роботи Інтернет

Для доступу в Інтернет виконуємо налаштування прикордонного маршрутизатора з динамічним NAT з використанням наданого пулу адрес з 209.165.200.5 по 209.165.200.30.

Baidak_ISP (config)#interface Serial0/1/1

Baidak_ISP (config-if)#ip nat outside

Baidak_ISP (config)#interface Serial0/0/0

Baidak_ISP (config-if)#ip nat inside

Baidak_ISP (config-if)#exit

Baidak_ISP (config)# ip access-list extended FOR-NAT

Baidak_ISP (config-std-nacl)# deny ip 192.168.16.0 0.0.7.255 192.168.100.0 0.0.0.127

Baidak_ISP (config-std-nacl)# permit ip 192.168.96.0 0.0.7.255 any

Baidak_ISP (config-std-nacl)#deny any

Baidak_ISP (config)# ip nat pool INTERNET 209.165.200.5 209.165.200.30 netmask 255.255.255.224

Baidak_ISP (config)# ip nat inside source list FOR-NAT pool INTERNET overload

Налаштовуємо VPN(site-to-site) з використанням IPsec для трафіку, що проходить між мережею головного офісу та віддаленою мережею IT-Academy через Інтернет. Необхідно додати властивості криптографічної політики ISAKMP 10, а також загальний ключ шифрування cisco:

Baidak_Router_4 (config)#license boot module c2900 technology-package securityk9 //Активація модуля securityk9

Baidak_Router_4 (config)#crypto isakmp policy 1

Baidak_Router_4 (config-isakmp)#encryption 3des

Baidak_Router_4 (config-isakmp)#hash md5

Baidak_Router_4 (config-isakmp)#authentication pre-share

Baidak_Router_4 (config-isakmp)#group 2

Baidak_Router_4 (config-isakmp)#ex

Baidak_Router_4 (config)#crypto isakmp key cisco address 64.100.13.2

Baidak_Router_4 (config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac //набір перетворень

Baidak_Router_4 (config)#ip access-list extended FOR-VPN // access-list, який визначає який трафік шифруватиметься і йтиме по vpn тунелю

Baidak_Router_4 (config-ext-nacl)#permit ip 192.168.96.0 0.0.7.255 192.168.100.0 0.0.0.127

Baidak_Router_4 (config)#crypto map CMAP 10 ipsec-isakmp //криптографічне зіставлення

Baidak_Router_4 (config-crypto-map)#set peer 64.100.13.2

Baidak_Router_4 (config-crypto-map)#set transform-set TS

Baidak_Router_4 (config-crypto-map)#match address FOR-VPN

Baidak_Router_4 (config-crypto-map)#ex

Baidak_Router_4 (config)# interface S0/0/1

Baidak_Router_4 (config-if)# crypto map CMAP //прив'язка криптографічного зіставлення CMAP до вихідного інтерфейсу

4.4.4 Перевірка роботи комп'ютерної системи

Після налаштування моделі комп'ютерної системи на симуляторі Cisco Packet Tracer проводиться її тестування, з дотриманням всіх умов, зазначених в ТЗ, а також відповідність вимогам безпеки. Для достовірності, нижче зображені результати команд, які показують інформацію по технологіям.

На рисунку 4.5 показано таблицю маршрутизації Baidak_Router_3 до налаштування протоколу EIGRP.

На рисунку 4.6 показано таблицю маршрутизації Baidak_Router_3 після налаштування протоколу EIGRP. Додались динамічні маршрути, позначені літерою D, та D*EX – зовнішній статичний маршрут, доданий до поширення шляхом EIGRP.

```
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.2.0/30 is directly connected, Serial0/1/0
L       10.1.2.1/32 is directly connected, Serial0/1/0
C       10.1.2.4/30 is directly connected, Serial0/1/1
L       10.1.2.6/32 is directly connected, Serial0/1/1
     192.168.18.0/24 is variably subnetted, 8 subnets, 2 masks
C       192.168.18.128/27 is directly connected, GigabitEthernet0/0.100
L       192.168.18.129/32 is directly connected, GigabitEthernet0/0.100
C       192.168.18.160/27 is directly connected, GigabitEthernet0/0.12
L       192.168.18.161/32 is directly connected, GigabitEthernet0/0.12
C       192.168.18.192/27 is directly connected, GigabitEthernet0/0.22
L       192.168.18.193/32 is directly connected, GigabitEthernet0/0.22
C       192.168.18.224/27 is directly connected, GigabitEthernet0/0.32
L       192.168.18.225/32 is directly connected, GigabitEthernet0/0.32
```

Рисунок 4.5 – Таблиця маршрутизації до налаштування протоколу EIGRP

```
Gateway of last resort is 10.1.2.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.1.2.0/30 is directly connected, Serial0/1/0
L       10.1.2.1/32 is directly connected, Serial0/1/0
C       10.1.2.4/30 is directly connected, Serial0/1/1
L       10.1.2.6/32 is directly connected, Serial0/1/1
D       10.1.2.8/30 [90/2681856] via 10.1.2.5, 00:05:34, Serial0/1/1
D       10.1.2.12/30 [90/21024000] via 10.1.2.2, 00:05:33, Serial0/1/0
D       10.1.2.16/30 [90/2681856] via 10.1.2.2, 00:05:33, Serial0/1/0
     192.168.17.0/27 is subnetted, 1 subnets
D       192.168.17.224/27 [90/2170112] via 10.1.2.5, 00:05:34, Serial0/1/1
     192.168.18.0/24 is variably subnetted, 8 subnets, 2 masks
C       192.168.18.128/27 is directly connected, GigabitEthernet0/0.100
L       192.168.18.129/32 is directly connected, GigabitEthernet0/0.100
C       192.168.18.160/27 is directly connected, GigabitEthernet0/0.12
L       192.168.18.161/32 is directly connected, GigabitEthernet0/0.12
C       192.168.18.192/27 is directly connected, GigabitEthernet0/0.22
L       192.168.18.193/32 is directly connected, GigabitEthernet0/0.22
C       192.168.18.224/27 is directly connected, GigabitEthernet0/0.32
L       192.168.18.225/32 is directly connected, GigabitEthernet0/0.32
     192.168.19.0/25 is subnetted, 1 subnets
D       192.168.19.128/25 [90/2170112] via 10.1.2.2, 00:05:33, Serial0/1/0
     192.168.23.0/26 is subnetted, 1 subnets
D       192.168.23.192/26 [90/2170112] via 10.1.2.5, 00:05:34, Serial0/1/1
     192.168.24.0/26 is subnetted, 1 subnets
D       192.168.24.192/26 [90/2170112] via 10.1.2.2, 00:05:33, Serial0/1/0
D*EX 0.0.0.0/0 [170/7289856] via 10.1.2.2, 00:05:33, Serial0/1/0
```

Рисунок 4.6 – Таблиця маршрутизації після налаштування протоколу EIGRP

На рисунку 4.7 наведено таблицю перетворень між локальними і глобальними адресами, отриману завдяки налаштуванню протоколу NAT на граничному маршрутизаторі.

```
Router#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.5:4   192.168.19.254:4   209.165.200.4:4    209.165.200.4:4
icmp 209.165.200.5:5   192.168.19.254:5   209.165.200.4:5    209.165.200.4:5
icmp 209.165.200.6:3   192.168.23.254:3   209.165.200.4:3    209.165.200.4:3
icmp 209.165.200.7:9   192.168.18.235:9   209.165.200.4:9    209.165.200.4:9
icmp 209.165.200.8:1   192.168.18.204:1   209.165.200.4:1    209.165.200.4:1
icmp 209.165.200.9:3   192.168.17.254:3   209.165.200.4:3    209.165.200.4:3
```

Рисунок 4.7 – Таблиця перевотрювань NAT на Baidak_ISP

На рисунку 4.8 наведено приклад перевірки налаштування мережі шляхом опитування віддаленого хоста за допомогою команди ping командного рядка. На рисунку 4.9 показано DHCP-binding, тобто привязка динамочної ip-адреси до MAC-адреси пристрою.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.16.254

Pinging 192.168.16.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.16.254: bytes=32 time=2ms TTL=125
Reply from 192.168.16.254: bytes=32 time=4ms TTL=125
Reply from 192.168.16.254: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.16.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms
```

Рисунок 4.8 – Вдале пінгування віддаленої мережі

```
Baidak_Router_3#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.18.173   0001.979A.6E75           --                     Automatic
192.168.18.172   0001.6419.0765           --                     Automatic
192.168.18.206   0090.0C3A.78A1           --                     Automatic
192.168.18.205   0060.5C6A.76B5           --                     Automatic
192.168.18.204   0003.E4CD.B73A           --                     Automatic
192.168.18.236   00E0.B04D.2428           --                     Automatic
192.168.18.238   0007.ECA5.3C20           --                     Automatic
192.168.18.235   0010.115E.BA43           --                     Automatic
192.168.18.237   000C.8538.27BC           --                     Automatic
```

Рисунок 4.9 – Видані адреса через DHCP

На рисунку 4.10 показано перевірку підключення до маршрутизатора за допомогою SSH через командний рядок.

На рисунку 4.11 показано перевірку налаштування протоколу IPsec.

```
C:\>ssh -l 123161_Baidak 192.168.16.129

Password:


Unauthorized access is strictly prohibited.

Baidak_Router_2>enable
Password:
Baidak_Router_2#
```

Рисунок 4.10 – Перевірка підключення до маршрутизатора за допомогою SSH

```
interface: Serial0/1/1
    Crypto map tag: CMAP, local addr 209.165.200.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.96.0/255.255.248.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.128/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 12, #pkts decrypt: 12, #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.: 209.165.200.2, remote crypto endpt.:64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/1
     current outbound spi: 0x0B9E0DBE(194907582)

     inbound esp sas:
      spi: 0x3E4B3D78(1045118328)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4525504/2835)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x0B9E0DBE(194907582)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4525504/2835)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Рисунок 4.11 – Перевірка налаштування протоколу IPsec

Таким чином проведена перевірка роботи мережі компанії «ThinkServeInc.» в симуляторі Packet Tracer.

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1 Розробка методів для захисту інформації в комп'ютерній системі

Для забезпечення захисту інформації в комп'ютерній системі потрібно впровадити технології VLAN та Port security. Port Security - це функція канального рівня, яка створена для запобігання несанкціонованого зміни MAC адреси мережевого підключення. Також, дана функція захищає комутатор від атак, які можуть бути спрямовані на переповнення таблиці MAC адрес. Для системи буде використаний динамічний спосіб обмеження MAC адрес з максимальною кількістю у 2 адреси на порт. Динамічний - коли адміністратор вказує, скільки адрес дозволено, а комутатор навчається, запам'ятовуючи, які адреси зараз звертаються через вказаний порт.

5.2 Налаштування мереж VLAN

Сегментуємо мережу Head-Department на окремі віртуальні мережі згідно з таблицею 5.1.

Назва відділу	Назва підмережі VLAN	VLAN	Розподіл портів
Бухгалтерія	Bookkeeping	12	F0/1 - F0/4
Відділ кадрів	Human Resources	22	F0/5- F0/8
Відділ менеджменту	Management	32	F0/9 - F0/12
Native	Native	100	G0/1

Таблиця 5.1 – Таблиця розподілу портів для окремих мереж VLAN.

Нижче в таблиці 5.2 наведена схема адресації в цих віртуальних логічних мережах.

Назва підмережі	Розмір	VLAN	Адреса	Десятинна маска	Діапазон допустимих адресів	Широкомовна адреса
Bookkeeping	30	12	192.168.18.160	255.255.255.224 (/27)	192.168.18.161-192.168.18.190	192.168.18.191
Human Resources	30	22	192.168.18.192	255.255.255.224 (/27)	192.168.99.193-192.168.99.222	192.168.99.223
Management	30	32	192.168.18.224	255.255.255.224 (/27)	192.168.99.225-192.168.99.254	192.168.99.255
Native	30	100	192.168.18.128	255.255.255.224 (/27)	192.168.99.129-192.168.99.158	192.168.99.159

Таблиця 5.2 – Схема адресації мереж VLAN

В таблиці 5.3 наведена схема адресації пристроїв в підмережі Head-Department.

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз	VLAN
Baidak_ Router_1	Gig0/0.12	192.168.18.161	255.255.255.224(/27)	-	12
	Gig0/0.22	192.168.18.193	255.255.255.224(/27)	-	22
	Gig0/0.32	192.168.18.225	255.255.255.224(/27)	-	32
	Gig0/0.100	192.168.18.129	255.255.255.224(/27)	-	100

Таблиця 5.3 – Таблиця адресації для пристроїв в Administration

Налаштування технології VLAN на прикладі комутатора Baidak_Switch_3:

− Оголошення підмереж:

Baidak_Switch_3(config)#vlan 12

Baidak_Switch_3(config-vlan)#name Bookkeeping

Baidak_Switch_3(config-vlan)#ex

Baidak_Switch_3(config)#vlan 22

Baidak_Switch_3(config-vlan)#name HR

Baidak_Switch_3(config-vlan)#ex

Baidak_Switch_3(config)#vlan 32

Baidak_Switch_3(config-vlan)#name Management

Baidak_Switch_3 (config-vlan)#ex

Baidak_Switch_3(config)#vlan 100

Baidak_Switch_3(config-vlan)#name Native

Baidak_Switch_3(config-vlan)#ex

− Налаштування портів та портів доступу:

Baidak_Switch_3(config)#int range fastEthernet 0/1-4

Baidak_Switch_3(config-if-range)#switchport mode access

Baidak_Switch_3(config-if-range)#switchport access vlan 12

Baidak_Switch_3(config-if-range)#ex

Baidak_Switch_3(config)#interface range fastEthernet 0/5-8

Baidak_Switch_3(config-if-range)#switchport mode access

Baidak_Switch_3(config-if-range)#switchport access vlan 22

Baidak_Switch_3(config-if-range)#ex

Baidak_Switch_3(config)#int range fastEthernet 0/9-12

Baidak_Switch_3(config-if-range)#switchport mode access

Baidak_Switch_3(config-if-range)#switchport access vlan 32

Baidak_Switch_3(config-if-range)#ex

5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

В усіх підмережах, окрім Серверної, підключено технологію DHCP, для забезпечення коректної роботи безпровідних точок доступу та економії часу при розрахунку системи. Для налаштування DHCP на VLAN потрібно налаштувати його на підінтерфейсах маршрутизатора.

З пулу адрес для DHCP буде виключено по 10 адреси тому, що вони використовуються для адресації мережних пристроїв.

```
Baidak_Router_3(config)#no ip dhcp pool poolvlan12
Baidak_Router_3(config)#no ip dhcp pool poolvlan22
Baidak_Router_3(config)#no ip dhcp pool poolvlan32
Baidak_Router_3(config)#do show ip dhcp pool
Baidak_Router_3(config)#ip dhcp pool poolvlan12
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#no ip dhcp pool poolvlan12
Baidak_Router_3(config)#ip dhcp excluded-address 192.168.18.161 192.168.18.170
Baidak_Router_3(config)#ip dhcp excluded-address 192.168.18.193 192.168.18.202
Baidak_Router_3(config)#ip dhcp excluded-address 192.168.18.225 192.168.18.234
Baidak_Router_3(config)#ip dhcp pool poolvlan12
Baidak_Router_3(dhcp-config)#network 192.168.18.160 255.255.255.224
Baidak_Router_3(dhcp-config)#default-router 192.168.18.161
Baidak_Router_3(dhcp-config)#dns-server 192.168.24.254
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#ip dhcp pool poolvlan22
Baidak_Router_3(dhcp-config)#network 192.168.18.192 255.255.255.224
Baidak_Router_3(dhcp-config)#default-router 192.168.18.193
Baidak_Router_3(dhcp-config)#dns-server 192.168.24.254
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#ip dhcp pool poolvlan32
Baidak_Router_3(dhcp-config)#network 192.168.18.224 255.255.255.224
Baidak_Router_3(dhcp-config)#default-router 192.168.18.225
Baidak_Router_3(dhcp-config)#dns-server 192.168.24.254
Baidak_Router_3(dhcp-config)#exit
Baidak_Router_3(config)#do write
Building configuration...
[OK]
Baidak_Router_3(config)#
```

2.1 Налаштування безпеки портів в мережі Server_room

Налаштовуємо Port Security на портах з серверами:

Baidak_Switch_6(config)#interface range fastEthernet 0/2-5

Baidak_Switch_6(config-if-range)#switchport mode access

Baidak_Switch_6(config-if-range)#switchport port-security

Baidak_Switch_6(config-if-range)#switchport port-security maximum 2

Baidak_Switch_6(config-if-range)#switchport port-security mac-address sticky

Baidak_Switch_6(config-if-range)#switchport port-security violation restrict

2.2 Налаштування ACL-списку для захисту від несанкціонованого доступу с гостьового Wi-Fi

ACL-список додається на порт маршрутизатора і забороняє трафік, який зазначений в ньому. Це дозволить гостям без перешкоди відвідувати сторінки Інтернету а компанії не перейматися, що зловмисники можуть скористатися цією можливістю.

Baidak_Router_3(config)#ip access-list extended FOR-GUEST

Baidak_Router_3(config-ext-nacl)#deny ip 192.168.98.0 0.0.0.255 192.168.96.0 0.0.1.255

Baidak_Router_3(config-ext-nacl)#deny ip 192.168.98.0 0.0.0.255 192.168.101.0 0.0.0.31

Baidak_Router_3(config-ext-nacl)#deny ip 192.168.98.0 0.0.0.255 192.168.99.0 0.0.0.255

Baidak_Router_3(config-ext-nacl)#deny ip 192.168.98.0 0.0.0.255 192.168.100.0 0.0.0.127

Baidak_Router_3(config-ext-nacl)#deny ip 192.168.98.0 0.0.0.255 192.168.100.128 0.0.0.127

Baidak_Router_3(config-ext-nacl)#permit ip any any

Baidak_Router_3(config-ext-nacl)#ex

Baidak_Router_3(config)#int gigabitEthernet 0/1

Baidak_Router_3(config-if)#ip access-group FOR-GUEST in

6 ЕКОНОМІЧНА ЧАСТИНА

6.1 Розрахунки капітальних витрат

У дипломному проекті розглядається економічна доцільність розробки системи комп'ютерної мережі компанії. При розробці системи запропоновано використовувати активне мережеве обладнання Cisco.

Деякі комплектуючі системи вже були в наявності. Тому для вдосконалення комп'ютерної системи потрібно докупити деяке обладнання. Капітальні витрати на закупівлю відсутніх елементів наведені в таблиці 6.1.

$$К = К_{об} + К_{тр} + К_{мн} + К_{пз}, \quad (6.1)$$

де $К_{об}$ – витрати на придбання встаткування;

$К_{тр}$ – витрати на транспортування;

$К_{мн}$ – на монтаж і налагодження системи керування;

$К_{пз}$ – на програмне забезпечення.

Таблиця 6.1 – Капітальні витрати, грн.

№ п/п	Найменування статей витрат	Кіл. од.	Вартість за ед. товару, грн.	Загальна вартість, грн.
1	Комутатор Cisco Catalyst WS-C2960-24TT	5	26800	214400
2	Кабель UTP вита пара кат.5е	10	3972	39720
3	Маршрутизатор Cisco 2901	3	53352	160056
4	Cisco Aironet 3600i (AIR-CAP3602I-E-K9)	4	4200	16800
	Разом			430976

Транспортно-заготівельні витрати визначаються по всіх розділах залежно від вартості устаткування, матеріалів, виробів, конструкцій та дорівнюють 8% від загальної вартості.

$$Д_{тр} = С_{кв} \cdot 0{,}08, \quad (6.2)$$

де, $С_{кв}$ – вартість комплектуючих виробів, грн.

Таким чином, витрати на транспортно-заготівельні роботи становлять

$Д_{тр}$ = 430976*0,08 = 34479 грн

Вартість монтажно-налагоджувальних робіт ухвалюємо на рівні 7% від вартості устаткування.

$$М_{мн} = С_{об} \cdot 0,07 \qquad (6.3)$$

Витрати на монтажно-налагоджувальні роботи складуть

$М_{мн}$ = 430976*0,07 = 30169 грн.

Капітальні витрати по проекту складуть:

$К_{пр}$ = 430976+ 30169 + 34479 = 495624 грн.

6.2 Розрахунки експлуатаційних витрат

До основних статтям експлуатаційних витрат ставляться:

− амортизація основних фондів $C_а$;

− заробітна плата обслуговуючого персоналу $C_з$;

− відрахування на соціальні заходи від заробітної плати $C_с$;

− витрати на ремонт та технічне обслуговування $C_{р.т..о.}$;

− вартість електроенергії, споживаної об'єктом проектування $C_{ее}$;

− інші витрати $C_{інш}$.

Таким чином, річні експлуатаційні витрати складуть:

$$C_е = C_а + C_з + C_с + C_{р.т.о.} + C_{ее} + C_{інш}, \qquad (6.4)$$

6.2.1 Амортизація основних фондів

Обладнання, розробленої в дипломному проекті системи керування, належить до 4 групи за нормами нарахування амортизації основних фондів. Передбачуваний термін експлуатації системи становить 5 роки.

При використанні методу прискореного зменшення залишкової вартості норма амортизації визначається за формулою:

$$H_a = (2 / T) \times 100\% \qquad (6.5)$$

T – термін корисного використання об'єкта;

H_a – норма амортизації;

$$C_a = (ПВ \times H_a)/100\%, \qquad (6.6)$$

C_a – амортизація основних фондів (річна);

$ПВ$ – первинна вартість, дорівнює капітальним витратам $ПВ = К$;

Отже, норма амортизації для проектованої системи керування складе:

$H_a = (2/5) \times 100\% = 40\%$

Сума амортизації для проектованої системи становитиме:

$C_{a.пр} = (495624 \times 40\%)/100\% = 198250$ грн.

6.2.2 Розрахунки річного фонду заробітної плати

Фонд основної заробітної плати (Зосн) – це заробітна плата, що нараховується за виконану роботу, чи відпрацьований час за відрядними розцінками, тарифними ставками та посадовими окладами. Розраховується за наступною формулою:

$$Зосн = Тст * Чоб * Теф, \qquad (6.7)$$

де Тст – тарифна ставка, яка відповідає певному розряду робіт грн/год;

Чоб – облікова чисельність;

Теф – ефективний фонд часу роботи одного середньостатистичного співробітника, год.

Номінальний річний фонд робочого часу одного працівника:

$T_{ном.рік} = (T_к - T_{вих.св} - T_{відп}) \times T_{зм}$, годин (6.8)

де, $T_к$ – календарний фонд робочого часу, 365 днів;

$T_{вих.св}$ – вихідні дні та свята, 115 дні;

$T_{відп}$ – відпустка, 21 день;

$T_{зм}$ – тривалість зміни, 8 год.

Таким чином, річний фонд робочого часу працівника складе:

$T_{ном.рік} = (365 - 115 - 21) \times 8 = 1832$ годин

Для керування процесом потрібно 1 спеціаліст з устаткування.

Розрахунок фонду заробітної плати для головного інженера по формулі (6.7):

Зосн = 50* 2 * 1 * 1832 = 183200 грн/рік

Після впровадження проектованої системи керування штат персоналу не зміниться, отже заробітна плата і відрахування на соціальні заходи будуть однакові.

Розрахунок річного фонду заробітної плати виробничих робітників здійснюється у відповідності з формою, наведеною в таблиці 6.2.

Посада	Кіл-ть,	Годинна	Номінальний	Пряма	Доплати	Основна

	чол	тарифна ставка, грн	річний фонд робочого часу, год	зарплата по тарифу, грн/рік	(5%)	зарплата
Головний інженер	1	45.23	1832	165722,72	8286,136	183200
Всього						183200

Таблиця 6.2 – Розрахунок заробітної плати персоналу

6.2.3 Розрахунки відрахувань на соціальні заходи

Відрахування на соціальні заходи складуть:

$$C_с = 0,22 \times C_з \qquad (6.9)$$

$$C_{с.пр} = C_{с.баз} = 0,22 \times 183200 = 40304 \text{ грн.}$$

6.2.4 Визначення річних витрат на технічне обслуговування й ремонт

Річні витрати на технічне обслуговування й поточний ремонт електротехнічного встаткування й мереж включають витрати на матеріали, запасні частини, заробітну плату ремонтником.

Витрати, пов'язані з ремонтом та технічним обслуговуванням нового обладнання, становлять 4% від вартості, тобто:

$$C_{р.т.о.} = К \times 0,04, \text{ грн.} \qquad (6.10)$$

$$C_{р.т.о.\ пр} = 495624 \times 0,04 = 19825 \text{ грн.}$$

6.2.5 Розрахунки вартості споживаної електроенергії

Система працює цілодобово, упродовж року.

Розрахуємо вартість електроенергії, споживаної системою керування, розробленої у проекті:

$$C_{ее} = К_е \times Кд \times Т \qquad (6.11)$$

де $К_е$ – кількість електроенергії, спожите проектованої системою керування за годину, кВт*год;

$К_{др}$ – кількість днів у році, Кдр = 365 днів;

Т – тариф на електроенергію для підприємств (Для користувачів електроенергії 2 класу тариф складає 1,63 грн. за кВт без ПДВ. З урахуванням ПДВ тариф Т = 1,63 × 1,2 = 1,956 грн).

Виходячи з технічних характеристик обладнання споживання електроенергії адміністрацією складає приблизно 5 кВт.

Здійснимо розрахунок вартості споживаної електроенергії при впровадженні системи.

Витрати на електроенергію будуть становити:

$C_{ее.пр} = 5 \times 365 \times 24 \times 1{,}956 = 85673$ грн

6.2.6 Визначення інших витрат

Інші витрати з експлуатації об'єкта проектування включають витрати з охорони праці, на спецодяг та інше згідно практиці, ці витрати визначаються в розмірі 4% від річного фонду заробітної плати обслуговуючого персоналу:

$$C_{інш} = C_з \cdot 0{,}04 \text{ грн.} \qquad (6.12)$$

$C_{інш.пр} = 183200 \times 0{,}04 = 7328$ грн.

За формулою 6.12 розраховуємо річні експлуатаційні витрати для проектного та базового варіантів:

Розраховані експлуатаційні витрати по варіантах представлено в табл. 6.3.

Таблиця 6.3 – Експлуатаційні витрати по варіантах

− Найменування показника	− Проектний варіант
− Амортизація	− 198250
− Фонд заробітної плати	− 183200
− Відрахування на соц. виплати	− 40304
− Ремонт і тех.обслуговування	− 19825
− Електроенергія	− 85673
− Інші	− 7328

6.3 Висновки до економічного розділу

Розроблена система потребує 495624 грн капітальних витрат для налаштування комп’ютерної мережі підприємства. А також щорічних експлуатаційних витрат:

Ер = 198250 + 183200 + 40304 + 19825 + 85673+ 7328 = 534580 грн/рік

Впровадження цієї системи сприяє підвищенню безпеки та надійності об’єкту.

7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1 Аналіз небезпечних та шкідливих факторів

Об’єктом дослідження є офісне приміщення головного офісу компанії. Для електропостачання використовується електрична мережа частотою 50 Гц і напругою 220В. В приміщенні розташована достатня кількість вікон, є 2 пасажирських та 1 вантажний ліфт, сходи. На території офісу необхідно розташувати достатню кількість вогнегасників для протидії виникненню пожежі.

При експлуатації електричних приладів можливі впливу наступних небезпечних факторів:

- небезпечної напруги в електричному ланцюзі,
- замикання якого може відбутися через тіло людини;
- ймовірність виникнення пожежі.

4.2 Інженерно-технічні заходи щодо охорони праці

7.2.1 Заходи по забезпеченню електробезпеки

Основними заходами щодо забезпечення електробезпеки є:

- захист від випадкового дотику;
- контроль і профілактика ушкодженої ізоляції;
- занулення всіх неструмоведучих частин;
- застосування електрозахисних засобів;

До роботи з електроприборами допускаються працівники:

- пройшли інструктаж;
- знаючі пристрій приладів;

− ознайомлені з інструкціями щодо їх застосування;

− мають 1 групу з електробезпеки.

Обслуговуючий електротехнічний персонал повинен вивчати діючі правила улаштування електроустановок, правила технічної експлуатації електроустановок споживачів і правила техніки безпеки при експлуатації електроустановок споживачів, а також знати прийоми звільнення потерпілого від дії електричного струму і надання долікарської допомоги.

7.2.2 Загальні вимоги з техніки безпеки

Основні правила використання електрообладнання, незалежно від того де вони будуть використовуватись:

- регулярно потрібно проводити перевірку справності та працездатності розеток, щитків, електропроводки і штепсельних роз'ємів. Потрібно мати на увазі, що електроустановки прилади споживають набагато більший струм, ніж інші. Тому при їх включенні вихід з ладу електричної проводки відбувається швидше;
- не використовувати пошкоджені і саморобні електроустановки. І в тому, і в іншому випадку небезпека загоряння істотно зростає;
- не можна пропускати провід під килимами та покриттям. Там він може перетертися, що може спричинити загоряння .
- не встановлювати установки на займистих підставках;
- перед початком експлуатації потрібно прочитати правила роботи саме з цим приладом і ретельно стежити за їх виконанням;

7.2.3 Розрахункова частина

Розрахунки штучного освітлення виконується для приміщення, де працюють Web-розробники.

Вихідні дані: розміри приміщення: А = 18 м, В = 12 м, Н = 3 м.

На підставі того, що розрахунки освітлення проводяться для офісного приміщення розробників, приймемо Е = 300 лк. Ухвалюємо загальну рівномірну систему освітлення. У якості джерела світла виберемо LED-SH-595-20 панель з кривою силою світла М (рівномірної). Для даного джерела світла $\boldsymbol{\lambda}$ =1,5.

Такі панелі рекомендується встановлювати в офісах з невисоким рівнем запиленості, тому що він виконаний у незахищеному корпусі. Характеристики наведено в таблиці 7.1.

Таблиця 7.1 – Характеристики лампи LED-SH-595-20

Розміщення світильників у приміщенні при системі загального освітлення залежить від розрахованої висоти їх підвісу h, яка звичайно задається розмірами приміщень. Найбільш вигідне співвідношення відстані між світильниками до розрахункової висоти підвісу:

$$\boldsymbol{\lambda} = \frac{\mathbf{L}}{\mathbf{h}}, \text{м}, \qquad (7.1)$$

де $\boldsymbol{\lambda}$ - ухвалюється залежно від типової кривої сили світла світильника.

Висота підвісу світильника визначається за формулою:

$$\boldsymbol{h} = \boldsymbol{H} - h_{св} - h_{рп} \qquad (7.2)$$

де:

Н-висота приміщення ;

$h_{св}$ - висота звисання світильника (від перекриття), м;

$h_{рп}$ - висота робочої поверхні над підлогою, м;

h $= \mathbf{3} - \mathbf{0},\mathbf{1} - \mathbf{0}.\mathbf{75} = \mathbf{2},\mathbf{15}$ м

Визначимо відстань між рядами світильників:

$\boldsymbol{L} = \ \boldsymbol{\lambda} \cdot \boldsymbol{h}$

$\boldsymbol{L} = \mathbf{1},\mathbf{5} \cdot \mathbf{2},\mathbf{15} = \mathbf{3},\mathbf{2}$м (7.3)

Відстань між крайніми світильниками й стіною, якщо робочі місця розташовані безпосередньо біля стін:

$$l = (0{,}25\ldots0{,}3)L = 0{,}25 \cdot \boldsymbol{L}\text{,м.} \quad (7.4)$$

1 = 0,25 · 3,2 = 0,8м.

Кількість рядів світильників $N_р$= 18/3,2 = 5,62 = 5 рядів.

Визначаємо число світильників в ряду:

$$\boldsymbol{N} = (\boldsymbol{A} - \boldsymbol{l}_{\text{св}})/\boldsymbol{l}_{\text{св}} \quad (7.5)$$

де А – ширина приміщення; $l_{св}$ – довжина світильника разом з відступами $l_{св}$=1,5.

$$\boldsymbol{N} = \frac{\mathbf{18} - \mathbf{1},\mathbf{5}}{\mathbf{1},\mathbf{5}} = \mathbf{11}(\text{од.});$$

Приймемо $\boldsymbol{N}$`=11 од.

Кількість світильників визначається по формулі:

N = N` · Np, од. (7.6)

N = 11 · 5 = 55 од.

Розрахунки загального освітлення виконаємо методом коефіцієнта використання. Необхідний світловий потік ламп у кожному світильнику F:

$$F = (E \cdot S \cdot k \cdot z)/N_{\sum} \cdot \eta \text{ (лм)} \quad (7.7)$$

де F – необхідний світловий потік ламп у кожному світильнику, лм;

S – освітлювана площа, м2;

k- коефіцієнт запасу (приймемо k =1,3);

z – коефіцієнт мінімальної освітленості, величина якого для LED ламп z = 1,2;

$\boldsymbol{N}$– число світильників у приміщенні, в даному випадку $\boldsymbol{N = 55}$

$\boldsymbol{\eta}$– коефіцієнт використання світлового потоку.

Для визначення коефіцієнта використання $\boldsymbol{\eta}$ визначимо індекс приміщення і:

$$\boldsymbol{i = \frac{A \cdot B}{h \cdot (A+B)}} \qquad (7.8)$$

где h – розрахункова висота підвісу, м.

$$\boldsymbol{i = \frac{18 * 12}{2,15 \cdot (18 + 12)} = 3,35}$$

Отримане значення і округляємо до найближчого табличного значення й ухвалюємо і = 3,5. Оцінюємо коефіцієнти відбиття поверхонь приміщення: стелі($\boldsymbol{\rho}_{\text{п}}$), стін ($\boldsymbol{\rho}_{\text{пс}}$) і робочої поверхні ($\boldsymbol{\rho}_{\text{р}}$).

Ухвалюємо: $\boldsymbol{\rho}_{\text{п}} = \boldsymbol{30\%}, \boldsymbol{\rho}_{\text{с}} = \boldsymbol{50\%}, \boldsymbol{\rho}_{\text{р}} = \boldsymbol{30\%}.$ За отриманими значенням і й $\boldsymbol{\rho}$ Визначаємо величину коефіцієнта використання світлового потоку для обраного світильника LED-SH-595-20. Для даного світильника $\boldsymbol{\eta}$ = 68%.

По формулі (7.7) визначаємо необхідний світловий потік світильника:

$\Phi = \boldsymbol{\frac{300 \cdot 216 \cdot 1,3 \cdot 1,2}{55 \cdot 0,68} = 2702}$ лм.,

Вибираємо лампу. У світильник слід встановити дві лампи LED-SH-595-20. Технічні характеристики обраної лампи:

− потужність 65 Вт;

− напруга 103 В;

− світловий потік після 100 годин горіння $\Phi_л = \mathbf{3000}$ лм.

Визначаємо розбіжність розрахунків при виборі лампи:

$$\mathbf{\Delta E} = \frac{((\Phi_л - \Phi_н) \cdot \mathbf{100\%})}{\Phi_н}, \% \qquad (7.10)$$

$$\mathbf{\Delta E} = \frac{\left((\mathbf{3000} - \mathbf{2702}) \cdot \mathbf{100\%}\right)}{\mathbf{2702}} = +\mathbf{11\%}.$$

Оскільки **ΔE** = +11 %, то результати розрахунків задовольняють умові припустимого відхилення розрахункової освітленості від нормованої освітленості більш ніж на -10…+20%. Звідси можна зробити вивід, що лампа LED-SH-595-20 може бути використана в даному приміщенні в якості джерела світла.

7.2.4 Безпека у випадку надзвичайної ситуації

На території Дніпропетровської області, у порівнянні з іншими регіонами, надзвичайні ситуації природного характеру спостерігаються нечасто. У регіоні практично не буває землетрусів, сходу сніжних лавин і зсувів, зазвичай морози не досягають -25°С, а спека +45°С.

Можливі надзвичайні ситуації природного, техногенного й соціального характеру:

− ураганний вітер, смерч;

− повінь;

− сильні снігопади

− виникнення аварії на енергетичних, інженерних і технологічних системах;

− радіоактивне зараження;

− вибух.

8 ВИСНОВКИ

Під час виконання курсового проекту була реалізована комп’ютерна система IT компанії “ThinkServeInc.” з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі, яка спеціалізується на розробці мобільних додатків та WEB сайтів. Для цього підприємства біло розраховано схему адресації для мережі 192.168.16.0/24 за принципом VLSM;

- було виконано вибір мережевого обладнання, яке б виконувало вимоги замовника і відповідало сучасним стандартам якості;
- налаштовано основні параметри пристрої і параметрів безпеки;
- налаштовано мережі VLAN, маршрутизація між VLAN;
- налаштовано маршрутизацію за допомогою протоколу EIGRP;
- реалізовані технології DHCP, PAT та ACL;
- виконано налаштування VPN тунелю між головним та віддаленим офісом;

Дипломний проект виконаний повністю відповідно до теми і завдання, оформлений відповідно до нормативних документів і методичного керівництва. Цілі, поставлені перед дипломним проектуванням, повністю виконані.

9 ПЕРЕЛІК ПОСИЛАНЬ

1. https://en.wikipedia.org/wiki/Industry_4.0

2. **https://ain.ua/2019/08/29/it-obzor-nix/**
3. **https://dou.ua/lenta/articles/coronacrisis-in-ukrainian-it-may/?from=header**
4. Новожилов, О. П. Інформатика: підручник для прикладного бакалаврату / О. П. Новожилов. - 3-е вид.
5. Стивенс У. Р. Протоколы TCP/IP: практичное рук. / У. Р. Стивенс / пер. с англ. – СПб. : «Невский диалект» – «БХВ-Петербург», 2003. – 672 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101" Уэнделл Одом (Cisco CCENT/CCNA ICND1 100-101: Official Cert Guide)
7. https://escadra.com.ua/ua/ukraina-zanyala-pervoe-mesto-v-evrope-v-otrasli-it-autsorsinga-i-razrabotki-po.html
8. CCNA: Cisco Certified Network Associate: Review Guide Todd Lammle 978-1-118-06346-0
9. В. Олифер, Н. Олифер "Компьютерные сети. Принципы, технологии, протоколы. Учебник" (2016)
10. Д. Куроуз, К. Росс "Компьютерные сети. Нисходящий подход" (2016)

Додаток А.

Текст програми налаштування корпоративної мережі

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.20005-01 2 2

Листів 12

2020

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи.

Програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену комп’ютерної системи.

Зміст

Налаштування маршрутизатора Baidak_Router_3

```
version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

//Шифрування паролів

service password-encryption

!

//Ім’я пристрою

hostname Baidak_Router_3

!

//Пароль до привілейованого режиму

enable secret cisco

!

ip dhcp excluded-address 192.168.18.128 192.168.18.137

ip dhcp excluded-address 192.168.18.161 192.168.18.170

ip dhcp excluded-address 192.168.18.193 192.168.18.202

ip dhcp excluded-address 192.168.18.225 192.168.18.234

!
```

Налаштування DHCP

```
ip dhcp pool poolVlan12
 network 192.168.18.160 255.255.255.224
 default-router 192.168.18.161
 dns-server 192.168.24.254
ip dhcp pool poolVlan22
 network 192.168.18.192 255.255.255.224
 default-router 192.168.18.193
 dns-server 192.168.24.254
ip dhcp pool poolVlan32
 network 192.168.18.224 255.255.255.224
 default-router 192.168.18.225
 dns-server 192.168.24.254
```

Налаштування AAA

```
aaa new-model
!
aaa authentication login RADIUS_LIST group radius local
aaa authentication login default local
!
no ip cef
no ipv6 cef
!
//Створення користувача з паролем
```

```
username 123161_Baidak password 7 082048430017061E010803
username Baidak_Router_1 password 7 082048430017544541
!
license udi pid CISCO2901/K9 sn FTX152446OQ-
license boot module c2900 technology-package securityk9
!
```

Створення VPN

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp key cisco address 64.100.13.2
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map CMAP 10 ipsec-isakmp
 set peer 64.100.13.2
 set transform-set TS
 match address FOR-VPN
!
```

Створення домену

```
no ip domain-lookup

ip domain-name Baidak_Router_1

!

spanning-tree mode pvst

!
```

Налаштування інтерфейсів

```
interface GigabitEthernet0/0

 no ip address

 ip nat inside

 duplex auto

 speed auto

!

//Налаштування підінтерфейсів VLAN

interface GigabitEthernet0/0.12

 encapsulation dot1Q 12

 ip address 192.168.18.161 255.255.255.224
```

Налаштування протоколу маршрутизації

```
router eigrp 1

 redistribute static

 passive-interface GigabitEthernet0/0

 passive-interface GigabitEthernet0/1

network 192.168.18.160
```

network 192.168.18.192

network 192.168.18.224

network 192.168.18.128

network 10.1.2.0

!

Налаштування NAT

ip nat pool INTERNET 209.165.200.5 209.165.200.30 netmask 255.255.255.224

ip nat inside source list FOR-NAT pool INTERNET overload

ip classless

ip route 209.165.201.0 255.255.255.0 209.168.200.1

ip route 0.0.0.0 0.0.0.0 209.165.200.1

!

ip flow-export version 9

!

ip access-list extended FOR-VPN

permit ip 192.168.96.0 0.0.7.255 192.168.100.0 0.0.0.127

ip access-list extended FOR-NAT

deny ip 192.168.96.0 0.0.7.255 192.168.100.0 0.0.0.127

permit ip 192.168.96.0 0.0.7.255 any

! //Налаштування банеру

banner motd Baidak_Router_1

```
!
radius-server host 192.168.101.27 auth-port 1645 key radius123
!
```

Налаштування консольних та vty ліній

```
line con 0
 password 7 0822455D0A16
 login authentication RADIUS_LIST
!
line aux 0
!
//Налаштування паролів
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
```