

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 бакалавра
(бакалавра, спеціаліста, магістра)

студента Постольника Костянтина Олеговича
(ПІБ)

академічної групи 123-17-ск1
(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 комерційного банку "Райзе Банк" з
детальним опрацюванням побудови, налаштування та безпеки
корпоративної мережі»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	ас. Бешта Л.В.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розрахунок мережі	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 системта технологій

(повна назва)

Гнатушенко В.В.

(підпис)

(прізвище, ініціали)

**ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр**студента Постольника К.О.

(прізвище та ініціали)

академічної групи 123-17-ск1

(шифр)

спеціальності 123 «Комп'ютерна інженерія»за освітньо-професійною програмою 123 «Комп'ютерна інженерія»

(офіційна назва)

на тему "Комп'ютерна система комерційного банку "Райзе Банк" здетальним опрацюванням побудови, налаштування та безпеки корпоративноїмережі» затверджену наказом ректора НТУ «Дніпровська політехніка» від21.05.2020 № 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	10.05.209
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи	17.05.2019
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи з опрацюванням побудови і захисту інформації та налаштуванням корпоративної мережі	24.05.2019
Економічна частина	Економічно обґрунтувати доцільність витрат на створення та дослідження системи керування	30.06.2019
Охорона праці	Розробити організаційно-технічні заходи, щодо реалізації правил безпеки при експлуатації системи	1.06.2019

Завдання видано

ас.Бешта Л.В.

(прізвище, ініціали)

(підпис керівника)

Дата видачі 27 січня 2020 р.

Дата подання до екзаменаційної комісії

24.06.2020 р.

Прийнято до виконання

Постольник К.О.

(прізвище, ініціали)

(підпис студента)

РЕФЕРАТ

Пояснювальна записка: 98 с., 19 рис., 11 табл., 1 додаток, 28 джерел.

Об'єкт розробки: комп'ютерна система комерційного банку з опрацюванням побудови та налаштуванням корпоративної мережі.

Завданням на кваліфікаційну роботу є побудова комп'ютерної системи комерційного банку "Райзе Банк" з опрацюванням побудови, безпеки та налаштуванням корпоративної мережі. Також у побудові схеми банку необхідно використати технологію VPN для захисту даних.

Мета: модернізація комп'ютерної системи комерційного банку "Райзе Банк".

Розроблена комп'ютерна система з можливістю швидко та безпечно обмінюватися інформацією, орієнтована на оброблення вхідних даних, а також для збору і підготовки статистичної інформації.

Система виконана відкритою і дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання наступних функцій:

- швидкий обмін інформацією;
- збільшення надійності зберігання, обробки та передавання інформації;
- полегшення роботи у системі.

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

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

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатку.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів	6
Вступ	7
1 Стан питання і постановка завдання	8
1.1 Стисла характеристика галузі та умов застосування системи, що проектується	10
1.2 Характеристика і структура об'єкта впровадження з наведенням необхідного графічного матеріалу у вигляді схеми організаційної структури підприємства	11
1.3 Стислі відомості про технології збору та передачі інформації для об'єкта впровадження з топологічною схемою розміщення структурних підрозділів підприємства	14
1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об'єкта впровадження	16
1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об'єкта проектування, відомих рішень у галузі, що розглядається, або в інших галузях	20
1.6 Завдання і мета роботи, що виконується	21
1.7 Визначення можливих напрямків рішення поставлених завдань	22
2 Технічні вимоги до системи	21
2.1 Вимоги до системи в цілому	
2.2 Вимоги до структури і функціонуванню системи	22
2.3 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему	
2.4 Вимоги до показників призначення системи	24
2.5 Вимоги до безпеки системи	25
3 Розробка апаратної частини комп'ютерної системи підприємства	37
3.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи	
3.2 Розробка специфікації апаратних засобів КС	39
3.3 Розробка архітектури мережі підприємства	41

3.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства	45
4 Проектування корпоративної мережі та перевірка роботи комп'ютерної системи підприємства	48
4.1 Розрахунок схеми адресації корпоративної мережі	
4.2 Розробка фізичної топологічної схеми корпоративної мережі	52
4.3 Налаштування та перевірка роботи комп'ютерної системи	54
4.3.1 Базове налаштування конфігурації пристроїв	
4.3.2 Налаштування маршрутизаторів корпоративної мережі	56
4.3.3 Налаштування роботи Інтернет	60
4.4.4 Налаштування агрегування каналів	62
4.4.5 Налаштування віртуальної приватної мережі site-to-site VPN	63
4.4.6 Перевірка роботи комп'ютерної системи	65
5 Захист інформації в комп'ютерній системі від несанкціонованого доступу	69
5.1 Розробка методів для захисту інформації в комп'ютерній системі	
5.2 Налаштування маршрутизаторів на підтримку служби AAA	
5.3 Налаштування мереж VLAN	70
5.4 Налаштування параметрів безпеки комутаторів та адресації	74
ПК в мережах VLAN	
6 Економічна частина	77
6.1 Техніко-економічне обґрунтування розробки	
6.2 Розрахунок капітальних витрат на придбання складових КС	
6.2.2 Розрахунок капітальних витрат на програмне забезпечення	79
6.2.2.1 Розрахунок часу на розробку програмного забезпечення	
6.2.2.2 Розрахунки витрат на розробку програмного продукту	81
6.3 Розрахунок річних експлуатаційних витрат	83
6.3.1 Розрахунок амортизаційних відрахувань	
6.3.2 Розрахунок річного фонду заробітної плати	84

	5
6.3.3 Розрахунок відрахувань на соціальні заходи	85
6.3.4 Визначення річних витрат на технічне обслуговування і поточний ремонт	
6.3.5 Розрахунок вартості споживаної електроенергії	86
6.3.6 Визначення інших витрат	
6.4 Визначення та аналіз показників економічної ефективності проекту	87
6.5 Висновок	88
7 Охорона праці	89
7.1 Інженерно-технічні заходи щодо охорони праці на об'єкті	
7.1.1 Клас приміщення по небезпеці поразки електричним струмом	
7.1.2 Режим нейтралі електричних мереж, застосовуваних на об'єкті	
7.1.3 Заходи щодо електробезпеки	90
7.1.4 Протипожежні заходи для об'єкта досліджень	91
7.2 Розрахунок системи освітлення.	93
Висновок	96
Перелік посилань	97
Додаток	98

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БМ – банківська мережа

КМ – комп'ютерна мережа

VPN – мережа VPN

LAN - локальна обчислювальна мережа, ЛВС

ЕОМ - Електронна обчислювальна машина

ПВХ - Полівінілхлоридна ізоляція

Cisco Packet Tracer - це багатofункціональна програма моделювання мереж

DNS-сервер, Domain name system - додаток, призначений для відповідей на DNS-запити за відповідним протоколом

VLAN - Virtual Local Area Network — віртуальна локальна комп'ютерна мережа

TCP/IP - набір протоколів мережі Інтернет

Ethernet - LocalAreaNetwork - з'єднує кілька різних пристроїв, розташованих поруч

IP-адреса - унікальний ідентифікатор комп'ютера локальної мережі або мережі Інтернет.

грн. – гривень

люд.-годин – людино-годин

міс. – місяців

м. – метрів

шт. – штук

Лк. – люкси

ВСТУП

В даний час у зв'язку з поголовної інформатизацією і комп'ютеризацією банківської діяльності вагу інформаційної безпеки банків сильно зріс. Це обумовлено повсюдним розповсюдженням електронних платежів, пластикових карт, комп'ютерних мереж об'єктом інформаційних атак стали безпосередньо грошові кошти, як банків, так і їх клієнтів. Більше 90% всіх злочинів пов'язана з використанням автоматизованих систем обробки інформації банку.

Це послужило серйозним приводом до прийняття рішення про створення надійної корпоративної мережі комерційного банку, з використанням захисту мережі у вигляді VPN-мережі. Віртуальна приватна мережа (скорочено: VPN) перенаправляє ваш інтернет-трафік через сервери VPN. При цьому також ховається вашу IP-адресу, а ваш вихідний трафік стає анонімним. Крім того, всі передані через підключення дані шифруються. Це означає, що ніхто не зможе відстежувати ваші цифрові транзакції.

У минулому році був схожий проект, коли будували VPN-мережу між головним банком і відділенням банку. Основною проблемою було те, що корпоративна мережа замовника характеризувалася високим рівнем вразливості до інсайдерських атак і загрозам ззовні. Результатом було зниження спроб до отримання даних клієнтів, та збільшення рівня захисту секретних даних.

Тема безпеки БМ дуже актуальна у наш час, через те, що здійснити спробу розкрадання може будь-хто, необхідно лише наявність комп'ютера, підключеного до мережі та Інтернет. Причому для цього не потрібно фізично проникати в банк, можна «працювати» і за тисячі кілометрів від нього.

Метою даної кваліфікаційної роботи було побудування мережі банку з передаванням даних з відділення у головний банк, використовуючи оптоволокну, та огляд обладнання та безпеки інформації банку використовуючи VPN-мережу.

1 СТАН ПИТАННЯ

1 Стан питання і постановка завдання

1.1 Стисла характеристика галузі та умов застосування виробу, що проектується

У загальному вигляді під банківською системою розуміється сукупність різних видів банків та банківських інститутів, за допомогою яких здійснюється мобілізація коштів і надаються клієнтурі різноманітні послуги з прийому вкладів і надання кредитів.

Банківська система — це не довільне явище, а складова частина кредитно-грошової системи, елемент економічного базису суспільства, що розвивається за законами ринкової економіки. Ця система є внутрішньо організована, взаємопов'язана, має загальну мету та завдання.

Банківська система існує в будь-якій країні в певний історичний період і є складовою частиною кредитної системи держави. Для нормального функціонування банківська система має відповідати наступним вимогам.

Сучасні комерційні банки є багатофункціональними установами, які діють в різних секторах ринку позичкового капіталу і фактично займаються всіма видами кредитних і фінансових операцій, пов'язаних з обслуговуванням господарської діяльності своїх клієнтів. Враховуючи, що основне навантаження щодо фінансово-кредитного обслуговування припадає саме на комерційні банки, їх часто називають "супермаркетами фінансового ринку".

В сучасних умовах спостерігаються тенденції розмежування функцій та операцій комерційних банків з метою універсалізації їхньої роботи, підвищення ефективності банківської діяльності та одержання прибутків.

Різноманітність послуг, що надаються комерційними банками, не означає, що всі вони виконують однаковий набір операцій. Кожен банк визначає сферу своєї діяльності, виходячи із потреб клієнтури, яку він обслуговує. Проте існує ряд основних, базових функцій комерційного банку, які дозволяють зарахувати даний фінансовий інститут до установ банківської системи. До таких основних функцій комерційного банку, що визначають його економічну суть, слід віднести: посередництво в кредиті, посередництво в розрахунках і платежах, випуск кредитних знарядь обігу.

Банківська система України є одним з найбільш динамічно розвинутих секторів національної економіки, де перехід до ринкових відносин відбувався досить швидко і де реально проходив процес демонополізації, проявилася конкуренція, гроші та кредит набули ринкового змісту.

У дипломному проекті була задача розробити мережу банку, що має головний банк, та відділення з описом побудови та оглядом цієї мережі та технології VPN для захисту переданих даних.

1.2 Характеристика і структура об'єкта впровадження з наведенням необхідного графічного матеріалу у вигляді схеми організаційної структури підприємства



Рисунок 1.1 – Схема організації структури банку

Основними органами управління банком є збори акціонерів банку. Цей орган збирається, як правило, 1 раз на рік і здійснює загальне керівництво діяльністю (приймає і вносить зміни до статуту банку, затверджує річний звіт про роботу банку, визначає основні напрями його роботи).

Збори акціонерів обирають голову та Раду банку, а також призначають голову правління банком. Раду і голову обирають на 5 років у представників, засновників та акціонерів банку, вони здійснюють загальне керівництво діяльністю банку в період між зборами акціонерів. Засідання Ради банку збирається 1 раз на квартал.

Правління банку є виконавчим органом банку, здійснює керівництво і управління поточною діяльністю банку. Воно збирається не більше 2 разів на місяць. Голова Правління банку керує всією діяльністю банку, представляє

банк в інших організаціях, підписує договори, несе відповідальність за його роботу.

Ревізійна комісія банку є його контролюючим органом, формується із представників акціонерів і затверджується рішенням зборів акціонерів.

Функціональними підрозділами, що безпосередньо здійснюють банківські операції та обслуговують клієнтів, є управління, департаменти та відповідні служби банку.

Мережа у банку необхідна відділам, які виконують операції з клієнтами, та які потребують передачі даних до головного офісу, а саме: економічне управління; управління депозитів; управління розрахунків; управління цінних паперів; управління валютних операцій; операційне управління; управління касових операцій; управління з розвитку міжнародних зв'язків; депозитні відділи; кредитні відділи. Даним відділенням необхідна мережа для з'єднання з головним банком та передачі усіх даних безпосередньо до нього, а саме : передавання та отримання даних щодо кредитів, отримання інформації щодо клієнтів та надсилання запиту щодо тих чи інших питань клієнтів, надсилання інформації щодо сплати рахунків та інших платежів, отримання кредитної історії клієнтів тощо.

1.3 Стислі відомості про технології збору та передачі інформації для об'єкта впровадження з топологічною схемою розміщення структурних підрозділів підприємства

У проекті було побудовано мережу, що з'єднує головний офіс банку та відділення банку, задля збирання інформації у відділенні та передачі даних до головного офісу.

Збір інформації передбачає отримання максимально вивіреної вихідної інформації і є одним з відповідальних етапів в роботі з інформацією. Технологія збору на увазі використання певних методів збору інформації та технічних засобів, які обирають залежно від виду інформації і

застосовуваних методів її збору. Заключним етапом збору є її перетворення в дані, тобто в інформацію, придатну для обробки засобами обчислювальної техніки.

Коли збір інформації завершено, зібрані дані зводяться в систему для створення, зберігання та підтримання в актуальному стані інформаційного фонду, необхідного для виконання різних завдань в діяльності об'єкта управління.

Для збору текстової та графічної інформації застосовуються такі засоби як клавіатура, маніпулятори, сканер, планшет, сенсорний екран, монітор.

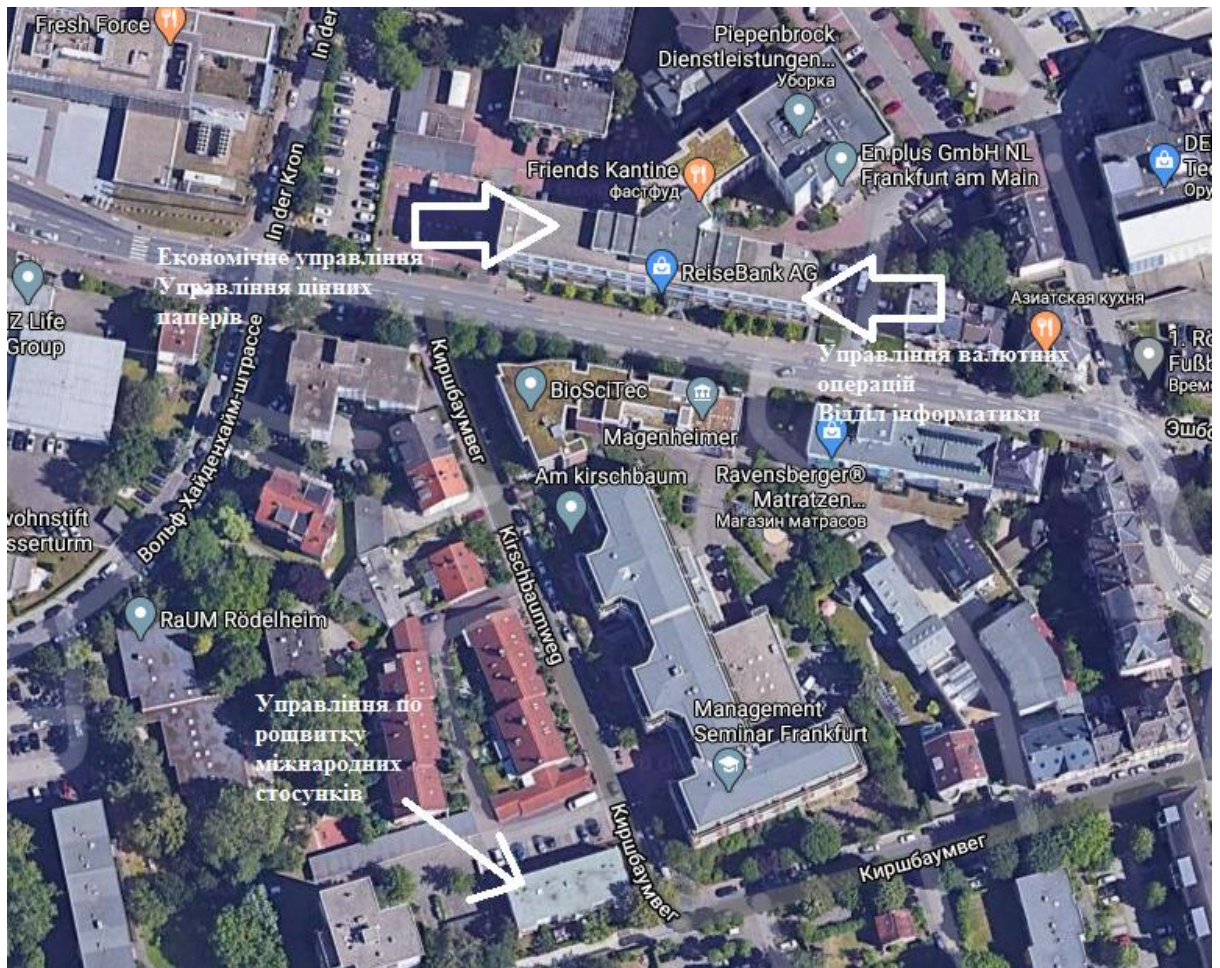


Рисунок 1.2 – Топографічна схема об'єкта впровадження

Тобто, іншими словами, локальна комп'ютерна мережа - це два або більше комп'ютерів, об'єднаних між собою будь-якими засобами передачі даних. Засоби передачі даних в основному в себе включають:

середу передачі даних - пасивне обладнання (кабель - вита пара, оптоволокло або радіоканал, розетки, монтажні коробки, монтажні шафи, панелі і т. д.); активне мережеве обладнання (сервер, концентратор, комутатор, маршрутизатор, модем та ін.).

Прокладка комп'ютерної мережі, як правило, складається з ряду етапів:

1. Вивчаються і вимірюються приміщення, в яких буде прокладатися мережа, складається план приміщень з нанесенням на нього передбачуваних місць розміщення робочих станцій.

Проектується топологія мережі, схеми розводки кабелю між робочими станціями, сервером і іншим мережевим обладнанням, які наносяться на план приміщення.

2. Вивчається функціональне призначення кожного робочого місця, розраховується загальне навантаження на мережу.

3. Складається перелік мережевого обладнання, яке буде використано в проектованій мережі.

4. Складається список необхідних сервісів мережі. Виконується розрахунок оптимальної конфігурації сервера.

5. Складається загальний кошторис витрат на будівництво мережі. Кошторис затверджується клієнтом.

6. Закупаються мережеве обладнання та компоненти сервера і робочих станцій.

7. Проводяться кабель, при необхідності - коробка (пасивне мережеве обладнання).

8. Встановлюється і підключається активне мережеве обладнання.

9. Встановлюються і налаштовуються сервери і робочі станції.

Отже, організація локальної комп'ютерної мережі вимагає від підприємства таких витрат:

- на оплату проектування, прокладки кабелю, монтажу розеток, установки роз'ємів, коробів і т.д.
- на закупівлю пасивного та активного мережевого обладнання;
- на установку і підключення (наладку) активного мережного обладнання.

1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об'єкта впровадження

Для побудування мережі LAN (локальна обчислювальна мережа, ЛВС) усередині банку використовується вита пара. Вита пара являє собою структурований LAN кабель з ПВХ оболонкою, який містить в собі від однієї до кількох ізольованих і скручених між собою пар певною кількістю витків на одиницю довжини. Точніше використовується вита пара типу FTP, за рахунок фольги може захистити сигнал від незначних перешкод при невисокій напрузі.

У якості категорії кабеля виті пари використовують CAT5e (частотна смуга 125 МГц). Це вдосконалена кручена пара п'ятої категорії. При використанні 2-х пар підтримує швидкість передачі даних до 100 Мбіт / с і до 1000 Мбіт / с в 4-х парному кабелі. Як правило, використовується 4-х парний кабель для побудови локальної комп'ютерної мережі. Це найпоширеніший тип крученої пари.

Для передавання інформації між відділенням банку та центральним банком, використовується універсальний оптоволоконний кабель. Дана група кабелів універсальна. Вона підходить для прокладки всередині приміщення, і для зовнішньої прокладки, і навіть прокладки в кабельну каналізацію і застосовується для задування в спеціальні кабельний труби. Ці кабелі вологостійкі, в них закладені велике розтяжне зусилля за рахунок додаткових

силових елементів і в той же час такі оптичні кабелі досить простої конструкції і дуже зручні при установці і монтажі.

У якості сфери застосування кабелю використовується прокладка у ґрунті. Прокладаються кабелі в землю також і в звичайні траншеї, шириною близько 50 см, а також в міні-траншеї. Останні мають ширину близько десяти сантиметрів. Вони використовуються при прокладанні в землі на котеджних ділянках і газонах. Глибина прокладки кабелю таким способом не велика, зате при цьому не псується зовнішній вигляд ділянок. В Європі популярна технологія монтажу кабелю в асфальтне покриття. Асфальт прорізається за допомогою спеціального ножа, аналогічного тому, який використовується у нас для ремонту доріг. Далі, в отриману траншею шириною від 19 до 32 мм і глибиною до 305 мм укладається кабель. Кабель може захищатися або спеціальним коробом, або декількома шарами захисних матеріалів, які укладаються над ним. Вузька і дрібна траншея забезпечує проходження оптоволокна в ґрунті над наявними комунікаціями, завдаючи мінімальної шкоди інфраструктурі доріг. Після прокладки кабелю, такі траншеї заливаються бітумом. Найбільшого поширення цей метод отримав в Скандинавії. У нашій же країні він не знайшов широкого застосування в основному через низьку якість дорожнього покриття.

Кабелем для прокладання в ґрунт є кабель, який має в своїй конструкції броню, що забезпечує можливість монтажу оптики в різних трубопроводах і інших ділянках, що відрізняються несприятливим середовищем. Для захисту від попадання вологи, такий кабель оснащений стрічкою, яка блокує потрапляння води, вона розташована між бронею і модулями.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об'єкта проектування, відомих рішень у галузі, що розглядається, або в інших галузях

Обробка інформації полягає в отриманні одних "інформаційних об'єктів" з інших "інформаційних об'єктів" шляхом виконання деяких алгоритмів і є однією з основних операцій, здійснюваних над інформацією, і головним засобом збільшення її обсягу і різноманітності.

На самому верхньому рівні можна виділити числову і нечислову обробку. У зазначені види обробки вкладається різне трактування змісту поняття "дані". При числовій обробці використовуються такі об'єкти, як змінні, вектори, матриці, багатовимірні масиви, константи і т.д. При нечисловій обробці об'єктами можуть бути файли, записи, поля, ієрархії, мережі, відносини і т.д. Інша відмінність полягає в тому, що при числовій обробці зміст даних не має великого значення, в той час як при нечисловій обробці нас цікавлять безпосередні відомості про об'єкти, а не їх сукупність в цілому.

З точки зору реалізації на основі сучасних досягнень обчислювальної техніки виділяють наступні види обробки інформації:

- послідовна обробка, застосовувана в традиційній Фоннеймановській архітектурі ЕОМ, котра володіє одним процесором;
- паралельна обробка, застосовувана при наявності декількох процесорів в ЕОМ;
- конвеєрна обробка, пов'язана з використанням в архітектурі ЕОМ одних і тих же ресурсів для вирішення різних завдань, причому якщо ці завдання тотожні, то це послідовний конвеєр, якщо завдання однакові - векторний конвеєр.

Способи передачі даних в мережах здійснюються трьома способами:

Напівдуплексна передача. Прийом і передача даних виконуються по черзі.

Двунаправлена (дуплексний). В даному випадку кожна зі станцій одночасно отримує і передає інформацію.

Односпрямована (симплексна). Так само як радіо і ТБ.

Для того щоб виконати передачу інформації в інформаційних системах, в більшості випадків використовується найперша організація передачі даних в мережі.

Передача даних класифікується на два основні методи:

- асинхронний. Застосовується він в тих системах, де обмін даними здійснюється постійно і не потребує високої швидкості передачі.

- синхронний. В даному випадку інформація передається певними блоками. Тут можуть передаватися не тільки символи, а й потік бітів. Ці способи передачі даних в обчислювальних мережах вважаються найефективнішими з вбудованим надійним механізмом виявлення помилок.

Відомим випадком застосування VPN-технологій, був випадок застосування в банку в 2018 році. Інфраструктура Банку концентрується на 18 майданчиках: один головний офіс і сімнадцять додаткових. Локально-обчислювальні мережі додаткових офісів компанії об'єднані з головним в єдину мережу засобами провайдера зв'язку. Однак комунікації між ними мали ряд недоліків:

- використання одного провайдера зв'язку не забезпечувало відмовостійкості каналів зв'язку;

- послуги, що надаються провайдером, були дорогими для компанії;

- використовуваний раніше маршрутизатор не володів серйозними засобами захисту інформації, використання його для подальшого розвитку Банку було небезпечно;

- фактично банк не міг керувати своєю мережею, тому що вона була побудована на обладнанні провайдера.

Таким чином, корпоративна мережа замовника характеризувалася високим рівнем вразливості до інсайдерськими атакам і загрозам ззовні. Це послужило серйозним приводом до прийняття рішення про створення надійної VPN-мережі всередині організації, без прив'язки до одного провайдера з використанням нового сучасного обладнання.

Виконання проекту по створенню захищеної мережі передачі даних між головним і додатковими офісами Банк Розвитку Регіону довірив фахівцям компанії Softline. Забезпечення мережевої безпеки є одним з найбільш актуальних і затребуваних напрямів в портфелі послуг і рішень компанії Softline. Накопичений досвід реалізації комплексних проектів, професійна підготовка інженерів зумовили вибір Банку на користь компетенцій Softline.

Перед проектною командою Softline були поставлені наступні завдання:

- побудова VPN-каналу між головним і додатковими офісами замовника і філіями;

- виділення демілітаризованої зони, яка відділяє загальнодоступні сервери від внутрішньої мережі;

- виділення в головному офісі замовника двох каналів зв'язку.

Фахівці Softline провели аналіз існуючої мережевої інфраструктури, за результатами якого було визначено перелік вимог до системи. Проектна команда Softline в якості оптимального засоби організації надійної VPN-мережі запропонувала використовувати програмно-апаратний комплекс Cisco в головному і в усіх додаткових офісах замовника. Вибір на користь ПО Cisco був зроблений не випадково: по-перше, продукти виробника є провідними для вирішення завдань даного класу і, по-друге, компетенції Softline, підтвержені статусом Cisco Premier Partner і спеціалізацією Advanced Security, дозволяють здійснювати комплексні проекти по напрямку мережевої безпеки і гарантувати необхідний замовником рівень сервісу.

Реалізація проекту здійснювалася в два етапи. Перша частина робіт виконувалася в головному офісі Банку, де була сформована тестова зона, яка відображала реалізовану схему модернізації.

Другий етап, в ході якого проведено роботи по підключенню, налаштуванню і введення в експлуатацію нового обладнання, проходив в додаткових офісах і операційних касах Банку. По завершенні проекту фахівці Softline запропонували ряд рекомендацій щодо подальшого вдосконалення мережевої інфраструктури, а також концепцію розвитку ІТ в цілому.

За словами Михайла Селіванова, керівника відділу управління проектами Softline, «модернізація мережевої інфраструктури - це лише перший крок Банку на шляху побудови і модернізації своєї ІТ-інфраструктури, яка буде відповідати світовим стандартам. Я впевнений, керівництво Банку Розвитку Регіону оцінить нашу допомогу в цьому проекті, і ми продовжимо нашу співпрацю з побудови ефективної системи ІТ ».

«Головним результатом реалізованого проекту ми вважаємо те, що фахівці Softline створили захищену корпоративну VPN-мережу, не прив'язану до одного провайдера. До цього в компанії все локально-обчислювальні мережі були пов'язані засобами провайдера зв'язку, що не забезпечувало необхідного рівня відмовостійкості та безпеки. Крім того, використовуваний раніше маршрутизатор не відповідав необхідному рівню захисту зростаючого бізнесу. Установка і введення в промислову експлуатацію нового обладнання Cisco дозволили нам не тільки забезпечити безперервність ключових бізнес-процесів, а й скоротити експлуатаційні витрати за рахунок об'єднання в ньому можливостей брандмауера, запобігання вторгнень і VPN. Ми задоволені рівнем професіоналізму фахівців Softline, умінням розуміти, оперативно і ефективно вирішувати реальні завдання бізнесу. Всі поставлені в рамках проекту завдання були вирішені в повній мірі і в строк », - каже Габанна Володимир, начальник ІТ-відділу Банку Розвитку Регіону.

1.6 Завдання і мета роботи, що виконується

Метою проекту було всебічне та достовірне вивчення побудови мережі для комерційного банку з використанням технологій VPN.

У даному проекті необхідно побудувати мережу між головним банком та невеликим відділенням, використовуючи оптоволокно для з'єднання між банком та відділенням, та використовуючи виту пару всередині банку. Також при побудуванні проекту необхідно використати технологію VPN, для захисту переданих даних банку. Дану схему необхідно побудувати у програмі Cisco Packet Tracer.

1.7 Визначення можливих напрямків рішення поставлених завдань

Для вирішення поставлених завдань було запропоновано використання всередині банку витої пари, для з'єднання між відділенням та банком використати оптоволокно. Також побудувати локальну мережу (LAN), вони з'єднують групи комп'ютерів і різні низьковольтні на коротких відстанях (одна будівля, група з двох або трьох будівель які знаходяться поруч) для обміну даними та ресурсами. У якості технології передачі даних використовується Ethernet. Ethernet - це набір описів способів фізичної передачі сигналів на першому рівні моделі OSI і формування кадрів на другому рівні моделі OSI всередині локальних мереж LAN. У якості програми для побудови мережі використовується Cisco Packet Tracer.

2 ТЕХНІЧНІ ВИМОГИ ДО СИСТЕМИ

2.1 Вимоги до системи в цілому

Відповідність до стандартів є лише однією з багатьох вимог, що пред'являються до сучасної мережі. Важливішим є виконання мережею певного набору послуг, наприклад, надання доступу до файлових архівів або веб-сторінок публічних Internet-сайтів, обмін електронною поштою в межах підприємства або в глобальних масштабах, інтерактивний обмін голосовими повідомленнями IP-телефонії тощо.

Решта вимог — продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість — пов'язані з якістю виконання цього основного завдання.

І хоча всі перераховані вище вимоги є важливими, часто поняття «Якість обслуговування» КМ трактується вузьче: воно містить лише дві важливі характеристики мережі — продуктивність і надійність.

У мережі повинно бути три сервера, розподіл функцій по ним наступне:

- на першому: тільки сервер додатки;
- на другому: файловий сервер, міст в глобальну мережу, засоби шифрування, засоби моніторингу трафіку;
- на резервному: копії програм з першого і другого серверів (але без зв'язку з глобальною мережею), а також копії даних з основних серверів.

На резервний сервер дані автоматично копіюються кожен день. Резервний сервер включається в роботу в разі збою одного (або обох) з основних. Також, з резервного сервера можуть бути відновлені випадково зіпсовані дані.

До серверів підключені клієнтські машини співробітників банку. Склад працівників вважається досить статичним, тому для кожного створена своя обліковий запис з конкретними правами.

Вимоги до задач виконуваних мережею:

- по кожній підсистемі – перелік функцій, задач чи їхніх комплексів (у тому числі частин, що забезпечують взаємодію системи Системи), що підлягають автоматизації;
- при створенні системи в двох чи більше черг – перелік функціональних підсистем, окремих функцій чи задач, що вводяться в дію в 1-й і наступних чергах;
- часовий регламент і вимоги до якості реалізації кожної функції, задачі (чи комплексу задач), форми представлення вихідної інформації, характеристики необхідної точності і часу виконання, вимоги одночасності виконання групи функцій, вірогідності видачі результатів;
- перелік і критерії відмов для кожної функції, по якій задаються вимоги до надійності.

2.2 Вимоги до структури і функціонування системи

Продуктивність. Потенційно висока продуктивність — це одна з основних переваг розподілених систем, до яких відносяться КМ. Ця властивість забезпечується принциповою можливістю розподілу робіт.

Основні характеристики продуктивності мережі:

- час реакції мережі.
- швидкість передачі трафіку.
- пропускна здатність.
- затримка передачі і варіанти затримки передачі.

Час реакції мережі

В загальному випадку час реакції визначається як інтервал між відправленням запиту користувача до мережної служби і отриманням відповіді на нього.

Час реакції мережі є інтегральною характеристикою продуктивності мережі з погляду користувача. Саме цю характеристику має на увазі користувач, коли говорить: «Сьогодні мережа працює поволі».

Значення цього показника залежить від типу служби, до якої звертається користувач, від того, який користувач і до якого сервера звертається, а також від поточного стану елементів мережі — завантаженості сервера та сегментів, комутаторів і маршрутизаторів, через які проходить запит.

Тому, варто усереднювати цей показник по користувачах, серверах і годинах доби (від чого в значній мірі залежить завантаження мережі).

Час реакції мережі складається з кількох складових.

- час підготовки запитів на клієнтському комп'ютері.
- час передачі запитів між клієнтом і сервером через сегменти мережі і проміжне комунікаційне устаткування.
- час обробки запитів на сервері.
- час передачі відповідей від сервера до клієнта.
- час обробки отриманих від сервера відповідей на клієнтському комп'ютері.

Очевидно, що розкладання часу реакції на складові користувачу не є цікавим, головним є кінцевий результат. Проте, для мережного фахівця дуже важливим є виділення з загального часу реакції складових, що відповідають етапам власне мережної обробки даних, — передачі даних від клієнта до сервера через сегменти мережі і комунікаційне обладнання.

Знання мережних складових часу реакції дозволяє оцінити продуктивність окремих елементів мережі, виявити вузькі місця і за

необхідності виконати модернізацію мережі для підвищення її загальної продуктивності.

2.3 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему

Офіс банку розрахований на 30-40 працівників. Серед них кілька (3-5) касирів, один адміністратор мережі, один керівник відділення, інші - звичайні працівники, які виконують основні завдання.

Необхідні компоненти системи:

1. Сервер програми (з підтримкою банківської програмної системи).
2. Файловий сервер.
3. Засоби доступу в глобальну мережу.

2.4 Вимоги до показників призначення системи

Для технічного забезпечення системи наводять вимоги:

- до видів технічних засобів, у тому числі до видів комплексів технічних засобів, програмно-технічних комплексів та інших комплектуючих виробів, припустимих до використання в системі;
- до функціональних, конструктивних і експлуатаційних характеристик засобів технічного забезпечення системи .
- У вимогах до метрологічного забезпечення приводять:
- попередній перелік вимірювальних каналів;
- вимоги до точності вимірів параметрів і до метрологічних характеристик вимірювальних каналів;
- вимоги до метрологічної сумісності технічних засобів системи;
- перелік керуючих і обчислювальних каналів системи , для яких необхідно оцінювати характеристики точності;

- вимоги до метрологічного забезпечення технічних і програмних засобів, що входять до складу вимірювальних каналів системи, засобів убудованого контролю, метрологічної придатності вимірювальних каналів і засобів вимірів, використовуваних при налагодженні й випробуваннях системи;
- вид метрологічної атестації (державна чи відомча) із указівкою порядку її виконання й організацій, що проводять атестацію.
- Для організаційного забезпечення наводять вимоги:
 - до структури і функцій підрозділів, що беруть участь у функціонуванні системи чи забезпечують її експлуатацію;
 - до організації функціонування системи Системи і порядку взаємодії персоналу системи і персоналу об'єкта об'єкту автоматизації впровадження;
 - до захисту від помилкових дій персоналу системи.

2.5 Вимоги до безпеки системи

1. Збереження даних, як у випадку збою, так і в разі випадкового зміни. В системі завжди повинні бути актуальні (і відповідають дійсності) дані.
2. Висока відмовостійкість основних компонентів системи (серверів з ключовими програмами). Час можливого простою повинно бути зведене до мінімуму, так як будь-який простій призводить до фінансових втрат.
3. Високий ступінь безпеки від вторгнення, а також конфіденційність даних, що передаються через глобальну мережу. Важливі дані повинні передаватися тільки їх реальному адресату. Під час передачі не повинно бути можливості змінити або перехопити ці дані.

Дотримання всіх цих вимог має дуже велику важливість, так як в банківській системі помилки призводять до більш серйозних наслідків, ніж в інших областях застосування мереж комп'ютерів.

Крім безпеки потрібно ще створити зручні умови для роботи співробітників. Всі завдання повинні виконуватися настільки швидко, щоб обчислювальна система не затримувала роботу співробітників.

Швидкість передачі трафіку.

- середня швидкість обчислюється шляхом ділення загального об'єму переданих даних на час їх передачі, зазвичай обирається достатньо тривалий проміжок часу — година, день або тиждень.

- миттєва швидкість відрізняється від середньої тим, що для усереднення вибирається дуже маленький проміжок часу — наприклад, 10 мс або 1 с.

- максимальна швидкість— це найбільша швидкість передачі, що зафіксована протягом періоду спостереження.

Зазвичай, при проектуванні, налаштуванні і оптимізації мережі використовуються такі показники, як середня і максимальна швидкість.

Середня швидкість, з якою обробляє трафік окремих елементів мережі або мережа в цілому, дозволяє оцінити роботу мережі впродовж тривалого часу, протягом якого піки і спади інтенсивності трафіку компенсують один одного.

Максимальна швидкість дозволяє оцінити, як мережа буде долати пікові навантаження, які є характерними для особливих періодів роботи, наприклад в ранкові години, коли співробітники підприємства майже одночасно реєструються в мережі і звертаються до розподілених файлів чи баз даних.

Зазвичай, при визначенні швидкісних характеристик певного сегменту чи пристрою в переданих даних не виділяється трафік певного користувача, застосування або комп'ютера — обчислюється загальний об'єм переданої інформації. Проте, для точної оцінки якості обслуговування така деталізація є бажаною, і системи керування мережами дозволяють її виконувати.

Пропускна здатність. Пропускна здатність - це максимально можлива швидкість обробки трафіку, що визначена стандартом технології, на якій побудована мережа. Пропускна здатність відображає максимально можливий об'єм даних, що передається по мережі або її частині в одиницю часу.

Пропускна здатність не є характеристикою, призначеною для користувача, оскільки вона свідчить про швидкість виконання внутрішніх операцій мережі передачі пакетів даних між вузлами мережі через різні комунікаційні пристрої. Вона безпосередньо характеризує якість виконання основної функції мережі — транспортування повідомлень, тому її частіше використовують при аналізі продуктивності мережі, ніж час реакції або швидкість.

Пропускна здатність вимірюється або в бітах в секунду, або в пакетах в секунду.

Пропускна здатність мережі залежить як від характеристик фізичного середовища передачі (мідний кабель, оптичне волокно, скручена пара) так і від наявного способу передачі даних (технологія Ethernet, FastEthernet, ATM). Пропускна здатність часто використовується як характеристика не стільки мережі, скільки власне технології, на якій побудована мережа.

На відміну від часу реакції або швидкості передачі трафіку пропускна здатність не залежить від завантаженості мережі і має постійне значення, що визначається використаними в мережі технологіями.

На різних ділянках гетерогенної мережі, де використовується кілька різних технологій, пропускна здатність може бути різною. Для аналізу і налаштування мережі корисно знати дані про пропускну здатність окремих її елементів.

Важливо відзначити, що із-за послідовного характеру передачі даних різними елементами мережі загальна пропускна здатність будь-якого складеного шляху в мережі буде мінімальною з пропускових здатностей

елементів маршруту. Для підвищення пропускної здатності складеного шляху необхідно в першу чергу звернути увагу на найповільніші елементи.

Іноді корисно оперувати загальною пропускною здатністю мережі, яка визначається як середня кількість інформації, що передається між всіма вузлами мережі за одиницю часу. Цей показник характеризує якість мережі в цілому, не розкладаючи його по окремих сегментах або пристроях.

Затримка передачі. Затримка передачі визначається як час між моментом надходження даних на вхід мережевого пристрою або частини мережі та моментом появи їх на виході цього пристрою.

Цей параметр продуктивності за сенсом є близьким до часу реакції мережі, але відрізняється тим, що завжди характеризує лише мережні етапи обробки даних, без затримок обробки кінцевими вузлами мережі.

Звичайну якість мережі характеризують величинами максимальної затримки передачі і варіантом затримки. Не всі типи трафіку є чутливими до затримок передачі, оскільки, зазвичай затримки не перевищують сотень мілісекунд, рідше — кількох секунд.

Затримки пакетів, що зумовлені файловою службою, службою електронної пошти або службою друку, мало впливають на якість цих служб з погляду користувача мережі.

З іншого боку, затримки пакетів, що містять голосові або відеодані, можуть призводити до значного зниження якості наданої користувачу інформації — виникає ефект «відлуння», неможливість розібрати деякі слова, вібрації зображення тощо.

Всі вказані характеристики продуктивності мережі є достатньо незалежними. Тоді як пропускна здатність мережі є постійною величиною, швидкість передачі трафіку може коливатися в залежності від завантаження мережі, не перевищуючи встановлених меж пропускної здатності.

Надійність і безпека. Однією з первинних цілей створення розподілених систем, до яких відносяться і комп'ютерні мережі, було

досягнення більшої надійності у порівнянні з окремими обчислювальними машинами. Важливо розрізняти кілька аспектів надійності.

Для простих технічних пристроїв використовуються наступні показники надійності:

- Середній час напрацювання на відмову.
- Вірогідність відмови.
- Інтенсивність відмов.

Проте, ці показники є придатними лише для оцінки надійності простих елементів і пристроїв, які можуть знаходитися лише в двох станах, — працездатному або непрацездатному. Складні системи, що складаються з багатьох елементів, окрім станів працездатності і непрацездатності, можуть мати інші проміжні стани, які ці характеристики не враховують.

Для оцінки надійності складних систем застосовується інший набір характеристик:

- готовність або коефіцієнт готовності.
- збереження даних.
- узгодженість (несуперечність) даних.
- вірогідність доставки даних.
- безпека.
- відмовостійкість.

Готовність або коефіцієнт готовності означає період часу, протягом якого система є готовою до використання. Готовність може бути підвищена шляхом введення надлишковості до структури системи: ключові елементи системи повинні існувати в кількох екземплярах, щоб при відмові одного з них функціонування системи забезпечували інші елементи.

Високоннадійна комп'ютерна система повинна як мінімум мати високу готовність, але цього недостатньо. Необхідно забезпечити збереження даних і захист їх від спотворень. Крім того, повинна підтримуватися узгодженість (несуперечність) даних, наприклад якщо для підвищення

надійності на кількох файлових серверах зберігається кілька копій даних, то потрібно постійно забезпечувати їх ідентичність.

Оскільки мережа працює на основі механізму передачі пакетів між кінцевими вузлами, однією з характеристик надійності є вірогідність доставки пакету до вузла призначення без спотворень. Разом з цією характеристикою можуть використовуватися і інші показники: вірогідність втрати пакету (із-за переповнення буфера маршрутизатора, не збігання контрольної суми, відсутності працездатного шляху до вузла призначення тощо), вірогідність спотворення окремого біта переданих даних, співвідношення кількості втрачених і доставлених пакетів.

Іншим аспектом загальної надійності є безпека, тобто здатність системи захистити дані від несанкціонованого доступу. В розподіленій системі це зробити набагато складніше, ніж в централізованій. В мережах повідомлення передаються по лініях зв'язку, що часто проходять через загальнодоступні приміщення, в яких можуть бути встановлені засоби прослуховування ліній. Іншим вразливим місцем можуть стати залишені без нагляду персональні комп'ютери. Крім того, завжди є потенційна загроза злому захисту мережі від неавторизованих користувачів, якщо мережа має виходи в глобальні загальнодоступні мережі.

Ще однією характеристикою надійності є відмовостійкість. В мережах під відмовостійкістю розуміють здатність системи приховати від користувача відмову окремих її елементів. Наприклад, якщо копії таблиці бази даних зберігаються одночасно на кількох файлових серверах, користувачі можуть просто не помітити відмови однієї з них. У відмовостійкій системі вихід з ладу одного з її елементів призводить до певного зниження якості її роботи (деградації), а не до повного останову. Так, при відмові одного з файлових серверів збільшується лише час доступу до бази даних із-за зменшення ступеня розпаралелювання запитів, але в цілому система буде продовжувати виконувати свої функції.

Розширюваність і масштабованість. Розширюваність означає можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, застосувань, служб), нарощування довжини сегментів мережі і заміни існуючої апаратури на більш потужну. При цьому є важливим, що легкість розширення системи іноді може забезпечуватися в обмеженому діапазоні.

Наприклад, локальна мережа Ethernet, яка побудована на основі одного сегменту товстого коаксіального кабелю, має хорошу розширюваність, що дозволяє без зусиль під'єднувати нові станції. Проте, така мережа має обмеження на число станцій — воно не повинне перевищувати 30–40. Хоча мережа допускає фізичне під'єднання до сегменту і більшого числа станцій (до 100), але при цьому, зазвичай, різко знижується продуктивність мережі. Наявність такого обмеження і є ознакою поганої масштабованості системи при хорошій розширюваності.

Масштабованість означає можливість нарощувати кількість вузлів і протяжність зв'язків мережі в дуже широких межах, при цьому її продуктивність не погіршується. Для забезпечення масштабованості мережі доводиться застосовувати додаткове комунікаційне обладнання і спеціальним чином структурувати мережу. Наприклад, хорошу масштабованість має багатосегментна мережа, що побудована з використанням комутаторів і маршрутизаторів і має ієрархічну структуру зв'язків. Така мережа може містити кілька тисяч комп'ютерів і при цьому забезпечувати кожному користувачеві мережі потрібну якість обслуговування.

Прозорість. Прозорість мережі досягається, коли мережа представлена користувачам не як множина окремих комп'ютерів, що зв'язані між собою складною системою кабелів, а як єдина традиційна обчислювальна машина з системою розділення часу.

Прозорість може бути досягнута на двох різних рівнях — на рівні користувача і на рівні адміністратора. На рівні користувача прозорість означає, що для роботи з віддаленими ресурсами він використовує ті ж команди і звичні процедури, що і для роботи з локальними ресурсами. На адміністративному рівні прозорість полягає в тому, що застосуванню для доступу до віддалених ресурсів потрібні ті ж виклики, що і для доступу до локальних ресурсів. Прозорості на рівні користувача досягти простіше, оскільки всі особливості процедур, що пов'язані з розподіленим характером системи, є прихованими від користувача програмістом, який створює застосування. Прозорість на рівні застосування вимагає приховування всіх деталей розподілення засобами мережної операційної системи.

Прозорість — це властивість мережі приховувати від користувача деталі свого внутрішнього устрою, що спрощує роботу в мережі.

Мережа повинна приховувати всі особливості операційних систем і відмінності в типах комп'ютерів. Користувач комп'ютера Macintosh повинен мати можливість звертатися до ресурсів, що підтримуються UNIX-системою, а користувач UNIX — розділяти інформацію з користувачами Windows.

Концепція прозорості застосовується до різних аспектів мережі. Наприклад, прозорість розташування означає, що користувачу не потрібно знати місцезнаходження програмних і апаратних ресурсів, таких як процесори, принтери, файли і бази даних. Ім'я ресурсу не повинне містити інформацію про місце його розташування.

Аналогічно, прозорість переміщення означає, що ресурси можуть вільно переміщатися з одного комп'ютера до іншого без зміни імен. Ще одним з можливих аспектів прозорості є прозорість паралелізму, яка полягає в тому, що процес розпаралелювання обчислень відбувається автоматично, без участі адміністратора, при цьому система сама розподіляє паралельні гілки застосування по процесорах та комп'ютерах мережі.

Підтримка різних видів трафіку. КМ спочатку призначалися для сумісного доступу до ресурсів комп'ютерів: файлів, принтерів тощо. Трафік, що створюється традиційними службами комп'ютерних мереж, має свої особливості і істотно відрізняється від трафіку повідомлень в телефонних мережах або, наприклад, в мережах кабельного телебачення. Проте з 90-их років в комп'ютерних мережах з'являється трафік мультимедійних даних (звук і відео в цифровій формі).

КМ стали використовуватися для організації відеоконференцій, навчання на основі відеофільмів, прямих теле- та радіотрансляцій тощо. Природно, що для динамічної передачі мультимедійного трафіку потрібні інші алгоритми та протоколи, і, відповідно, інше устаткування.

Головною особливістю трафіку, що утворюється при динамічній передачі голосу або зображення, є наявність жорстких вимог до синхронності переданих повідомлень. Для якісного відтворення безперервних процесів, якими є звукові коливання чи зміни інтенсивності світла у відеозображенні, необхідним є отримання вимірних і закодованих амплітуд сигналів з тією ж частотою, з якою вони були виміряні на стороні відправника. При запізненні повідомлень будуть спостерігатися спотворення.

В той же час трафік комп'ютерних даних характеризується вкрай нерівномірною інтенсивністю надходження повідомлень до мережі за відсутності жорстких вимог до синхронності доставки цих повідомлень. Наприклад, доступ користувача, що працює з текстом на віддаленому диску, породжує випадковий потік повідомлень між віддаленим і локальним комп'ютерами, що залежить від дій користувача, причому затримки при доставці в певних (достатньо широких з комп'ютерної точки зору) межах мало впливають на якість обслуговування користувача мережі.

Всі алгоритми комп'ютерного зв'язку, відповідні протоколи і комунікаційне устаткування були розраховані саме на такий «пульсуючий» характер трафіку, тому необхідність передавати мультимедійний трафік

вимагає внесення принципових змін, як до протоколів, так і до устаткування. Сьогодні всі нові протоколи надають підтримку мультимедійного трафіку.

Особливу складність представляє поєднання в одній мережі традиційного комп'ютерного і мультимедійного трафіку. Передача виключно мультимедійного трафіку по комп'ютерній мережі хоч і пов'язана з певними складнощами, але доставляє менше клопоту. А ось співіснування двох типів трафіку з протилежними вимогами до якості обслуговування є набагато складнішим завданням.

Керованість. В ідеалі засоби керування мережами є системою, що здійснює спостереження, контроль і управління кожним елементом мережі, — від простих до найскладніших пристроїв, при цьому така система розглядає мережу як єдине ціле, а не як розрізнений набір окремих пристроїв.

Керованість мережі передбачає можливість централізованого контролю стану основних елементів мережі, виявлення і вирішення проблем, що виникають при роботі мережі, виконання аналізу продуктивності і планування розвитку мережі.

Хороша система керування:

- спостерігає за мережею і при виявленні проблеми, активізує певну дію, виправляє ситуацію і повідомляє адміністратора про те, що відбулося і які кроки зроблено.

- повинна накопичувати дані, на підставі яких можна планувати розвиток мережі.

- повинна бути незалежною від виробника і мати зручний інтерфейс, що дозволяє виконувати всі дії з однієї консолі.

Вирішуючи тактичні завдання, адміністратори і технічний персонал стикаються з щоденними проблемами забезпечення працездатності мережі. Ці завдання вимагають швидкого рішення, обслуговуючий персонал мережі повинен оперативно реагувати на повідомлення про несправності, що поступають від користувачів або автоматичних засобів управління мережею.

Поступово стають помітними загальні проблеми продуктивності, конфігурації мережі, обробки збоїв і безпеки даних, що вимагають стратегічного підходу, тобто планування мережі. Планування, також містить прогноз змін вимог користувачів до мережі, питання застосування нових додатків та мережних технологій.

Необхідність в системі керування виявляється у великих мережах: корпоративних або глобальних. Без системи керування в таких мережах потрібна присутність кваліфікованих фахівців з експлуатації в кожній будівлі кожного міста, де встановлено устаткування мережі, що в результаті приводить до необхідності формування великого штату обслуговуючого персоналу.

Сумісність. Сумісність або інтегрованість означає, що мережа може містити різноманітне програмне і апаратне забезпечення, тобто в ній можуть співіснувати різні операційні системи, що підтримують різні стеки комунікаційних протоколів, а також апаратні засоби та застосування від різних виробників.

Мережа, що складається з різнотипних елементів, називається неоднорідною або гетерогенною. Якщо гетерогенна мережа працює без проблем, то вона є інтегрованою. Основним шляхом побудови інтегрованих мереж є використання модулів, які виконані відповідно до відкритих стандартів і специфікацій.

Якість обслуговування

Якість обслуговування визначає кількісні оцінки вірогідності того, що мережа буде передавати певний потік даних між двома вузлами відповідно до потреб застосування або користувача.

Важливі параметри для оцінювання якості обслуговування:

- пропускна здатність.
- затримки передачі пакетів.
- рівень втрат і спотворень пакетів.

Якість обслуговування гарантується для любого потоку даних, тобто для послідовності пакетів, що мають певні загальні ознаки, наприклад адресу вузла-джерела, інформацію, що ідентифікує тип застосування тощо.

До потоків застосовують поняття агрегації та диференціювання. Так, потік даних від одного комп'ютера може бути представлений як сукупність потоків від різних застосувань, а потоки від комп'ютерів одного підприємства агреговані до одного потоку даних абонента певного провайдера послуг.

Механізми підтримки якості обслуговування самі по собі не створюють пропускної здатності. Фактична пропускна здатність каналів зв'язку і транзитного комунікаційного устаткування — це ресурси мережі, що є відправною точкою для роботи механізмів QOS. Механізми QOS лише керують розподілом наявної пропускної здатності відповідно до вимог застосувань і налаштувань мережі. Найочевиднішим способом перерозподілу пропускної здатності мережі є керування чергами пакетів.

Оскільки дані, якими обмінюються два кінцеві вузли, проходять через певну кількість проміжних мережних пристроїв, таких як концентратори, комутатори і маршрутизатори, то підтримка QOS вимагає взаємодії всіх мережних елементів на шляху трафіку, тобто «з-кінця-в-кінець». Будь-які гарантії QOS настільки відповідають дійсності, наскільки їх забезпечує найбільш «слабкий» елемент в ланцюжку між відправником і одержувачем. Тому, слід чітко розуміти, що підтримка QOS лише в одному мережному пристрої, нехай навіть і магістральному, може лише дещо покращити якість обслуговування або ж зовсім не мати впливу на параметри QOS.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

На структурній схемі комплексу технічних засобів показані основні компоненти комп'ютерної системи комерційного банку «Райзе Банк» з мережним обладнанням. Показані рівні ієрархічні моделі організації мережі та підмережі, на які поділена корпоративна мережа підприємства.

Зі структурної точки зору корпоративна мережа – мережа змішаної топології, містить кілька локальних мереж. Корпоративна мережа буде об'єднувати структурні підрозділи банку «Райзе Банк», створюючи загальне інформаційне корпоративне простір. З цієї точки зору корпоративна мережа відображає структуру підприємства.

До складу технічних засобів КМ відносяться: робочих станції (хости), сервери підприємства, загальні ресурси, маршрутизатори, комутатори і мережні комунікації у вигляді кабелів і бездротових адаптерів.

Проектується мережа виходячи з технічних вимог на КС банку «Райзе Банк».

На рисунку 3.1 наведена структурна схема комплексу технічних засобів комп'ютерної системи банку «Райзе Банк».

Рівень ядра, де виконується комутація трафіка, складається з п'яти маршрутизаторів, що об'єднані мережами WAN. Доступ до віддаленої мережі «Управління по розвитку міжнародних зав'язків» здійснено за допомогою технології VPN. Через прикордонний маршрутизатор рівня ядра виконується підключення проектованої мережі до Інтернет.

Враховуючи невеликий розмір мережі, рівень ядра і розподілу будуть поєднуватися в маршрутизаторах КС банку «Райзе Банк».

Рівень доступу до середовища передачі даних складається з восьми комутаторів, що забезпечують формування підмереж LAN та VLAN.

Комутатор передає дані лише безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, позбавляючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися. В КС банку «Райзе Банк» в підмережі «Економічне управління» встановлено два комутатори. Всі користувачі цього підрозділу підключаються до мережі з використанням технології VLAN на комутаторах. В підмережі «Відділ інформатики» встановлено 3 комутатори. Всі користувачі цього підрозділу підключаються до мережі з використанням технології PAgP на комутаторах, що забезпечує збільшення пропускної здатності і надійності каналу передачі даних.

В інших LAN мережі встановлено по одному комутатору.

Комутатори об'єднують в локальну мережу кінцеві мережні пристрої. В КС банку «Райзе Банк» кінцевими мережними пристроями є: комп'ютери, що є робочими місцями працівників з встановленим ПО для роботи адміністративного персоналу; сервери підприємства: файловий сервер TFTP, Web-сервер HTTP та сервер DNS.

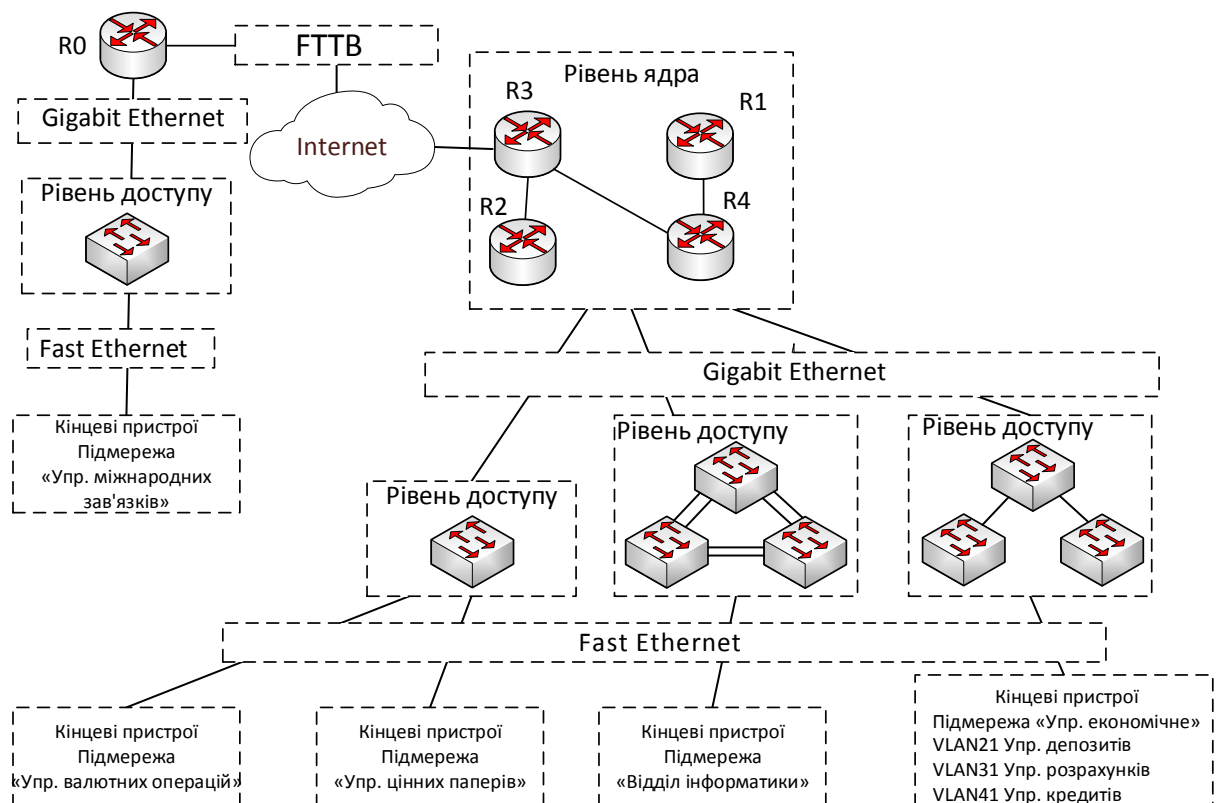


Рисунок 3.1 – Структурна схема комплексу технічних КС банку «Райзе Банк»

3.2 Розробка специфікації апаратних засобів КС

Головним етапом є обрання «інтелектуальних» пристроїв. Це в першу чергу маршрутизатори, комутатори, мережеві адаптери і принт-сервери. Активними їх називають через те, що вони не обмежуються тільки лише передачею сигналу на відміну від пасивної апаратури. Пасивна апаратура включає різні види проводів (оптоволоконні, мідні кабелі), розетки, конектори, сплітери і т.д. Ці пристрої необхідні для створення єдиних мереж, по яких проходить сигнал. Апаратні засоби КС банку «Райзе Банк» повинно відповідати технічним вимогам за показниками: швидкість – найважливіша характеристика корпоративної мережі; здатність до адаптації – властивість мережі розширюватися і встановлювати робочі станції там, де це потрібно; надійність – властивість локальної мережі зберігати повну або часткову працездатність незалежно від виходу з ладу деяких вузлів або кінцевого обладнання.

Мережа банку «Райзе Банк» розрахована на невелику кількість абонетів. Для реалізації рівня ядра мережі необхідно обрати маршрутизатори з підтримкою технології Ethernet, стека протоколів TCP/IP, мати гігабітні Ethernet порти з можливістю переходу в оптику (SFP-роз'єми), слоти розширення EHWIC, підтримку VPN-мереж із застосуванням технологій GETVPN, DMVPN і Enhanced Easy VPN з вбудованими апаратними функціями шифрування IPsec/SSL.

При цьому доцільно обрати маршрутизатори з інтеграцією сервісів для з серії Cisco 2900.

Маршрутизатор Cisco 2901-SEC/K9 – це пристрої з інтегрованими сервісами другого покоління сімейства ISR G2 (Integrated Services Router Generation 2). Серія маршрутизаторів Cisco 2900 представлена 4-ма фіксованими і безліччю розширених за допомогою ліцензій і модулів моделями. До особливостей маршрутизаторів Cisco 2900 серії можна віднести гігабітні Ethernet порти з можливістю переходу в оптику (SFP-

роз'єми), слоти розширення EHWIC, сумісні з модулями попереднього покоління WIC/VWIC/HWIC і слоти розширення під модулі SM (Service Modules). Також, є внутрішні роз'єми під модулі ISM (Internal Service Modules). Новітня технологія Services Ready Engine (SRE) забезпечує окреме, за запитом, розгортання апаратних і програмних сервісів, а підтримка VPN-мереж гарантує високу масштабування і високу продуктивність всіх сервісів захисту і розгортання мереж VPN, і забезпечує віддаленим співробітникам захищений доступ до ресурсів компанії з безпечного з'єднання.

Технічні характеристики Cisco 2901-SEC/K9: пам'ять: RAM 512 ГБ; флеш пам'ять 256 ГБ; мережа: технологія з'єднання провідна; протокол передачі даних Ethernet, Fast Ethernet, Gigabit Ethernet; протоколи маршрутизації BGP, GRE, OSPF, DVMRP, EIGRP, IGMPv3, PIM-SM, PIM-SSM, статична IPv4 і IPv6 маршрутизація; відповідність стандартам IEEE 802.1Q, IEEE 802.1ag; інтерфейси: 2 порти 100Base-TX / 1000Base-T, роз'єм RJ-45, 1 консольний порт управління, роз'єм RJ-45, 2 слоти HWIC, 1 порт USB 4-пін USB тип A; ОС базова Cisco IOS IP Base.

В будівлі організації необхідно встановити вісім комутаторів. Комутатори повинні підтримувати роботу технології DHCP, PAgP, VLSM, підтримувати велику кількість кінцевих пристроїв, забезпечувати швидкість передачі даних не менш як 100 Мбіт/с.

В якості комутаторів робочих груп використаний Cisco SB SF200-24FP [10]. Цей комутатор має 24 порти (100 Мбіт/с) для підключення роз'ємів RJ-45, 2 порти Gigabit Ethernet. По GigabitEthernet комутатори робочих груп підключаються до маршрутизаторів будівлі.

Технічні характеристики: підтримка PoE на 4 портах 8 x RJ-45 10/100/1000 Gigabit Ethernet; додатково IEEE 802.3 10BASE-T Ethernet; IEEE 802.3u 100BASE-TX Fast Ethernet; IEEE 802.3ab 1000BASE-T Gigabit Ethernet; IEEE 802.3ad LACP; IEEE 802.3z Gigabit Ethernet; IEEE 802.3x Flow Control; IEEE 802.1D (STP); IEEE 802.1Q/p VLAN IEEE 802.1w RSTP; IEEE

802.1X Port Access Authentication; IEEE 802.3af.

Таблиця 3.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість
1	2	3	4	5
1	2901-SEC/K92 EHWIC slots, Secure, VPN, IP Base, 2x-10/100/1000Base-T, Gigabit Ethernet	Postolnik_R1 Postolnik_R2 Postolnik_R3 Postolnik_R4 Postolnik_R0	шт	5
3	SB SF200-24FP Ethernet Switch 24 x Fast Ethernet Network; 2 x Gigabit Ethernet Uplink; Fast Ethernet; 10Base-T	Postolnik_Sw3.0 Postolnik_Sw3.1 Postolnik_Sw0 Postolnik_Sw5 Postolnik_Sw2 Postolnik_SW0 Postolnik_SW1 Postolnik_SW2	шт	8

3.3 Розробка архітектури мережі підприємства

Мережева архітектура завжди лежить в основі і є фундаментом для повноцінної роботи мережі. Найчастіше, вона складається з декількох важливих складових:

- топологія мережі;
- лінійно-кабельна інфраструктура;
- мережні протоколи;
- активне мережеве обладнання (комутатори, маршрутизатори).

Корпоративна мережа КС банку «Райзе Банк» ґрунтується на дворівневої ієрархічної моделі (верхній рівень – ядро, нижній – рівень доступу), враховуючи невеликий розмір мережі. Рівень ядра реалізовуватимуть маршрутизатори. Рівень доступу реалізовуватимуть комутатори робочих груп.

На рівні ядра розташовані п'ять маршрутизаторів, чотири в будівлі банку і

один будівлі, де розташований відділ розвитку міжнародних стосунків. Мережа організації має єдиний простір IP-адресації 172.16.84.0/22. Сегменти середовища (IP-підмережі) поділяються маршрутизаторами на п'ять підмереж. В мережі застосована адресація IP версії 4. Тому для забезпечення виходу до мережі Internet застосована технологія NAT. Маршрутизатор Postolnik_R3 розташований в серверній кімнаті та є пограничним маршрутизатором. Адреса мережі для доступу в Internet 209.165.202.0/27. Для забезпечення маршрутизації застосований протокол динамічної маршрутизації OSPF. На маршрутизаторі Postolnik_R1 застосована технологія інкапсуляції 802.1Q для забезпечення маршрутизації між VLAN. Для каналів між маршрутизаторами застосований блок адрес 10.0.11.0/24. В мережах VLAN застосована адресація кінцевих пристроїв за протоколом DHCP.

Для впровадження КС банку «Райзе Банк» була обрана логічна топологія «ієрархічна зірка». Як базова технологія мережі обрана технологія Ethernet. На рівні доступу для під'єднання робочих груп застосовано технологію FastEthernet. Між маршрутизатором і комутатором – GigabitEthernet.

Кінцеві мережні пристрої розділені на п'ять підмереж, з огляду на функціонал та напрямок підрозділів організації. Підмережа №1 «Відділ інформатики» розрахована на підключення 95 абонентів. Підмережа №2 «Управління цінних паперів» розрахована на підключення 142 абонентів. Підмережа №3 «Управління економіки» розрахована на підключення 86 абонентів. Підмережа №4 «Управління розвитку міжнародних стосунків» розрахована на підключення 137 абонентів. Підмережа №5 «Управління валютних операцій» розрахована на підключення 61 абонентів.

Підмережа «Управління економіки», з огляду на безпеку даних, розбита на три віртуальні мережі: VLAN21 «Упр. депозитів», VLAN31 «Упр. розрахунків», VLAN41 «Упр. кредитів». На комутаторах, що реалізують мережі VLAN застосований протокол VTP. Функціонал віртуальних мереж підтримують два комутатори Cisco SB SF200-24FP та маршрутизатор Cisco 2901-SEC/K92.

Підмережа «Управління розвитку міжнародних стосунків», з огляду на

швидкість передачі даних, організована на базі трьох комутаторів, на яких застосований протокол RAgP.

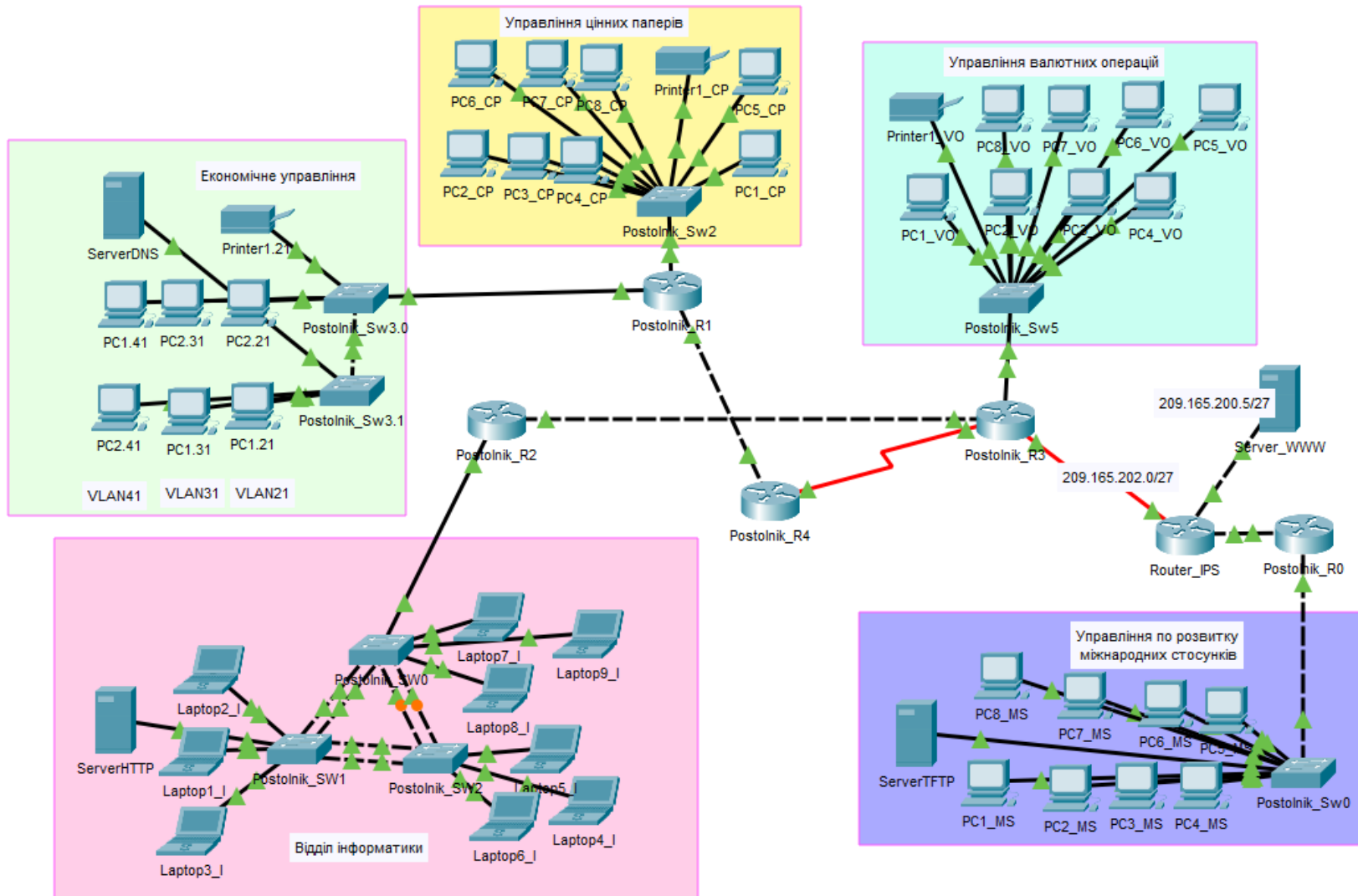


Рисунок 3.2 – Архітектура мережі банку «Райзе Банк»

3.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

В підмережі «Управління цінних паперів» встановлений комутатор Cisco SB SF200-24FP та маршрутизатор 2901-SEC/K9, що об'єднують ПК підмережі. Вихідний трафік пересилається на маршрутизатор Cisco 2901-SEC/K9 в лінію з пропускною здатністю 1000Мбіт/с.

Для того, щоб комутатор SB SF200-24FP не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку $\mu=210$ (кадрів/с), а середня довжина повідомлення – 650 байт.

Розрахуємо пропускну здатність мережі адміністративної будівлі допускаючи, що послугами одночасно користуються 100% користувачів. Пропускна здатність мережі розраховується наступним чином. Так як в нас 2 комутатори рівня доступу, а загальна кількість користувачів дорівнює 142, то пропускна здатність мережі на рівні доступу буде дорівнює:

$$P_{p.p} = \mu * l * N * 8 = 210 * 650 * 142 * 8 = 143 \text{ (Мбіт/с)}, \text{ де}$$

N – кількість вузлів в мережі.

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

Комутатор рівня доступу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{\text{вих}} = 1000\ 000\ 000 / (650 * 8) = 43333 \text{ пакетів/с}$$

Оскільки кожне джерело виробляє в середньому 210 пакетів/с, то ми обмежені приєднанням до комутатора рівня доступу максимум:

$$N = 43333 / 210 = 206 \text{ джерел.}$$

Що задовольняє нашу мережу на 142 ПК.

Кожен з 142 ПК посилає потік заявок з інтенсивністю 210 кадрів/с.
Інтенсивність вихідного трафіку від всіх користувачів:

$$\lambda = N * \mu = 65 * 210 = 29820 \text{ (пакетів/с)}$$

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час стояння в черзі:

$$\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{29820}{43333} = 0,68$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \frac{\rho}{1 - \rho} = \frac{0,12}{1 - 0,12} = 0,02$$

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

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{43333 - 29820} = 7,4 * 10^{-6} \text{ с}$$

Середня довжина черги:

$$L_{\text{чер}} = \frac{\rho^2}{1 - \rho} = \frac{0,12^2}{1 - 0,12} = 0,001$$

Ця цифра може бути корисною при налаштуванні черг на обладнанні – в апаратурі можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні менше 1 пакету, значення досить умовне; воно свідчить про те, що система працює з дуже великим запасом по продуктивності.

Середній час перебування пакета в черзі:

$$T_{\text{оч}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0,001}{29820} = 3,3 \text{ мкс}$$

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

Пропускна здатність каналу:

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

$$b = \lambda * l = 29820 * 650 * 8 = 143136000 \text{ біт/с} = 144 \text{ Мбіт/с}$$

Що задовольняє пропускній здатності вихідного каналу в 1000Мбіт/с.

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

4.1 Розрахунок схеми адресації корпоративної мережі

Для проектування корпоративної мережі необхідно розробити адресацію з критеріями – найкраща суммаризація, мінімальна витрата адрес. При проектуванні необхідно врахувати вимоги до мережі: виділений блок IP-адрес, кількість підмереж і кількості вузлів в підмережах, мережа підприємства повинна мати єдиний простір IP-адресації. Сегменти середовища (IP-підмережі) виконується маршрутизаторами.

Розрахунок схеми IP-адресації методом VLSM дозволив поділити адресний простір на невеликі підмережі, які відповідають топології і максимально наближені до вимог необхідної кількості вузлів. Підмережі дозволяють створювати кілька логічних мереж в межах однієї мережі. VLSM дав можливість більш ефективно використовувати IP-адреси, ніж звичайний поділ на підмережі з використанням класової адресації.

При використанні VLSM довжина маски підмережі залежить від числа бітів, запозичених для окремої підмережі від частини ідентифікатора хоста адреси для створення ID підмережі. Тобто від «змінної» частини маски підмережі змінної довжини. VLSM дозволяє розділити простір мережі на нерівні частини.

При використанні VLSM мережу спочатку розділяється на підмережі, а потім підмережі, в свою чергу, також розбиваються на підмережі. Цей процес можна повторювати багаторазово для створення підмереж різних розмірів.

Для побудови мережі організації використаний адресний простір 172.16.84.0/22. Розподіляти IP-адреси необхідно згідно до вимог, вказаних в таблиці 4.1.

Таблиця 4.1 – Кількість вузлів в підмережах

172.16.84.0/22				
LAN1 Відділ інформатики	LAN2 Управління цінних паперів	LAN3 Управління економіки	LAN4 Управління розвитку міжнародних стосунків	LAN5 Управління валютних операцій
95	142	86	137	61

З рисунка 3.2 видно, що топологія об'єднує 5 мереж з хост-вузлами, 3 мережі маршрутизаторів з адресами мереж з адресного простору 10.0.11.0/24, одна мережа зовнішнього шлюзу з адресою мережі 209.165.202.0/27. Мережі маршрутизаторів та зовнішнього шлюзу потребують по 2 IP-адреси кожна.

Для поділу вихідної мережі необхідно визначити кількість біт, необхідних для визначення п'яти підмереж. Таким чином, необхідно виділити 2 біти ($2^3=9$).

Далі необхідно упорядкувати мережі за кількістю необхідних IP-адрес. Спочатку виділяються біти під адресацію найбільшої мережі (LAN2 включає 142 вузлів), і далі до найменшої мережі. Для LAN2 необхідно 7 біт для IP-адресації кінцевих пристроїв ($2^7=128$).

Таким чином, розрахунок IP-адрес методом VLSM для мережі LAN2 має вигляд:

172.16.0101 01|00. |0000 0000

Символами «|» виділена частина IP-адреси, що визначає підмережу в вихідній мережі 172.16.84.0/22. Маска підмережі – 24 одиниці (255.255.255.0). Адреса підмережі – 172.16.84.0/24. Перша допустима адреса підмережі визначається як значення 1 в молодшому біті IP-адреси у вузловій частині – 172.16.0101 0100. |0000 0001| (172.16.84.1). Остання допустима адреса визначається як значення одиниць в усіх розрядах вузлової частини, окрім молодшого – 172.16.0101 0100. |1111 1110| (172.16.84.254).

Розрахунок IP-адрес методом VLSM для підмережі LAN_4:

Необхідний розмір під мережі: 137.

Виділений розмір підмережі: 137 ($N = 2^8 - 2 = 254$).

Адреса підмережі –172.16.85.0/24

172.16. 0101 01|01|. 0000 0000

255.255.1111 1111.0000 0000

Десятковий формат адреси підмережі для визначеної маски:
255.255.255.0. Префікс: /24

Діапазон допустимих IP-адрес вузлів:

172.16. 01010101. |00000001 – 172.16. 0101 0101|. 11111110

172.16.85.1 – 172.16.85.254

Подальші розрахунки виконуються аналогічно.

В таблиці 4.2 представлена схема IP-адресації мережі КС банку «Райзе Банк», розрахована за методом VLSM.

Таблиця 4.2 – Схема адресації мережі

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN2	142	172.16.84.0	255.255.255.0	172.16.84.1 - 172.16.84.254
LAN4	137	172.16.85.0	255.255.255.0	172.16.85.1 - 172.16.85.254
LAN1	95	172.16.86.0	255.255.255.128	172.16.86.1 - 172.16.86.126
LAN3	86	172.16.86.128	255.255.255.128	172.16.86.129 - 172.16.86.254
LAN5	61	172.16.87.0	255.255.255.192	172.16.87.1 - 172.16.87.62
VLAN21	20	172.16.86.0	255.255.255.224	172.16.86.1 - 172.16.86.30
VLAN31	20	172.16.86.32	255.255.255.224	172.16.86.33 - 172.16.86.62
VLAN41	20	172.16.86.64	255.255.255.224	172.16.86.65 - 172.16.86.94
VLAN99	20	172.16.86.96	255.255.255.224	172.16.86.97 - 172.16.86.126
WAN1	2	10.0.11.0	255.255.255.252	10.0.11.1 - 10.0.11.2
WAN2	2	10.0.11.4	255.255.255.252	10.0.11.5 - 10.0.11.6
WAN3	2	10.0.11.8	255.255.255.252	10.0.11.9 - 10.0.11.10
WAN IPS	2	209.165. 202.0	255.255.255.224	209.165.202.1-209.165.202.2
WAN Remote Network	2	64.100.13.0	255.255.255.252	64.100.13.1-64.100.13.2

Відповідно до вихідного блока IP-адрес, доступно адрес – 2046. Відповідно до необхідної кількості ПК, що потребують об'єднання в мережу, кількість необхідних IP-адрес – 521. Близько 24% доступного адресного простору вихідної мережі використано, таким чином, за методом VLSM, виконана вимога до мінімальної витрати адрес.

Згідно технічних вимог проектування КС банку «Райзе Банк», необхідно скласти таблицю адресації мережевих пристроїв. При цьому:

- перші можливі для використання IP-адреси призначено інтерфейсам і підінтерфейсам маршрутизаторів у LAN;
- другі IP-адреса призначаються комутаторам у кожній LAN;
- сервери налаштовано і їм привласнено IP-адреси за правилом: IP-адрес дорівнює першому можливому адресу у мережі+11+9;
- останні з використовуваних IP-адрес призначено вузлам;
- в мережах VLAN використовується адресація кінцевих пристроїв по протоколу DHCP.

У таблиці 4.3 представлена адресація всіх пристроїв мережі банку «Райзе Банк». Таблиця заповнюється на основі даних таблиці 4.2 та логічної топології корпоративної мережі банку «Райзе Банк».

Таблиця 4.3 – Схема адресації пристроїв мережі

Ім'я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Управління цінних паперів						
Postolnik_R1	G0/1	172.16.85.1	/24	-	-	G0/1
	G0/0	10.0.11.1	/30	-	-	G0/0
Postolnik_Sw1	Vlan1	172.16.85.2	/24	172.16.85.1	-	G0/1
PC1_CP - PC8_CP	NIC	172.16.85.254- 172.16.85.246	/24	172.16.85.1	-	Fa0/1- Fa0/8
Printer_CP	NIC	172.16.85.10	/24	172.16.85.1	-	Fa0/24
Управління валютних операцій						
Postolnik_R3	G0/1	172.16.87.1	/26	-	-	G0/1
	S0/0/0	209.165.202.2	/30	-	-	S0/0/0
	S0/0/1	10.0.11.9	/30	-	-	S0/0/1

Продовження таблиці 4.3

	G0/0	10.0.11.6	/30	-	-	G0/0
Postolnik_Sw5	Vlan1	172.16.87.2	/26	172.16.87.1	-	G0/1
PrinterVO	NIC	172.16.87.10	/26	172.16.87.1	-	F0/24
PC_VO1- PC_VO8	NIC	172.16.87.62- 172.16.87.59	/26	172.16.87.1	-	F0/0-F0/7
Відділ інформатики						
Postolnik_R2	G0/0	172.16.84.1	/24	-	-	G0/0
	G0/1	10.0.11.5	/30	-	-	G0/1
Postolnik_SW0	Vlan1	172.16.84.2	/24	172.16.84.1	-	G0/1
Postolnik_SW1	Vlan1	172.16.84.3	/24	172.16.84.1	-	G0/1
Postolnik_SW2	Vlan1	172.16.84.4	/24	172.16.84.1	-	G0/1
Laptop1_I – Laptop9_I	NIC	172.16.84.254- 172.16.84.245	/24	172.16.84.1	-	Fa0/1- Fa0/9
Server_HTTP	NIC	172.16.84.20	/24	172.16.84.1	-	Fa0/24
Управління розвитку міжнародних стосунків						
Postolnik_R0	G0/1	172.16.86.129	/25	-	-	G0/1
	G0/2	64.100.13.2	/27	-	-	G0/2
Postolnik_Sw0	Vlan1	172.16.86.130	/25	172.16.86.129	-	G0/1
PC1_MS – PC8_MS		172.16.86.254- 172.16.86.246	/25	172.16.86.129	-	Fa0/1- Fa0/8
ServerTFTP	NIC	172.16.86.141	/25	172.16.86.129	-	Fa0/24
Управління економіки						
Postolnik_R1	G0/1	-	-	-	-	-
	G0/1.21	172.16.86.1	/27	-	21	G0/1
	G0/1.31	172.16.86.33	/27	-	31	G0/1
	G0/1.41	172.16.86.65	/27	-	41	G0/1
	G0/0.99	172.16.86.97	/27	-	99	G0/1
PC21.1-PC21.3	NIC	172.16.86.30- 172.16.86.22	/27	172.16.86.33	21	Fa0/15- Fa0/24
PC31.1-PC31.2	NIC	172.16.86.62- 172.16.86.50	/27	172.16.86.65	31	Fa0/10- Fa0/14
PC41.1-PC41.2	NIC	172.16.86.94- 172.16.86.82	/27	172.16.86.97	41	Fa0/5- Fa0/9
ServerDNS	NIC	172.16.86.75	/27	172.16.86.65	-	Fa0/24
Postolnik_Sw3.0	F0/12	172.16.86.98	/27	172.16.86.97	99	-
Postolnik_Sw3.1	F0/1	172.16.86.99	/27	172.16.86.97	99	-
Postolnik_R4	G0/0	10.0.11.2	/30	-	-	G0/0
	S0/0/1	10.0.11.10	/30	-	-	S0/0/1
IPS						
Rout_IPS	S0/0/0	209.165.202.1	/27	-	-	S0/0/0
	G0/2	64.100.13.1	/30	-	-	G0/2
Host_IPS	NIC	209.165.200.5	/25	209.165.200.5	-	G0/0

4.2 Розробка фізичної топологічної схеми корпоративної мережі

Фізична топологія мережі показує, як розташоване обладнання мережі на об'єкті впровадження, де і якого типу будь укладені кабелі, де і яке обладнання встановлено, підключення живлення обладнання мережі, яка довжина у якого кабельного прольоту, який кабель в який порт включений.

Як базова технологія мережі обрана технологія Ethernet. Обрана

технологія здатна забезпечити найбільшу швидкість, надійність і якість передачі даних та найбільш розповсюджена. На рівні доступу для під'єднання робочих груп застосовано технологію Fast Ethernet. Між маршрутизатором і комутатором – GigabitEthernet.

Кабельна інфраструктура повинна відповідати стандартам TIA/EIA-568-A та TIA/EIA-569. Кабельна розводка всередині будівлі адміністрації виконується кабелем типу «неекранована кручена пара» (UTP-кабель категорії 5e), що забезпечує високу надійність і швидкість передачі даних в поєднанні з високою технологічністю.

Підмережі КС розбиті на підмережі. Максимальний сегмент кабелю в підмережі має довжину 160 м, що відповідає вимогам.

Підмережі, що оснащуються мережним обладнанням, розташовані на першому поверсі будівлі банку.

Віддалена підмережа «Управління розвитку міжнародних стосунків» розташована в окремій будівлі за 2120м . Між будівлями застосований оптоволоконний кабель SC G657A для підвіски і експлуатації на опорах повітряних ліній зв'язку, міського електротранспорту та повітряних ліній електропередачі в умовах впливу навантажень від вітру, ожеледі, температури і їх комбінацій. Застосовані конектори SC SM MM.

В цілому в даних підмережах встановлюється 40 точок підключення. Точка підключення являє собою двох портову інформаційну розетку RJ-45.

Для виконання з'єднання WAN між маршрутизаторами будівель необхідне застосування технології послідовної передачі даних Serial DCE/DTE. В мережі WAN використаний кабель Serial CAB-6060X DCE для інтерфейсів Serial.

В будівлі банку поверх 2 розташований «Відділ інформатики». Маршрутизатор Postolnik_R2 та комутатори Postolnik_SW0, Postolnik_SW2, Postolnik_SW3, сервер HTTP розміщені в приміщенні «Серверна» з точки зору безпеки. Приміщення оснащено системою вентиляції і блоками

безперебійного живлення. Кабель прокладений за допомогою металевих лотків, забезпечуючи точками підключення кожне приміщення.

Кінцеві пристрої підмережі розташовані в двох кімнатах.

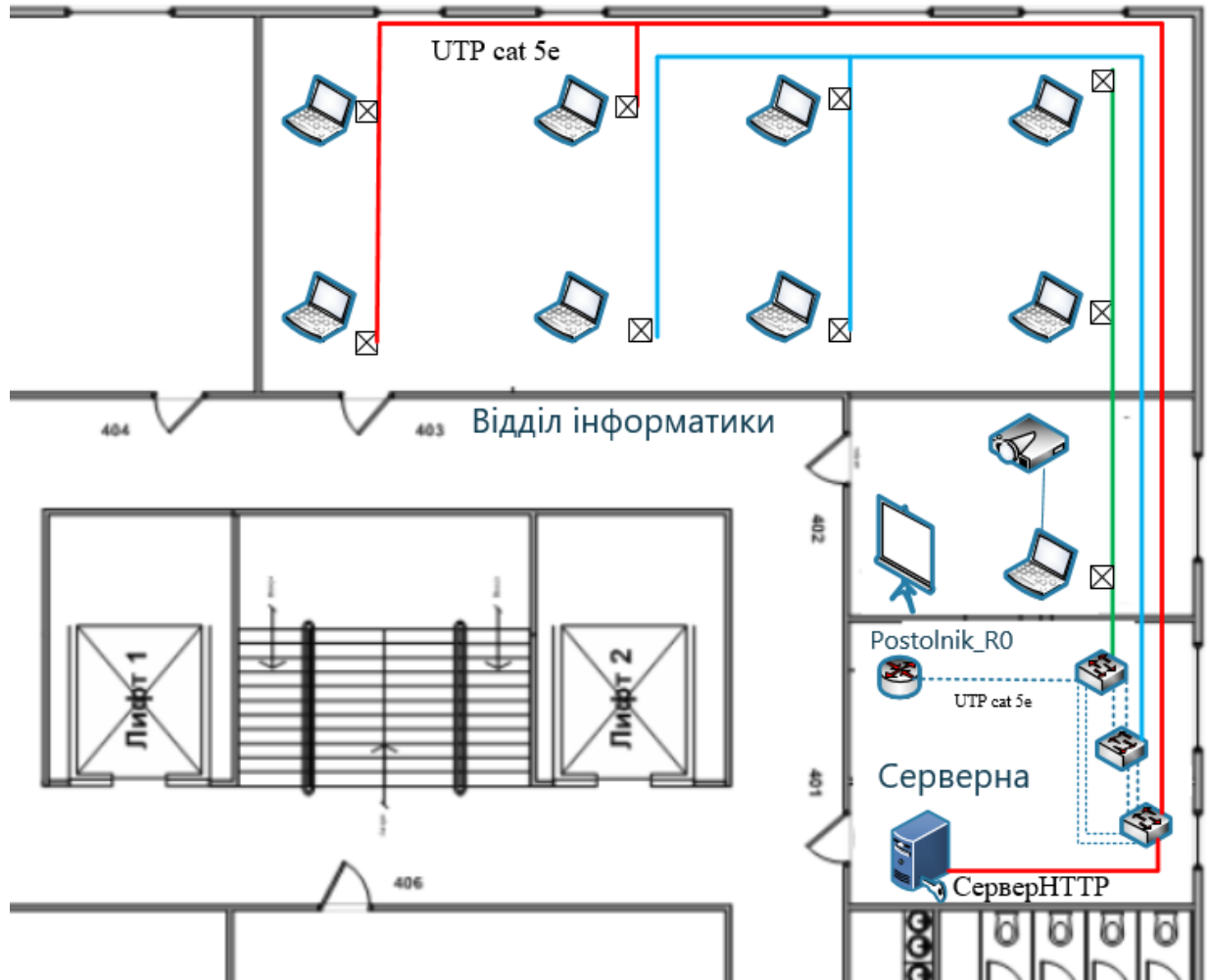


Рисунок 4.1 – Схема фізичної топології мережі будівлі банку

4.3 Налаштування та перевірка роботи комп'ютерної системи

4.3.1 Базове налаштування конфігурації пристроїв

Згідно до технічних вимог було приведено базове налаштування активних мережних пристроїв комп'ютерної системи.

Розроблено базову конфігурацію пристроїв. При цьому додатково:

- застосувати паролі для привілейованого режиму, консолі і vty;
- зашифровано усі паролі, що зберігаються у відкритому вигляді;
- настроєно банер MOTD;

- настроєно на усіх лініях vty використання протоколу ssh і локальних облікових записів. Для цього створено користувача 12316sk_Postolnik паролем admincisco. В якості імені домена використані назви пристроїв. Для шифрування даних створено ключ RSA завдовжки 1024 біт;
- налаштовано IPv4-адреси відповідно до таблиці 4.3;
- на DCE-інтерфейсах маршрутизаторів встановлено значення тактової частоти – 128000.

Приклад налаштування на Postolnik _R4.

```
Router>en
Router# configure terminal
Router(config)#hostname Postolnik _R4
Postolnik _R4(config)#username 12316sk_Postolnik password
                        admincisco
Postolnik _R4(config)#ip domain-name Postolnik _R4
Postolnik _R4(config)#banner motd # 123-16sk Postolnik Autorized Heve PASSWORD #
Postolnik _R4(config)#line con 0
Postolnik _R4(config-line)# password cisco
Postolnik _R4(config-line)# login
Postolnik _R4(config-line)#line vty 0 4
Postolnik _R4 (config-line)# password cisco
Postolnik _R4(config-line)# login
```

Даним блоком команд виконане: іменування пристрою; створення користувача з його паролем; створення доменного імені пристрою; створення баннерного повідомлення при захищеному вході до пристрою; захист паролем входу до пристрою при підключеннях консольно.

Згідно до технічних вимог, на лініях VTY необхідно налаштувати протокол SSH. SSH (Secure Shell – «безпечна оболонка») – мережевий протокол прикладного рівня, що дозволяє виробляти віддалене управління операційною системою і тунелювання TCP-з'єднань (наприклад, для передачі файлів). SSH шифрує весь трафік, включаючи і паролі.

```
Postolnik _R4(config-line)# transport input ssh
Postolnik _R4(config-line)#line vty 5 15
Postolnik _R4(config-line)# password cisco
```



```
Postolnik _R4(config-line)# login
```

```
Postolnik _R4(config-line)# transport input ssh
```

Згідно з табл. 4.4 налаштовані IP-адреси на інтерфейсах.

Базове налаштування інших пристроїв наведено в Додатку А.

4.3.2 Налаштування маршрутизаторів корпоративної мережі

Згідно технічних вимог, в мережі банку «Райзе Банк» використовується протокол динамічної маршрутизації OSPF 11. 11 – номер автономної системи, це сукупність мереж під єдиним адміністративним керуванням, що забезпечує загальну для всіх вхідних в автономну систему маршрутизаторів політику маршрутизації.

OSPF (англ. Open Shortest Path First) – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology) і використовує для знаходження найкоротшого шляху алгоритм Дейкстри. Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

Для кожного маршрутизатора оголошені безпосередньо підключені мережі і відключено поширення оновлень маршрутизації на інтерфейси в локальні мережі. На Postolnik _R2 налаштований маршрут за замовчуванням в інтернет (ISP) і поширене його через оновлення маршрутизації.

Включити протокол OSPF на маршрутизаторі командою:

```
Postolnik _R2(config)#router ospf 11
```

Протоколу потрібно об'явити мережі, підключені до маршрутизатора.

```
Postolnik _R2(config-router)#network 172.16.84.0 0.0.0.255 area 0
```

```
Postolnik _R2(config-router)#network 10.0.11.4 0.0.0.3 area 0
```

На serial-інтерфейсах відповідно до технічних умов задано пропускну спроможність = 128 Кб/с та визначим швидкість каналу 128000.

```
Postolnik _R2(config)#interface s0/0/0
```

```
Postolnik _R2(config-if)#bandwidth 128
```

```
Postolnik _R2(config-if)# clock rate 128000
```

Виконаємо перевірку таблиць маршрутизацій на маршрутизаторах (рисунок 4.2-4.6). Кожний маршрутизатор окрім безпосередньо підключених мереж з символом «С» має відомості про всі віддалені мережі, отримана по протоколу OSPF з символом «О». Також мають записи маршруту за замовчуванням, який складається з восьми нулів, для підключення до маршрутизатора IPS.

Routing Table for Postolnik_R1				
Type	Network	Port	Next Hop IP	Metric
S	0.0.0.0/0	---	209.165.202.1	1/0
C	10.0.11.0/30	GigabitEthernet0/0	---	0/0
L	10.0.11.1/32	GigabitEthernet0/0	---	0/0
O	10.0.11.4/30	GigabitEthernet0/0	10.0.11.2	110/7502
O	10.0.11.8/30	GigabitEthernet0/0	10.0.11.2	110/7501
O	172.16.84.0/24	GigabitEthernet0/0	10.0.11.2	110/15002
C	172.16.85.0/24	GigabitEthernet0/2	---	0/0
L	172.16.85.1/32	GigabitEthernet0/2	---	0/0
C	172.16.86.0/27	GigabitEthernet0/1.21	---	0/0
L	172.16.86.1/32	GigabitEthernet0/1.21	---	0/0
C	172.16.86.32/27	GigabitEthernet0/1.31	---	0/0
L	172.16.86.33/32	GigabitEthernet0/1.31	---	0/0
C	172.16.86.64/27	GigabitEthernet0/1.41	---	0/0
L	172.16.86.65/32	GigabitEthernet0/1.41	---	0/0
C	172.16.86.96/27	GigabitEthernet0/1.99	---	0/0
L	172.16.86.97/32	GigabitEthernet0/1.99	---	0/0
O	172.16.87.0/26	GigabitEthernet0/0	10.0.11.2	110/7502
O	209.165.202.0/27	GigabitEthernet0/0	10.0.11.2	110/15001

Рисунок 4.2 – Таблиця маршрутизації на Postolnik_R1

```

Postolnik_R2#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 209.165.202.1 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O   10.0.11.0/30 [110/7502] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
C   10.0.11.4/30 is directly connected, GigabitEthernet0/0
L   10.0.11.5/32 is directly connected, GigabitEthernet0/0
O   10.0.11.8/30 [110/7501] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
 172.16.0.0/16 is variably subnetted, 8 subnets, 4 masks
C   172.16.84.0/24 is directly connected, GigabitEthernet0/1
L   172.16.84.1/32 is directly connected, GigabitEthernet0/1
O   172.16.85.0/24 [110/7503] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
O   172.16.86.0/27 [110/7503] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
O   172.16.86.32/27 [110/7503] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
O   172.16.86.64/27 [110/7503] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
O   172.16.86.96/27 [110/7503] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
O   172.16.87.0/26 [110/2] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
 209.165.202.0/27 is subnetted, 1 subnets
O   209.165.202.0/27 [110/7501] via 10.0.11.6, 01:46:44, GigabitEthernet0/0
S*  0.0.0.0/0 [1/0] via 209.165.202.1

```

Рисунок 4.3 – Таблиця маршрутизації на Postolnik_R2

```

Postolnik_R3#show 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 209.165.202.1 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O   10.0.11.0/30 [110/7501] via 10.0.11.10, 01:49:41, Serial0/0/1
C   10.0.11.4/30 is directly connected, GigabitEthernet0/0
L   10.0.11.6/32 is directly connected, GigabitEthernet0/0
C   10.0.11.8/30 is directly connected, Serial0/0/1
L   10.0.11.9/32 is directly connected, Serial0/0/1
 172.16.0.0/16 is variably subnetted, 9 subnets, 5 masks
S   172.16.84.0/22 is directly connected, GigabitEthernet0/1
O   172.16.84.0/24 [110/7501] via 10.0.11.5, 01:49:41, GigabitEthernet0/0
O   172.16.85.0/24 [110/7502] via 10.0.11.10, 01:49:31, Serial0/0/1
O   172.16.86.0/27 [110/7502] via 10.0.11.10, 01:49:31, Serial0/0/1
O   172.16.86.32/27 [110/7502] via 10.0.11.10, 01:49:31, Serial0/0/1
O   172.16.86.64/27 [110/7502] via 10.0.11.10, 01:49:31, Serial0/0/1
O   172.16.86.96/27 [110/7502] via 10.0.11.10, 01:49:31, Serial0/0/1
C   172.16.87.0/26 is directly connected, GigabitEthernet0/1
L   172.16.87.1/32 is directly connected, GigabitEthernet0/1
 209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.202.0/27 is directly connected, Serial0/0/0
L   209.165.202.2/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.165.202.1

```

Рисунок 4.4 – Таблиця маршрутизації на Postolnik_R3

```

Postolnik_R4#show 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 209.165.202.1 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.11.0/30 is directly connected, GigabitEthernet0/0
L       10.0.11.2/32 is directly connected, GigabitEthernet0/0
O       10.0.11.4/30 [110/7501] via 10.0.11.9, 01:50:27, Serial0/0/1
C       10.0.11.8/30 is directly connected, Serial0/0/1
L       10.0.11.10/32 is directly connected, Serial0/0/1
    172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
O       172.16.84.0/24 [110/15001] via 10.0.11.9, 01:50:27, Serial0/0/1
O       172.16.85.0/24 [110/2] via 10.0.11.1, 01:50:27, GigabitEthernet0/0
O       172.16.86.0/27 [110/2] via 10.0.11.1, 01:50:27, GigabitEthernet0/0
O       172.16.86.32/27 [110/2] via 10.0.11.1, 01:50:27, GigabitEthernet0/0
O       172.16.86.64/27 [110/2] via 10.0.11.1, 01:50:27, GigabitEthernet0/0
O       172.16.86.96/27 [110/2] via 10.0.11.1, 01:50:27, GigabitEthernet0/0
O       172.16.87.0/26 [110/7501] via 10.0.11.9, 01:51:02, Serial0/0/1
    209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/15000] via 10.0.11.9, 01:51:02, Serial0/0/1
S*    0.0.0.0/0 [1/0] via 209.165.202.1

```

Рисунок 4.5– Таблиця маршрутизації на Postolnik _R4

Виходячи з адресації маршрутизаторів ми бачимо, що всі наявні мережі вказані в таблицях, тому топологія повністю сходиться, а це значить, що з будь-якої мережі можна відправляти повідомлення до іншої, та це повідомлення буде обов'язково прийняте.

4.3.3 Налаштування роботи Інтернет

Згідно до технічних вимог для розгортання корпоративної мережі заданий блок адрес з діапазону приватних адрес. Для надання можливості доступу робочих станцій організації до мережі Internet, на прикордонному маршрутизаторі необхідно застосувати технологію NAT.

NAT – це механізм зміни мережевої адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення одного адресного простору в інший. Завдяки NAT можна, використовуючи одну або кілька зовнішніх IP-адрес, виданих провайдером, підключити до мережі практично будь-яку кількість комп'ютерів. Більшість

маршрутизаторів дозволяють виконувати трансляцію адрес, завдяки чому їх можна використовувати для підключення невеликих мереж до інтернету, використовуючи одну зовнішню IP-адресу.

NAT на прикордонному маршрутизаторі налаштовано згідно з вимогами:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 172.16.86.89/25 – адреса Server HTTP;
- номер списку доступу: 11;
- ім'я пулу: Internet.

NAT на Postolnik_R3:

Postolnik_R3(config)#access-list 11 permit 172.16.84.0 0.0.3.255//список контролю доступу, що дозволяє всі адреси внутрішньої мережі

Postolnik_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224// пул для динамічного виділення інтернет адрес

Postolnik_R3(config)#ip nat inside source list 11 pool Internet// підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу

Postolnik_R3(config)#i ip nat inside source static 172.16.84.21 209.165.200.5// статичний NAT для серверу HTTP

Postolnik_R3(config)#interface Serial0/1/0

Postolnik_R3(config-if)#ip nat outside // коли пакет надходить на порт то відбувається заміна інтернет адреси на адресу внутрішньої мережі при проходженні через порт

Postolnik_R3(config-if)#interface Serial0/0/0

Postolnik_R3(config-if)#ip nat inside // коли пакет надходить на порт то відбувається заміна адреси внутрішньої мережі на інтернет адресу

Для перевірки роботи NAT відобразим таблицю перекотрювань (рис.4.6).

NAT Table for Postolnik_R3

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.6:6	172.16.85.17:6	209.165.200.5:6	209.165.200.5:6
icmp	209.165.202.7:1	172.16.85.18:1	209.165.200.5:1	209.165.200.5:1
icmp	209.165.202.8:4	172.16.86.13:4	209.165.200.5:4	209.165.200.5:4
icmp	209.165.202.5:3	172.16.87.19:3	209.165.202.1:3	209.165.202.1:3
icmp	209.165.202.5:4	172.16.87.19:4	209.165.200.5:4	209.165.200.5:4
---	209.165.200.5	172.16.84.21	---	---

Рисунок 4.6 – Таблиця перевотрювань NAT на Postolnik_R3

4.4.4 Налаштування агрегування каналів PAgP

Port Aggregation Protocol (PAgP) (агрегування каналів) – пропріетарний протокол компанії Cisco Systems, 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.

Налаштування EtherChannel на Postolnik_Sw0.1:

```
Postolnik_SW0(config)# interface range f0/1-4
Postolnik_SW0(config-if-range)# switchport mode trunk
Postolnik_SW0(config-if-range)# channel-group 1 mode auto
Postolnik_Sw0.2(config)# interface Port-channel 1
Postolnik_Sw0.2(config)# switchport mode trunk
```

Налаштування EtherChannel на Postolnik_Sw0.2:

```
Postolnik_SW1(config)# interface range f0/1-2
Postolnik_SW1(config-if-range)# channel-group 1 mode desirable
```

```

Postolnik_SW1(config)# interface range f0/5-6
Postolnik_SW1(config-if-range)# channel-group 2 mode desirable
Postolnik_SW1(config)# interface Port-channel 1
Postolnik_SW1(config)# switchport mode trunk
Postolnik_SW1(config)#interface Port-channel 2
Postolnik_SW1(config)# switchport mode trunk

```

Налаштування EtherChannel на Postolnik_SW2:

```

Postolnik_SW2(config)# interface range f0/3-4
Postolnik_SW2(config-if-range)# channel-group 3 mode auto
Postolnik_SW2(config)# interface range f0/5-6
Postolnik_SW2(config-if-range)# channel-group 2 mode desirable
Postolnik_SW2(config)# interface Port-channel 2
Postolnik_SW2(config)# switchport mode trunk
Postolnik_SW2(config)#interface Port-channel 3
Postolnik_SW2(config)# switchport mode trunk

```

Для перевірки роботи протоколу PAgP застосуємо команду `Postolnik_SW0#sh etherchannel summary`. Результат перевірки наведений на рисунку 4.7.

```

Postolnik_SW2#show 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
-----+-----+-----+-----
2      Po2 (SU)          PAgP       Fa0/5 (P) Fa0/6 (P)
3      Po3 (SD)          PAgP       Fa0/3 (I) Fa0/4 (I)

```

Рисунок 4.7– Перевірка роботи протоколу PAgP, сумарна інформація про стан Etherchannel на Postolnik_SW0

З наведеного результату роботи команди, можна зробити висновок, що налаштування протоколу PAgP виконані вірно.

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

Налаштувати віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку, що проходить між підмережею «Управління цінних паперів» та віддаленою підмережею «Управління розвитку міжнародних стосунків» через Internet.

Налаштування на Postolnik_R0:

```
Postolnik_R0(config)#access-list 110 permit ip 172.16.85.0 0.0.0.255
172.16.86.128 0.0.0.127
```

Налаштування параметрів 1 фази ISAKMP

```
Postolnik_R0(config)#crypto isakmp policy 10
```

```
Postolnik_R0(config-isakmp)#encryption aes
```

```
Postolnik_R0(config-isakmp)#authentication pre-share
```

```
Postolnik_R0(config-isakmp)#group 2
```

```
Postolnik_R0(config-isakmp)#exit
```

```
Postolnik_R0(config)#crypto isakmp key cisco address 64.100.13.2
```

Налаштування параметрів 2 фази ISAKMP

```
Postolnik_R0(config)#crypto ipsec transform-set VPN-CONF esp-3des esp-
sha-hmac
```

```
Postolnik_R0(config)#crypto map VPN-MAP 10 ipsec-isakmp
```

```
Postolnik_R0(config-crypto-map)#description VPN connection to Postolnik_R1
```

```
Postolnik_R0(config-crypto-map)#set peer 64.100.13.2
```

```
Postolnik_R0(config-crypto-map)#set transform-set VPN-CONF
```

```
Postolnik_R0(config-crypto-map)#match address 110
```

```
Postolnik_R0(config-crypto-map)#exit
```

Налаштування криптографічного порівняння

```
Postolnik_R0(config)#interface Serial 0/0/1
```


Postolnik_R0(config-if)#crypto map VPN-MAP

```

Postolnik_R0# SH Crypto IPsec SA

interface: GigabitEthernet0/0
  Crypto map tag: VPN-MAP, local addr 64.100.13.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (172.16.86.128/255.255.255.128/0/0)
remote  ident (addr/mask/prot/port): (172.16.87.0/255.255.255.192/0/0)
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

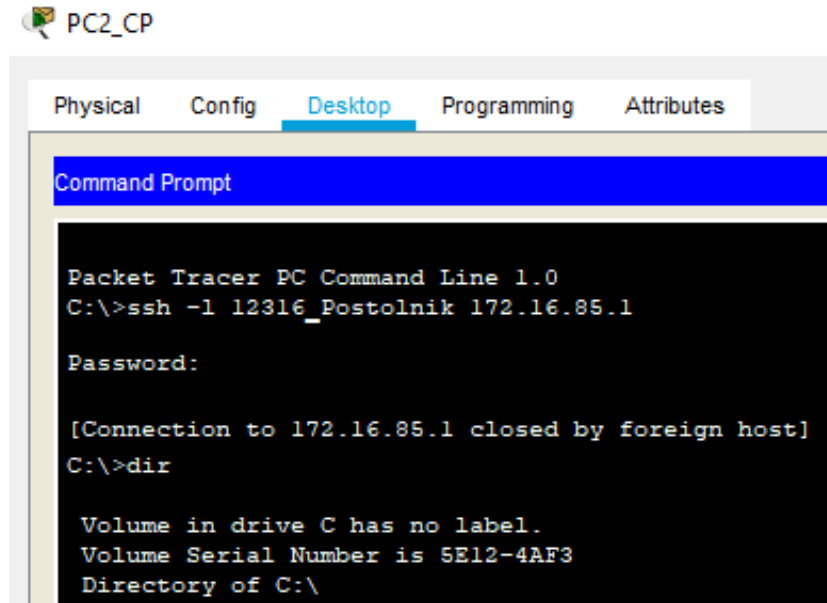
local crypto endpt.: 0.0.0.0, remote crypto endpt.:64.100.13.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x0(0)

```

Рисунок 4.8 – Перевірка стану IPSec SA

4.4.6 Перевірка роботи комп'ютерної системи

Для перевірки SSH зробимо підключення з командного рядка PC2_CP з підмережі «Управління цінних паперів» маршрутизатора Postolnik_R1 від користувача 12316sk_Postolnik з паролем *admincisco* командою, що наведена на рисунку 4.9.



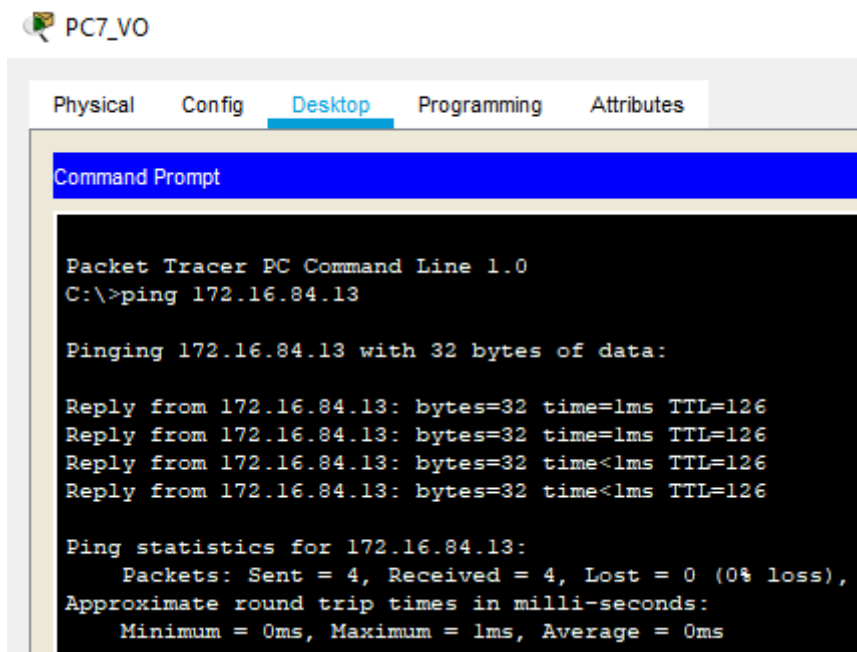
```

PC2_CP
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ssh -l 12316_Postolnik 172.16.85.1
Password:
[Connection to 172.16.85.1 closed by foreign host]
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

```

Рисунок 4.9 – Перевірка підключення до маршрутизатора Postolnik_R1 за допомогою SSH

Для перевірки роботи доступність вузлів мережі виконаємо команду ping для вузлів з різних підмереж, вузол PC7_VO з підмережі «Управління валютних операцій» пінгує хост з підмережі «Відділ інформатики».



```

PC7_VO
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.84.13
Pinging 172.16.84.13 with 32 bytes of data:
Reply from 172.16.84.13: bytes=32 time=1ms TTL=126
Reply from 172.16.84.13: bytes=32 time=1ms TTL=126
Reply from 172.16.84.13: bytes=32 time<1ms TTL=126
Reply from 172.16.84.13: bytes=32 time<1ms TTL=126
Ping statistics for 172.16.84.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Рисунок 4.10 – Результат перевірки доступності вузлів мережі

В мережах VLAN користувачі отримують мережеві налаштування по протоколу DHCP. Для цього необхідно налаштувати маршрутизатор *Postolnik_R1* та вузли мережі на підтримку DHCP.

DHCP – це протокол, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Протокол DHCP працює за схемою клієнт-сервер. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри. При цьому налаштований в проекті сервер DHCP працює в режимі динамічного розподілу - на сервері DHCP присвоєний діапазон IP-адрес і кожен клієнтський комп'ютер в мережі повинен запросити IP-адресу від DHCP-сервера.

Згідно до технічних вимог налаштовано маршрутизатор, що здійснює маршрутизацію між VLAN і виступає в якості DHCP-серверу для мереж VLAN. Створені пули DHCP під назвою *pollvlan24*. Виключені з пулу перші 10 адрес. Для кожного пулу вказана адреса DNS-сервера і шлюз за замовчуванням.

Налаштування маршрутизації між VLAN за допомогою технології інкапсуляції на маршрутизаторі *Postolnik_R1*:

```
Postolnik_R1(config)#interface GigabitEthernet0/1
Postolnik_R1(config-if)#no shutdown
Postolnik_R1(config-if)#interface GigabitEthernet 0/1.21
Postolnik_R1(config-if)#encapsulation dot1Q 21
Postolnik_R1(config-if)#ip address 172.16.86.1 255.255.255.224
Postolnik_R1(config-if)#interface GigabitEthernet 0/1.31
Postolnik_R1 (config-if)#encapsulation dot1Q 31
Postolnik_R1(config-if)#ip address 172.16.86.33 255.255.255.224
Postolnik_R1(config-if)#interface GigabitEthernet 0/1.41
Postolnik_R1(config-if)#encapsulation dot1Q 41
Postolnik_R1(config-if)#ip address 172.16.86.65 255.255.255.224
Postolnik_R1(config-if)#interface GigabitEthernet 0/1.99
Postolnik_R1(config-if)#encapsulation dot1Q 99
Postolnik_R1(config-if)#ip address 172.16.86.97 255.255.255.224
```

Перевіримо динамічне призначення IP-адрес вузлам за допомогою протоколу DHCP, які знаходяться у VLAN-ах, а також перевіримо маршрутизацію між ними.

```

Postolnik_R1#sh ip dhcp binding
IP address          Client-ID/
                    Hardware address
172.16.85.11        0040.0B81.5846    --
172.16.85.12        000C.CF8C.DD39    --
172.16.85.13        0005.5E74.7E39    --
172.16.85.16        0060.5C08.645E    --
172.16.85.14        0007.ECA1.A0A8    --
172.16.85.18        0001.96B9.CCAA    --
172.16.85.19        0001.C716.4074    --
172.16.85.15        0002.4A4B.0C82    --
172.16.85.17        0050.0F83.B2AC    --
172.16.86.11        000A.4141.E6E0    --
172.16.86.12        0002.17AD.D273    --
172.16.86.13        0003.E4A0.30BB    --
172.16.86.44        0005.5E11.A89C    --
                    Type
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic
Automatic

```

Рисунок 4.12 – Таблиця призначення IP-адрес вузлам за протоколом DHCP

Для перевірки роботи комп'ютерної системи перевіримо доступність вузлів мережі, налаштування безпечного віддаленого доступу до активних мережних пристроїв, перевірку зв'язку між вузлами з різних VLAN при автоматичному призначенні адрес.

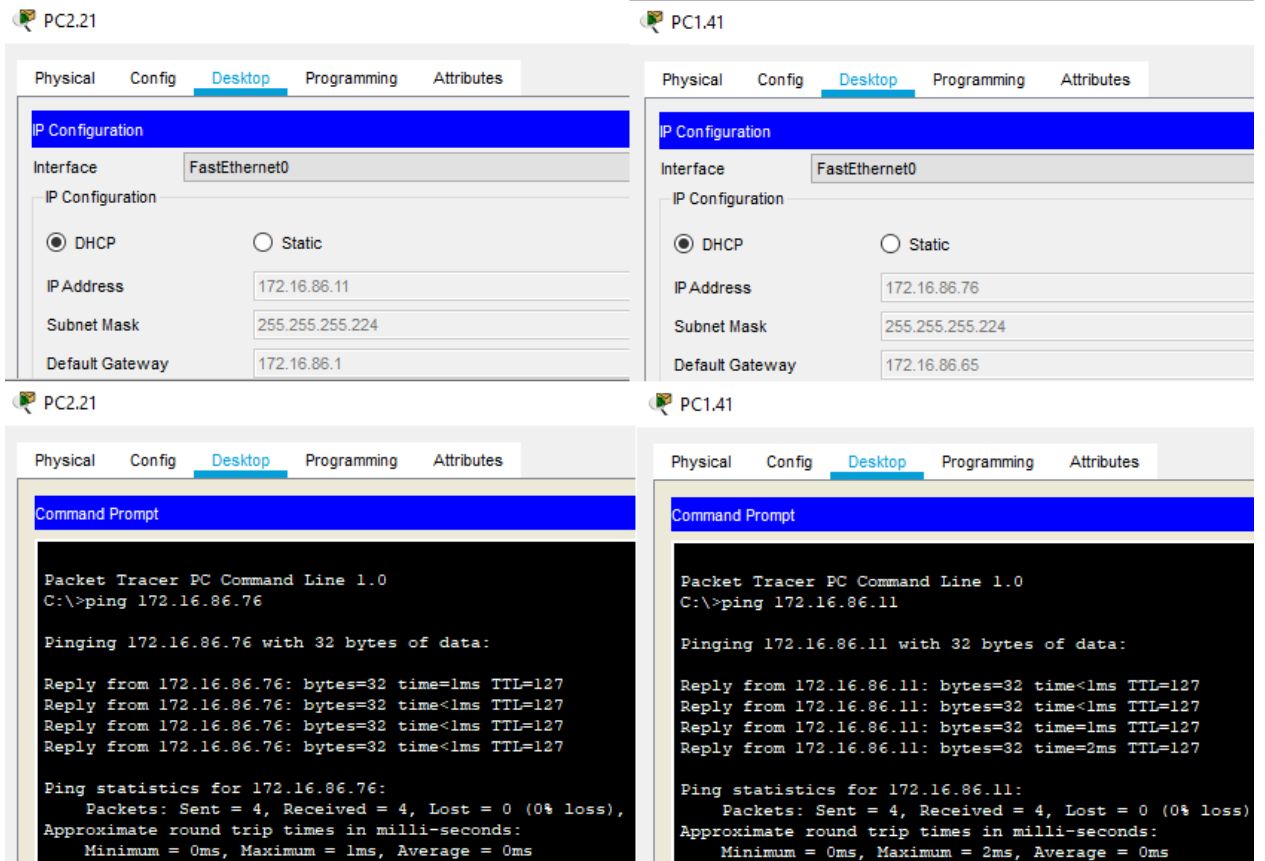


Рисунок 4.13 – Перевірка зв'язку між вузлами з різних VLAN при автоматичному призначенні адрес через DHCP

Виконане пінгування хостів, один з яких належить мережі VLAN 21, а інший мережі VLAN 41.

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1 Розробка методів для захисту інформації в комп'ютерній системі

Для захисту інформації в комп'ютерній системі від несанкціонованого доступу розробляються і описуються методи:

- налаштування мереж VLAN і маршрутизації між ними;
- на портах комутаторів, підключених до серверів, налаштовуються функції безпеки портів;
- маршрутизатори мережі налаштовуються на підтримку служби AAA та RADIUS-сервера.

5.2 Налаштування маршрутизаторів на підтримку служби AAA

Авторизація користувачів при підключенні до мережевих пристроїв виконується за допомогою сервісів AAA (Authentication Authorization and Accounting). AAA – система аутентифікації, авторизації і обліку подій, вбудована в операційну систему Cisco IOS, служить для надання користувачам безпечного віддаленого доступу до мережного обладнання Cisco. Вона дозволяє централізовано керувати користувачам та доступом їх до мережевого обладнання. Вона пропонує різні методи ідентифікації користувача, авторизації, а також збору і відправки інформації на сервер.

Postolnik_R2(config)#aaa new-model //запуск служби AAA

Postolnik_R2(config)#aaa authentication login default local //
налаштування методу аутентифікації за замовчуванням з використання локальної бази користувачів

Postolnik_R2(config)#aaa authentication login Login group radius local //
налаштування методу аутентифікації Login з використанням серверу RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів

```
Postolnik_R2(config)#line console 0
```

Postolnik_R2(config-line)#login authentication Login // застосування методу аутентифікації Login на консольній лінії

```
Postolnik_R2(config)#line vty 0 4
```

Postolnik_R2(config-line)#login authentication default // застосування методу аутентифікації за замовчуванням на vty-лінії

Налаштування RADIUS-сервер:

```
Postolnik_R4(config)#radius-server host 172.16.86.94 auth-port 1645
```

```
Postolnik_R4(config)#radius-server key radius12316
```

В якості облікового запису користувачів використовується ім'я пристрою з паролем *Admin12316*.

Перевіримо роботу аутентифікації, приєднавшись до маршрутизатора *Postolnik_R2*(через консоль (рисунок 5.1), провівши аутентифікацію через сервер RADIUS.

```
123-16 Postolnik Enter with PASSWORD
User Access Verification
Username: Postolnik_R2
Password:
Postolnik_R2>enable
Password:
Postolnik_R2#
```

Рисунок 5.1 – Аутентифікація на маршрутизаторі за допомогою служби AAA та сервера RADIUS

Для того що зайти в режим користувача потрібно було ввести ім'я користувача та пароль, що був налаштований на сервері RADIUS.

5.3 Налаштування мереж VLAN

VLAN (від англ. Virtual Local Area Network) – віртуальна локальна обчислювальна мережа, відома так само як VLAN, являє собою групу хостів

із загальним набором вимог, які взаємодіють так, як якщо б вони були підключені до ширококомовному домену, незалежно від їх фізичного місцезнаходження. VLAN має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим станціям, групуватися разом, навіть якщо вони не знаходяться в одній фізичній мережі. Така реорганізація може бути зроблена на основі програмного забезпечення замість фізичного переміщення пристроїв.

На пристроях Cisco, протокол VTP (VLAN Trunking Protocol) передбачає VLAN-домени для спрощення адміністрування. Згідно до вимог підмережа «Управління економіки» розділяється на чотири підмережі VLAN, та до них ще одна підмережа для керування VLAN. Відповідно до архітектури мережі в КС банку «Банк Райзе» створені мережі VLAN з присвоєним кожній з них ім'ям.

Таблиця 5.1 – Назви VLAN для підмережі «Управління економіки»

Номер VLAN	Ім'я VLAN	Примітка
1	Default	Не використовується
21	Depozit_Upr	Упр. депозитів
31	Rozrahunki_Upr	Упр. розрахунків
41	Kredit_Upr	Упр. кредитів
99	Management	Для управління пристроями
100	Native	Власна

Додатково виконані налаштування:

- відповідно до технічних вимог настроєно транкові порти і порти доступу;
- вимкнено усі невикористовувані фізичні порти комутаторів;
- на портах комутаторів, підключених до серверів, настроєно функцію безпеки портів так, щоб:

- а) тільки двом унікальним пристроям був дозволений доступ до порту;
 - б) MAC- адреса пристрою розпізнавалася динамічно і додавалася в поточну конфігурацію;
 - с) при порушенні системи безпеки вирушало повідомлення, а порт залишався включеним;
- налаштовано SVI-інтерфейси на комутаторах, призначивши по таблиці 4.3 IPv4- адреси з мережі Management VLAN;
 - налаштовано маршрутизацію між мережами VLAN.

Налаштування на Postolnik_Sw3.0:

Об'ява VLAN:

```
Switch (config)#hostname Postolnik_Sw3.0
Postolnik_Sw3.0(config)#vlan 21
Postolnik_Sw3.0(config-vlan)#name Depozit_Upr
Postolnik_Sw3.0(config-vlan)# vlan 31
Postolnik_Sw3.0(config-vlan)#name Rozrahunki_Upr
Postolnik_Sw3.0(config-vlan)#vlan 41
Postolnik_Sw3.0(config-vlan)#name Kredit_Upr
Postolnik_Sw3.0(config-vlan)#vlan 99
Postolnik_Sw3.0(config-vlan)# name Management
Postolnik_Sw3.0(config-vlan)#vlan 100
Postolnik_Sw3.0(config-vlan)# name Native
```

Налаштування транкових каналів:

```
Postolnik_Sw3.0(config)#interface g0/1, g0/2
Postolnik_Sw3.0(config-if)#switchport trunk native vlan 100
Postolnik_Sw3.0(config-if)#switchport mode trunk
Postolnik_Sw3.0(config-if)#exit
```

Налаштування SVI-інтерфейсу:

```
Postolnik_Sw3.0(config)# interface Vlan99
Postolnik_Sw3.0(config-if)# ip address 172.16.86.97 255.255.255.224
Postolnik_Sw3.0(config-if)#no shutdown
```

Для перевірки налаштування відобразимо сумарну інформацію про налаштування VLAN на комутаторах і відповідних їм портів (рис. 5.2-5.3)

```
Postolnik_Sw3.0#sh vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/11
21 Depozit_Upr	active	Fa0/12, Fa0/13, Fa0/14
31 Rozrahunki_Upr	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
41 Kredit_Upr	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
99 Management	active	
100 Native	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Рисунок 5.2 – Налаштування VLAN на Postolnik_Sw3.0

Port Status Summary Table for Postolnik_Sw3.1				
Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	0050.0F75.EB01
FastEthernet0/2	Down	1	--	0050.0F75.EB02
FastEthernet0/3	Down	1	--	0050.0F75.EB03
FastEthernet0/4	Down	1	--	0050.0F75.EB04
FastEthernet0/5	Up	41	--	0050.0F75.EB05
FastEthernet0/6	Down	41	--	0050.0F75.EB06
FastEthernet0/7	Down	41	--	0050.0F75.EB07
FastEthernet0/8	Down	41	--	0050.0F75.EB08
FastEthernet0/9	Down	41	--	0050.0F75.EB09
FastEthernet0/10	Up	41	--	0050.0F75.EB0A
FastEthernet0/11	Down	1	--	0050.0F75.EB0B
FastEthernet0/12	Up	21	--	0050.0F75.EB0C
FastEthernet0/13	Down	21	--	0050.0F75.EB0D
FastEthernet0/14	Down	21	--	0050.0F75.EB0E
FastEthernet0/15	Up	31	--	0050.0F75.EB0F
FastEthernet0/16	Down	31	--	0050.0F75.EB10
FastEthernet0/17	Down	31	--	0050.0F75.EB11
FastEthernet0/18	Down	31	--	0050.0F75.EB12
FastEthernet0/19	Down	31	--	0050.0F75.EB13
FastEthernet0/20	Down	31	--	0050.0F75.EB14
FastEthernet0/21	Down	31	--	0050.0F75.EB15
FastEthernet0/22	Down	31	--	0050.0F75.EB16
FastEthernet0/23	Down	31	--	0050.0F75.EB17
FastEthernet0/24	Down	31	--	0050.0F75.EB18
GigabitEthernet0/1	Down	1	--	0050.0F75.EB19
GigabitEthernet0/2	Up	--	--	0050.0F75.EB1A
Vlan1	Down	1	<not set>	0009.7C51.371E
Vlan99	Up	99	172.16.86.100/27	0009.7C51.3701
Hostname: Postolnik_Sw3.1				

Рисунок 5.3 – Налаштування VLAN на Postolnik_Sw2.1

5.4 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

На портах комутаторів, підключених до серверів, використана функція безпеки портів таким чином, що:

- тільки одному узлу дозволений доступ до порту;
- MAC-адреса пристрою додається статично в поточну конфігурацію;
- при порушенні системи безпеки порт виключається.

Команди використані на комутаторі Postolnik_SW2 згідно технічних вимог:

```
Postolnik_SW2(config)#int fa0/24 // вхід в інтерфейс
```

Postolnik_SW2(config-if)#switchport mode access // режим інтерфейса для отримання доступу

Postolnik_SW2(config-if)#switchport port-security // ввімкнення засобів безпеки

Postolnik_SW2(config-if)#switchport port-security maximum 2 // забезпечення доступу до порту тільки для одного вузла

Postolnik_SW2(config-if)#switchport port-security mac-address 0001.6300.BABD // MAC – адреса 1 вузла для доступу до порта

Передача трафіку між VLAN здійснюється за допомогою маршрутизатора. Для того щоб маршрутизатор міг передавати трафік з одного VLAN в інший (з однієї мережі в іншу), необхідно щоб в кожній мережі у нього був інтерфейс. Для того щоб не виділяти під мережу кожного VLAN окремий фізичний інтерфейс, створюються логічні підінтерфейсів на фізичному інтерфейсі для кожного VLAN. Налаштування маршрутизації між VLAN буде здійснюватись на маршрутизаторі Postolnik_R1 на інтерфейсі GigabitEthernet 0/1 рf технологією інкапсуляції 802.1Q .

На комутаторі Postolnik_Sw3.0 порт G0/1, що веде до маршрутизатора, налаштований як тегований порт (в термінах Cisco – транк).

Для логічних підінтерфейсів на маршрутизаторі необхідно вказувати те, що інтерфейс буде отримувати тегований трафік і вказувати номер VLAN відповідний цьому інтерфейсу.

Postolnik_R1(config)#interface g0/1
Postolnik_R1(config-if)#no shutdown
Postolnik_R1(config)#interface g0/0.21 // налаштування підінтерфейсу для маршрутизації трафіку між VLAN

Postolnik_R1(config-subif)#encapsulation dot1Q 21 // тегування пакетів для данного підінтерфейсу.

Postolnik_R1(config-subif)#ip address 172.16.86.1 255.255.255.224

Перевірка налаштувань наведена на рисунку 5.5.

 Port Status Summary Table for Postolnik_R1

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	10.0.11.1/30	<not set>	0001.6495.3B0B
GigabitEthernet0/1	Up	--	<not set>	<not set>	0090.2B2E.0CD1
GigabitEthernet0/1.21	Up	--	172.16.86.1/27	<not set>	0090.2B2E.0CD1
GigabitEthernet0/1.31	Up	--	172.16.86.33/27	<not set>	0090.2B2E.0CD1
GigabitEthernet0/1.41	Up	--	172.16.86.65/27	<not set>	0090.2B2E.0CD1
GigabitEthernet0/1.99	Up	--	172.16.86.97/27	<not set>	0090.2B2E.0CD1
GigabitEthernet0/2	Up	--	172.16.85.1/24	<not set>	00D0.9782.37B4
Serial0/0/0	Down	--	<not set>	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Serial0/1/0	Down	--	<not set>	<not set>	<not set>
Serial0/1/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0000.0CA2.B814

Hostname: Postolnik_R1

Рисунок 5.5 – Перевірка налаштування VLAN на Postolnik_R1

Інкапсуляції 802.1Q на Postolnik_R1 налаштована.

6 ЕКОНОМІЧНА ЧАСТИНА

6.1 Техніко-економічне обґрунтування розробки

В кваліфікаційній роботі розглядається побудова комп'ютерної системи комерційного банку "Райзе Банк" з опрацюванням побудови, безпеки та налаштуванням корпоративної мережі. Для побудови КС необхідно облаштувати підрозділи банку комп'ютерною технікою та активним мережним обладнанням, що дозволить автоматизувати процеси ведення діяльності підприємства, надасть доступ працівникам відділу до загального електронного документообороту підприємства. Впровадження КС дозволяє надати якісну та швидку мережу з мінімальними витратами.

Для удосконалення КС комерційного банку "Райзе Банк" застосовується обладнання спеціалізованих виробників. Для обґрунтування економічної доцільності застосування КС, необхідно виконати:

- розрахунок капітальних витрат на придбання складових КС;
- розрахунок річних експлуатаційних витрат проектної апаратури;
- величину річного економічного ефекту.

6.2 Розрахунок капітальних витрат на придбання складових КС

Капітальні вкладення – це кошти, призначені для створення і придбання основних фондів та нематеріальних активів, що підлягають амортизації.

Кошторис капітальних витрат на обладнання, яке необхідно для реалізації комп'ютерної системи, приведена в таблиці 6.1.

Капітальні витрати розраховуються за формулою:

$$K_{\text{пр}} = K_{\text{об}} + K_{\text{тр}} + K_{\text{мн}} + K_{\text{пз}}, \quad (6.1)$$

де $K_{\text{об}}$ – вартість обладнання, грн.,

$K_{\text{тр}}$ – вартість транспортно-заготівельних витрат, грн.,

$K_{\text{мн}}$ – вартість монтажних-налагоджувальних робіт, грн.,

$K_{пз}$ – вартість розробки програмного забезпечення.

Таблиця 6.1 – Кошторис капітальних витрат

№ п/п	Найменування обладнання	Ед. виміру	Кількість	Вартість од. облад-я, грн	Сумма, грн.
1	Маршрутизатор Cisco 2901-SEC/K9	шт	6	36450	218700
2	Комутатор Cisco SB SF200-24FP	шт	8	12500	100000
3	Сервер Dell PowerEdge T40	шт	4	26500	106000
4	Персональний комп'ютер	шт	30	18000	540000
5	Лептоп	шт	9	14000	126000
6	Мережний принтер Kyocera Ecosys P6230cdn	шт	3	7700	23100
7	Кабель UTP Cat 5e	м	1400	22	30800
8	Кабель SC G657A	м	2120	5	10600
9	Конектор RJ-45	шт	40	5	200
10	Розетки RJ-45	шт	40	30	1200
Ітого					1156600

Загальна вартість обладнання $K_{об}=1156600$ грн.

Вартість транспортно-заготівельних і складських витрат становить 7% від вартості обладнання.

$K_{тр}=1156600*7\%=80962$ грн.

Вартість монтажних-налагоджувальних робіт становить 8% від вартості обладнання.

$K_{мн}=1156600*8\%=92528$ грн.

6.2.2 Розрахунок капітальних витрат на програмне забезпечення

6.2.2.1 Розрахунок часу на розробку програмного забезпечення

Трудомісткість розробки програмного забезпечення:

$$t = t_o + t_d + t_a + t_n + t_{\text{нал}} + t_{\text{док}}, \quad (6.2)$$

де t_o - витрати праці на підготовку й опис поставленого завдання

t_d - витрати праці на дослідження алгоритму розв'язку завдання;

t_a - витрати праці на обробку блок-схеми алгоритму;

t_n - витрати праці на програмування по готовій блок-схемі;

$t_{\text{нал}}$ - витрати праці на налаштування програм на ЕОМ;

$t_{\text{док}}$ - витрати праці на підготовку документації за завданням.

Складові частини витрат праці визначаються на підставі умовної кількості оброблюваних операторів у програмному забезпеченні. До них відносять ті оператори, які необхідно написати в процесі роботи над програмою з урахуванням можливих уточнень у постановці завдання й удосконалення алгоритму.

Умовна кількість операторів у програмі:

$$Q = q \cdot c \cdot (1+p), \quad (6.3)$$

де q –кількість операторів, використовуваних у програмі.

Виходячи з ПЗ $q = 50$;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її обробки.

Коефіцієнт складності «с» програми визначає відносну складність програми відносно типового завдання, складність якого відповідає 1. $c = 1,25$.

Коефіцієнт корекції програми «р» визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму в результаті уточнення постановки завдання. Ухвалюємо $p=0,1$, це відповідає внесенню 3...5 корекцій, що тягнуть за собою переробку 5-10% готової програми.

Таким чином, для програми, описаної в кваліфікаційній роботі:

$$Q = 50 \cdot 1,25(1+0,1) = 69$$

Оцінка витрат праці на підготовку й опис завдання становлять

$$t_0 = 50 \text{ люд.-годин.}$$

Витрати праці на вивчення опису завдання визначаються з урахуванням уточнення опису й кваліфікації програміста по формулі:

$$t_d = \frac{Q \cdot B}{(50 \dots 60) \cdot k} \text{ люд.-годин}$$

(6.4)

де B – коефіцієнт збільшення витрат праці, $B=1,4$;

k – коефіцієнт кваліфікації програміста, які визначається залежно від стажу роботи зі спеціальності. У нашому випадку коефіцієнт кваліфікації програміста становить $k=1,2$.

Для розроблюваного програмного забезпечення:

$$t_d = \frac{69 \cdot 1,4}{55 \cdot 1,2} = 1,5 \text{ люд.-годин.}$$

Витрати на розробку алгоритму розв'язку завдання:

$$t_a = \frac{Q}{(20 \dots 25) \cdot k} \text{ люд.-годин} \quad (6.5)$$

Для розроблювального програмного забезпечення:

$$t_a = \frac{69}{20 \cdot 1,2} = 2,9 \text{ люд.-годин.}$$

Витрати праці на складання програми по готовій блок-схемі алгоритму:

$$t_n = \frac{Q}{(20 \dots 25) \cdot k} \text{ люд.-годин} \quad (6.6)$$

Для розроблюваного програмного продукту:

$$t_n = \frac{69}{20 \cdot 1,2} = 2,9 \text{ люд.-годин.}$$

Витрати праці на налагодження програми на ЕОМ розраховуються по формулі:

$$t_{нал} = \frac{Q}{(4 \dots 5) \cdot k} \text{ люд.-годин} \quad (6.7)$$

Для конкретного програмного продукту:

$$t_{нал} = \frac{69}{5 \cdot 1,2} = 11,5 \text{ люд.-годин.}$$

Витрати праці на підготовку документації за завданням визначаються по формулі:

$$t_D = t_{ДР} + t_{ДО}, \text{ люд.-година} \quad (6.8)$$

де $t_{ДР}$ – трудомісткість підготовки матеріалів до написання;

$t_{ДО}$ – трудомісткість редагування, друку й оформлення документації.

$$t_{ДР} = \frac{Q}{(15 \dots 20) \cdot k} \quad (6.9)$$

$$t_{ДР} = 69/18 \cdot 1,2 = 3,2 \text{ люд.-година};$$

$$t_{ДО} = 0,75 \cdot t_{ДР}, \quad (6.10)$$

$$t_{ДО} = 0,75 \cdot 3,2 = 2,4 \text{ люд.-година.}$$

Для розроблюваного програмного забезпечення витрати праці на підготовку документації за завданням будуть становити:

$$t_D = 3,2 + 2,4 = 5,6 \text{ люд.-година.}$$

Трудомісткість розробки програмного забезпечення буде становити:

$$t = 50 + 1,5 + 2,9 + 2,9 + 11,5 + 5,6 = 74,4 \text{ людино-годин.}$$

6.2.2.2 Розрахунки витрат на розробку програмного продукту

Витрати на розробку програмного продукту $K_{ПЗ}$ містять витрати на заробітну плату розробника програми $Z_{ЗП}$ і вартість машинного часу, необхідного для налаштування програми на ЕОМ $Z_{МЧ}$

$$K_{ПЗ} = Z_{ЗП} + Z_{МЧ}, \text{ грн.} \quad (6.11)$$

Заробітна плата розробника програмного забезпечення:

$$Z_{ЗП} = t \cdot C_{пр}, \text{ грн.} \quad (6.12)$$

де t – загальна трудомісткість обробки програмного забезпечення;

$C_{пр}$ – середня годинна тарифна ставка програміста становить:

$$C_{пр} = 91 \text{ грн./година.}$$

Заробітна плата за розробку програмного забезпечення дорівнює:

$$Z_{ЗП} = 85,5 \cdot 91 = 7780 \text{ грн.}$$

Вартість машинного часу, необхідного для налаштування програми на

ЕОМ:

$$Z_{мч} = t_{нал} \cdot C_{мг}, \text{ грн.} \quad (6.13)$$

де:

$t_{отл}$ – трудомісткість налаштування програми на ЕОМ, людино-годин;

$C_{мг}$ – вартість машино-години ЕОМ, грн./година. $C_{мг} = 5$ грн./година.

$$Z_{мч} = 17 \cdot 5 = 85 \text{ грн.}$$

Витрати на розробку програмного забезпечення системи керування будуть становити:

$$K_{пз} = 7780 + 85 = 7865 \text{ грн.}$$

Певні, таким чином, витрати на створення програмного забезпечення є частиною одноразових капітальних витрат на створення системи керування.

Очікувана тривалість розробки програмного забезпечення:

$$T = \frac{t}{B_k \cdot F_p}, \text{ міс.} \quad (6.14)$$

де, B_k – кількість розробників. Програма розроблялася однією людиною, тому $B_k = 1$;

F_p – місячний фонд робочого часу ($F_p = 176$ годин).

Визначимо тривалість розробки ПО:

$$T = \frac{85,5}{1 \cdot 176} = 0,49 \text{ міс.}$$

Таким чином, капітальні витрати розраховані за формулою (6.1) дорівнюють:

$$K_{пр} = 1156600 + 80962 + 92528 + 7865 = 1337955 \text{ грн.}$$

6.3 Розрахунок річних експлуатаційних витрат

Експлуатаційні витрати визначаються за такими статтями витрат:

- амортизаційні відрахування (C_a);
- заробітна плата обслуговуючого персоналу ($C_{зп}$);
- відрахування на соціальні заходи (C_c);
- витрати на технічне обслуговування і поточний ремонт обладнання ($C_{то}$);
- вартість спожитої електроенергії (C_e);
- інші (C_i).

Таким чином, експлуатаційні витрати розраховуються за формулою:

$$C = C_a + C_{зп} + C_c + C_{то} + C_e + C_i \quad (6.15)$$

Для розрахунку показників економічної ефективності необхідно розрахувати експлуатаційні витрати по проектному варіанту КС.

6.3.1 Розрахунок амортизаційних відрахувань

Комп'ютерні системи відносяться до четвертої групи відповідно до класифікації груп основних засобів та інших необоротних активів. Для систем на базі комп'ютерної техніки мінімальний термін експлуатації становить 5 років. Амортизація для КС підприємства «Альфа-ЕТЕКС» визначається методом прискореного зменшення залишкової вартості.

Норма амортизації розраховується за формулою:

$$Na = \frac{2}{T} \quad (6.16)$$

де T – строк корисного використання КС.

$$Na = 2/5 = 0,4$$

Таким чином, амортизаційні відрахування по обладнанню, будуть визначатися по формулі 6.17:

$$C_a = K_{пр} \cdot Na, \text{ грн.} \quad (6.17)$$

Амортизаційні відрахування (за перший рік експлуатації) для апаратного забезпечення системи становитимуть:

$$C_a = 1337955 * 0,4 = 535182 \text{ грн.}$$

6.3.2 Розрахунок річного фонду заробітної плати

Розрахунок річного фонду заробітної плати обслуговуючого персоналу, згідно форми, наведено в таблиці 6.2.

Відділ «Логістичний» підприємства «Альфа-ЕТЕКС» має в своєму складі 5 спеціалістів з логістики, 2 помічники та начальник відділу. Робочий день має тривалість 8 годин.

Номінальний річний фонд робочого часу одного працівника визначається за формулою 6.5.

$$F_{\text{НОМ}} = (T_{\text{к}} - T_{\text{пр}} - T_{\text{вих}} - T_{\text{відп}}) * T_{\text{см}}, \text{ ГОДИН} \quad (6.5)$$

Номінальний річний фонд робочого часу спеціаліста з логістики:

$$F_{\text{НОМ}} = (365 - 9 - 104 - 21) * 8 = 1848 \text{ годин}$$

Номінальний річний фонд робочого часу керівника відділу:

$$F_{\text{НОМ}} = (365 - 9 - 104 - 28) * 8 = 1792 \text{ годин}$$

Таблиця 6.2 – Річний фонд заробітної плати

№ п/п	Найменування професії працівників	Кількість працюючих, люд.		Годинна тарифна ставка, грн	Номінальний річний фонд робочого часу (годин)	Всього пряма заробітна плата, грн.	Додаткова заробітна плата (10%)	Доплати (7%)	Всього заробітна плата, грн.
		явочне	списочне						
1	2	3	4	5	6	7	8	9	10
Існуючий варіант									

Продовження таблиці 6.2

1	Оператор ПК	39	39	55	1848	3963960	37884	265188	4267032
2	Керівник	1	1	70	1792	125440	8064	5644,8	139148,8
3	Помічник	2	2	50	1848	184800	12936	9055	206791
Всього									4612971,8
Проектний варіант									
4	Оператор ПК	35	35	55	1848	3557400	30307	212150	3799857
5	Керівник	1	1	70	1792	125440	8316	5821	139577
Всього									3939434

6.3.3 Розрахунок відрахувань на соціальні заходи

Відрахування на соціальні заходи становлять 22% від заробітної плати (формула 4.19):

$$C_c = C_{zn} * 22\%, \text{ грн.} \quad (6.19)$$

$$C_{c.i} = 4612971,8 * 0,22 = 1014853,8 \text{ грн.}$$

$$C_{c.п} = 3939434 * 0,22 = 866675,48 \text{ грн.}$$

6.3.4 Визначення річних витрат на технічне обслуговування і поточний ремонт

Витрати на технічне обслуговування і поточний ремонт включають витрати на матеріали, запасні частини, заробітну плату ремонтним робітником. Вони складають 20% від капітальних витрат:

$$C_{mp} = K_{np} * 20\%, \text{ грн.} \quad (6.20)$$

$$C_{o.p} = K_{np} * 0,2 = 1337955 * 0,2 = 267591 \text{ грн.}$$

6.3.5 Розрахунок вартості споживаної електроенергії

Вартість спожитої електроенергії визначається за формулою:

$$C_e = M * F_p * a, \text{ грн}, \quad (6.21)$$

де M – встановлена потужність апаратури,

F_p – річний фонд робочого часу апаратури (2 920 годин – обладнання працює 8 годин на добу),

a – тариф на електроенергію для підприємств (на передачу 1,5540 грн/КВт·ч, на послуги диспетчерського управління – 0,1023 грн/КВт·ч, $a = 1,5563$ грн).

Сумарна споживана потужність пристроїв автоматики складе 30 Вт. Споживання електроенергії одним персональним комп'ютером 30 Вт (30 шт) – 900 Вт. Споживання електроенергії одним лептопом 20 Вт (9 шт) – 180 Вт. Споживання електроенергії маршрутизатором (6 шт) – 400 Вт. Разом – 4400 Вт (4,4 КВт).

$$C_e = 4,4 * 2920 * 1,5563 = 19995,3 \text{ грн.}$$

6.3.6 Визначення інших витрат

Інші витрати по експлуатації об'єкта проектування включають витрати на навчання персоналу підприємства обслуговування нового обладнання, з охорони праці, придбання спец одягу та ін. Ці витрати складають 4% від річного фонду заробітної плати обслуговуючого персоналу.

$$C_i = C_{зп} * 4\%, \text{ грн.} \quad (6.22)$$

$$C_{i.п} = 3939434 * 0,04 = 157577,36 \text{ грн.}$$

$$C_{i.і} = 4612971,8 * 0,04 = 184518,9 \text{ грн.}$$

Відповідно до формули 4.15 експлуатаційні витрати для КС складуть:

$$C_{п} = 1847021,14 \text{ грн.}$$

$$C_i = 2022141 \text{ грн.}$$

6.4 Визначення та аналіз показників економічної ефективності проекту

Результати розрахунків експлуатаційних витрат по проектуваному і існуючому варіантам зведені в табл. 6.3.

існуючому варіантам зведені в табл. 6.3.

Таблиця 6.3 – Річні експлуатаційні витрати

Найменування показника	Проектний варіант	Існуючий варіант
Амортизація	535182	
Фонд заробітної плати	3939434	4612971,8
Відрахування на соц. виплати	866675,48	1014853,8
Ремонт і тех.обслуговування	64683	
Електроенергія	19995,3	
Інші	10341	37104
Разом	5436310,8	5664929,6

Річна економія на експлуатаційних витратах становить:

$$\Delta C = C_i - C_p, \quad (6.23)$$

$$\Delta C = 5664929,6 - 5436310,8 = 228618,8 \text{ грн.}$$

Термін окупності (T_p) проектуваної системи:

$$T_p = K_{пр} / \Delta C, \text{ років} \quad (6.24)$$

$$T_p = 1337955 / 228618,8 = 5,8 \text{ років}$$

Отже, капітальні витрати на впровадження проектної системи окупляться через 5,7 років.

Коефіцієнт ефективності капітальних витрат визначається за формулою:

$$K_{эфф} = 1 / T_p, \text{ грн.} \quad (6.25)$$

$K_{\text{эфф}} = 1/5,8 = 0,17$ грн.

Отже, на 1 грн. капітальних витрат припадає 0,17 грн. прибутку.

6.5 Висновок

Удосконалення комп'ютерної системи комерційного банку "Райзе Банк" з опрацюванням побудови, налаштування та безпеки корпоративної мережі доцільно, так як при капітальних витратах в 1337955 грн., капіталовкладення окупляться через 5,8 років. Коефіцієнт ефективності капітальних витрат дорівнює 0,17 грн. при мінімальному терміні експлуатації в 6 років.

7 ОХОРОНА ПРАЦІ

7.1 Інженерно-технічні заходи щодо охорони праці на об'єкті

Офіс підприємства розташований в одноповерховій будівлі. Системи каналізації та водопостачання у комерційному банку централізовані і виходять за межі контрольованої зони. Система опалення на підприємстві також централізована і відбувається за допомогою опалювальних радіаторів. Система ж вентиляції даного об'єкта. Централізоване електропостачання приміщення здійснюється від трансформаторної електростанції. Система заземлення виконана згідно вимог Правил безпечної експлуатації електроустановок і забезпечує заземлення всіх приладів присутніх на підприємстві на загальний контур заземлення, який виходить за межі контрольованої зони. Також у банку встановлені системи охоронної та пожежної сигналізації..

7.1.1 Клас приміщення по небезпеці поразки електричним струмом

Клас приміщення по небезпеці поразки електричним струмом – 1, згідно з ПУЕ-85 (без підвищеної небезпеки поразки електричним струмом: сухе, безпилоче, з нормальною температурою та з ізольованими підлогами.

7.1.2 Режим нейтралі електричних мереж, застосовуваних на об'єкті

Електричні мережі за режимом нейтралі поділяють на:

- мережі з глухозаземленою нейтраллю джерела живлення;
- мережі з ізольованою нейтраллю джерела живлення.

На об'єкті застосовується електричні мережі з глухозаземленою нейтраллю, тому що одну з нейтралей силових трансформаторів заземлено безпосередньо.

7.1.3 Заходи щодо електробезпеки

На даному об'єкті всі заходи щодо електробезпеки повинні виконуватись згідно ГОСТ 12.1.019 «ССБТ. Електробезпека. Загальні вимоги і номенклатура видів захисту», ГОСТ 12.1.030 «ССБТ. Електробезпека. Захисне заземлення, занулення».

Заходи щодо електробезпеки складаються з технічних засобів та організаційних заходів. Вони спрямовані на забезпечення недоступності до струмопровідних частин та неможливості випадкового дотику до них, усунення небезпеки поразки у замиканні струму на корпус електрообладнання або на землю; запобігання помилкових дій персоналу в електроустановках.

Персонал, який працює безпосередньо всередині, систематично навчають, перевіряють знання і тренують по техніці безпеки .

На даному об'єкті існують наступні шкідливі фактори:

- 1) Підвищений рівень шуму на робочому місці;
- 2) підвищена або знижена іонізація повітря;
- 3) підвищений рівень статичної електрики;
- 4) підвищений рівень електромагнітних випромінювань;
- 5) перенапруження зорового аналізатора;
- 6) монотонність праці;
- 7) розумове перенапруження.

Для запобігання дії цих шкідливих факторів потрібно:

1) в основному шумовий фон створюють комунікації з клієнтами банку, а також офісна оргтехніка - комп'ютери, сканери, принтери і ін. Вплив подібного роду шуму здатне відобразитися в основному на психологічному стані людини: можлива поява нервових розладів;

2) повітря в приміщеннях зі скупченням людей і наявністю обчислювальної техніки, насичений позитивно зарядженими іонами кисню. Підвищений вміст позитивно заряджених іонів призводить до погіршення

здоров'я, пригнічення нервової системи, настає недолік кисню, який необхідний очам, м'яз;

3) під час роботи на ПК при дотику до будь-якого з елементів обладнання можуть виникнути розрядні струми статичної електрики. Внаслідок цього відбувається електризація пилу дрібних частинок, які притягається до екрану. Зібралася на екрані електризуватися пил погіршує видимість, а при підвищенні рухливості повітря, потрапляє на обличчя і в легені людини, викликає захворювання шкіри і дихальних шляхів. Для захисту від статичної електрики передбачені спеціальні шнури харчування з вбудованим заземленням. Також для захисту від впливу електричного струму всі корпуси обладнання, клавіатура, засувки дисководів і кнопки управління виконані з ізоляційного матеріалу;

4) в даному випадку основним джерелом електромагнітного випромінювання є монітор комп'ютера. У разі знаходження джерела випромінювання в безпосередній близькості від людини, можливі патологічні зміни в органах зору, порушення обміну речовин;

5) для запобігання перенапруження зорового аналізатора потрібно виконувати спеціальну гімнастику для очей, правильно розміщувати персональний комп'ютер;

6) для запобігання монотонності праці необхідно вибирати програмне забезпечення, що зменшує одноманітні операції, використання нових технічних засобів введення;

7) для запобігання розумового перенапруження потрібно дотримання режимів праці і відпочинку.

7.1.4 Протипожежні заходи для об'єкта досліджень

На даному об'єкті присутні не горючі стіни і підлоги, що не підтримують горіння, і стелі, не містять вибухонебезпечних, легкозаймистих

або токсичних речовин і матеріалів а також присутні електрообладнання, а відповідно належить до класу «Г» по пожежній безпеці.

У приміщеннях такого класу присутні:

- система пожежної сигналізації;
- вогнегасники;
- аптечка;

Пожежна профілактика – це комплекс організаційних і технічних заходів, спрямованих на гарантування безпеки людей, запобігання пожежам, обмеження їх поширення, а також створення умов для успішного гасіння пожежі.

Забезпечення пожежної безпеки об'єкта передбачає створення системи попередження пожеж та протипожежного захисту. Велике значення при цьому мають організаційно-технічні заходи, які умовно можна поділити на:

а) організаційні (організація пожежної охорони, навчань, інструктажів та ін.);

б) технічні (суворе дотримання правил і норм, визначених чинними нормативними документами, при реконструкції приміщень, технічному переоснащенні виробництва, експлуатації електромереж, опалення, освітлення та ін.);

в) заходи режимного характеру (заборона паління та застосування відкритого вогню в недозволених місцях та ін.);

г) експлуатаційні (своєчасне проведення профілактичних оглядів, ремонтів устаткування тощо).

З метою попередження пожеж, їх поширення та боротьби з ними усі працівники підприємства комерційного банку "Райзе Банк", проходять навчання та інструктажі з питань пожежної безпеки.

7.2 Розрахунок системи освітлення.

Розрахунок штучного освітлення виконується одним з наступних методів: коефіцієнта використання, питомої потужності чи крапковим. Для розрахунку штучного освітлення потрібно вибрати систему освітлення, джерело світла і світильник, визначити кількість світильників для забезпечення нормованої освітленості і розташувати їх в правильному місці .

Розрахунок освітлення проводиться для кімнати комерційного відділу площиною 25м^2 , довжина якої 5м, ширина - 5м. Розрахунок буде здійснюватись методом коефіцієнта використання.

Для визначення кількості світильників визначимо світловий потік, який поступає на поверхню за формулою :

$$F = E \cdot S \cdot K \cdot Zh, \text{ де} \quad (7.1)$$

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

E – нормована мінімальна освітленість, лк. У нашому випадку, роботу персоналу можна віднести до розряду точних робіт, отже, мінімальна освітленість буде $E = 300\text{Лк}$.

k – коефіцієнт запасу, враховує зменшення світлового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення залежить від типу приміщення і характеру проводимих у ньому робіт і в даному випадку згідно за таблицею 5.4 $k = 1,5$);

S – освітлювана площа, м^2 (у нашому випадку $S = 25\text{м}^2$);

z – коефіцієнт мінімальної освітленості (у нашому випадку для люмінесцентних ламп $z = 1,1$);

h – коефіцієнт використання світлового потоку (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп і обчислюється в частках одиниці; залежить від характеристик світильника, розмірів приміщення, фарбування стін і стелі, характеризується коефіцієнтами відображення від стін (P_C) стелі (P_{II}), та

робочої поверхні (P_p)), значення коефіцієнтів P_c , P_{Π} і P_p були знайдені по таблиці 5.6:

$P_c = 50\%$, $P_{\Pi} = 70\%$, $P_p = 30\%$. Значення h визначимо по таблиці 5.7 коефіцієнтів використання різних світильників. Для цього обчислимо індекс приміщення за формулою (4.2) :

$$I = Sh \cdot (A+B) \quad , \text{де} \quad (6.2)$$

S – площа приміщення, $S = 25 \text{ м}^2$;

h – розрахункова висота підвісу, $h = 3.05$;

A – ширина приміщення, $A = 5 \text{ м}$;

B – довжина приміщення, $B = 5 \text{ м}$.

Підставивши значення отримаємо:

$$I = 253,05 \cdot (5+5) = 0,832$$

Знаючи індекс приміщення I , знаходимо $h = 0,29$

Підставимо всі значення у формулу (6.1) для визначення світлового потоку F :

$$F = 300 \cdot 25 \cdot 1,5 \cdot 1,10,29 = 42674 \text{ лм}$$

Для освітлення обираємо люмінесцентні лампи типу ЛТБ80-4, потужність яких - 80 Вт, напруга - 102 В, світловий потік після 100 годин горіння $F = 4300 \text{ Лк}$. Розрахуємо необхідну кількість ламп за формулою (6.3):

N - число ламп, яке необхідно визначити;

F - світловий потік, $F = 42674 \text{ лм}$;

$F_{\text{л}}$ - світловий потік лампи, $F_{\text{л}} = 4300 \text{ лм}$.

Знаходимо N : 10 ламп.

Таким чином, для забезпечення оптимальних умов освітлення робочого

місця в комерційному відділі необхідно встановити 10 люмінесцентних ламп обраного типу.

Висновок

У розділі «Охорона праці» розроблено інженерно-технічні заходи щодо охорони праці на об'єкті. Також зроблено розрахунок системи освітлення приміщення комерційного відділу.

ВИСНОВОК

В ході виконання дипломного проекту була здійснена модернізація корпоративної мережі банку “Райзе Банк”. При цьому можна зробити наступні висновки:

В мережі було використано якісні комплектуючі всередині мережі, що дозволяє без проблем виконувати операції всередині мережі.

Був досягнутий високий рівень безпеки обмінюваних даних що дозволяє безпечно обмінюватися даними між “Управлінням розвитку міжнародних стосунків” та самим банком.

З негативних висновків була дороговизна якісної мережі, але вона перекивається на виході якісною мережею, що працює без збоїв у роботі, та окупиться менш ніж за 6 років, що дуже непоганий показник серед інших прикладів галузей.

Дуже значущу роль відіграє висока безпечність обміну даних, що у сучасних реаліях являє собою дуже актуальне вирішення проблем боротьби з витоком банківської інформації.

Побудована комп’ютерна мережа може використовуватися у точних галузях у яких є необхідність якісного, безпечного та швидкого обміну даних у мережа, таких як банківська сфера і тд.

Корпоративна мережа банку може при необхідності модифікуватися і налаштовуватися.

Надалі планується впровадити розроблену комп’ютерну систему на підприємство, для якого вона розроблялася.

У дипломному проекті представлений розрахунок техніко-економічних обґрунтування вартості впровадження даної програми на підприємство, а також дотримані всі вимоги для безпечної роботи.

Розрахунки показали, що впровадження в організацію запропонованих рішень економічно ефективно, а розроблена схема розположення відповідає вимогам екологічності та безпеки праці.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні вказівки для бакалаврів 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 «Дніпровська політехніка», 2020. – 67 с.
2. Болілий В.О., котяка В.В. Комп'ютерні мережі. Навчальний посібник. - Кіровоград: ЦОП Авангард, 2008.- 146с.
3. Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. 4-е вид.- 2012. - 944 с.
4. Новожилов О.П., Новожилов Е.О. Комп'ютерні мережі. - Academia, 2011. - 304 с.
5. Леонов В. Комп'ютерна мережа своїми руками. - Ексмо, 2010. - 240 с.
6. Кондратенко С.В., Новіков Ю.В. Основи локальних мереж. Курс лекцій. - Інтуїт, 2012.- 360 с.
7. Трулав Дж. Мережі. Технології, прокладка, обслуговування. 3-е изд. - НТ Пресс, 2009. - 560 с.
8. Кулаков Ю.А., Омелянській С.В. Комп'ютерні мережі. Вибір, установка, використання і адміністрування.- К .: Юніор, 1999.- 544с.
9. Шеннон Р. Імітаційне моделювання систем-мистецтво і наука: Пер. з англ. - М .: Мир, 1978.
10. Максимей І.В. Імітаційне моделювання на ЕОМ. - М .: Радио и связь, 1988.
11. Кудрявцев Е.М. GPSS Word. Основи імітаційного моделювання різних систем. - М .: ДМК Пресс, 2004. - 320 с .: іл. (Серія «Проектування»)
12. Новіков Ю.В., Карпенко Д.Г. Апаратура локальних мереж: функції, вибір, розробка.- М .: ЕКОМ, 1998.- 288 с.
13. Бібліотека TechNet: планування мереж DHCP, [електронний ресурс]. - Режим доступу до інформації: <http://technet.microsoft.com/ru-ru/library/cc786002%28v=WS.10%29.aspx>.
14. Брайан Хілл. Повний довідник по Cisco. - Вільямс, 2006. - 1088 с.

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.20005-01 12 011

Листів 9

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 и ssh комп'ютерної системи.

ЗМІСТ

		Стор.
1.	Налаштування маршрутизатора Postolnik_R1	4
2.	Налаштування комутатора Postolnik_Sw3.0	7

1. Налаштування маршрутизатора Postolnik_R1

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

//Шифрування паролів

service password-encryption

!

//Ім'я пристрою

hostname Postolnik_R1

!

//Пароль до привілейованого режиму

enable secret 5

\$1\$mERr\$hX5rVt7rPNoS4wqbXKX7m0

!

*//Виключення адрес з пулу DHCP*ip dhcp excluded-address 172.16.85.1
172.16.85.10ip dhcp excluded-address 172.16.86.1
172.16.86.10ip dhcp excluded-address 172.16.86.33
172.16.86.43ip dhcp excluded-address 172.16.86.65
172.16.86.75ip dhcp excluded-address 172.16.86.97
172.16.86.87

!

//Створення пулів для VLAN

ip dhcp pool POOL_LAN_Cen_Paper

network 172.16.85.0 255.255.255.0

default-router 172.16.85.1

dns-server 172.16.86.94

ip dhcp pool POOL_VLAN21

network 172.16.86.0 255.255.255.224

default-router 172.16.86.1

dns-server 172.16.86.94

ip dhcp pool POOL_VLAN31

network 172.16.86.32 255.255.255.224

default-router 172.16.86.33

dns-server 172.16.86.94

ip dhcp pool POOL_VLAN41

network 172.16.86.64 255.255.255.224

default-router 172.16.86.65

dns-server 172.16.86.94

!

// Налаштування AAA

aaa new-model

!

aaa authentication login Login group radius
localaaa authentication login default group radius
local

!

*// Створення користувача з паролем*username 12316_Postolnik password 7
082048430017061E010803

!

```

! license udi pid CISCO2911/K9 sn
FTX15242QEJ-

license boot module c2900 technology-
package securityk9

!

// Створення VPN

crypto isakmp policy 10

  encr aes

  authentication pre-share

  group 2

crypto isakmp key cisco address 64.100.13.2

crypto ipsec transform-set VPN-CONF esp-
3des esp-sha-hmac

crypto map VPN-MAP 10 ipsec-isakmp

  description VPN connection to
Postolnik_R0

  set peer 10.0.11.1

  set transform-set VPN-CONF

  match address 110

!

// Створення домену

no ip domain-lookup

ip domain-name Postolnik_R1

!

!

interface GigabitEthernet0/0

  description LAN R4

  ip address 10.0.11.1 255.255.255.252

  duplex auto

  speed auto

!

interface GigabitEthernet0/1

  no ip address

  duplex auto

  speed auto

!

// Налаштування інтерфейсу G0/1 з
інкапсуляцією

interface GigabitEthernet0/1.21

  encapsulation dot1Q 21

  ip address 172.16.86.1 255.255.255.224

!

interface GigabitEthernet0/1.31

  encapsulation dot1Q 31

  ip address 172.16.86.33 255.255.255.224

!

interface GigabitEthernet0/1.41

  encapsulation dot1Q 41

  ip address 172.16.86.65 255.255.255.224

!

interface GigabitEthernet0/1.99

  encapsulation dot1Q 99

  ip address 172.16.86.97 255.255.255.224

!

interface GigabitEthernet0/2

  description LAN Cen_Paper

  ip address 172.16.85.1 255.255.255.0

```

```

duplex auto
speed auto
crypto map VPN-MAP
!
interface Serial0/0/0
interface Vlan1
no ip address
shutdown
!
//Налаштування протоколу
маршрутизації
router ospf 11
log-adjacency-changes
redistribute static
passive-interface GigabitEthernet0/2
passive-interface GigabitEthernet0/1.21
passive-interface GigabitEthernet0/1.31
passive-interface GigabitEthernet0/1.41
passive-interface GigabitEthernet0/1.99
network 172.16.86.0 0.0.0.31 area 0
network 172.16.86.32 0.0.0.31 area 0
network 172.16.86.64 0.0.0.31 area 0
network 172.16.86.96 0.0.0.31 area 0
network 172.16.85.0 0.0.0.255 area 0
network 10.0.11.0 0.0.0.3 area 0
default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
access-list 110 permit ip 72.16.86.128
0.0.0.127 172.16.87.0 0.0.0.63
!
//Налаштування банеру
banner motd
_____123-16
Postolnik Enter with
PASSWORD_____
!
//Налаштування серверу Radius
radius-server host 172.16.86.94 auth-port
1645
radius-server key radius123
!
// Налаштування консольних та vty ліній
у ssh
line con 0
password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15

```



```

password 7 0822455D0A16
transport input ssh
end

2. Налаштування комутатора
Postolnik_Sw3.0
!
version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime
msec

service password-encryption
!
//Ім'я пристрою
hostname Postolnik_Sw3.0
!
//Пароль до привілейованого режиму
enable secret 5
$1$mERr$hX5rVt7rPNoS4wqbXKX7m0
!
// Створення домену
ip domain-name Postolnik_SW_Gosp3.0
!
// Створення користувача з паролем
username 12316_Postolnik privilege 1
password 7 082048430017061E010803
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
//Ранжування інтерфейсів
interface FastEthernet0/5
switchport access vlan 41
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 41
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 41
switchport mode access
!

```

```
interface FastEthernet0/8
  switchport access vlan 41
  switchport mode access
!
interface FastEthernet0/9
  switchport access vlan 41
  switchport mode access
!
interface FastEthernet0/10
  switchport access vlan 41
  switchport mode access
!
interface FastEthernet0/11
  shutdown
!
interface FastEthernet0/12
  switchport access vlan 21
  switchport mode access
!
interface FastEthernet0/13
  switchport access vlan 21
  switchport mode access
!
interface FastEthernet0/14
  switchport access vlan 21
  switchport mode access
!
interface FastEthernet0/15
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/16
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/17
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/18
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/19
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/20
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/21
  switchport access vlan 31
  switchport mode access
!
```

```

interface FastEthernet0/22
switchport access vlan 31
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 31
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 31
switchport mode access
!
//Налаштування TRUNK
interface GigabitEthernet0/1
switchport trunk native vlan 100
switchport trunk allowed vlan 21,31,41,99-100
switchport mode trunk
!
//Налаштування TRUNK
interface GigabitEthernet0/2
switchport trunk native vlan 100
switchport trunk allowed vlan 21,31,41,99
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
//Налаштування інтерфейсу керування
interface Vlan99
description LAN Ekonom_99
mac-address 0001.c938.d901
ip address 172.16.86.99 255.255.255.224
!
ip default-gateway 172.16.86.97
!
//Налаштування банеру
banner motd
-----123-16
Postolnik Enter with
PASSword-----
!
!
// Налаштування консольних та vty ліній и
ssh
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

```