Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Комп'ютерна мережа розподіленого офісу
Назва теми

Галузь знань 12 «*Інформаційні технології*»
Спеціальність *123 «Комп'ютерна інженерія»*
Освітня програма «*Комп'ютерна інженерія*»
Шифр *КРКІ.180115.18.02.13 ПЗ*

Виконав: студент IV курсу, група КІ–18–2 _____ Т.Ю. Приймак
Підпис Ініціали, прізвище

Керівник _____ Ю. П.Кльоц
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С.В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:

Зав. кафедри кібербезпеки _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

« 16 » червня 2022 р.

Хмельницький 2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П.Кльоц

" 01 " 03 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Приймак Тарас Юрійович
Прізвище, ім'я, по батьков студента

1. Тема проекту (роботи): Комп'ютерна мережа розподіленого офісу
Керівник роботи Кльоц Юрій Павлович к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджено наказом ректора університету від 01.03.2022 року 1, додаток №18
2. Строк подання студентом проекту на кафедру: 07.06. 2022 р.
3. Вихідні дані до проекту Завдання на дипломне проектування
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Здійснити огляд, провести аналіз та дослідження існуючих рішень по реалізації комп'ютерної мережі розподіленого офісу. Описати етапи дослідження та здійснити проектування комп'ютерної мережі розподіленого офісу, схеми мережі та необхідні розрахунки. Виконати обгрунтування кваліфікаційної роботи та побудову комп'ютерної мережі розподіленого офісу на базі відомих моделей створення систем віддаленого офісу, який забезпечить стабільну роботу та взаємодію будь-яких її сервісів, тому вона будуть тут ефективним інструментом для створення такій мережі єдиного інформаційного простору для цього офісу.
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Структурна схема мережі, Схема розміщення комп'ютерів у мережі. Структура підприємства. Динамічна маршрутизація у мережі. Мережева статистика роботи мережі. Логічна структура мережі. Інформаційні потоки розподіленого офісу. Організаційна структура мережі.

16.06.2022

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання Видав	Завдання Прийняв
Нормоконтроль	Мостовий С.В., викладач кафедри КБ		
Плагіат	Мостовий С.В., викладач кафедри КБ		

7. Дата видачі завдання 06.03.2022

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапу (розділу) кваліфікаційної роботи	Строк виконання етапу роботи	Примітка
1.	Вступ. Огляд існуючих методів, засобів.	1 декада Лютий	Виконано
2.	Обгрунтування вибраного варіанту.	2 декада. Лютий	Виконано
3.	Опис характеристики та роботи .	3 декада. Лютий	Виконано
4.	Розробка організаційної структури	1 декада. Березень	Виконано
5.	Розробка схеми розташування станцій	2 декада. Березень.	Виконано
6.	Підготовка ескізів креслень.	3 декада. Березень	Виконано
7.	Розробка частини по захисту	1 декада . Квітень	Виконано
8.	Розрахункова частина.	2 декада . Квітень	Виконано
9.	Висновки.	3 декада. Квітень.	Виконано
10.	Погодження з консультантами.	1 декада. Травень	Виконано
11.	Оформлення графічного матеріалу.	1 декада. Травень	Виконано
12.	Оформлення пояснювальної записки.	2 декада. Травень	Виконано
13.	Попередній захист кваліфікац. роботи.	3 декада. Травень	Виконано
14.	Подання роботи на плагіат	3 декада. Травень	Виконано
15.	Захист кваліфікаційної роботи	1 декада . Червень	Виконано

Студент _____ Т.Ю. Приймак
(підпис) (Ініціали, прізвище)

Керівник роботи _____ Ю. П. Кльоц
(підпис) (прізвище та ініціали)

Формат | Зона | Позиц
A4 1
A4 2
A4 3
A4 4
A4 5
A4 6
A4 7
A4 8
A4 9
A4 10

Зм. Арк.
Розробив
Перев.
Н. контр.
Затверд.

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
				Текстові документи		
А4		1	КРКІ.180115.18.02.13 ПЗ	Пояснювальна записка	70	
				Графічні матеріали		
А4		2	КРКІ.180115.18.02.13	Інформаційні потоки	1	
				мережі		
А4		3	КРКІ.180115.18.02.13	Схема комп'ютерної	1	
				мережі		
А4		4	КРКІ.180115.18.02.13	Схема розташування	1	
				комп'ютерів мережі		
А4		5	КРКІ.180115.18.02.13	Логічна структура	1	
				мережі		
А4		6	КРКІ.180115.18.02.13	Статистика роботи	1	
				мережі		
А4		7	КРКІ.180115.18.02.13	Динамічна маршрутизація	1	
				мережі		
А4		8	КРКІ.180115.18.02.13	Організаційна	1	
				структура офісу		
А4		9	КРКІ.180115.18.02.13	Класифікація віртуальних	1	
				мереж		
А4		10	КРКІ.180115.18.02.13	Вибір технології	1	
				віртуальних мереж		

КРКІ.180115.18.02.13 ВП

Зм.	Арк.	№ Докум.	Підпис	Дата
Розробив		Приймак Т.Ю.		
Перев.		Кльоц Ю.П.		
Н. контр.		Мостовий С.В.		
Затверд.		Кльоц Ю.П.		

Відомість проекту

Літера	Аркуш	Аркушів
у	1	1

ХНУ, КІ-18-2

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Комп’ютерна мережа розподіленого офісу»

Автор роботи: Приймак Тарас Юрійович

Керівник роботи: Кльоц Юрій Павлович

Пояснювальна записка: 70 с., 11рис., форм.11, табл. 5, 25 джерел.

Графічна частина: 10 презентаційних слайдів.

КОМП’ЮТЕРНА МЕРЕЖА , ДОСТУП ДО РОБОТИ ОФІСУ, ПЕРЕДАЧА ІНФОРМАЦІЙНИХ ПОТОКІВ, ЕФЕКТИВНІСТЬ РОБОТИ, ВІДДАЛЕНИЙ ОФІС.

Метою кваліфікаційної роботи є проектування та розробка комп’ютерної мережі розподіленого офісу яка має відповідати певним їх параметрам. Комп’ютерна мережа повинна повноцінно відповідати прийнятим стандартам та забезпечити передачу для усіх видів потоків інформації та із врахуванням перспектив розвитку різних сучасних інформаційних технологій по забезпеченню параметрів їх якості. Ця мережа повинна забезпечити інтеграцію та працездатність усіх елементів та систем у мережі для розподілених систем віддаленого доступу та повинна враховувати можливість вдосконалення і розширення. Поставлена у кваліфікаційній роботі мета досягається розв’язанням наступних задач:

1) виконати дослідження та аналіз існуючих подібних систем побудови сучасних комп'ютерних мереж на основі віртуальних каналів;

2) уточнити та визначити вибір, обґрунтування топології та структури мережі;

3) виконати їх інфраструктурну реалізацію та спроектувати комп’ютерну мережу для розподіленого офісу та її програмно-апаратних пристроїв із додержанням забезпеченням параметрів якості роботи для такої мережі.

Отримані результати і їх новизна – комп’ютерна мережа розподіленого офісу повинна забезпечити параметрів якісної роботи для співробітників розподіленої віддаленої комп’ютерної мережі, що дозволить задавати необхідні параметри для якісної їх роботи.

ЗМІСТ

ВСТУП

На сьогодні основою інфраструктури сучасних підприємств та офісів є корпоративні комп'ютерні мережі передачі даних. Сучасна корпоративна комп'ютерна мережа - це досить складна система, що забезпечує передачу потоків різноманітної інформації між різними додатками та їх системами, що використовуються у цій мережі офісу. Така розподілена комп'ютерна мережа може включає у себе сервіси та системи для усіх підрозділів та їх базу даних, електронний документообіг та організацію їх нарад, відео конференції із віддаленими їх підрозділами, забезпечення усіх потреб для офісу у високоякісному місцевому, міжміському, міжнародному зв'язку. Усе це достатньо зменшує час реакції на поточні зміни, що відбуваються у офісі та забезпечує раціональне їх управління процесами для офісу у реальному часі. Для організації необхідних конференцій та якісного зв'язку у комп'ютерних мережах використовують сучасну IP-телефонію, що значно знижує залежність офісу від операторів зв'язку. Також, комп'ютера мережа дає можливість передавати всюди будь-яку конфіденційну інформацію їх фінансового чи виробничого характеру із упевненістю, що ніхто не має до неї доступу. Такі комп'ютерні мережі приходять на зміну різним спеціалізованим мережам. Із розвитком комп'ютерних мереж та їх сервісів, вимоги до такої мережі зростають. Необхідно також забезпечення фізичної їх безпеки для складу офісу уже шляхом відеоспостереження. Дана комп'ютерна мережа повинна включати у себе сервіс відео конференцій.

При побудові комп'ютерної мережі розподіленого офісу головна ідея об'єднати у єдиній мережевій інфраструктурі, яка заснована на пакетному протоколі та можливість передачі потоків даних, голосових потоків і відео – є досить привабливою для офісів, адже мережа здатна скоротити витрати та збільшити продуктивність роботи працівників. Відомі на сьогодні рішення побудови таких мереж досить специфічні, по скільки розглядаються конкретні системи та уже наявні їх результати практично неможливо використовувати при побудові та аналізі інших мереж із потрібними параметрами. Це пояснюється тут сильною залежністю від початкових параметрів комп'ютерної мережі від уже

пропонованих вимог для обробки та захисту, представлення потоків інформації та її сервісів, які така комп’ютерна мережа надає. Приймаючи необхідне рішення про побудову комп’ютерної мережі розподіленого офісу із інтеграцією у неї сервісу IP-телефонії, офіс прогнозує значне зростання регіональних його філій. Така мережа, зазвичай уже є територіально розподіленою та об'єднує офіси та інші підрозділи, що знаходяться на досить великій відстані один від одного. Тому іноді під мережі комп’ютерної мережі є розташованими у різних частинах та містах, а інколи у різних країнах. Самі підходи, за якими уже будується така комп’ютерна мережа, уже сильно відрізняються від тих, що застосовуються при створенні простої мережі.

При проектуванні комп'ютерної мережі розподіленого офісу основною відмінністю буде полягати у тому, що територіально розподілені комп’ютерні мережі використовують досить повільні відомі орендовані лінії для зв'язку. Якщо ж при створенні простої мережі основні витрати тут припадають на закупівлю нового мережевого обладнання та прокладку кабелю, то у сучасних територіально-розподілених комп’ютерних мережах найдорожчою їх складовою виявляється просто орендна їх плата за використання цих каналів, що швидко зростає із збільшенням їх якості та швидкості передачі потоків даних [1]. Тут це обмеження є досить принциповим і тому при побудові комп’ютерної мережі слід вживати певних заходів для мінімізації обсягів потоків даних, що тут передаються. Перша є проблема, що доводиться вирішувати при створенні комп’ютерної мережі для об’єднання підрозділів офісу. Якщо ж у межах одного міста можна уже розраховувати на оренду для виділених каналів, у тому числі і високошвидкісних, то при переході до географічно віддалених вузлів мережі вартість для оренди таких каналів стає дорогою, а якість а надійність їх часто виявляється досить низькою. Тут очевидною альтернативою побудови є використання уже існуючої мереж Інтернет. В цьому випадку досить просто забезпечити ці канали від підрозділів офісу до найближчих вузлів такої мережі і завдання для обміну інформацією між вузлами мережі Інтернет вона візьме на себе.

На сьогодні навіть при створенні досить невеликої комп’ютерної мережі у межах одного міста слід закладати тут можливість для подальшого розширення та використовувати технології, що сумісні із існуючої мережею Інтернет. При використанні мережі Інтернет у якості головної основи для комп’ютерної мережі передачі потоків даних з'ясовується уже цікава річ, якщо заглянути у структуру самої мережі Інтернет, можна побачити, що вся інформація тут проходить через абсолютно незалежних та некомерційні вузли, які пов'язані через різноманітні інформаційні канали та мережі для передачі даних. Якщо тут говорити про приватну комп’ютерну мережу то інформацію, що передається у ній просто захистити від чужого її впливу. Непередбачуваність же шляхів для потоків інформації між незалежними вузлами Інтернету тут не тільки підвищує ризик того, що така інформація може тут бути перехоплена, проте робить неможливим для визначення місця витоку цієї інформації. На сьогодні існують способи та засоби для шифрування потоків інформації, що передається, що дозволяють частково уже вирішити таку проблему [2].

Зовсім інший аспект цієї проблеми безпеки уже пов'язаний із децентралізацією самої мережі Інтернет бо немає нікого, хто міг обмежити повний доступ до ресурсів приватної комп’ютерної мережі. По скільки це є відкрита система, де усі бачать усіх тому будь-який бажаючий тут може спробувати сам потрапити у цю комп’ютерну мережу та отримати доступ до її даних. Є деякі методи, способи та засоби, такі як брандмауер, але це тут не дає повного захисту для мережі, бо потрібно враховувати ще забезпечення самої безпеки до потоків інформації, що передається у рамках такої мережі, щоб тут доступ до неї мав отримувати лише конкретні співробітники, що повинні її самі побачити. Все це досягається за допомогою уже поділу комп’ютерної мережі на її віртуальні мережі та застосування необхідних політик її безпеки. У такому зв’язку із непередбачуваними обставинами у світі та карантин, перед офісами компаній постало питання для організації віддаленого режиму доступу для безпечної роботи своїх співробітників. По скільки багато фірм та організацій раніше не реалізовували такий перехід до роботи, то швидке впровадження такого режиму віддаленої роботи призвело до проблем і їх інформаційною безпекою. В умовах

пандемії значно підвищилась активність від дій шахраїв та зловмисників, що через комп'ютери віддалених співробітників офісів можуть отримати повний доступ до ресурсів комп'ютерної мережі через те що, організації не створили умов для захищеного доступу до своїх інформаційних систем. Найчастіше для такої дистанційної роботи уже використовуються віддалені підключення, тому що у практично усіх нових версіях операційних систем є необхідне для цього програмне забезпечення, що використовує незахищений протокол. Тому при організації своєї дистанційної роботи користувачам офісів рекомендується не використовувати такий варіант, а тому слід зупинитися на більш захищених сучасних технологіях та їх протоколах [3].

По скільки зазначена проблема при проектуванні комп'ютерної мережі розподіленого офісу є актуальною, у даній кваліфікаційній роботі планується розглянути основні аспекти для роботи VPN, визначити відмінності між їх проколами та технологіями, розробити модель найбільш захищеного доступу до комп'ютерної мережі.

Саме ж створення віртуальних приватних мереж дозволяє тут об'єднати усі підрозділи розподіленого офісу, що мають географічно-розгалужену його структуру. Тому незалежно від взаємної віддаленості їх територіальних підрозділів офісу та їх складів, система забезпечує їх повну зв'язність, стабільну роботу та взаємодію будь-яких її сервісів, тому вона тут є ефективним інструментом для створення у мережі єдиного інформаційного простору для офісу.

Актуальність кваліфікаційної роботи полягає у розробці та вдосконалені заданої комп'ютерної мережі розподіленого офісу із застосуванням віртуальних під мереж. Основна задача забезпечення якості доступу у комп'ютерній мережі є пошуком певного компромісу між параметрами передачі у мережі та складністю їх віртуальних технічних рішень, що тут застосовуються.

Метою кваліфікаційної роботи є проектування та розробка комп'ютерної мережі розподіленого офісу яка має відповідати певним їх параметрам. Комп'ютерна мережа повинна повноцінно відповідати прийнятим стандартам та забезпечити передачу для усіх видів потоків інформації та із врахуванням

перспектив розвитку різних сучасних інформаційних технологій по забезпеченню параметрів їх якості. Поставлена у кваліфікаційній роботі мета досягається розв’язанням наступних *задач*:

1) виконати дослідження та аналіз існуючих подібних систем побудови сучасних комп'ютерних мереж на основі віртуальних каналів;

2) уточнити та визначити вибір, обґрунтування топології та структури мережі;

3) виконати їх інфраструктурну реалізацію та спроектувати комп’ютерну мережу для розподіленого офісу та її програмно-апаратних пристроїв із додержанням забезпеченням параметрів якості роботи для такої мережі.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОГЛЯД ІСНУЮЧИХ ТЕХНОЛОГІЙ, МЕТОДІВ ТА ЗАСОБІВ

1.1 Дослідження та аналіз особливостей концепцій побудови та проектування сучасних комп’ютерних мереж

При дослідженні та аналізі сучасних комп’ютерних мереж врахуємо, що у основний перелік складових елементів сучасних телекомунікаційних технологій, які присутні на більшості виробничих офісів, входять декілька діючих мереж, а це телефоні та комп'ютерна, охоронної та пожежної сигналізації, диспетчерського зв'язку та управління технологічними процесами, гучномовний зв'язок та деякі інші типи. Для повноцінної підтримки усіх перерахованих мереж на нині діючих виробничих потужностях прокладені багато кілометрів кабельних систем. Самим молодшим із них уже близько 20 років, а основна ж маса таких має вік більше 40 років [4].

При проектуванні та будівництві будь-якої промислової будівлі та його офісу у ньому відразу закладають різні кабельні траси. У міру розвитку фірм еволюціонує і його система комунікації тобто збільшується їх абонентська ємність, розгалужується комп’ютерна мережа для зовнішніх зв'язків тощо. Хоча саме обладнання для систем каналів передачі та зв'язку зазвичай належить ще до того ж покоління, що і саме це підприємство. Проте з часом абонентська ємність досягає своєї межі завантаження бо її кабельна система повністю забита, а самі кабелі, що давно прокладені практично майже непрацездатні через досить важкі умови їх експлуатації. Виникають також складнощі із організацією зовнішніх каналів передачі та зв'язків, по скільки наявні тут автоматичні станції практично не стикуються із їх новими станціями міського та міжміського зв'язку. Тому приходить пора для заміни усього обладнання цих систем зв'язку. Причому нові доводиться вводити так, щоб не зупиняти усю мережу відразу і таким чином модернізуючи її досить поступово. Це також відноситься і до кабельної системи,

бо деякі підлягають заміні, а внутрішня розводка по будівлях офісів повинна бути збережена.

Існуючі комп'ютерні мережі тут створювалися у такий простий спосіб, якщо потрібно з’єднати комп'ютери, що знаходяться сусідній кімнаті, туди підводився додатковий кабель, а при необхідності охопити ще одну таку кімнату ще проводився інший кабель тощо. У результаті такого проектування виходила складна мережа із досить заплутаною її структурою. Описаний такий підхід до розгортання нової мережі обмежувався межами одного офісу підприємства, а іноді і одного підрозділу. У разі необхідності для приєднання комп'ютерів, які розташовані у інших будівлях чи навіть у інших частинах будинку проблеми ставали ще складнішими. Із появою потужних інформаційних систем для управління виробництвом ефективність використання комп’ютерних мереж у виробничих підрозділах стала низькою. Відомості про динаміку розвитку таких виробничих процесів тут надходять із різних джерел по каналах передачі різної якості і тому досить часто запізнюються, у результаті чого все оперативне управління та планування виявляється відірваними від самого фактичного стану цих виробничих об'єктів. Самі ж диспетчерські служби у більшості фірм працюють на граничному рівні їх завантаження та вручну реалізуючи багато своїх управлінських процедур і виконуючи досить великий обсяг облікових операцій та постійно відволікаючись на телефонні запити [5].

Сучасна інтеграція комп’ютерних мереж надає можливість доступу до неї різним її користувачам та до будь-яких даних чи додатків у рамках політики інформаційної безпеки. На сьогодні немає такого інформаційного ресурсу де б доступ до якого не можна було отримати по комп’ютерній мережі. Сучасні комп’ютерні мережі мають властивість керованості та має високий рівень безвідмовності, живучості та обслуговуються за підтримки критично важливих для діяльності сервісів, а також це інфраструктура організації, що підтримує вирішення її актуальних завдань та забезпечує досягнення її виробничих цілей. Мережа об'єднує у єдиний інформаційний простір усі об'єкти офісу підприємств. Комп’ютерна мережа створюється як апаратно-технічна основа такої системи, як її головний системо утворюючий її компонент, на базі якого уже конструюються

інші необхідні системи та сервіси [6]. Така мережа задумана та проектується у єдиній системі її координат, основу для якої складає поняття її системно-технічної інфраструктури, системної її функціональності, а це сервіси та додатки і її експлуатаційних характеристик. Кожне її поняття тут знаходить своє відображення у тому чи іншому компоненті комп'ютерної мережі та реалізується у конкретних технічних її рішеннях.

При проектування комп'ютерної мережі розподіленого офісу із функціональної точки зору це є ефективне середовище для передачі актуальною поточної інформації, необхідної для вирішення різних завдань. Із системно-технічної точки зору така комп'ютерна мережа являє собою цілісну інформаційну структуру, що складається із декількох взаємопов'язаних та взаємодіючих рівнів, а це комп'ютерна мережа, різні телекомунікації, комп'ютерні платформи, програмне забезпечення проміжного шару та додатки. Із точки зору системної функціональності мережа виглядає як єдине ціле, що надає своїм користувачам набір корисних у роботі сервісів, загальносистемних та спеціалізованих додатків, що володіють набором корисних якостей та властивостей. Тут одним з принципів, які покладені у основу створення комп'ютерної мережі є максимальне використання її типових рішень та стандартних уніфікованих її компонентів. Цей принцип стосовно її прикладного програмного забезпечення можна виділити у ряд універсальних сервісів, які доцільно було б зробити базовими компонентами для додатків, а такими сервісами є сервіс для системи управління базою даних, файловий сервіс, інформаційний сервіс, V o IP сервіс телефонії, сервіс відео конференцій, мережевий друк тощо.

Для комп'ютерної мережі розподіленого офісу відзначимо, що основним засобом для побудови її прикладних та системних сервісів є програмні засоби проміжного її шару. Поняття сервісів програмного забезпечення для проміжного шару корисно при опрацюванні архітектури комп'ютерної мережі. Тому фактично, програмна інфраструктура комп'ютерної мережі розподіленого офісу є багатошаровою системою. Нижні шари тут складають низько рівневі сервіси, такі як сервіс для імен, сервіс для реєстрації, мережевий сервіс тощо. А вище лежачі шари включають також сервіси управління документами, управління її

повідомленнями та подій. Верхній шар уже являє собою сервіси, до яких як опосередковано звертаються усі користувачі. Для комп'ютерної мережі розподіленого офісу зручно описувати у термінах її сервісів. Політику інформаційної безпеки доцільно було б будувати уже виходячи із потреби у захисті існуючих сервісів. До основних загально системних додатків тут відносять засоби для автоматизації їх індивідуальної праці, що використовуються за різноманітними категоріями цих користувачів та орієнтовані на вирішення типових її офісних завдань, а це електронні таблиці та графічні редактори, календарі та записні книжки тощо. Ці загально системні додатки представляють собою уже тиражовані локалізовані її програмні продукти, які нескладні у освоєнні та прості у використанні і орієнтовані на кінцевих її користувачів.

Самі ж спеціалізовані додатки спрямовані на вирішення тих завдань, які неможливо чи технічно досить складно автоматизувати за допомогою уже загально системних її додатків. Спеціалізовані додатки купуються у компаній їх розробників, що спеціалізуються у своїй діяльності уже на конкретну сферу діяльності чи створюються компаніями-розробниками уже на замовлення самих підприємства або уже розробляються силами самого офісу організації. У більшості випадків такі спеціалізовані програми звертаються у процесі їх роботи до загально системних її сервісів, як файловий сервіс, бази даних тощо. Спеціалізовані додатки та їх сервіси, що розглядаються у сукупності у масштабах офісу організації та визначають увесь спектр для прикладної їх функціональності. Термін служби для системно-технічної інфраструктури у декілька разів більше, ніж у її додатків. У комп'ютерної мережі розподіленого офісу забезпечується можливість для розгортання нових її додатків та їх ефективне функціонування при збереженні повноцінних інвестицій у неї і повинна мати властивість її відкритості та продуктивності, збалансованості та масштабованості, високої готовності та безпеки, керованості тощо. Усі перераховані властивості являють собою її експлуатаційні характеристики для мережі та визначаються у сукупності якістю продуктів та рішень, що покладені у її основу.

Тому зрозуміло, що хороші показники по конкретних їх властивостях будуть досягатися уже за рахунок грамотних її технічних рішень для системного

конструювання. Так ця інформаційна система буде мати усі властивості для безпеки, високої її готовності та керованості за рахунок повної реалізації у проекті комп’ютерної мережі розподіленого офісу відповідних її служб. Сама ж масштабованість у контексті комп'ютерних платформ означає можливість для адекватного її нарощування потужностей комп'ютеру та досягається такими якостями лінії їх серверів, як плавне нарощування їх потужності від моделі до нової моделі, єдина операційна система для усіх моделей, зручна та продумана її політика для модифікації молодших її моделей у напрямку старших моделей. У мережі загальносистемні служби це є сукупність програмного забезпечення, що не спрямовані уже безпосередньо на вирішення її прикладних задач, проте необхідні для забезпечення їх нормального функціонування у мережі офісу підприємства. У якості уже обов'язкових для комп’ютерної мережі розподіленого офісу повинні бути включені служби її інформаційної безпеки, їх основного централізованого моніторингу та адміністрування. Розглянутий тут набір понять є досить абстрактним для того, щоб сформулювати комп’ютерну мережу поза прив'язкою до її конкретних програмно-апаратних рішень тау той же час достатньо конкретний для визначення їх корисної функціональності як засіб для вирішення завдань користувача мережі та експлуатаційних її характеристик для служби мережі [7]. Викладені вище поняття та принципи уже цілком конкретні і будучи прийнятими у якості основоположних при побудові комп’ютерної мережі розподіленого офісу, вони виливаються у конкретні кроки та технічні дії.

1.2 Застосування віртуальних мереж для покращення параметрів мережі

Сама історія виникнення віртуальних мереж почалася ще із середини 60-х років 20 століття, коли уже була запроваджена система для автоматичного з'єднання абонентів телефонії. На той час це був спосіб для надання послуг зв'язку своїм абонентам із декількох компаній на основі їх спільного обладнання для однієї станції. Тут можна сказати, що це була перша віртуальна приватна телефонна мережа тому що орендувалися уже раніше створені канали передачі, завдяки чому тут створювалися віртуальні канали для передачі інформації. [8]

Основна перевага компанії розробника полягала у тому, що фірми могли досить заощадити кошти на покупку своїх власних станцій, їх монтаж, а також їх експлуатацію. Абоненти компанії створювали замкнуті групи для користувачів, у яких був тут обмежений зовнішній їх доступ та для них у станціях мережі також використовувались віртуальні станції [9].

Виникнення таких віддалених робочих місць ще почалося у 1996 році, коли фірма MICROSOFT розробила VPN віртуальну мережу для доступу до її віддалених працівників до своїх доступних ресурсів [10] . Уже у 1999 році була розроблена нова модель перевірки та додаткові засоби для конфігурації її клієнтів. А уже в 2000 році відбулося включення системи VPN до WINDOWS [11]. На сьогодні існує велике різноманіття визначень для VPN, проте усі вони засновані на тому, що їх основною відмінністю є передача пакетів за допомогою мережі Інтернет. Найбільш вузьке та загальне визначення виглядає уже наступним чином VPN – віртуальна приватна мережа як узагальнена назва для технологій, що дозволяють забезпечити одне чи кілька мережних з'єднань або логічну мереж поверх іншої комп’ютерної мережі. Дане таке визначення уже жодним чином не вказує на якісь особливості такої технології. У різних наступних визначеннях уже вказуються певні важливі її характеристики технології де VPN це безпечне та зашифроване підключення між двома її мережами чи між окремим користувачем та мережею [12] чи VPN це є мережева технологія, що створює захищене мережеве його з’єднання через загально доступну таку мережу Інтернет чи приватну мережу, що належить до постачальника послуг.

Сам термін віртуальна приватна мережа використовується також для позначення досить стійких інформаційних потоків для одного підприємства, що існують у публічній мережі із комутацією пакетів та які у достатній мірі захищені від впливу їх потоків даних від інших користувачів цієї публічної мережі [13]. А на думку деяких витоків VPN є об'єднанням для окремих машин чи локальних мереж у віртуальну комп’ютерну мережу, що забезпечує цілісність та безпеку переданих даних. Вона тут має властивості їх виділеної приватної мережі та дозволяє передавати свої дані між двома комп'ютерами через їх проміжну мережу

Інтернет [14]. Головною метою VPN є організація для доступу до комп'ютерної мережі компанії за допомогою уже мереж загального користування.

Загалом VPN мережа використовується для вирішення наступних її завдань: - для організації глобального її зв'язку між філіями для однієї компанії;

- для з'єднання приватної мережі компанії із її діловими партнерами і клієнтами;

- для взаємодії окремих її мобільних користувачів чи співробітників, що працюють удома, із мережею за допомогою віддаленого доступу [15]. Тут VPN забезпечує конфіденційність, цілісність та доступність її інформації. Тобто тут гарантує те, що ця інформація не буде доступна для небажаних особах, буде збережена та доступна тут лише визначеним її користувачам. Дані тут характеристики забезпечується уже за допомогою основних компонентів системи VPN, що наведені на рис. 1.1.

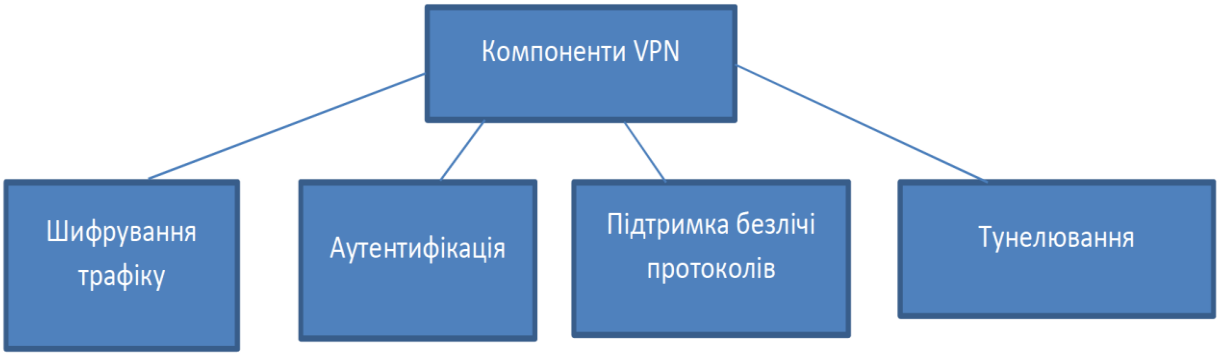


Рисунок 1.1 – Основні компоненти мережі VPN

У віртуальній мережі шифрування потоку передачі включає у себе кодування потоків інформації для запобігання отримання цих даних уже третіми особами. Доступ до таких потоків інформації будуть мати лише ті її користувачі, яким для системи дешифрування було надано їх відповідний ключ. Система шифрування має бути складними для забезпечення конфіденційності її інформації, що уже передається у межах такого періоду, до якого вона буде уже актуальна. Алгоритм для шифрування повинен протидіяти її протизаконному дешифруванню потоку даних на довгий період [16]. Щодо процесів аутентифікації, то тут мається на увазі, що на її центральному сервері

відбувається уже аутентифікація її користувачів. Також тут може відбуватися взаємна їх аутентифікація для з’єднаних уже вузлів, а для більшої їх безпеки рекомендується уже використовувати двох факторну аутентифікацію [17]. Самі ж протоколи VPN визначають рівень для захищеності потоків даних та уже те як VPN взаємодіє із іншими системами у мережі Інтернет. Система VPN забезпечує підтримку досить великої кількості їх протоколів. Остання її характеристика указує на те, що система VPN створює свій відокремлений канал між уже з’єднаними пристроями. При цьому тут кожен кінцевий вузол системи VPN здатен забезпечувати кілька своїх одночасних з'єднань із іншими її вузлами. Також водночас за допомогою системи шифрування потік даних розділяється та всі ці вузли є відокремленими один від одного [18].

1.3 Особливості побудови та класифікації віртуальних мереж

При розгляді особливостей побудови та класифікації віртуальних мереж була досліджено, що у літературі існують різні варіанти по класифікації систем VPN за її різноманітними параметрами. Основна консолідована класифікація тут наведена на рис. 1.2. Розглянемо конкретно кожний вид системи VPN більш детально. За рівнем захисту це довіритель ні бо використовуються для налаштування самої віртуальної нової мережі під основною її мережею. При цьому тут не приділяється особлива увага проблемам для забезпечення безпеки, по скільки середовище для передачі потоку даних є довірчою. Це захищені віртуальні мережі і використовуються для налаштування надійних та високо захищених комп’ютерних мереж на основі існуючих незахищених мереж [19].

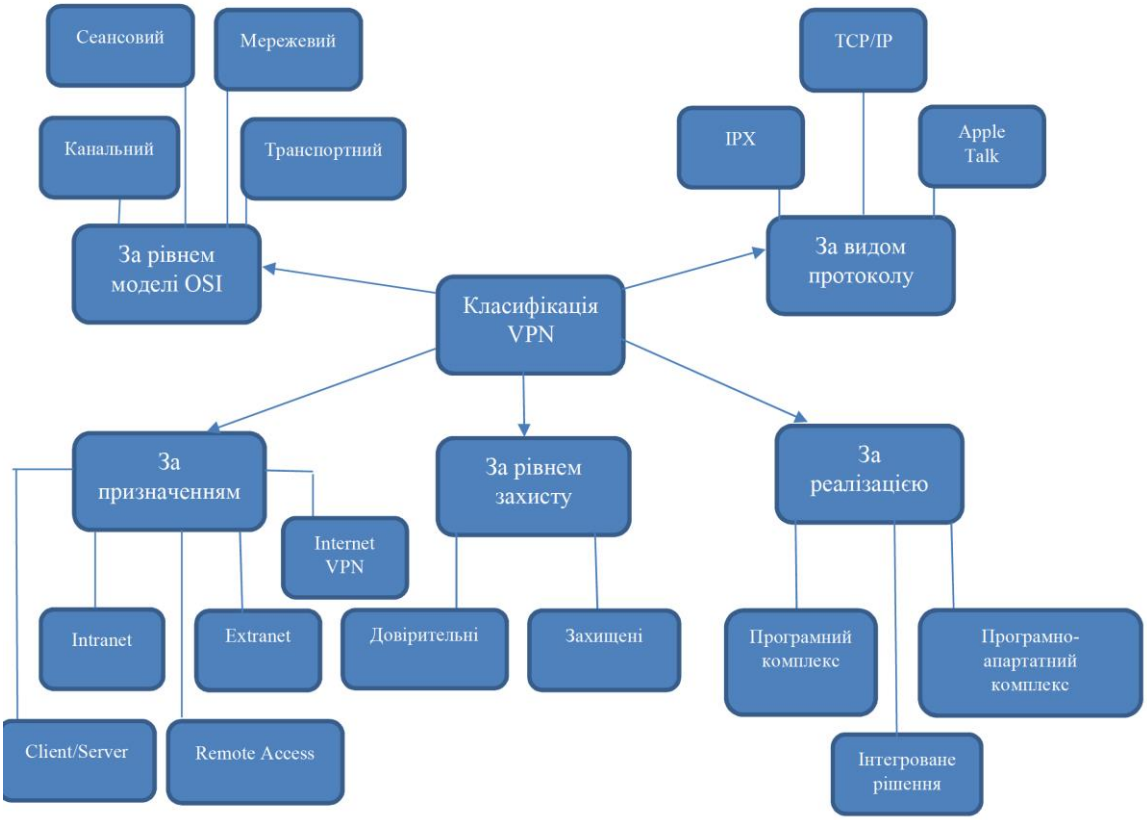


Рисунок 1.2 – Основна консолідована класифікація віртуальних мереж

Класифікація за реалізацією, а це інтегроване рішення, що використовується програмно-апаратним комплекс, який налаштовує свій мережевий екран та фільтрує потік передачі. Це програмно-апаратний комплекс, що реалізується за рахунок спеціалізованих програмно-апаратних засобів комп'ютерної мережі. Далі програмний комплекс, що використовує комп'ютер клієнту зі спеціальним програмним забезпеченням. Поділ за призначенням, а це мережа Інтранет, що об'єднує філії різних організації у високо захищену комп'ютерну мережу для обміну різною інформацією за рахунок створення уже відкритих каналів. Далі це мережа Екстра яка об'єднує кілька різних її компаній у єдину комп'ютерну мережу, але для небажаних тут користувачів обмежується доступ до усієї конфіденційної інформації. Це мережа REMOTE ACCESS, яка створює захищений канал між її віддаленим співробітниками та мережею офісу компанії. Це мережа Client/Server, що поділяє саму фізичну мережу на декілька її логічних під мереж. Це мережа Інтернет, що забезпечує доступ по спільному її фізичному каналу для декількох її користувачів у мережі їх провайдеру [20]. За рівнем

моделі OSI це канальний рівень, протоколи SLIP, PPP, PPTP, L2TP, які здійснюють інкапсуляцію декількох типів потоку даних, а також створює віртуальні тунелі за принципом точка-точка. Це мережевий рівень протоколи IP sec, MPLS, що забезпечує інкапсуляцію одного IP пакету у інший. Це транспортний рівень протоколи SSL/TLS, який забезпечує цілісність та конфіденційність потоку даних, управляє ключами у процесі передачі даних, а також здійснює їх перевірку як відправника так і отримувача. Це сеансів рівень протокол SOCKS, який забезпечує підтримку необхідних програм, для яких потрібно встановити умови по доступу для їх користувачів та спрямувати їх інформаційний потік . За видом протоколу можна виділити системи VPN під IPX, Apple-Talk та TCP/IP де найбільш популярним є протокол TCP / IP.

У рамках проектування комп'ютерної мережі розподіленого офісу розглянемо основні способи організації VPN такій мережі. Основою для створення VPN є побудова його тунелю, тобто такого каналу між двома пристроями для передачі потоку даних . Найбільш поширеними віртуальними мережними підключеннями є самі підключення для віддаленого користувача до мережі офісу компанії , це є з'єднання двох офісів за типом точка - точка. У першому випадку створюється тунель між комп'ютером їх клієнта та сервером офісу компанії. Тут клієнтський VPN на віддаленому пристрої уже підключається до його VPN-шлюзу комп'ютерної мережі, за допомогою якого уже перевіряється реальний чи істинний характер паролю тобто процедура встановлення належності користувачеві інформації у системі пред'явленого ним ідентифікатора користувачі. Після успішної перевірки надається доступ до ресурсів у комп'ютерній мережі офісу компанії, а це сервери даних, бази їх знань, адміністративні пристрої тощо. Від сайту до сайту VPN (рис.1.3) який налаштовується за рахунок побудови уже стабільного тунелю між двома їх пристроями чи маршрутизаторами, завдяки цьому немає тут необхідності у додатковому програмному забезпечені на комп'ютері користувачів у офісах [20].

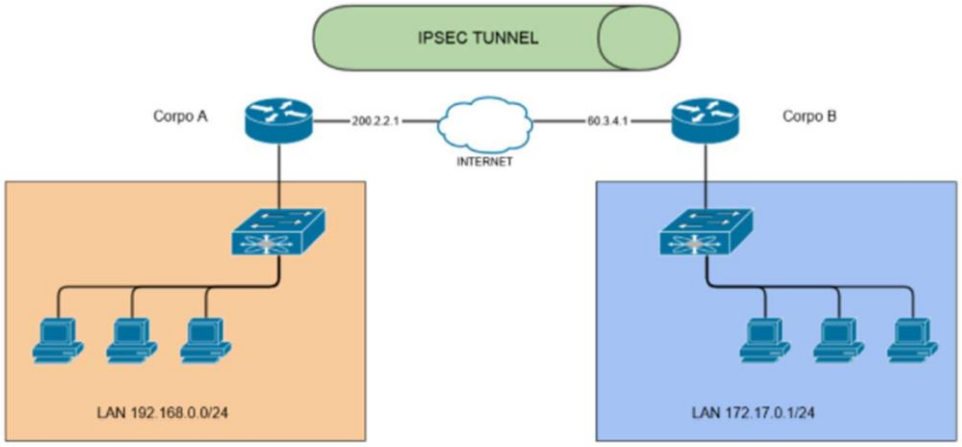


Рисунок 1.3 – Структура від сайту до сайту системи VPN

Віртуальна технологія створення тунелів має досить широкий спектр їх застосовування при формуванні таких захищених каналів для доступу. Для такої реалізації цього типу використовуються протоколи на таких рівнях як канальний, мережевий та транспортний. Канальний рівень використовує протоколи PPTP та L2TP, де PPTP протокол працює лише на пристроях, робота яких уже базується на системі WINDOWS та використовує протокол TCP / IP. За допомогою даного протоколу у мережі будується тунель до серверу одержувача, по якому також передаються PPP - пакети. Після цього сервер та комп'ютер-клієнт уже починають обмінюватись своїми службовими пакетами. Далі тут відбувається інкапсуляція її даних де PPP - кадр вставляється у пакет, який у свою чергу вставляється у кадр із додаванням його IP-заголовку. У цьому заголовку уже зазначаються адреси одержувача та відправника цього пакету. Далі протокол PPTP указує відповідні PPP закінчення та їх заголовок [25]. У протоколі PPTP виявлено досить велику кількість її недоліків.

У віртуальних мережах замість нього рекомендується використовувати протокол L2TP бо він створює VPN-мережі із розмежуванням прав доступу. Протокол L2TP використовує UDP протокол як його транспорт, а також застосовує аналогічний йому формат для повідомлень по управлінню конфігурація тунелем та передачі її пакетів. Даний прокол вставляє свої кадри PPP у протокол для мережевого рівня, проте попередньо проводить перевірку користувача. Протокол L2TP додає свій заголовок PPP, а потім заголовок L2TP

до поля його інформаційних даних PPP. Отриманий такий пакет вставляється за допомогою протоколу UDP. Протокол L2TP може тут шифрувати UDP повідомлення та також додавати до них свій заголовок та закінчення ESP. Далі після цього відбувається інкапсуляція у пакет IP де додається IP-заголовок, який уже містить адреси для одержувача та його відправника. [21]. Уже після цього протокол L2TP виконує другу його PPP- інкапсуляцію по підготовці потоку даних до відправлення. Комп'ютер користувача тут одержує ці пакети, а далі відбувається обробка цього PPP закінчення та PPP заголовку та при цьому заголовок IP видаляється із цього пакету. Також після цього обробляється уже UDP заголовок та для визначення тунелю уже використовується L2TP заголовок. Далі після виконання усіх вище вказаних дій у PPP пакеті залишаться лише ті актуальні дані, що будуть направлені користувачеві.

У комп’ютерній мережі розподіленого офісу мережевий рівень представлений набором протоколів IP Sec де AH заголовок гарантує цілісність заголовків та усіх даних усередині пакетів, однак вона не в змозі забезпечити їх конфіденційність. Протокол ESP шифрує та захищає цілісність інкапсуляцію IP пакетів, додатково перевіряє ESP заголовок та гарантує їх конфіденційність для цих даних. Він передає своїм граничним вузлам для захищеного каналу уже генеровані шифрувальні ключі. Загалом існує два режими роботи IP Sec де тунельний режим забезпечує захист пакету і його заголовку та транспортний який захищає дані усередині пакету. Загалом тунельний режим IP Sec для топології SSL VPN із AAA SERVER (рис. 1.4) здійснює додавання нового заголовку у IP-пакет де здійснюється інкапсуляція та шифрування первинного його IP-заголовку, а його адреса відправника та отримувача може тут бути змінена на адресу його граничного шлюзу, а шлюз VPN чи вузол отримувача уже здійснює його інкапсуляцію [22].

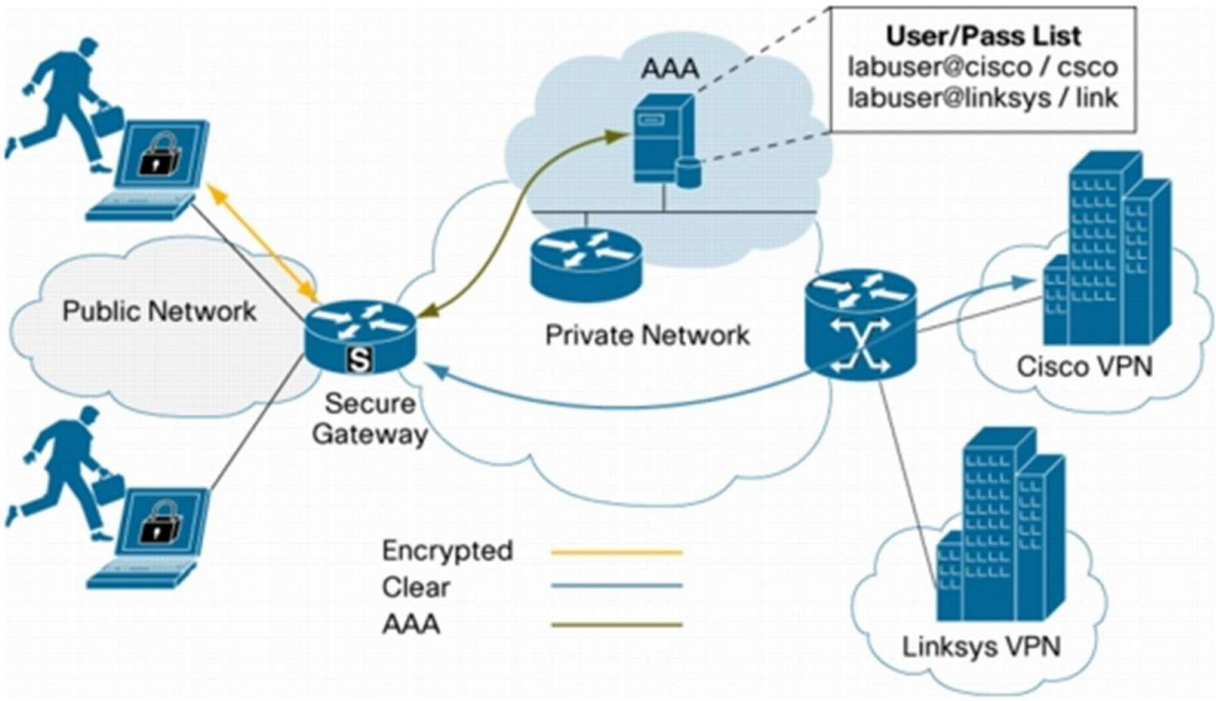


Рисунок 1.4 – Топологія SSL VPN із AAA SERVER
для тунельного режиму

У віртуальній мережі на транспортному рівні режим IP Sec для взаємної перевірка SSL на основі сертифікатів (рис. 1.5) використовується також первинний IP-заголовок та не змінюються адреси відправника та отримувача і кінцеві пристрої здійснюють інкапсуляцію даних. Для забезпечення більшої безпеки при підключенні віддалених співробітників до мережі офісу компанії рекомендується зробити такий VPN більш захищеним уже за рахунок встановлення VPN для клієнта та двох факторної авторизації. Сама двох факторна перевірка 2FA – це метод ідентифікації користувачів у будь-якому сервісі, де використовуються також два різних типи перевірки даних. Для підвищення його захисту для облікових даних користувачів окрім звичайних його паролів 2FA запроваджує уже додаткову перевірку для особи. Це все збільшує захист для облікового запису від їх зловмисників. Реалізація системи 2FA вимагає від користувачів наявність хоча б двох із наведених тут нижче видів ідентифікаційних даних це те, що йому відомо, що сам співробітник буде тут вводити при намаганні самому увійти у систему, а це пін-код чи пароль та те, чим

він уже володіє, а це блок, яким він уже як користувач володіє, що йому властиве біометричні його дані, відбитки пальців, сканери обличчя чи сітківки ока.

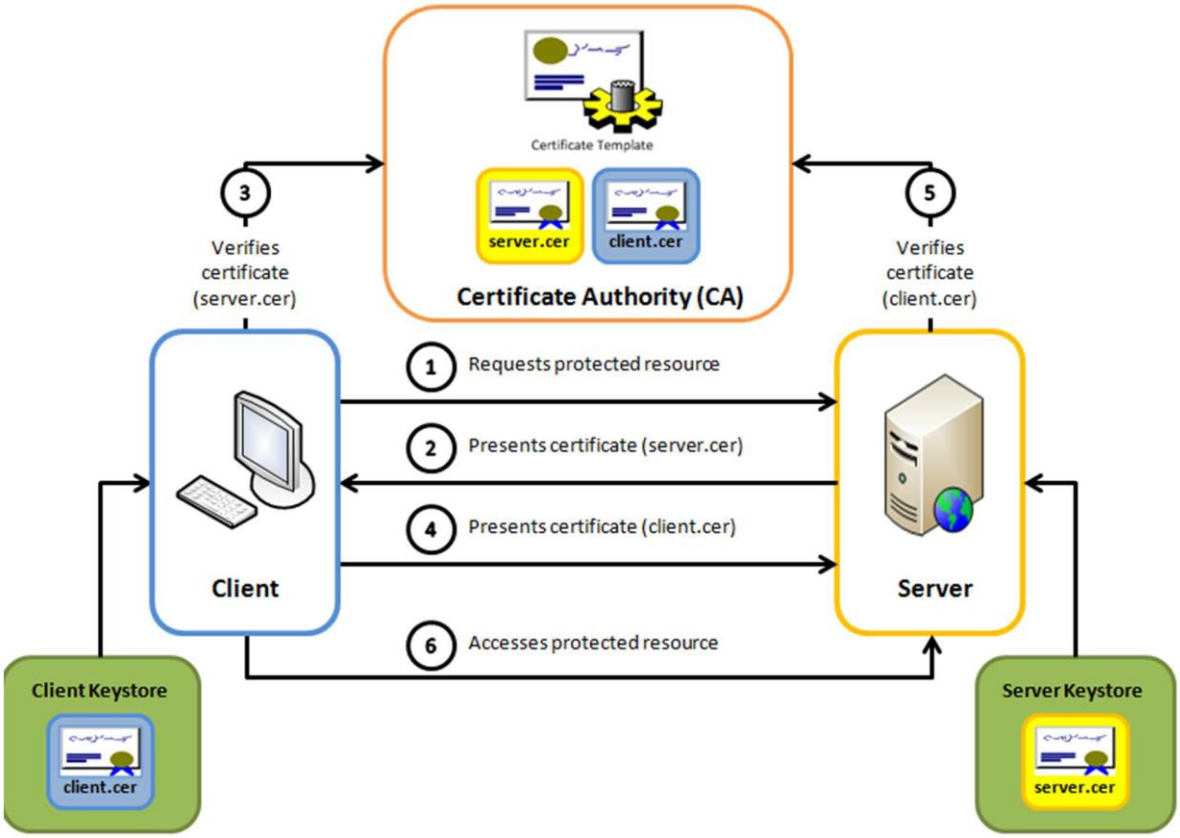


Рисунок 1.5 – Взаємна перевірка SSL на основі сертифікатів для транспортного режиму

Технологію захисту 2FA можна організувати загалом наступними способами: 1. Це одноразовий пароль коли у процесі роботи 2FA сам користувач вводить свій обліковий логін та свій пароль, а також ще одноразовий пароль, який йому уже надійшов на телефон чи електрону пошту. Такий його пароль забезпечує більш високий рівень захисту після перевірки паролю користувачем бо надсилається у вигляді цифр та є досить короткостроковим.

2. Перевірка на основі програмного забезпечення, що забезпечується за рахунок завантаження уже користувачем відповідного додатку на його мобільний телефон. Тут коли користувач здійснює свій вхід у такий додаток, то сама система автоматично генерує певну комбінацію символів кожну хвилину, які тут також отримує і сервер.

У системі захисту коли користувач вводить свій з генерований пароль, який також звіряється з тим кодом, що отримав його сервер і якщо вони є однаковими, то вхід для користувача буде дозволено. Використання резервного коду використовується якщо із певних причин сам користувач немає доступу до його телефону, додатку чи електронної пошти та відповідно також не має змоги увести другий пароль, то тут можна запросити уже резервний код, яким можна скористатися всього один раз. Апаратна перевірка у системі захисту реалізується за допомогою його ключа, що знаходиться на окремому USB-накопичувачі. Такий ключ є особистим і так званим ідентифікатором його користувача, за яким буде здійснена його перевірка.

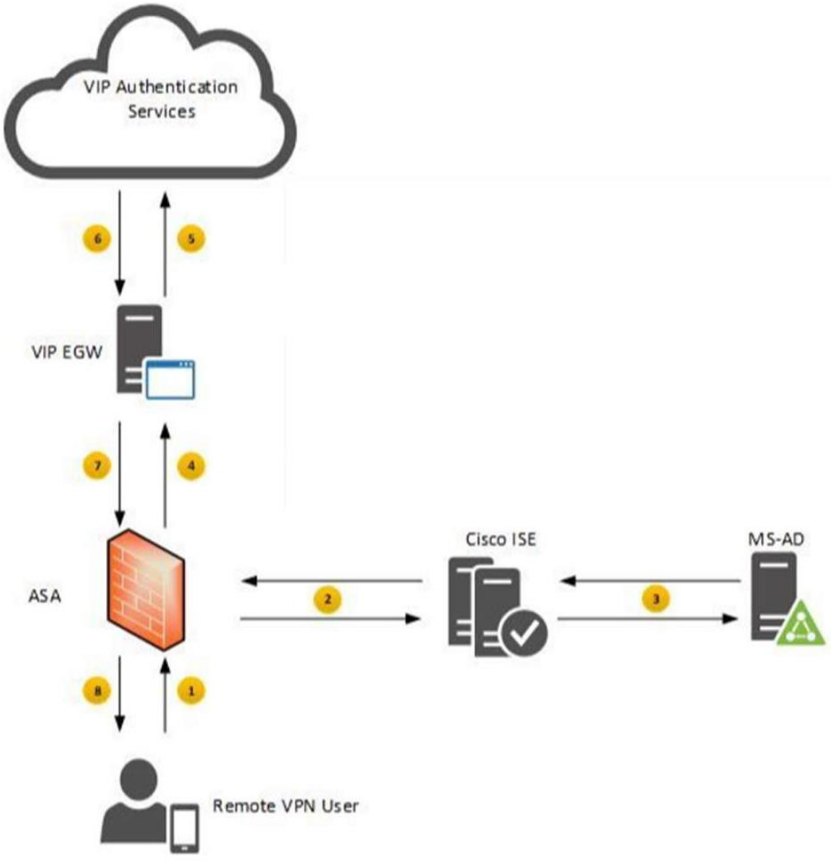


Рисунок 1.6 – Технологія захисту по топології 2 FA

У віртуальній системі захисту таким чином, це зменшує шанси доступу для небажаних осіб до ресурсів офісу компанії, навіть якщо вони отримали повний доступ до мобільного телефону його користувача. Тут найбільш популярним VPN

клієнтом для системи 2FA є відомі з'єднання. Даний додаток можна досить легко завантажити та встановити собі на мобільний телефон чи ноутбук із будь-якою операційною системою. Завдяки цьому офіс компанії може досить швидко організувати свій віддалений доступ для його користувачів, що працюють за межами офісу.

У такій комп'ютерній мережі розподіленого офісу на транспортному рівні використовується протокол SSL/TLS. Даний протокол надає необхідне шифрування та можливість перевірки на транспортному рівні між отримувачем повідомлення та його відправником. Протокол же складається із наступних фаз роботи, а це по перше для встановлення діалогу між його учасниками для сесії обирається необхідний алгоритм шифрування. Далі відбувається перевірка за допомогою сертифікатів чи за допомогою обміну їх ключами та здійснюється обмін поточними даними, що зашифровані за допомогою симетричних алгоритмів для шифрування. Протокол SSL тут складається із наступних протоколів, це протокол запису SSL, протокол рукостискання, протокол специфікації шифру змін, протокол оповіщення. Протокол SSL запис за допомогою сесій тут забезпечує цілісність та його конфіденційність.

Даний протокол захисту надає можливість вставити протоколи також вищого рівня. Сам же протокол SSL запис це протокол який здійснює поділ поточних даних на окремі частини. Надалі уже до усіх поділених частин додається перевірочний код, який шифрує ці дані та додається новий його SSL заголовок. Протокол рукостискання направляє короткі повідомлення усім учасникам цієї сесії, за допомогою яких він здійснює їх перевірку. Таким чином, тут забезпечується надійне з'єднання, а протокол уже працює наступним чином - відбувається посил між сервером та клієнтом, а після вдалого посилу клієнт отримує від серверу його ключ для обміну та сертифікат. У відповідь сервер уже отримує від його клієнта ключ для обміну та сертифікат і запускається Change-cipher протокол [23]. Сам же change-cipher- протокол складається із зашифрованого його повідомлення розміром у один байт який потрібен для його копіювання із очікуваного стану у поточний стан. Тут очікуваний стан буде у тому випадку, якщо ще не буде завершений протокол рукостискання. У іншому

випадку, його стан зміниться на поточний. Сама передача сповіщень для протоколу SSL реалізується за допомогою протоколу оповіщення. У такій системі записуватись може чи попереджуюче чи фатальне його повідомлення. Кожне таке повідомлення у цьому протоколі складаються із двох байтів та є уже зашифрованим.

1.4 Висновки. Постановка задачі

В розділі проведено дослідження предметної області та огляд існуючих технологій, методів та засобів. Також проведено дослідження та аналіз особливостей концепцій для побудови та проектування сучасних комп'ютерних мереж розподіленого офісу на основі віртуальних підходів. Сучасна інтеграція для комп'ютерних мереж надає можливість її доступу до неї різним її користувачам та будь-яких даних чи додатків у рамках їх політики інформаційної безпеки. На сьогодні уже немає такого інформаційного ресурсу доступ до якого не можна було б отримати по такій комп'ютерній мережі. Сучасні комп'ютерні технології та мережі мають властивість керованості та високий рівень безвідмовності, живучості. Вони обслуговуються за підтримки критично важливих для їх діяльності сервісів, а також це є інфраструктура організації, що підтримує вирішення для неї актуальних завдань та забезпечує досягнення її цілей. Також проведено дослідження по застосуванню віртуальних мереж для покращення параметрів роботи такої мережі. Поставлена у кваліфікаційній роботі мета буде досягатися розв'язанням наступних її задач:

1) виконати дослідження і аналіз подібних систем по забезпеченню параметрів роботи комп'ютерної мережі розподіленого офісу;

2) при плануванні та проектуванні мережі уточнити і визначити шляхи побудови для підвищення параметрів роботи такої комп'ютерної мережі для офісу;

3) виконати її інфраструктурну реалізацію та спроектувати цю комп'ютерну мережу та її програмно-апаратні віртуальні пристрої із забезпеченням параметрів роботи.

Постановка задачі. Враховуючи актуальність проблеми, у ході кваліфікаційної роботи необхідно:

1. Порівняти технології побудови VPN мереж та визначити яку із них краще використовувати для з’єднання між офісами, а яку для організації віддаленого доступу до робочих місця. 2. Визначити способи підсилення захисту VPN мережі. 3. Розробити та побудувати схему максимально захищеного доступу віддалених співробітників до комп’ютерної мережі із розподіленими офісами за допомогою віртуальних каналів. Розроблена модель дозволяє офісу компанії швидко налаштувати захищений доступ до комп’ютерної мережі розподіленого офісу.

2 ПРОЕКТУВАННЯ ПРОГРАМНО-ТЕХНІЧНИХ ЗАСОБІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ РОЗПОДІЛЕНОГО ОФІСУ

2.1 Вимоги до вибору VPN технології для технічних засобів мережі

При плануванні комп'ютерної мережі розподіленого офісу для вирішення задачі організації високо захищеного її віддаленого доступу для співробітників до комп'ютерної мережі із доступом до потоків інформації у декількох розподілених офісах слід обрати яка технологія для створення фрагментів VPN мережі буде використовуватися між офісами та між власним пристроєм такого користувача та його офісом, у якому знаходиться його робоча станція. На сьогодні існує велика різноманітність технологій для створення VPN мереж [24] (рис. 2.1):

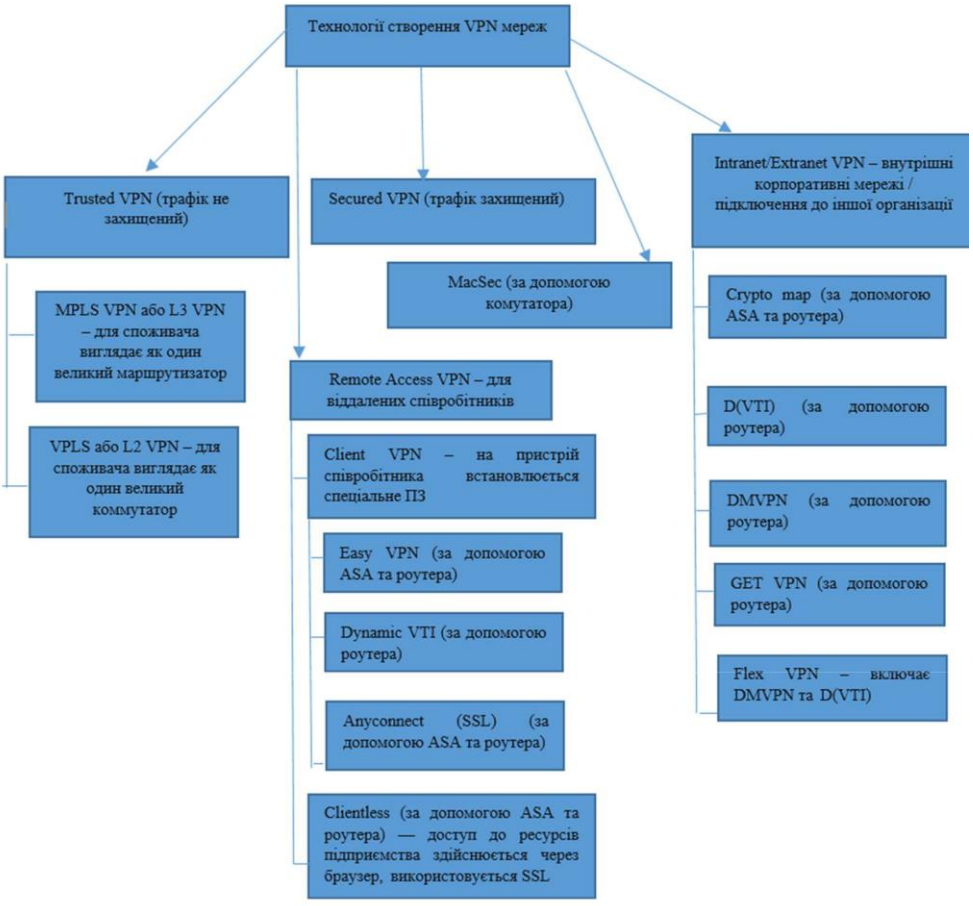


Рисунок 2.1 – Сучасні технології для створення VPN мереж

При роботі комп’ютерної мережі розподіленого офісу найчастіше виникає питання що тут краще обрати при реалізації мережної VPN технології , а це IP sec чи SSL VPN. Для вирішення цієї задачі проектування комп’ютерної мережі можна побудувати наступний процес візуалізації альтернативного запису (рис. 2.2):

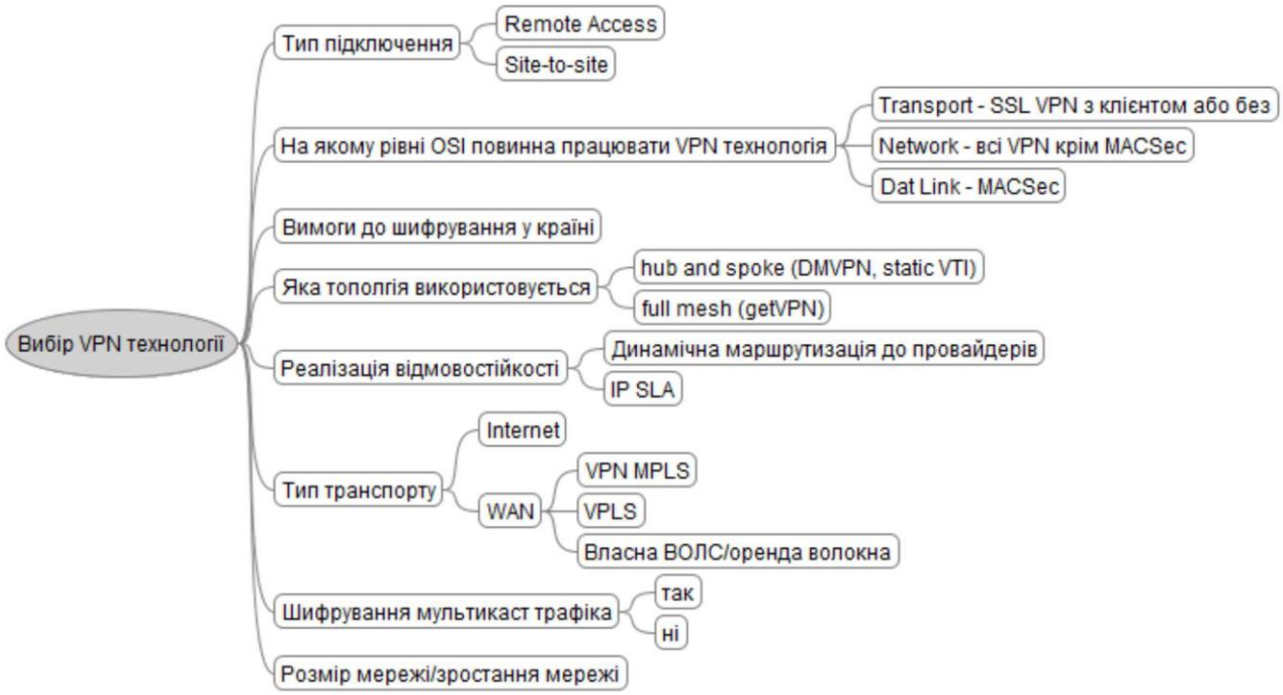


Рисунок 2.2 – Візуалізація альтернативного запису для вибору VPN технології

Для комп’ютерної мережі розподіленого офісу за допомогою рис 2.2. можна вирішити яку віртуальну технологію VPN можемо обрати. По скільки найбільш безпечними є технології IP sec VPN та SSL VPN, то вибір будемо уже здійснювати серед даних відомих технологій але для початку визначимо їх основі особливості. Для з’єднання декількох розподілених офісів компанії технологія IP sec VPN є найбільш економічним її варіантом. Для організації даної технології у мережі немає потреби уже витрачатися на відокремлені лінії каналів передачі та зв’язку, тут усе засновано лише на мережі Інтернет. У комп’ютерній мережі безперебійний зв’язок між розподіленими офісами створюється за допомогою єдиного їх IP-простору за рахунок їх налаштування для високо захищених тунелів. Для того, щоб уже застосувати IP sec технологію на існуючих пристроях

потрібно уже зробити відповідні налаштування та встановити також додаткове програмне забезпечення, а це у свою чергу сприяє для підвищенню захисту мережі. Із іншого боку, окрім вище зазначених її переваг також існує і ряд недоліків для технології IP sec VPN:

- це якщо розглядати IP sec для відділених співробітників, то тут у цьому випадку офіс компанії повинна буде запровадити різні додаткові налаштування для VPN клієнту із індивідуальною його конфігурацією IP sec. А це все призведе до додаткових її витрат;

- ця робота IP sec може погіршуватися за рахунок, що система шифрування сприяє збільшення потоку даних у мережі;

- протокол IP sec немає можливості щоб розмежувати доступ до ресурсів самої компанії, тому кожен її користувач тут має необмежений доступ;

- також для встановлення IP sec тунелю необхідно уже також пройти процедуру узгодження для відкриття необхідних її портів, що за замовченням тут можуть бути закритими.

При проектуванні комп'ютерної мережі розподіленого офісу використанні технології SSL VPN таких проблем не виникає. Для технології SSL VPN необхідне просте її налаштування та використанні уже відкриті порти. Додаткове ж встановлення програмного забезпечення на пристрої для користувачів не є необхідною дією. Співробітник розподіленого офісу повинен знати лише його логін та пароль, а також необхідну IP адресу. Технологія SSL VPN може бути тут двох видів:

1. Це клієнт SSL VPN із використанням програмного забезпечення CISCO:

- тут він може бути встановлений на пристрої як простий мобільний додаток;

- тут оцінується стан комп'ютеру для віддаленого клієнта;

- тут структура його клієнта є уже модульною;

- потік даних спрямовується до CISCO [25].

2. Це CLIENTLESS SSL де публікація HTTP та HTTPS їх ресурсів повинна бути уже здійснена на сервері самої компанії. На CISCO ASA завантажуються відповідні його модулі.

Тут таким чином, технологія SSL VPN має такі наступні переваги:

- це організовує високо захищений доступ до ресурсів офісу організації із зовнішніх вузлів;

- це якісь налаштування на стороні уже користувачів майже не потрібні;

- він не потребує додаткового програмного забезпечення з боку віддаленого клієнту;

- тут можна виділити ресурси, доступ до яких будуть мати окремі його користувачі.

Проте і технологія SSL VPN також має свої недоліки:

- це потрібно проводити певні її налаштування для її додатків, що працюють без використання мережі Інтернет бо швидкість передачі потоку даних знижується через необхідність його шифрування та подальшого її дешифрування. Із характеристик IP sec VPN та SSL VPN можна зробити такий висновок, що вони можуть тут функціонувати одночасно чи окремо. Можливо також виділити наступні критерії для вибору технології IP sec VPN та SSL VPN для її певних випадків та уже вибрати відповідну технологію для проекту кожного із них (рис. 2.3).

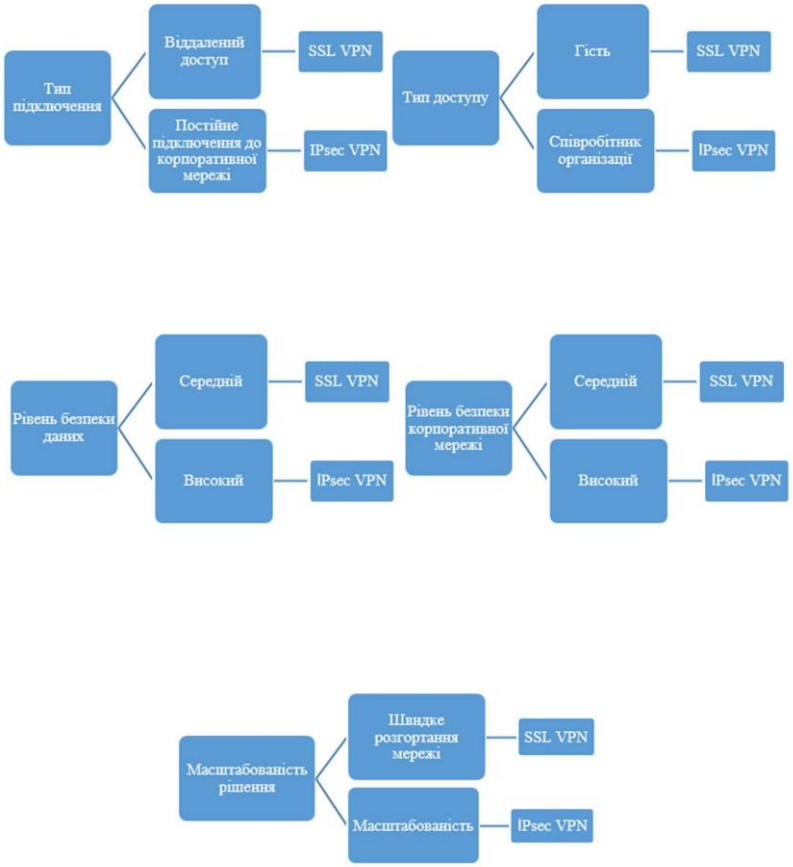


Рисунок 2.3 – Основні критерії для вибору між IP sec VPN та SSL VPN

Таким чином, при проектуванні комп'ютерної мережі розподіленого офісу найбільш захищеним варіантом вибору технології буде поєднання використання IP sec VPN та SSL VPN. Для планування та побудови захищеної комп'ютерної мережі між віддаленими її офісами будемо використовувати IP sec VPN, а також для налаштування віддаленого доступу для його співробітників уже технологію SSL VPN. На рисунку 2.4 приведено приклад схема IP sec VPN та SSL VPN для віддаленого офісу.

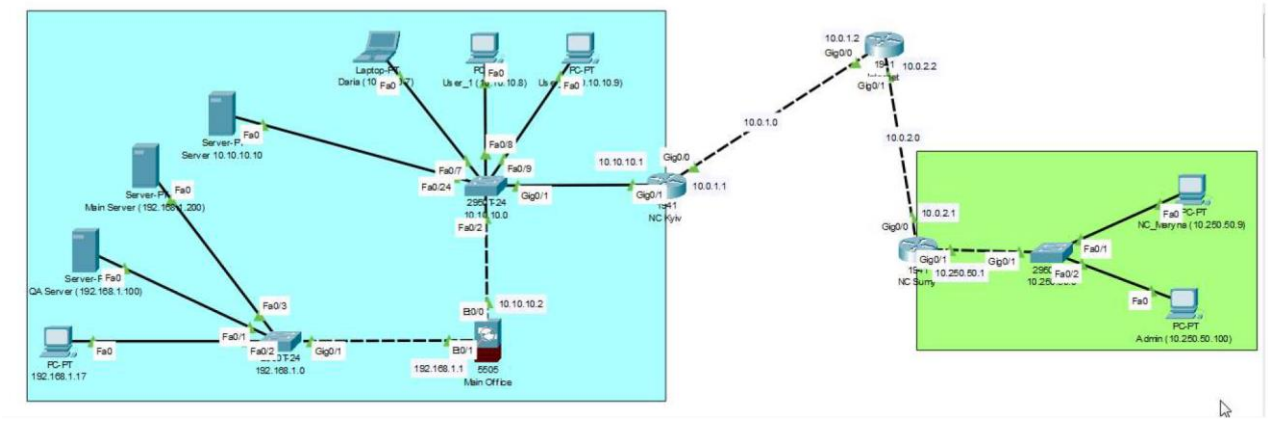


Рисунок 2.4 – Приклад схема IP sec VPN та SSL VPN для віддаленого офісу

На рис. 2.5 наведена приклад схеми мережі захищеного доступу до серверів офісу для працівників офісів. Віртуальний тунель між цими офісами побудований на основі IP sec VPN. Доступ до серверів тут обмежується за технологією клієнт SSL VPN.

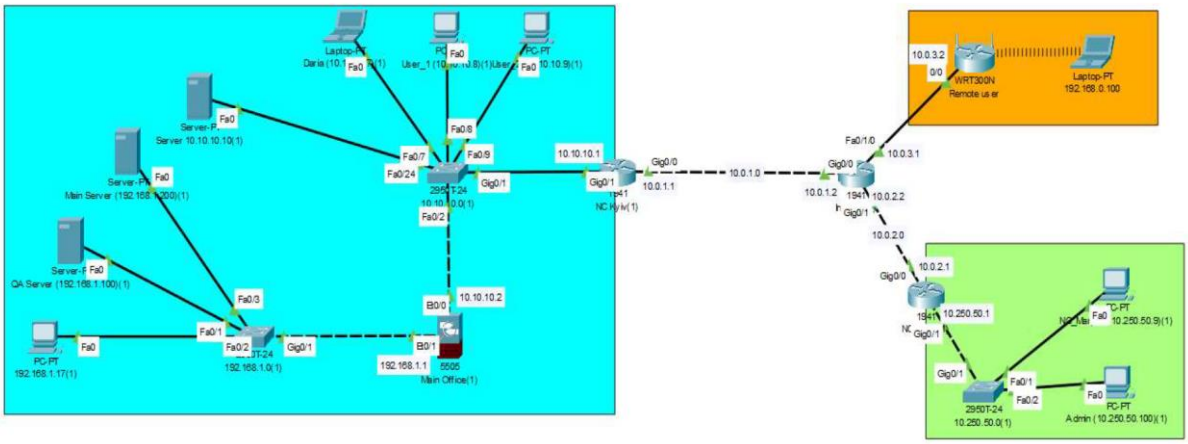


Рисунок 2.5 – Приклад схема IP sec VPN та SSL VPN для віддаленого офісу та його віддаленого працівника.

При проектуванні комп'ютерної мережі розподіленого офісу для віддаленого доступу її працівників будемо використовувати SSL VPN технологію, то тут потрібно враховуючи усі ризики та підсилити їх захист. Для підключення через технологію SSL VPN та підвищення її захисту для користувачів запроваджується уже певна кількість для перевірок, це стосується проходження перевірки дійсності. Така перевірка може бути трьох видів, а це сертифікати,

імена користувачів та паролю чи їх різна комбінація. Процес перевірки імені користувачів та паролю відбувається за наступними її етапами:

1. Сам користувач для входу у систему вводить його логін та пароль, що відправляються на SSL VPN його шлюз.

2. Перевірка користувача відбувається на сервері, що отримує пароль та логін від такого SSL VPN шлюзу.

Для простої авторизації користувача лише сертифікатів не потрібно вводити його логін та пароль. Сам сервер отримує сертифікат для авторизації, його обліку та перевірки від користувача. Така авторизація відбувається у такій послідовності:

1. Користувач сам намагається отримати доступ до системи Web-VPN за допомогою свого сертифікату перевірки.

2. Шлюз каналу Web-VPN перевіряє свого клієнта за допомогою його сертифікату перевірки, який був надісланий самим клієнтом. Також з'єднання не буде встановлено у випадку повного підтвердження недійсності цього сертифікату. У іншому випадку саме з'єднання успішно також встановлюється.

3. Також відбувається перевірка для даних користувача на сервері для підтвердження їх по відповідності даним у сертифікаті.

У такій комбінованій авторизації сам користувач вводить логін і пароль та надає сертифікат перевірки серверу. Даний процес тут відбувається наступним чином: 1. Здійснюється попередня перевірка особи клієнта та його сертифікату.

2. Для користувача тут же відкривається сторінка для авторизації.

3. Користувач сам зазначає логін та його пароль.

4. На сервер надходить новий запит від Web-VPN про перевірку та авторизацію.

5. Далі усі списки користувачів, налаштовані на сервері, будуть використовуватись для їх авторизації та перевірки.

При проектуванні комп'ютерної мережі розподіленого офісу для їх більшої безпеки при підключенні віддалених працівників до мережі компанії також рекомендується зробити систему VPN більш захищеною за рахунок встановлення у них VPN клієнтів та двох факторної їх авторизації та можливо організувати

віддалений доступ для кожного свого користувача, які працюють за межами самого офісу. Також окрім зазначених переваг у використанні система CISCO може підтримувати і додаткові функцій:

1. Завжди на VPN тут функція забезпечує постійний захист користувачів, якщо сам співробітник працює за межами комп'ютерної мережі через автоматичне його підключення до системи VPN.

2. Розподіл тунелів, що підходить для співробітників, які уже працюють віддалено за власним комп'ютером. Функція розподілу таких тунелів реалізується через забезпечення їх шифрування лише потоку даних до мережі офісу компанії, інший потік залишається без шифрування.

3. Різні правила для VPN, де компанія може встановлювати тут різні правила для своїх груп співробітників та таким чином лише окремий потік даних буде шифруватися.

Далі на прикладі клієнта системи CISCO розглянемо як відбувається двох факторна перевірка на 2FA :

1. Користувач системи відкриває клієнт CISCO. Вводить свій логін, пароль та уже другий пароль, який він отримав уже за допомогою додатку.

2. Система ASA відправляє до ISE для перевірки його логін та пароль.

3. Для перевірки ISE використовує AD, коли результат відправляється до ASA.

4. Система VIP EGW отримує від ASA пароль та його логін.

5. Система EGW відправляє запит на перевірку до VIP сервісу перевірки.

6. До системи VIP EGW надходить відповідь на перевірку.

7. Міжмережевий її екран для ASA отримує кінцевий результат перевірки.

8. Користувач далі отримує доступ, якщо перевірка пройшла успішно.

2.2 Налаштування та особливості функціонування комп'ютерної мережі

Побудова сучасної комп'ютерної мережі розподіленого офісу тісно пов'язана із необхідністю забезпечення для успішного функціонування уже існуючих систем, а також організацією сучасної багатофункціональної системи

передачі та впровадженням відео додатків. Для вирішення цих завдань була розробила архітектурна модель для побудови комп'ютерної мережі, що забезпечує уже можливість інтеграції різних існуючих додатків для даних, голосу та відео у рамках єдиної інтелектуальної мережевої інфраструктури. Особливість такої архітектури систем із інтеграцією голосу, відео та даних складається із чотирьох основних компонентів, таких як:

1. Сучасна інтелектуальна мережева комп'ютерна інфраструктура на базі протоколу IP, що включає у себе такі пристрої як маршрутизатори, комутатори, шлюзи та інше їх мережеве обладнання. Сучасна IP інфраструктура є основою для подальшого їх впровадження призначених для таких користувачів додатків та повинні тут забезпечувати підтримку таких важливих для комп'ютерної мережі таких сервісів, як її безпека, мережеве управління та механізмів гарантії для якості сервіс.

2. Різні інтелектуальні клієнтські місця із підтримкою протоколу IP, у тому числі такі як цифрова IP-телефонія, персональні їх комп'ютери із спеціалізованим для них програмним забезпеченням для вирішення уже різних задач, різні програмні емулятори, відео клієнти тощо.

3. Сучасні службові серверні додатки у тому числі сервери, щоб забезпечити управління системою передачі, система директорій, відео сервери тощо.

4. Сучасні користувальницькі такі додатки, які уже отримали завдяки розвитку нових інтегрованих систем із підтримкою голосу, відео та даних тобто система уніфікованої обробки їх повідомлень чи інтелектуальні центри для обробки викликів.

При роботі комп'ютерної мережі впровадження подібних програм уже дозволяє забезпечити нові додаткові можливості для користувачів такої мережі, щоб підвищити зручність та ефективність використання віртуальної системи. Характерною рисою для даної архітектури є її достатньо розподілена природа та завдяки якій сама система уже легко масштабується. Комп'ютерна мережа на базі такої архітектури може охоплювати як одну будівлю чи кілька поруч розташованих її будинків, об'єднаних високо швидкісною мережею. Також тут

можна забезпечити сервіси телефонії, відео та даних для усіх користувачів їх віддалених офісів та підрозділів, які об'єднані комп'ютерною IP мережею. Ще одна інша відмінна риса такої архітектури це її відкритість, орієнтація її на використання різних відкритих стандартів, а це дозволяє забезпечити уже поєднання із цілим рядом інших систем, як ще традиційної так і її пакетної передачі, а також із системами передачі для даних та відео. Підтримка таких відкритих стандартних для протоколів та відкритих інтерфейсів для розробки різних додатків, забезпечує тут можливість написання нових їх додатків, що інтегруються у такі системи, а також можливість для інтеграції додатків, які написані сторонніми їх виробниками.

Для забезпечення послуг зв'язку на базі мережі передачі даних уже дозволяє позбутися від необхідності для експлуатації таких роздільних комп'ютерних мереж для передачі потоку даних та зв'язку і забезпечує також можливість більш повного їх задоволення для потреб підприємств у послугах зв'язку. Так продукція уже дозволить замовнику значно зменшити витрати на їх впровадження, підтримку та розширення такої об'єднаної комп'ютерної мережі і підвищити його рентабельність для комунікаційної мережі. Переваги такої технології це можливість побудови єдиної комунікаційної інфраструктури на базі комп'ютерної IP мережі, а це простота побудови для розподілених комунікаційних систем за рахунок самої розподіленої природи такої архітектури і зниження загальної їх вартості для володіння системою.

Також скорочення різних витрат на канали за рахунок можливості їх ефективного використання по каналах для спільної передачі голосового потоку даних і відео додатків, скорочення витрат на оплату переговорів, спрощення їх налаштування, підтримки та адміністрування комунікаційної її інфраструктури, можливості використання таких додатків, що використовують усі переваги для інтеграції потоку голосу, відео та даних у рамках єдиної комунікаційної інфраструктури, повна орієнтація на підтримку відкритих її протоколів та інтерфейсів для усіх розробок додатків, що тут забезпечує можливість інтеграції із широким спектром для додатків, які пропоновані у даний час різними виробниками технічних пристроїв.

До основних недоліків функціонування комп'ютерної мережі можливо віднести неможливість використання тут стороннього обладнання, окрім відомих продуктів, досить висока вартість такої системи та досить застарілі інтерфейси для розробки їх додатків. Дане рішення підходить далеко не усім організаціям бо уперш воно є актуальним для великих компаній, що сильно зав'язані на використанні IP та обробці великої кількості вхідних потоків даних. У тих компаніях, де IP використовується лише працівниками офісу, дане рішення буде уже надлишковим та не менш важливим моментом тут є те, що рішення вимагають досить великих фінансових їх затрат. Розробляючи рішення для побудови комп'ютерної мереж розподіленого офісу постають наступні вимоги, а це розвиток мережевих їх сервісів, філіальна їх мережа повинна розвиватися із послугами, що вона надає такі як багато сервісів де підвищені вимоги до призначених для користувача їх додатків і при цьому забезпечуючи достатня якість для кожного такого сервісу окремо, також безпека для користувачів та повний мережевий захист повинен бути тут забезпечений по всьому периметру такої філіальної їх мережі, по управлінню та обслуговуванню мережі яке повинно бути простим та доступним для зниження різних управлінських витрат та експлуатаційних витрат.

Різні філії комп'ютерної мережі розподіленого офісу можуть отримати прямий доступ до мережі головного офісу, використовуючи тут повний інтегрований доступ який надає дротовий та бездротовий доступ до такої мережі через різні типи інтерфейсів та сервісів коли користувачі можуть спілкуватися уже використовуючи інтерактивні їх сервіси у режимі реального часу такі як телефонія, відео конференції та спостереження, їх інтегровану платформу яка формує єдину комп'ютерну мережа та мережеві політики на базі різних маршрутизаторів, комутаторів та міжмережевих екранів до самої кінцевої станції, що значно уже знижує експлуатаційні витрати на таку мережу. У деяких випадках користувачі повинні мати доступ до ресурсів із відкритим доступом до незахищених мереж таких як у готелях та аеропортах, що мають потенційно високі ризики із точки зору безпеки для мереж. Рішення ж із безпеки для філій офісів допомагає захистити комп'ютерні мережі та їх ресурси одним із таких їх

способів, використовувати VPN з'єднання для організації гнучких, масштабованих та зашифрованих VPN тунелів для забезпечення потоку передачі у межах комп'ютерної мережі, забезпечення надійної мережевої безпеки по периметрах комп'ютерної мережі де до складу якої входять мережеві екрани, безпеку рівня їх доступу, перевірка користувачів та керування політикою доступу, а також управління правами для користувачів офісів для забезпечення їх віддаленого доступу.

При проектуванні комп'ютерної мережі розподіленого офісу для забезпечення її роботи необхідно поставляти програмне забезпечення для система управління мережі, що спрощує їх віддалене керування та обслуговування такої мережі та надає її безперервне управління, простоту розгортання, підтримку відкритих стандартів тощо. Загалом ця мережа це є інфраструктура для офісу організації, що підтримує вирішення актуальних завдань та забезпечує досягнення її основних цілей. Тут вона об'єднує у єдиний інформаційний простір усі об'єкти розподіленого офісу, де мережа створюється як апаратно-технічна основа такої мережі та як її головний системо утворюючий компонент, на базі уже якого конструюються усі інші системи та сервіси. Сам же термін служби для системно-технічної інфраструктури мережі у декілька разів більше, ніж у додатків та її сервісів, а сама комп'ютерна мережа забезпечує можливість для розгортання нових сервісів та їх ефективне функціонування та при цьому повинна мати властивість високої продуктивності, масштабованості та її керованості. Також тут рекомендується використання уже багаторівневого підходу при побудові такої комп'ютерної мережі, а саме її трьох рівнів моделі, а такий підхід полягає у поданні нової архітектури для створюваної мережі у вигляді її ієрархічних рівнів, де кожен із яких вирішує свої, певні тільки для цього рівня завдання. Це уже дозволяє додавати для комп'ютерної мережі різні рівні, що розширюють її функціональні можливості та мінімізують ресурсні витрати для пошуку та усунення несправностей у такій мережі.

При проектуванні комп'ютерної мережі розподіленого офісу розглянуто та проаналізовано різні існуючі уже рішення щодо побудови комп'ютерних мереж. Ці відомі рішення підходить далеко не усім офісам організацій бо воно є

актуальним тільки для великих компаній, що сильно зав’язані на використанні IP та обробці великої кількості різних вхідних потоків. У організаціях де IP використовується лише працівниками офісу, дане рішення буде тут надлишковим. Також не менш важливим моментом є те, що такі рішення вимагають досить великих її фінансових затрат. Другі рішення у свою чергу не має прив’язки до конкретних уже виробників мережевого їх обладнання та має досить централізовану систему для управління мережею і постачає свої власні різноманітні сервіси, у тому числі із використанням штучного інтелекту.

2.3 Проектування роботи технічних засобів комп’ютерної мережі

При проектуванні роботи технічних засобів комп’ютерної мережі розподіленого офісу будемо виходити з того , що структурно дана організація складається із декількох підрозділів, а це головний офіс та віддалені його офіси. Усі віддалені офіси є географічно віддаленими та мають вихід у мережу Інтернет, тому доцільно буде використати її для з’єднання різних сегментів комп’ютерної мережі. При виборі та обґрунтуванні топології мережі врахуємо, що об'єднуючи у таку мережу кілька комп'ютерів тут необхідно вирішити, яким чином з'єднати їх один із одним тобто вибрати конфігурацію фізичних їх зв'язків чи топологію. У даному випадку під топологією мережі розуміємо конфігурацію графу, вершинам якого відповідають кінцеві вузли такої мережі та комунікаційне обладнання, а ребрами їх інформаційні зв'язки між цими вершинами. Від вибору самої топології їх зв'язків істотно залежать і характеристики комп’ютерної мережі. Відмінність між вузлами для декількох шляхів значно підвищує надійність мережі та робить можливим розподіл її завантаження між окремими інформаційними каналами. Простота ж приєднання нових вузлів, що уже властива деяким топологія, робить таку мережу легко масштабованою, а економічні міркування часто призводять до вибору топології для яких характерна мінімальна сумарна довжина ліній передачі.

Серед безлічі можливих існуючих конфігурацій розрізняють повно зв’язні та неповно зв’язні де повно зв'язна топологія відповідає такій мережі, у якій кожен її комп'ютер безпосереднім чином уже пов'язаний із усіма іншими. Та

незважаючи на логічну простоту, цей варіант побудови мережі виявляється на практиці досить громіздким та неефективним. У такому випадку уже кожен комп'ютер у мережі повинен мати досить велику кількість комунікаційних його портів, яка достатня для зв'язку із кожним інших комп'ютерів у цій мережі. А для кожної пари комп'ютерів ще повинна бути виділена ї окрема фізична лінія для зв'язку. Повно зв'язні топології у великих мережах застосовуються досить рідко, так як для зв'язку вузлів потрібно багато фізичних дуплексних каналів ліній передачі, тобто тут має місце квадратична залежність від числа таких вузлів. Зазвичай такий вид топології використовується у багато машинних комплексах чи в мережах, що об'єднують невелику кількість різних комп'ютерів. Усі інші варіанти топології засновані на неповно зв’язних топології, коли для обміну даними між її двома комп'ютерами може уже знадобитися транзитна передача їх даних через інші вузли мережі.

У даному випадку для структури офісу організації, доцільно буде використати топологію ієрархічної зірки чи дерева. Зіркоподібна топологія утворюється в тому разі, коли кожен комп'ютер уже підключається безпосередньо до її загального центрального пристрою, що зветься комутатором. У функції комутатора входить передача переданої самим комп'ютером інформації одному чи усім іншим комп'ютерам комп’ютерної мережі. Ієрархічна зірка, будується уже із використанням декількох комутаторів, що ієрархічно з’єднанні між собою її зіркоподібними зв'язками. Перевагою такої обраної топології є її масштабованість, легкий пошук проблемних її вузлів, висока продуктивність комп’ютерної мережі. До недоліків можливо віднести вихід із ладу комутатору, що впливає на роботу усієї мережі, високі витрати їх кабелів. Можна також побачити, що обрана топологія комп’ютерної мережі найкраще підходить для даного офісу, а збільшені ж витрати на додаткові кабелі легко нівелюються її основними перевагами.

При аналізі та досліджені віртуальних приватних мереж, а це мережа передачі даних, що використовує загальнодоступну комп’ютерну мережу Інтернет, шляхом додавання особливих процедур безпеки над незахищеними канали передачі та зв'язку. Усе це досягається, використовуючи комбінацію їх

шифрування, перевірки та тунелю. Тунель а іноді його називають інкапсуляцією відноситься до процесу такої інкапсуляції чи вбудовування одного його мережевого протоколу, що буде передаватися у пакети іншого. Така технологія VPN надає офісу можливості для дорогої приватної орендованої лінії за нижчою вартістю, використовуючи тут спільну її мережу, таку як мережа Інтернет. На сьогодні існує кілька різних реалізацій таких протоколів VPN де найбільш вживані протоколи віртуальних приватних мереж наступні PPTP, L2TP), IP Sec) та SOCKS. Тут перевага використання мережі Інтернету для зв'язку у тому, що такі тунелі можуть бути створеними за вимогою та уже включати співробітників, які знаходиться удома чи подорожують та має з'єднання із мережею Інтернет. Тут гнучкість є значно вищою, чим у виділеннях ліній та із точки зору самого користувача ця топологія для даної приватної мережі виглядає як локальна її мережа.

У комп'ютерній мережі захист інформації у процесі її передачі по відкритих каналах засновується тут на побудові уже захищених віртуальних каналів передачі, що називаються крипто захищеними тунелями. Тут кожен такий тунель представляє собою таке з'єднання, що проходить через її відкриту мережу, по якій передаються усі крипто графічно захищені пакети її повідомлень. Для створення захищеного тунелю тут виконують деякі компоненти такої віртуальної мережі, що функціонують на її вузлах та між якими формується тунель. Ці усі компоненти прийнято називати ініціатором та термінатором тунелю де ініціатор тунелю вставляє пакети у новий її пакет, що містять уже новий заголовок із інформацією про його відправлення та її отримання. Тут хоча усі пакети, що передаються по такому каналу є пакетами IP, де вставлені пакети можуть належати до будь-якого його протоколу. Маршрут же між ініціатором та термінатором тунелю визначає звичайна її IP-мережа, якою тут може бути мережа Інтернет. Термінатор тунелю виконує тут процес зворотній інкапсуляції де він видаляє нові його заголовки та направляє кожен такий вхідний пакет у локальному стеці його протоколів адресату у комп'ютерну мережу.

Уже сама по собі інкапсуляція ніяк не впливати на захист пакетів для повідомлень, що передаються по такому тунелю але завдяки такій інкапсуляції

з'являється уже можливість для повного криптографічного захисту цих пакетів. Конфіденційність для інкапсуляції пакетів забезпечується уже шляхом їх криптографічного закриття, тобто шифрування, а їх цілісність та справжність за допомогою формування цифрового підпису. Тут так як існує велика кількість для методів крипто захисту їх даних важливо, щоб ініціатор та термінатор тунелю використовували одні та ті ж методи і могли уже узгодити дані їх методи. Окрім того для можливості для розшифрування даних та перевірки такого цифрового підпису при прийомі цих даних ініціатор та термінатор тунелю повинні підтримувати свої функції для безпечного обміну їх ключами.

Сучасна віртуальна комп’ютерна мережа це є група вузлів такої мережі, потік даних якої, що включає у себе широкомовний потік на канальному рівні який уже повністю ізольований від потоку інших вузлах такої мережі. Основне призначення такої технології VLAN полягає у полегшенні процесу для створення ізольованих мереж, які потім зв'язуються між собою за допомогою їх маршрутизаторів. Така їх побудова для комп’ютерної мережі створює досить потужні бар'єри на шляху небажаного потоку даних із однієї мережі у іншу. На сьогодні вважається досить очевидним, що будь-яка досить велика мережа повинна включати різні маршрутизатори, інакше інформаційні потоки помилкових кадрів будуть періодично затоплювати усю комп’ютерну мережу через прозорі для них мережеві комутатори та приводячи її у неробочий стан. Основною перевагою технології віртуальних мереж є те, що вона уже дозволяє створювати у такій мережі повністю ізольовані сегменти шляхом логічної їх конфігурації для комутаторів, не вдаючись до якоїсь зміни їх фізичної структури. Також при створенні віртуальних мереж на основі хоча б одного комутатору використовують механізм групування для портів їх комутатору і при цьому тут кожен порт відноситься тільки тій чи іншій віртуальній її мережі. Сам же кадр, що прийшов на такий порт для віртуальній мережі уже ніколи не буде переданий порту, що не належить цій віртуальній мережі. Утім, порт тут можна приписати декільком її віртуальним мережам, хоча на практиці використання так роблять рідко бо зникає ефект їх повної ізоляції для мереж.

У комп’ютерній мережі розподіленого офісу якщо вузли будь-якої віртуальної мережі уже підключені до різних її комутаторів, то для підключення уже кожної такої мережі на цих комутаторах повинні бути виділені спеціальні пари портів. У вже іншому випадку, якщо ці комутатори будуть тут пов'язані тільки однією їх парою портів то інформація про приналежність такого кадру до тієї чи іншої віртуальної мережі при передачі із комутатору у інший комутатор може бути загублена. Тут таким чином, сам комутатори із групуванням його портів уже вимагають для свого спільного з'єднання стільки портів, скільки для віртуальних мереж вони можуть підтримувати. Порти та кабелі у комп’ютерній мережі використовуються у цьому випадку дуже марнотратно бо окрім того, що при з'єднанні таких віртуальних мереж через маршрутизатор тут для кожної віртуальної мережі уже виділяються окремі кабель та порт маршрутизатору, що також призводить до досить великих накладних їх витрат.

При проектуванні комп’ютерної мережі розподіленого офісу проведення групування MAC-адрес у їх віртуальній мережі на кожному їх комутаторі позбавляє від необхідності уже пов'язувати їх із кількох портів, по скільки у цьому випадку його MAC-адреса стає її міткою для віртуальної мережі. Проте цей спосіб вимагає уже виконання досить великої кількості ручних операцій по самому маркуванню їх MAC-адрес на кожному такому комутаторі комп’ютерної мережі. Ці обидва підходи тут засновані тільки на додаванні уже додаткової потокової інформації до її адресних таблиць для комутатору та у них відсутня також можливість для передачі у кадрі інформації про його приналежність до кадру такої віртуальної мережі. Тут тому таке широке поширення і отримав інший її підхід, який заснований на введенні у цей кадр додаткового поля, що зберігає його інформацію про приналежність такого кадру до тієї чи іншої віртуальної комп’ютерної мережі при його переміщеннях між різними комутаторами такої мережі. Тому тут немає необхідності пам'ятати у кожному їх комутаторі про приналежність усіх їх MAC-адрес до їх віртуальних мереж.

У мережі додаткове поле із позначкою про номер його віртуальної мережі уже використовується тільки тоді, коли сам кадр передається від одного комутатору до іншого комутатору, а при передачі такого кадру його кінцевому

вузлу воно уже видаляється. Також при цьому модифікуються тільки протоколи для взаємодії комутатор - комутатор, а його програмне та апаратне забезпечення для кінцевих вузлів тут залишається незмінним. Ще до прийняття стандарту IEEE 802.1Q уже існувало досить багато протоколів цього типу, проте усі вони мали один їх недолік бо усе їх обладнання від різних виробників при створенні мережі VLAN виявлялося уже несумісним. Сам же стандарт IEEE 802.1Q уводить у кадрі ETHERNET додатковий його заголовок це тег для віртуальної комп'ютерної мережі. Загалом же існує чотири режими для призначення мережі VLAN це на основі інтерфейсу, на основі його основної MAC-адреси, на основі його протоколу та на основі політик. Також при використанні мереж VLAN на основі їх інтерфейсів сам мережевий адміністратор попередньо налаштовує порти VLAN для кожного його інтерфейсу цього комутатору. Коли ж не тег кадр приходить на його інтерфейс, то комутатор додає PVID інтерфейс до його кадру. Усі переваги у тому, що учасників мережі VLAN досить легко призначати, хоча адміністратор повинен пере налаштувати мережу VLAN при зміні її учасників. Також рекомендується також використовувати до таких мереж будь-якого їх масштабу та пристроїв у фіксованих місцях їх розташування.

У комп'ютерні мережі в режимі призначення мережі VLAN на основі MAC-адреси уже адміністратор мережі попередньо налаштовує усі зіставлення між MAC-адресами та ідентифікаторами такої мережі VLAN. При отриманні ж не тег кадру його комутатор додає також тег VLAN, що відповідає його MAC-адресі для цього кадру до такого кадру. При зміні ж фізичного розташування його користувачів самому адміністратору не потрібно уже перенастроювати саму мережу VLAN, а це підвищує безпеку та гнучкість доступу у такій мережі. Сам адміністратор повинен попередньо визначити таку мережу VLAN для усіх учасників у комп'ютерній мережі. Це досить часто використовується у невеликих мережах, де усі призначені для користувача пристрої часто змінюють своє фізичне місцеположення, але їх NIC рідко тут змінюються. Наступний же режим мережі VLAN, що призначається на основі їх типів протоколів та форматів для інкапсуляції їх кадрів. Адміністратор мережі попередньо налаштовує усе зіставлення між типами їх протоколів та їх ідентифікаторами мережі VLAN. При

отриманні ж не тег кадру сам комутатор додає його тег мережі VLAN, що відповідний типу для протоколу кадру до такого кадру. Тут комутатор уже повинен аналізувати усі формати для адрес протоколу та перетворювати ці формати, що споживають тут надмірні їх ресурси.

При проектуванні комп'ютерної мережі розподіленого офісу визначено, що останній режим мережі VLAN, що призначаються на основі усіх таких політик, як їх комбінації для інтерфейсів його MAC-адрес та IP-адрес. У комп'ютерній мережі розподіленого офісу сам мережевий адміністратор попередньо тут налаштовує усі її мережеві політики. При отриманні ж нового не тег повноцінного кадру, який відповідає усім налаштованій політики, уже сам комутатор додає новий тег уже зазначеної мережі VLAN до його кадру а потім цей кадр передається у зазначений VLAN.

2.4 Висновок

У розділі кваліфікаційної роботи комп'ютерної мережі розподіленого офісу було проведено проектування програмно-технічних засобів та розглянуто вимоги до вибору VPN технології для технічних засобів для роботи мережі. Також було проведено налаштування та проведено огляд особливостей функціонування для такої комп'ютерної мережі. При проектуванні роботи технічних засобів комп'ютерної мережі визначено, що усі підрозділи офісу є географічно віддаленими та уже мають вихід у мережу Інтернет, тому тут буде доцільним використання її для з'єднання різних сегментів такої мережі. У ході аналізу структури було запропоновано використати топологію ієрархічної зірки бо перевагами такої топології є масштабованість, легкий пошук проблемних її вузлів та висока продуктивність мережі. У мережі для підвищення її відмово стійкості самого ядра комп'ютерної мережі буде використовуватись технології стеку комутаторів та протокол VRRP. У мережі даний протокол працює уже групуючи резервні маршрутизатори разом у їх єдиний віртуальний маршрутизатор. Цей мережевий віртуальний її маршрутизатор має свою власну IP-адресу і замість

відправлення потоку до окремого маршрутизатора, він надсилається до адреси його віртуального маршрутизатору.

Проектування програмно-технічних засобів для робочих параметрів такої комп'ютерної мережі дозволило розглянуто основні вимоги до їх технічних засобів при плануванні такої комп'ютерної мережі. При проектуванні програмно-апаратних пристроїв для забезпечення робочих параметрів комп'ютерної мережі для більшості сучасних систем не потрібні досить потужні пристрої, що використовують великі їх офісу а на сьогодні буде цілком достатньо менших мережних пристроїв працюючих на основі віртуальної мережі. У такій мережі вони повинні виконувати такі ж функції по маршрутизації та комутації, а для задоволення мережевої потреби були використані нові вироби, що уже виконують різні функції для декількох. У цьому розділі проведено також схему налаштування та опис функціонування проектує мої мережі та розглянуто процес роботи технічних засобів для комп'ютерної мережі розподіленого офісу.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ РОЗПОДІЛЕНОГО ОФІСУ

3.1 Апаратна реалізація комп'ютерної мережі розподіленого офісу

При проектування програмно-технічних засобів комп'ютерної мережі розподіленого офісу визначаємо плануванням його приміщень, у якому буде розташовуватись ця комп'ютерна мережа. Тут велике значення мають витрати на придбання та установку мережевого устаткування, що є досить важливим питанням для розподіленого офісу. Провівши детальний огляд існуючих інфраструктурних та архітектурних рішень та дослідивши нові мережні технології та також урахувавши усі потреби сьогодення для проектування такої комп'ютерної мережі на фізичному рівні буде використаний безпровідний стандарт 802.11n. На сьогодні існує дві основних топології для таких безпровідних мереж:

- це об'єднуючі усі комп'ютери у межах одного будинку, а це є внутрішні мережі;

- це з'єднуючі усі мережі, які розташовані у різних будинках, це є зовнішні мережі.

Так як приміщення розподіленого офісу розташовані у межах одного будинку, то тут розглядається тільки одна топологія типу внутрішня мережа. Основний безпровідний сегмент для комп'ютерної внутрішньої мережі тут може включати як мобільні так і різні настільні комп'ютери. У комп'ютерній мережі комп'ютер із установленим адаптером, усі користувачі розподіленого офісу одержують можливість вільно переміщатися у межах такого будинку та не втрачати зв'язок із комп'ютерною мережею. Тут застосування безпровідних технології у настільних комп'ютерах надає розподіленого офісу гнучкість, що уже неможливо у традиційній провідній комп'ютерній мережі. Бездротові комп'ютерні мережі сьогодні ідеальні для організації тимчасових робочих груп офісу та швидко зростаючих організацій.

Така система та мережа, а це пристрої які досить широко уже поширені на ринку існуючої сучасної техніки. Пристрої від різних виробників тут можуть уже взаємодіяти на базовому їх рівні цих сервісів. Сучасні комп'ютерні мережі підтримують також роумінг, і тому клієнтські станції зможуть досить вільно переміщатися у просторі офісу. Тому тут у разі встановлення додаткових точок для доступу при розширенні розподіленого офісу, працівники можуть вільно переходять від одного його пункту доступу до іншого. У зв'язку із поступовим переходом комп'ютерних мереж із провідної на безпровідну її основу, тут доцільним при проектуванні програмно-технічних засобів комп'ютерної мережі розподіленого офісу буде використання провідної технології Gigabit-Ethernet. Вона досить добре зарекомендували себе у мережах за свою багато річну історію, зберігши параметри надійності та перспективність для її використання. Також поряд із передбаченою їх зворотною сумісністю із попередніми її рішеннями вона забезпечує теоретичну пропускну здатність у 1- 10Гбіт/с. Такі можливості на практичному рівні досягають швидкості для шини комп'ютеру. Тут поряд із збільшенням швидкості система успадкувала усі попередні особливості цієї системи, такі як формат її кадрів, технологію CSMA/CD, повний дуплекс тощо.

Для комп'ютерної мережі розподіленого офісу сучасні високі швидкості для передачі потоків інформації і внесли свої нововведення, проте саме у спадкуванні старих стандартів тут складається величезна їх перевага та популярність. Основні критерії на вибір кабелю побудови мережі стали більш жорсткими, а для зменшення статичних та динамічних їх наведень, односпрямованої її передачі, зворотних втрат передачі, затримок та його фазового зрушення тут була прийнята до використання категорія кабелю 6 та 6а для неекранованої скрученої пари. При переході також скористалися другим її варіантом та скоротили діаметр для сегменту. Для нашого варіанту цей випадок для стандарту, що успадковував усі складові попередника, як мінімальний розмір його кадру, CSMA/CD та час для виявлення колізії , тут зможе уже працювати як у колізійних доменах із діаметром не більше 20 метрів. Тому у мережі було запропоновано збільшити час на основну передачу її мінімального кадру.

Тому з огляду на те, що для її сумісності із попередніми подібними мережами мінімальний розмір для кадру був залишений колишнім, а це 64 байта, а до самого його кадру додалося ще додаткове поле для розширення носія, що уже доповнює сам кадр до 512 байт, але саме поле не додається тут у тому випадку, коли розмір його кадру тут буде більше ніж 512 байт. При проектуванні таким чином, її мінімальний розмір для такого кадру уже вийшов рівним у 512 байту, а час на виявлення її колізії зріс, та уже сам діаметр для сегменту збільшився до цілих 200 метрів. При прийомі уже такого кадру це його поле відкидається ще на рівні його MAC, тому що далі розташовані рівні які уже продовжують працювати із її мінімальними кадрами де довжина 64 байти. Хоча тут розширення для носія дозволило б зберегти її сумісність із їх попередніми стандартами, то воно призвело до досить тут невиправданої витрати для смуги полоси її пропускання. Втрати ж тут можуть уже досягати аж до 448 байт (512 - 64) на один кадр у випадку коротких її кадрів. Тому сам стандарт був трохи модернізований бо тут ввели таке поняття як його пакетна їх перевантаженість, що дозволяє ефективніше використовувати це поле розширення пакету.

При реалізації комп'ютерної мережі розподіленого офісу це працює таким чином, якщо у адаптеру чи комутатору є кілька невеликих кадрів, що уже вимагають їх відправлення, то перший із них уже відправляється стандартно із тут додаванням йому поля із розширення до їх 512 байтів. Цей такий між кадровий інтервал уже заповнюється різними символами для розширення їх носію. Усе це відбувається поки увесь сумарний розмір для кадрів, що тут відправляються не досягне своєї основної межі уже у 1518 байтів. Таким чином, у мережі це середовище не замовкає на всьому її інтервалі передачі для таких малих її кадрів, тому уже колізія може виникнути тут як тільки на першому її етапі при передачі самого першого пакету правильного досить такого малого кадру із полем для розширення його носія. Увесь цей механізм тут дозволяє досить істотно підвищити його продуктивність для комп'ютерної мережі, особливо при її великих навантаженнях за рахунок по зменшенню їх імовірності для виникнення у них колізій.

У комп’ютерних мережах на початку розвитку Gigabit-Ethernet ще підтримував тільки стандартні розміри для кадрів, а це від мінімального 64 - 512 до їх максимального типу у 1518 байтів. Тут у них із 18 байт займає його стандартний службовий заголовок, а уже для самих даних тут залишається від 46-ти до 1500байтів. Для самої ж передачі файлів розміром у 1гігабайт по не завантаженій іще Fast-Ethernet комп’ютерній мережі, сам сервер обробляє до 8200 пакетів у секунду та затрачає на це уже мінімум аж до 11 секунд. У цьому ж випадку уже тільки на обробку переривань у такого комп'ютеру потужністю до 200MIPS піде близько 10 відсотків його часу роботи. Із представленої таблиці 3.1 видно, що навіть при всіх найкращих умовах усі кадри тут уже відстоять один від одного на такий часовий інтервал, що не перевищує всього 12мкс. У випадку ж використання кадрів їх меншого розміру тут часовий інтервал уже тільки зменшується.

Таблиця 3.1 – Характеристики системи передачі комп'ютерної мережі

Швидкість	10Мбіт/с		100Мбіт/с		1000Мбіт/с	
Розмір кадру	64 байт	1518 байт	64 байт	1518 байт	64 байт	1518 байт
Кадри в сек.	14.80K	812	148K	8,10K	1,480M	81K
Швидкість передачі , М біт/с	5,50	9,80	55,0	98,0	550,0	980,0
Проміжок між кадрами, м к с	67,0	1200,0	6,70	120,0	0,70	12,0

Тут очевидним виходом із даної ситуації є наступне:

- це можливість збільшення тимчасового проміжку між цими кадрами;

- це перекладання її частини для навантаження по обробки кадрів із центрального процесора на сам його мережевий адаптер.

На сьогодні у комп’ютерних мережах реалізовані уже обидва методи. Ще давно було запропоновано збільшити його розмір для самого пакету. Такі пакети уже одержали назву як ГІГА- кадри та їх розмір уже може бути від 1518 до 9018байтів. Усі ці кадри уже дозволили зменшити їх навантаження на роботу процесору до 6-и разів та значно також підвищити і продуктивність та ефективність роботи такої комп’ютерної мережі. Виграш уже тут у її продуктивності досягається за рахунок його зменшення свого часу на обробку такого досить великого кадру. А сам же час на обробку такого кадру залишився колишнім, хоча замість декількох його невеликих кадрів, кожний із яких він зажадав би для себе уже N тактів для роботи процесору та одне його переривання, бо тут обробляється тільки один великий кадр. сама ж комп’ютерна мережа у межах одного будинку буде доповнювати її традиційну уже провідну мережу із відомою її топологією зірка. Як і всі її кабельні аналоги, такі бездротові внутрішні її мережі складаються із декількох адаптерів та точок для доступу, що уже тут виконують функцію його комутатору. Для кращої їх функціональності та дальності для систем передачі така точка доступу може бути тут застосована як її центральний вузол для такої під мережі із топологією зірка та служити іще і мостом, що зв'язує тут безпровідний її сегмент зі звичайною кабельною системою.

У якості активного мереженого обладнання, що тут допомагає зв’язати усі сегменти комп'ютерної мережі використаємо точку доступу , а це маршрутизатор та комутатор. Сама узагальнена структурна її схеми для розробленої комп’ютерної мережі до кваліфікаційної роботи представлена та містить основні компоненти мережі такі як робочі станції PC1- PC8, PC9 - PC29 які сполучені за допомогою одного безпровідного маршрутизатора М 1 та комутатора К 1. Сам же маршрутизатор М 1 підключений до мережі Інтернет та уже з’єднує з нею комп’ютерну мережу розподіленого офісу. Комп’ютерна мережа офісу буде складатись із 29-ти робочих станцій та основного сервера-маршрутизатора. Також у комп’ютерну мережу розподіленого офісу входять також мережеві принтери, що підключаються до окремих її робочих станцій. Самі ж робочі ж станції розташовані у семи приміщеннях офісу. Три основні приміщення офісу

розташовані на першому поверсі та також чотири на другому їх поверсі. Логічна ж структура комп'ютерної мережі із основними компонентами та її мережевими ресурсами представлена на плакаті і її можна умовно поділити тут на 3-и такі основні сегменти:

Сегмент один: це комутатор К1 і робочі станції РС1- - РС8 які під'єднанні до нього кабелем звита пара категорії 6. Максимальна ж відстань від комутатору до кожної її робочої станції тут не перевищує 34м.

Сегмент два: це комутатор К 1 та маршрутизатор М 1, що з'єднані кабелем звита її пара категорії 6-ть.

Сегмент три: це маршрутизатор М 1як безпровідний сегмент системи WLAN де максимальна відстань до робочих станцій 20 м.

Приміщення комп'ютерної мережі розподіленого офісу – це є замкнутий простір у спеціально призначених для цього приміщеннях, у яких тут постійно чи періодично здійснюється уся трудова діяльність працівників офісу. Приміщення ж для їх роботи із комп'ютерами тут повинні відповідати СНІП - Виробничі приміщення та СНІП - Протипожежні норми і інших документів для побудови мережі. Найбільш необхідні та придатними є приміщення із самим одностороннім розташуванням вікон і тут бажано, щоб основна площа їх засклення не перевищувала об'єм до 25-50% загальної площі. Загалом найкраще коли усі вікна у приміщеннях орієнтовані бажано на північ чи північний схід, а їх поверхні у приміщеннях бажано повинні бути тут матовими. У комп'ютерній мережі розподіленого офісу організація робочого місця також повинна відповідати рекомендаціям ДНАОП, що тут регламентує вимоги щодо самої організації для робочого місця користувачів комп'ютерів згідно ергономічних вимог для ССБТ-Робоче місто при виконання робіт сидячи. Загальні вимоги , що передбачають:

- площа на комп'ютер повинна бути не менше ніж 6 м^2, а об'єм уже не менше 20 м^3;

- усі робочі місця користувачів повинні розміщуватись тут на відстані не менше ніж 1м від його стін зі світловими їх прорізями;

- відстань між їх бічними поверхнями комп’ютеру повинні бути не менше ніж 1,2м;

- відстань між основною тиловою частиною одного комп’ютеру та екраном другого тут повинна бути не менше ніж 2,5 м;

- прохід між основними рядами таких комп’ютерів не менше ніж 1м.

При проектуванні комп’ютерній мережі розподіленого офісу основні вимоги до електробезпеки у приміщеннях офісу, де встановлені різні комп’ютери, відображені у рекомендаціях ДНАОП. Основні лінії електромережі для живлення усіх існуючих комп’ютерів та периферійних пристроїв тут виконується, як відокремлена групова три провідна її електромережа тут шляхом прокладення фазового, нульового робочого та також нульового захисного його провідників. Основний нульовий захисний провідник тут прокладається від стійки його групового розподільчого щитку до їх розеток живлення та тут використовується для заземлення усіх електричних його приймачів. Самі електромережі для їх штепсельних з’єднань та електророзеток живлення усіх комп’ютерів та їх периферійних пристроїв тут слід виконувати за магістральною схемою по десь 3-6 з’єднання чи розеток у одному їх колі. Приміщення офісу повинні бути обладнані системою для автоматичної протипожежної їх сигналізації із основними димовими повідомленнями та переносними їх вуглекислотними вогнегасниками у розрахунку по 2-і штуки на 20м^2 площі приміщення офісу. Тут також треба враховувати усе вищезазначене робимо такі основні висновки:

- Перше є приміщення офісу, у якому знаходяться 5-ь робочих станцій РС9-РС13 та 1-н ноутбук і має площу до 72 м^2 (6м * 12м).

- Друге є приміщення офісу, у якому знаходяться 1-а робоча станція із точкою доступу та один її сервер і має площу до 36 м^2(6м * 6м).

- Третє є приміщення офісу, у якому знаходяться 3-и робочих станцій та 1-н ноутбук і має площу до 48 м^2 (6м * 8м).

- Четверте є приміщення офісу, у якому знаходяться 1-а робоча станція та 1-н ноутбук і має площу до 30 м^2 (6м * 5м).

- П’яте є приміщення офісу, у якому знаходяться 4-и робочих станції та 2-а ноутбуки і має площу до 72 м^2 (6м * 12м).

- Шосте є приміщення офісу, у якому знаходяться 4-и робочих станції та 1-н ноутбук і має площу до 60 м^2 (6м * 10м).

- Сьоме є приміщення офісу, у якому знаходяться 3-и робочих станції та 1-н ноутбук і має площу до 54 м^2 (6м * 9м).

- Кабелі у комп’ютерній мережі розподіленого офісу прокладаються у їх захисних коробах на стінах на відстані уже не менше ніж 1м від підлоги та обладнуються тут з’єднаними для підключення різних комп’ютерів.

- Кабелі силові електричної мережі виконуються за її магістральною схемою із різними електророзетками біля кожного робочого місця користувача.

- Приміщення комп’ютерної мережі розподіленого офісу також обладнується протипожежною сигналізацією та також вентиляцією.

Тому із врахуванням усіх вимог до розташування компонентів комп’ютерної мережі сама схема для розташування технічного обладнання у приміщеннях офісу представлена на відповідних їх кресленнях.

Як інформаційне та програмне забезпечення комп’ютерної мережі розподіленого офісу, а це комплекс програм для обробки включаючи і систему для передачі їх даних. Тут по своєму призначенню програмне забезпечення розподіленого офісу поділяється на його системне, допоміжне та також спеціалізоване. Системне ж програмне забезпечення, а це є різні операційні системи, що керують основним функціонуванням їх комп'ютерної техніки, мережного їх устаткування та прикладного програмного забезпечення роботи. У офісі в якості операційної системи для усіх робочих станції офісу було прийнято рішення обрати системи Windows-. А у якості операційної системи для основного серверу для даного офісу було прийнято рішення тут обрати систему Unix-FreeBSD. Така система Unix-FreeBSD – це є одна із самих надійніших операційних систем які були раніше розроблені.

Загалом при розробці системи Free-BSD, що вийшла у 2009 році, основна увага у ній приділялася інструментам для віртуальності, засобам для бездротового зв'язку та також технологіям для зберігання їх даних. Файлова система у ній ZFS яка оновилася та з'явилася її підтримка стандарту зв'язку 802.11 та також експериментальна підтримка її архітектури MIPS. Основні розробники підвищили їх загальну продуктивність та стабільність роботи для системи, оптимізували її основну платформу під сучасні уже багатоядерні процесори та удосконалили засоби для їх адміністрування і поліпшили їх підтримку для інтерфейсу USB. До складу самої системи Free-BSD входить розширена база їх драйверів тому визначимось із необхідним для них програмним забезпеченням по робочих станцій та потреб офісу.

У комп'ютерній мережі розподіленого офісу допоміжне програмне забезпечення, а це є сукупність різних програмних засобів, які необхідні для функціонування цих програм та представляючи своїм користувачам додатковий сервіс. До допоміжного відносяться також системи управління базами даних, інтерпретатори їх основних програм які розроблені засобами їх інтерпретуючих систем для програмування, різні типи зовнішніх бібліотек які необхідні для функціонування усіх таких програм, основні засоби їх архівування та захисту їх даних від несанкціонованого доступу тощо. Багато таких програм можуть формувати їх звіти у форматі MS-Excel і тому для перегляду усіх цих звітів необхідна наявність для комп'ютерів табличного процесору -Excel чи інших програм для перегляду файлів по формату Excel-. Також встановимо на робочих станціях комп'ютерної мережі розподіленого офісу офісні пакети Microsoft-Office, до складу якого входить програмне забезпечення для роботи із її різними типами документів, а це тексти, електронні таблиці, бази даних тощо.

Для комп'ютерної мережі розподіленого офісу використовуються сучасні прикладні програми для можливості перегляду їх звітів та для уведення даних, що вимагають наявності на такому їх комп'ютерах програми для перегляду Web-сторінок у мережі Інтернет та при їхній відсутності уже не можуть нормально функціонувати. Для самої ж організації SQL серверу, який є тут мережевою платформою, що займається зберіганням досить великих баз даних та їх основною

обробкою таких даних, що у них знаходяться бо тут встановимо на сервері My-SQL-Server. Також на цьому сервері встановимо і ВЕБ - сервер Apache- уже для власного сайту офісу де він уже приймає HTTP – потоки та запити від його клієнтів, а це зазвичай від ВЕБ їх браузерів та видає їм HTTP відповіді, а разом із тим його HTML сторінку, зображення, файли, медіа-потоки чи іншими даними. Саме спеціалізоване програмне забезпечення офісу являє собою сукупність деяких програм уже безпосередньо реалізуючи їх алгоритми для рішення основних функціональних задач для офісу.

У комп'ютерній мережі розподіленого офісу можливості автоматизації для обслуговування придбали уже комплексний характер та охоплюють тут усі процеси для функціонування комп'ютерної мережі та основних їх взаємин із клієнтами офісу. Загальними особливостями розподіленого офісу є автоматизація їх процесів для планування, обліку та управління уже основних її напрямків для діяльності. Тому їх тут можна розглядати уже як інтегровану програмну сукупність для наступних основних її підсистем, а це управління фінансами, матеріальними потоками, системне управління їх обслуговуванням, управління їх якістю роботи, управління їх персоналом та збутом, аналіз їх фінансів та управління маркетингом тощо. Системи для управління розподіленим офісом - це є уже сучасний підхід для управління відділом надання основних послуг та вирішення її задач із організації та проведення заходів у офісі, що є ефективно для управління їх діяльністю такого відділу. Також тут здійснюється групові продажі, аналізується прибутковість тих заявок, що надходять та формує їх основну цінову політику, складає необхідні контракти і контролює їх виконання, здійснює продажі та оренду їх відокремлених приміщень, допомагає клієнтам організовувати заходи. Вона також тут сприяє збільшенню продажів при істотній економії їх ресурсів та часу, а створення такого пакету необхідних послуг для клієнтів при організації необхідних заходів різного характеру тут відбувається за якісь уже лічені хвилини тобто сам користувач уже має доступ до необмеженої кількості для такої категорії як опис, опції тощо.

Сама комп'ютерна мережа розподіленого офісу використовує сучасні автоматизовані технології для управління офісом функціонують як в окремих

підрозділах так і у цілих ланцюгах даної системи. Перехресний продаж між офісами збільшує їх завантаження по групових продажах і вони оснащені досить могутнім їх інструментарієм по збереженню та управлінню усією кореспонденцією між відділом продажів та їх клієнтами. Функціональний блок для управління документацією офісу зберігає та організує їх роботу із документами, які відправлені їх клієнтами. Ефективність їх роботи досягається тут за допомогою впровадження досить нового покоління інформаційних технологій для офісів, що створюють свого роду таку інтерактивну інформаційну базу для загального ланцюга надання різних послуг, а також уже інтегровану із електронними їх системами. Запит же кінцевого клієнта офісу щодо їх послуг уже автоматично обробляється із врахуванням його індивідуальних їх переваг та дозволяючи їм миттєво уже скласти оптимальну пропозицію та із досить великою їх імовірністю по забезпеченню позитивної реакції для самих клієнтів офісу. Сучасний комплексний підхід по автоматизації основних бізнес - процесів офісу використовує за стосунки із застосуванням додаткового модулю, що дозволяє також автоматизувати не тільки завдання по керуванню та їх взаєминами із своїми клієнтами, але також і завдання які пов'язані із веденням їх бухгалтерського, податкового обліку та також здійсненням їх аналізу для фінансово-господарської діяльності офісу.

3.2 Вибір забезпечення для роботи комп’ютерної мережі

Для роботи комп’ютерної мережі розподіленого офісу виберемо апаратне його забезпечення для якісного функціонування мережі. Тому як у якості основної операційної системи використовується тут Windows-, а для його прикладного програмного забезпечення, що використовується для розрахункових її процесів, роботи із базами даних та системою для Web-серверу то тут для комп’ютерів повинні бути вимоги щодо їх потужності. Робочі офісні станції PC9-PC21 та їх сервер обладнаємо додатково ще безпровідним мережевими адаптерами, що підтримує стандарти Wi-Fi як мінімум IEEE802.11n та вище. Технічні характеристики Wi-Fi адаптеру ASUS як прикладу приведені в таблиці 3.2. Робочі

станції офісу PC1-PC8 обладнаємо Gigabit-Ethernet мережевим адаптерами Ethernet-Controller. Склад же самого апаратного забезпечення для комп‘ютерної мережі розподіленого офісу робочих станцій PC1-PC21 як приклад приведено у таблиці 3.3, 3.4 та для серверу у таблиці 3.5.

Таблиця 3.2 – Приклад технічних характеристик Wi-Fi адаптеру ASUS

1	2
Виробник	ASUS
Модель	WL
Антена	
Кількість	3
Тип	Знімні дипольні як тип антени
Можливість заміни антени	так
Частотний діапазон	2.4 – 2.5, 5ГГц
IEEE802.3x	Немає
Розширення протоколу IEEE802.11n	Так (до 300 М біт/с)
Можливість ручного завдання швидкості	Немає
Вихідна потужність	
Максимальна	16дБм
Чутливість приймача	
IEEE802.11b @11Мбіт/с	-88дБм
IEEE802.11g @54Мбіт/с	-75дБм
IEEE802.11n @300 М біт/с	-52дБм
Безпека	
Блокування широкомовного SS ID	так
Прив'язка до MAC адрес	немає
WEP	64/128 біт

Кінець таблиці 3.2

1	2
WPA-EAP	так
WPA-EAP	так
WPA-PSK (pre-shared-key)	так
WPA 2-EAP	так
WPA 2-PSK	так
WPA-Auto-EAP	немає
WPA-Auto-PSK	немає
IEEE802.1x	так

Таблиця 3.3 – Приклад апаратного забезпечення станцій PC1-PC8

Процесор	Intel-Atom N230 (2.6 ГГц)
Об’єм оперативної пам’яті	16-40 ГБ
Тип пам’яті	DDR
Тип відео карти	Intel-GMA 950
Чипсет материнської плати	Intel-945GC
Монітор	21" LG Electronics- W1942S-PF
Мережева карта	Realtek- 10/100/1000 Ethernet-Controller
Комплект поставки	системний блок, кабель живлення

Таблиця - 3.4. Приклад апаратного забезпечення станцій PC9-PC21

1	2
Процесор	Intel-Atom N230 (2.6 ГГц)
Об’єм оперативної пам’яті	16 -40 ГБ
Тип пам’яті	DDR
Тип відео карти	Intel-GMA 950

Кінець таблиці 3.4

Чипсет материнської плати	Intel-945GC
Монітор	21" LG Electronics- W1942S-PF
Мережева карта	ASUS WL Wi-Fi PCI адаптер, 802.11(n)
Комплект поставки	системний блок, кабель живлення

Апаратне забезпечення сервера приведено у таблиці 3.5.

Таблиця 3.5 - Апаратне забезпечення сервера CE1.

Процесор	Intel-Core E8500 (3.16 ГГц)
Об’єм оперативної пам’яті	16-40ГБ
Тип пам’яті	DDR-SDRAM PC5300 (700MHz)
Тип відео карти	Intel-GMA 3100
Материнська плата	ASUS P5E-VM DO
Чипсет материнської плати	Intel-® Q35-Express
Об’єм HDD	4 ТБ (7200 обертів) SATA
Монітор	Монітор 22" HP TFT LP2275w KE289A4
Мережева карта	ASUS WL Wi-Fi PCI адаптер, 802.11(n)

У якості активного мережевого обладнання у комп’ютерній мережі віддаленого офісу використане наступне:

Комутатор SR2016 16-port 10/100/1000 Gigabit-Switch.

При проектуванні комп’ютерної мережі віддаленого офісу використовується архітектурна ієрархія. Потрібно поділити усі об’єкти

комп’ютерної мережі за ієрархічними рівнями, уже відповідно до виконуваних цими об’єктами основних її функцій. При проектуванні, як правило, проаналізувавши один із ієрархічних рівнів комп’ютерної мережі, функції ж інших рівнів можемо не враховувати. Комп’ютерні мережі нашого часу є досить складними, тому що їх визначає уже безліч їх конфігурацій, протоколів та технологій. Для упорядкування усіх цих компонентів у легко аналізовану її модель, що може використати її архітектурну ієрархію. Також вона буде представляти характеристики для кожного рівня ієрархії. Ієрархічна модель комп’ютерної мережі віддаленого офісу сприяє у створенні, експлуатації та обслуговуванні її масштабних, ефективних та надійних таких об’єднаних мереж де загалом визначаються три ієрархічні її рівні і на кожному із цих рівнів реалізуються певні специфічні її мережеві функції.

3.3 Забезпечення якості управління у комп’ютерній мережі офісу

Головною основою для забезпечення якості управління у комп’ютерної мережі віддаленого офісу є процеси класифікації та маркування пріоритетних її пакетів. У комп’ютерній мережі лише ефективне рішення визначених завдань, що полягає у коректному визначенні типу та класу для переданого контенту та присвоєння йому відповідного пріоритету, уже дозволить у подальшому різним іншим засобам для управління потоком їх навантаження тут забезпечить належний розподіл їх мережевих ресурсів у інтересах таких даних для інформаційних потоків. Забезпечення у мережі якості управління можуть бути виконані за рахунок уже застосування спеціальних методів для управління потоком інформації, що також дозволяють більш ефективно розподілити її пропускну здатність для інформаційного каналу передачі комп’ютерної мережі між пакетами різних її типів за рахунок простого оптимального розподілу їх основних пріоритетів. Для комп’ютерної мережі віддаленого офісу є актуальним завдання для оцінки ефекту від введення її пріоритетів, що надаються таким пакетам, які критичні до затримок у такій мережі. Вирішення задачі вимагає уже використання дієвих моделей із неоднорідним їх інформаційним потоком для

основних заявок на передачу, що дозволяють тут виконати аналіз властивостей для пріоритетних систем при її передачі потоків даних та сформулювати основні рекомендації для проектування пріоритетних комп'ютерних мереж та оцінити необхідну її пропускну спроможність для каналів передачі для різної інформації.

Для комп'ютерної мережі віддаленого офісу перед приведенням розрахунків тут приймемо наступні припущення: для спрощення основних розрахунків будемо вважати, що якщо робоча станція уже почала передавати, то колізії поки відсутні. Це можливо зробити виходячи із досить їх високої швидкості для розповсюдження сигналу по середовищу каналу передачі комп'ютерної мережі віддаленого офісу:

$$v = C/\sqrt{K} = 3.0*10^8/\sqrt{K}. \text{ (м/с)}, \qquad (3.1)$$

де К – коефіцієнт діелектричного проникнення діелектрику та відносно її малою відстанню між кінцевими станціями мережі. Тому виходячи із цього припущення уже отримуємо, що затримка у комп'ютерній мережі та виконанні завдання визначається за наступною її формулою:

$$W = t_{д1} + t_{п1} + t_{в} + t_{д2} + t_{п.2} \quad , \qquad (3.2)$$

де $t_{д1}$ - це час необхідний щоб робоча станція отримала доступ до мережі для передачі основного завдання;

$t_{п1}$ – це час необхідний для передачі такого завдання по мережі від комп'ютеру замовника до комп'ютеру виконавця;

$t_{в}$ - це час виконання завдання її основним сервером;

$t_{д2}$ – це час необхідний для отримання комп'ютером у мережі виконавцем доступу до передачі її відповіді для комп'ютеру замовнику потоку передачі;

$t_{п2}$ - це час необхідний на передачу відповіді виконавцем його замовнику.

Далі виходячи із того, що у комп'ютерній мережі із загальним середовищем передачі усі станції тут рівноправні у доступі до середовища для передачі, маємо змогу уже прирівняти $t_{д1}$ та $t_{д2}$ та така формула буде мати наступний її вигляд

$$W = 2t_{д} + t_{п1} + t_{в} + t_{д2} + t_{п.2} \qquad (3.3)$$

де $t_д$ – це час необхідний для отримання доступу до середовища для їх передачі.

Час же передачі у таких комп'ютерних мережах залежить від пропускної можливості середовища їх передачі, довжини пакетів, що передається по мережі та від максимальної довжини їх пакету для такого стандарту, довжини її завдання, часу між початком її передачі цим комп'ютером та між замовником і початком його прийому виконавцем. У цьому випадку коли довжина пакетів та довжина їх завдання будуть співпадати $t_{п1}$, що обчислюється за такою її формулою:

$$t_{п1} = t_{зс} + t_{п.п} \qquad (3.4)$$

де $t_{зс}$ – це час затримки сигналів між початком передачі та її прийомом;

$t_{пп}$ – це час, що витрачається на передачу пакетів $t_{пп} = V / P_к$, де V – це довжина чи обсяг пакету, $P_к$ – це пропускна спроможність для середовища передачі.

У комп'ютерній мережі віддаленого офісу якщо довжина для пакету менше довжини її завдання у n раз, то формула (3.4) уже матиме наступний її вигляд:

$$t_{п1} = t^1_{зс} + t^1_{пп} + t^2_д + t^2_{зс} + t^2_{пп} + \ldots + t^n_д + t^n_{зс} + t^n_{пп} = n(t_{зс} + t_{п.п}) + (n-1)t_в \qquad (3.5)$$

Врахуємо, що при чому $t_д$ уже необхідно враховувати, так як її кожний такий пакет при передачі уже поставлено у рівні умови.

$$t_{зс} = d / v \qquad (3.6)$$

де d – це середня відстань між робочими станціями комп'ютерної мережі.

$$d = \frac{1}{n(n-1)} \sum_{i=1}^{n} \sum_{\substack{j=1 \\ j \neq i}}^{n-1} d_{i.j} , \qquad (3.7)$$

де d_{ij} – це відстань між і-ю та j-ю станціями мережі (це у випадку коли сам комп'ютер не передає пакети для станції j, то $d_{ij} = 0$, а n(n-1) зменшують на 1;

v – це швидкість розповсюдження сигналу у середовищі передачі мережі,

$$v = C/\sqrt{K}, \qquad (3.8)$$

де С – це є швидкість світла, К – це діелектрична проникливість для діелектрика.

Отже тут маємо:

$$t_{зс} = d\sqrt{K}/C \qquad (3.9)$$

Пріоритет у комп'ютерної мережі віддаленого офісу має сенс, коли її мережеві маршрутизатори та комутатори уже здатні розрізняти різні типи для потоків їх інформації. Для оцінки ж ефективності їх пріоритетних методів для управління потоком інформації у комп'ютерних мережах, як базова модель для каналу їх передачі то використовуватимемо тут систему для їх масового обслуговування із неоднорідним потоком для пакетів різного їх типу, що поступають у канал для передачі такої комп'ютерної мережі. У випадку ж, коли їх пакети із одного класу мають уже приблизно однакову довжину, а їх потоки цих пакетів є досить простими, то уже середня затримка такого пакету при використанні методу для управління потоком на основі відносних її пріоритетів у комп'ютерних мережах визначається по формулі:

$$T_{\text{затрпак}} = \frac{1}{W} \cdot \sum_{i=1}^{k} [P_{i\text{доп}} \cdot \sum_{j=1}^{m} j \cdot h_i^{-(m_i - j)} + n_i \cdot h_i (1 - P_{i\text{доп}})] P_{i.\text{доп}})] \qquad (3.10)$$

Завантаження даних у комп'ютерній мережі h буде оптимальною, якщо:

$$h^{\text{оптим}} = \frac{\lambda_i}{n_i \cdot \mu_i} = \frac{F_i}{C_i \cdot n_i} = f(m_i, n_i), i = \overline{1,k} \qquad (3.11)$$

Уже відома модель для системи управління у комп'ютерних мережах дозволяє тут вирішити проблему синтезу та більш його ефективного використання ресурсів та також забезпечити необхідну якість для обслуговування усіх користувачів інформаційних послуг у таких комп'ютерних мережах. Аналіз представлених її результатів тут дозволяє сформулювати наступні її виводи. Для забезпечення ж мінімальної їх затримки для усіх пакетів різних типів пріоритет необхідно надавати короткими пакетами. При великому їх навантаженні таких каналів передачі у мережах низько пріоритетні такі пакети мають практично уже

неприпустимі затримки, що перевищують для мовних їх пакетів обмеження у 200-250мс.

При їх подальшому збільшенні для пропускної спроможності такого каналу передачі у комп'ютерній мережі затримки для пріоритетних пакетів уже зменшилися більш ніж у два рази, а для низько пріоритетних – уже більш ніж на порядок. Тут у мережі однією із задач, що вирішуються на етапі для проектування комп'ютерної мережі, є визначення основних вимог до пропускної здатності для таких каналів передачі потоків інформації. Ці основні вимоги уже залежать від повного навантаження комп'ютерної мережі, що створюють пакети даних, що тут передаються та їх основних обмежень у мережі, які накладаються на величину їх затримки для пріоритетних її пакетів. Частка ж різнотипних таких пакетів протягом доби може досить часто змінюватися у значних для неї межах роботи.

У зв'язку із цим для комп'ютерної мережі віддаленого офісу пропонується уже оцінювати необхідну їх пропускну здатність для такого інформаційного каналу для передачі по всьому діапазону у такому каналі передачі. Результати самого їх розрахунку для пропускної здатності їх каналів передачі для такої комп'ютерної мережі при різних значеннях параметрів його навантаження та обмежень на затримку цих пакетів тут показують, що для якісної передачі такої інформації допустима. Дослідження та аналіз отриманих результатів показує, що введення такого пріоритетного управління для потоків передачі інформації у комп'ютерній мережі дозволяє уже понизити вимоги до пропускної здатності цих каналів передачі.

Таким чином, у комп'ютерній мережі віддаленого офісу запропонована модель для пріоритетного управління у каналі передачі, що дозволяє визначити пропускну здатність для каналів та оцінити ефект, що досягається за рахунок їх використання для пріоритетного управління цим потоком інформації офісу. Також за рахунок підвищення якості роботи та збільшення обсягів для надання основних послуг комп'ютерної мережі є кількість управляючої інформації у мережі для її управління уже стрімко зростає. Тому тут унаслідок цього сама комп'ютерна мережа та її управління може поглинути час основної роботи розподіленого офісу.

3.4 Висновок

У розділі проведено програмно-апаратну реалізацію роботи комп’ютерної мережі розподіленого офісу де було розглянуто апаратну реалізацію комп'ютерної мережі та визначено, що при проектування програмно-технічних засобів комп'ютерної мережі розподіленого офісу визначаємо планування його приміщень, у якому буде розташовуватись ця мережа. Провівши детальний огляд існуючих інфраструктурних та архітектурних її рішень та дослідивши нові мережні технології та також урахувавши усі потреби для проектування комп’ютерної мережі на фізичному її рівні буде використаний безпровідний стандарт 802.11n. Було проведено вибір забезпечення для роботи комп’ютерної мережі та забезпечення якості системи управління у комп’ютерній мережі офісу, що буде ефективним для обраного рішення у залежності від кількості вузлів комп’ютерної мережі.

ВИСНОВКИ

При проектуванні та виконанні кваліфікаційної роботи комп’ютерна мережа розподіленого офісу, була розроблена мережа, що тут проектується із певним ступенем надмірності її роботи. У цій роботі зроблено розрахунок кількості робочих станцій, її мережевої обстановки та середовище для серверної кімнати. Дана мережа для офісу із забезпеченням параметрів якості системи управління відповідає прийнятим міжнародним стандартам і забезпечує передачу усіх потоків та видів інформації з врахуванням роботи її на перспективу для подальшого розвитку самих сучасних інформаційних технологій по передачі такої інформації. Була спроектована комп’ютерна мережа, що забезпечує інтеграцію та працездатність для усіх її компонентів, елементів та систем розподіленого офісу із забезпеченням якості її роботи.

У основі комп’ютерної мережі лежить віртуальна мережа, а це є логічна мережа, яка створена поверх існуючої уже мережі та за допомогою системи шифрування створює нові закриті канали для обміну потоками даних. Завдяки створенню різних тунелів, застосуванню протоколів це дозволяє об'єднати у одну комп’ютерну мережу різні офіси компанії, організувати приватну мережу із партнерами та створює віддалений доступ для своїх співробітників. Для функціонування такої віртуальної мережі має великий вибір протоколів, які можуть працювати на різних рівнях моделі OSI і відповідають за безпеку підключення за допомогою особливостей системи шифрування та авторизації. Для розробки найбільш захищеного віртуального доступу віддалених співробітників офісу до мережі із розподіленими офісами було обрано поєднання використання різних протоколів. При цьому для забезпечення більш захищеного доступу для віддалених співробітників офісу треба було підсилити систему передачі за допомогою двох факторної перевірки.

Розроблена структура комп’ютерної мережі розподіленого офісу дозволяє швидко налаштувати високо захищений доступ до такої мережі. До основних елементів керування комп’ютерної мережі проводиться із робочих місць мережі, де використовується горизонтальна та вертикальна кабельна її підсистема. У

роботі також проведено аналіз обраного рішення у залежності від кількості її вузлів у комп’ютерній мережі, що спричинюють підвищення об’єму її службового потоку інформації та заходів по забезпеченню параметрів для якості її роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Арсенюк І.Р. Комп'ютерні мережі: навчальний посібник / І. Арсенюк, А.А. Яровий // – Вінниця: ВНТУ, 2020 . 145 с.

2. Горбатий, І. В. Телекомунікаційні системи і мережі. Принципи функціонування, технології і протоколи : навч. посібник / І.В. Горбатий, А.В. Бондарєв // – Львів : Видав. Львівської політехніки, 2016. 336 с.

3. Стеклов В. К. Інформаційна система: підручник студентам вищих навчальних закладів по напрямку «Телекомунікації» / В.К. Стєклов, Л.Б. Беркман // – К.: Техніка, 2014. 792 с.

4. Стасєв Ю.Б. Комп'ютерні мережі. Технології та протоколи для моделювання: навчал. посіб. / І.В. Рубан, С.В. Дуденко, О.І. Тимочко // – Х.: ХУПС, 2014. 359 с.

5. Казимир В. В. Інформаційні основи побудови їх телекомунікаційних мереж / В. В. Казимир, В.А. Литвинов, С.М. Шкарлет, С.В. Зайцев // Вісник Чернігівського держав. техн. універ. - Чернігів : ЧДТУ, 2013. 340 с.

6. Кривуца В.Г. Управління телекомунікаціями з застосуванням новітніх технологій / В.Кривуца, В.К.Стеклов, Л.Н.Беркман, Б.Костік, В.Олійник, С.Скляренко // Підручник для ВНЗ. – К.: Техніка, 2007. 384 с.

7. Климаш М.М. Сучасні перетворення в архітектурах розподілених їх систем: монографія / М.М. Климаш, А. Лунтовський, В. Романчук // – Львів-Дрогобич: Коло, 2015. 328 с.

8. Горбатий, І. В. Телекомунікаційні системи і мережі. Принципи функціонування, технології і протоколи : навч. посібник / І.В. Горбатий, А.В. Бондарєв // – Львів : Видав. Львівської політехніки, 2016. 336 с.

9. Романец, Ю.В. Защита информации в компьютерных системах и сетях /Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин // - К. : Зв'язок, 2019. 328 с.

10. Безрук В. М. Інформаційні мережі зв'язку. Ч. 2. Телекомунікаційні технології стаціонарних мереж зв'язку : навч. посібник / Безрук В. М., Бідний Ю. М., Колтун Ю. М., Астраханцев А. А., Свид І. В., Ширяєв А. В., Харченко Н.А// – Харків: ХНУРЕ, 2011. 492 с.

11. Галицкий А.В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д . Рябко, В.Ф. Шаньгин // - К.: Пресс, 2014. 616 с.

12. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко // – К. : Телеком, 2019. 452 с.

13. Воргуль О. В. Проблеми безпеки при використанні віртуальних приватних мереж / О. В. Воргуль, О. Г. Білоцерківець, А. О. Серіков // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Все- української науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. ЛДУ БЖ, 2020. С. 29–30.

14. Ерохин, В.В. Безопасность информационных систем /В.В.Ерохин, Д.А.Погонышева, И.Г.Степченко // – К. : Флинт - Наука, 2015. 182 с.

15. Завгородний, В.И. Комплексная защита информации в компьютерных системах: учебное пособие для вузов/ В.И. Завгородний. – К. : Логос, 2011. 264 с.

16. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев // – К.: Телеком, 2015. 416 с.

17. Лунтовський А. О. Етапи розвитку сучасних інфо-телекомунікаційних сервісів та енергетична ефективність мережевих технологій / А.О. Лунтовський, П. Гуськов, А. Масюк // *Вісник Націон. Універ. «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації*. — Львів: Вид. Львів. політ., 20 14. - № 796. С. 131-139.

18. Исаченко О. В. Введение в информационные технологи / О. В. Исаченко // - К.: Фенікс, 2019. 240 с.

19. Карабутов Н. К. Адаптивная идентификация систем. Информационный синтез / Н. К. Карабутов // -К.: КомерКнига, 2016. 384 с.

20. Бабич В.Д. Завадостійкість для каналів зв’язку : навч. посіб. / В.Д. Бабич, О.Д. Кувшинов, О.П. Лежнюк, С. Лівенцев // - К.: КВІУЗ, 2021. 150 с.

21. Советов, Б. Я. Моделирование систем: учебник для бакалавров / Б. Я. Советов, С. А Яковлев // — 7-е издан. — К. : Издат. Юрайтс, 2015. 343 с.

22. Кирик М.І. Багаторівнева модель для буферу даних в вузлах обслуговування мультисервісного потоку навантаження / М.І. Кирик, Н.

К.Плесканка, Ю.В. Климаш *// Фізико – техноогла. проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано - та мікроелектроніки*: матеріал. I V Міжнародн. науково-практичних конференцій (23-25 жовтня 2014 р. м. Чернівці), 2014. С. 110-111.

23. Жидецький В.Ц. Основи охорони праці / В.Ц. Жидецький, В.С. Джигирей, О.В. Мельников // - видання 2-е, стереотипне. - Львів: Афіша, 2010. 371с.

24. Романчук В.І. Дослідження методів для оцінювання якості сприйняття їх послуг для різних типів телекомунікаційних мереж / В.І. Романчук, М. Климаш, Б. Янишин *// Радіоелектроніка і телекомунікації [зб. пр.] / ред. Б.А. Мандзій*. – Л. : Вид-тво Нац. ун-т "Львів. Політех.", 2012. - № 73. С. 165-172.

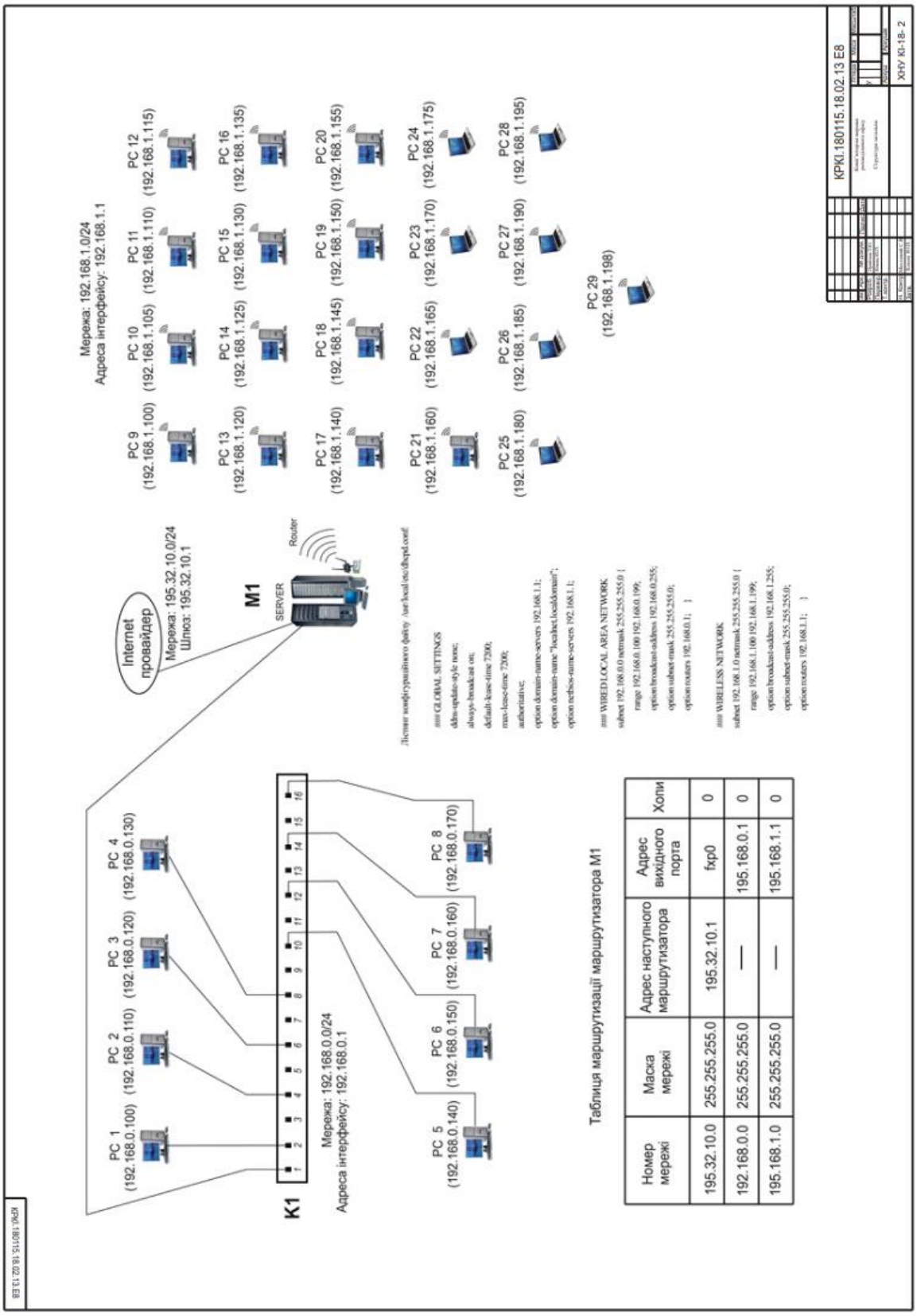
25. Лунтовський А. О. Етапи розвитку сучасних інфо-телекомунікаційних сервісів та енергетична ефективність мережевих технологій / А.О. Лунтовський, П. Гуськов, А. Масюк // *Вісник Націон. Універ. «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації*. — Львів: Вид. Львів. політ., 20 14. - № 796. С. 131-139.

Додаток А

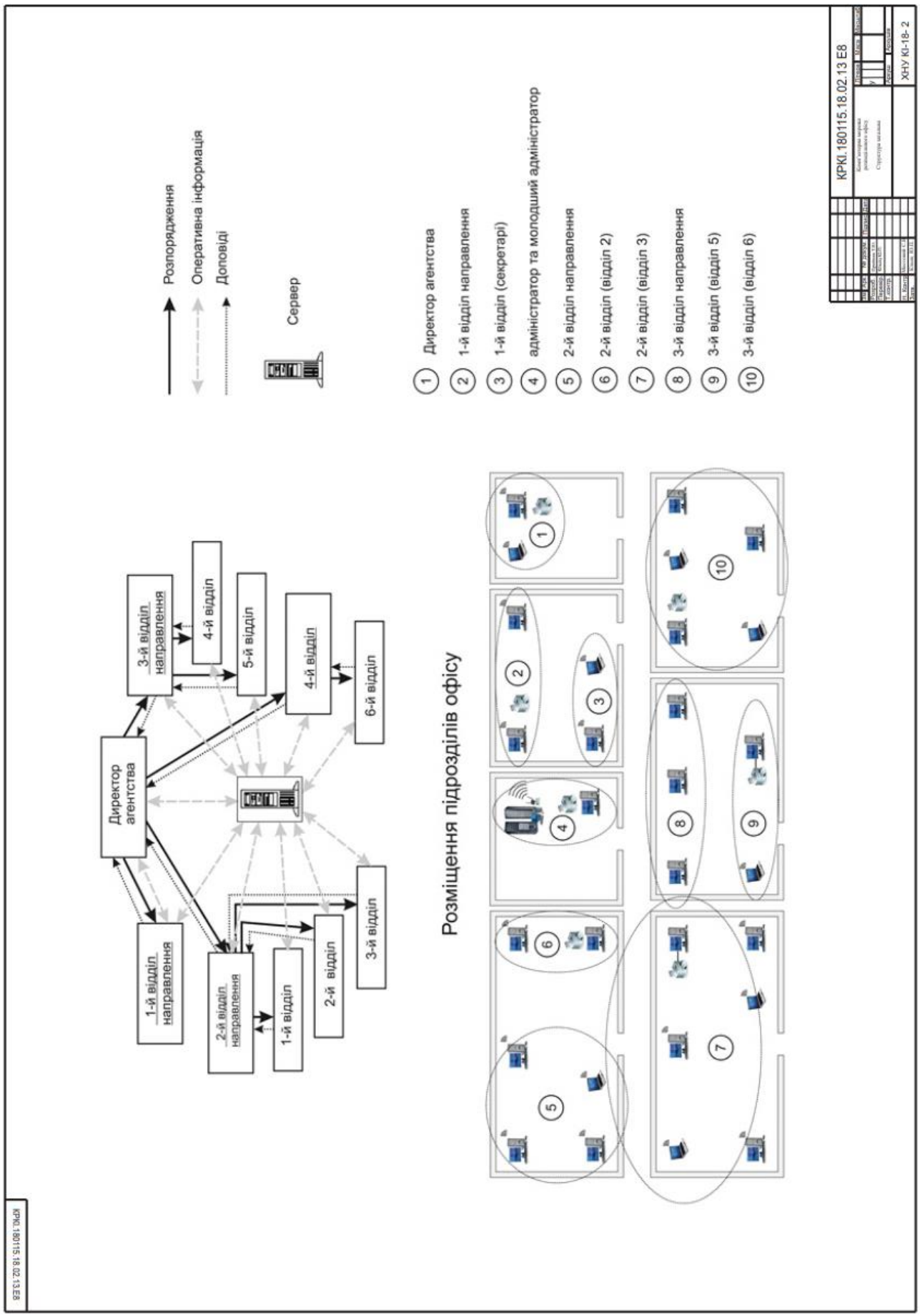
(Обов’язковий)

Копія графічної частини

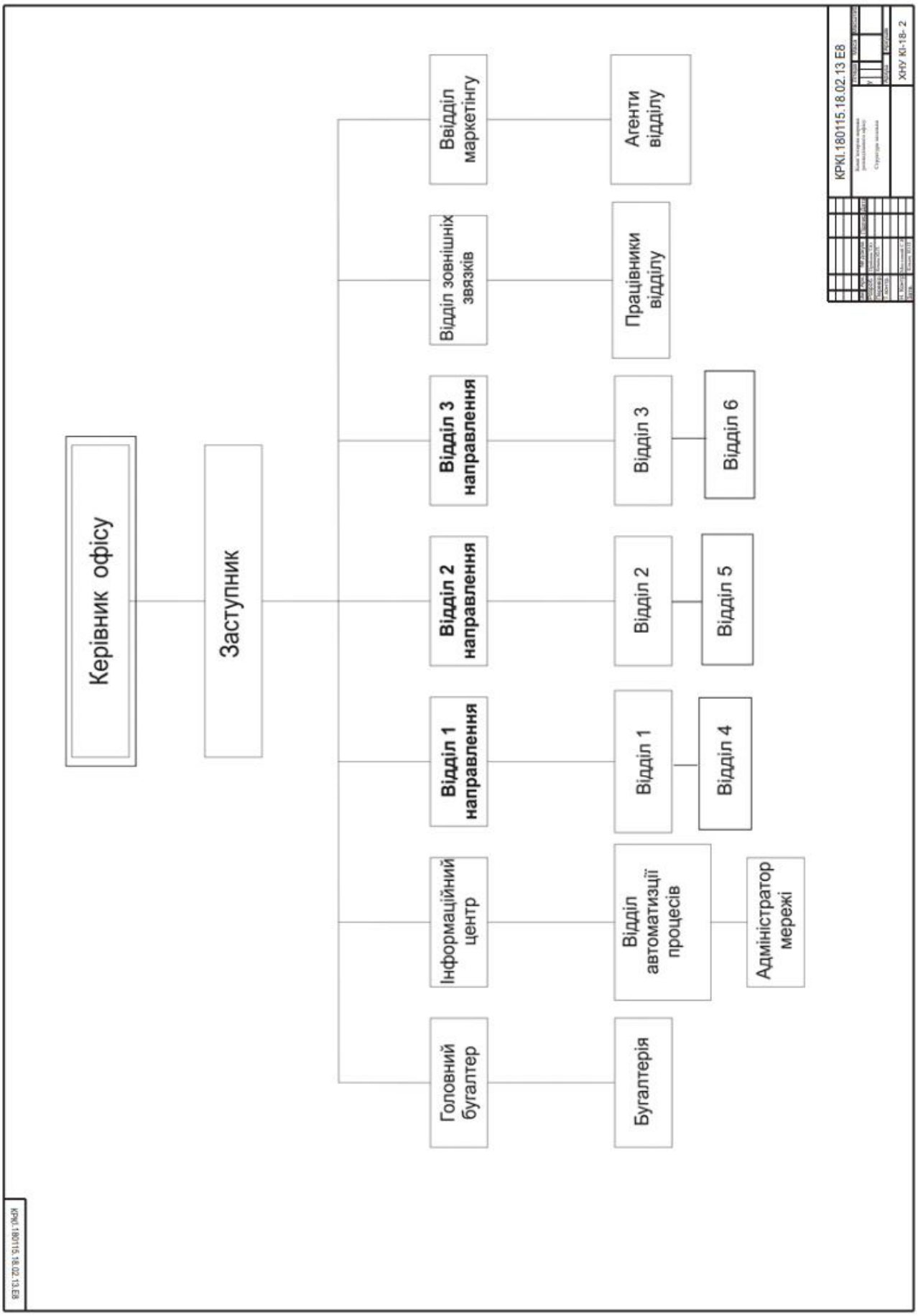
Динамічна маршрутизація мережі



Інформаційні потоки мереж



Організаційна структура офісу



Статистика роботи мережі

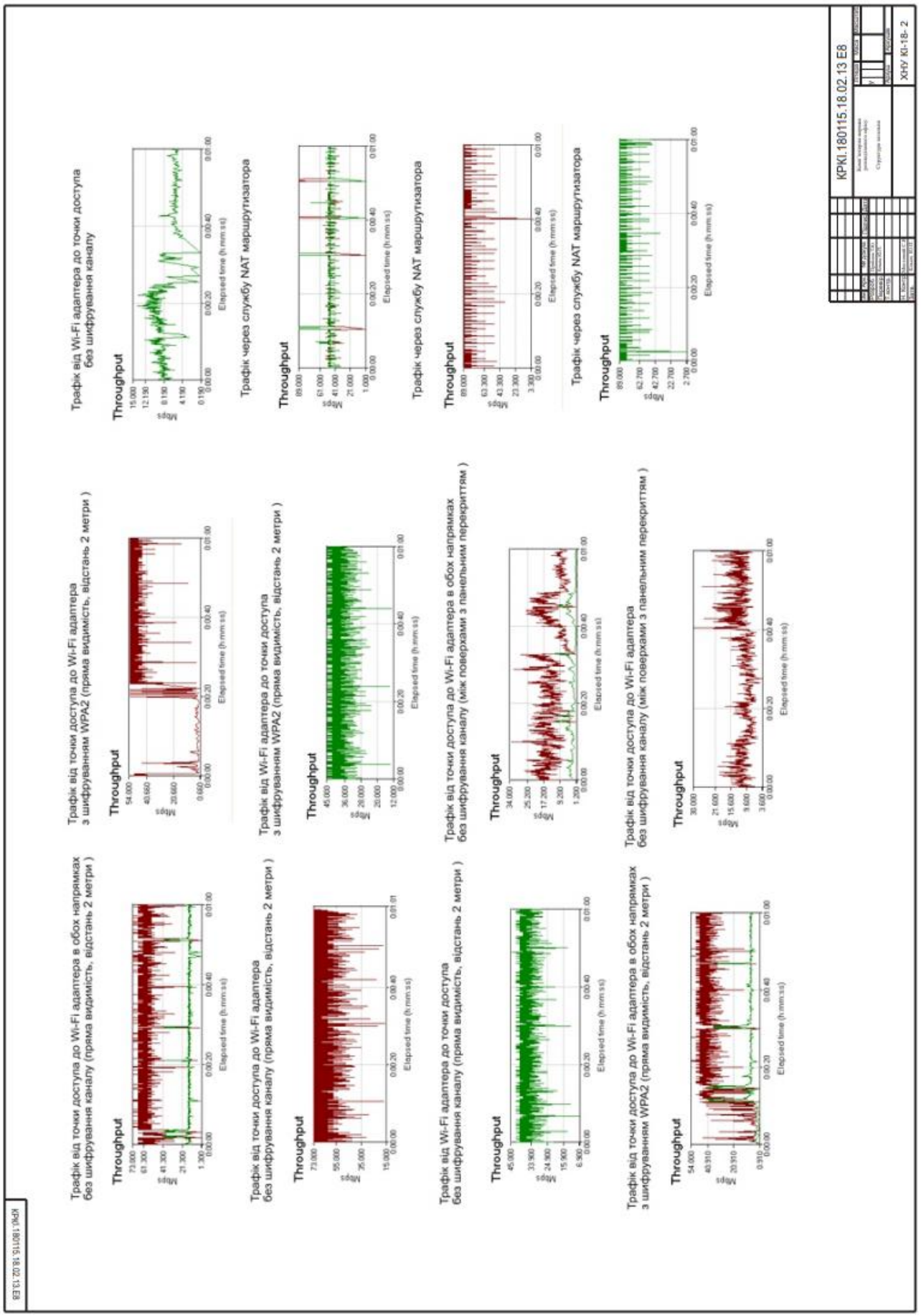


Схема комп’ютерної мереж

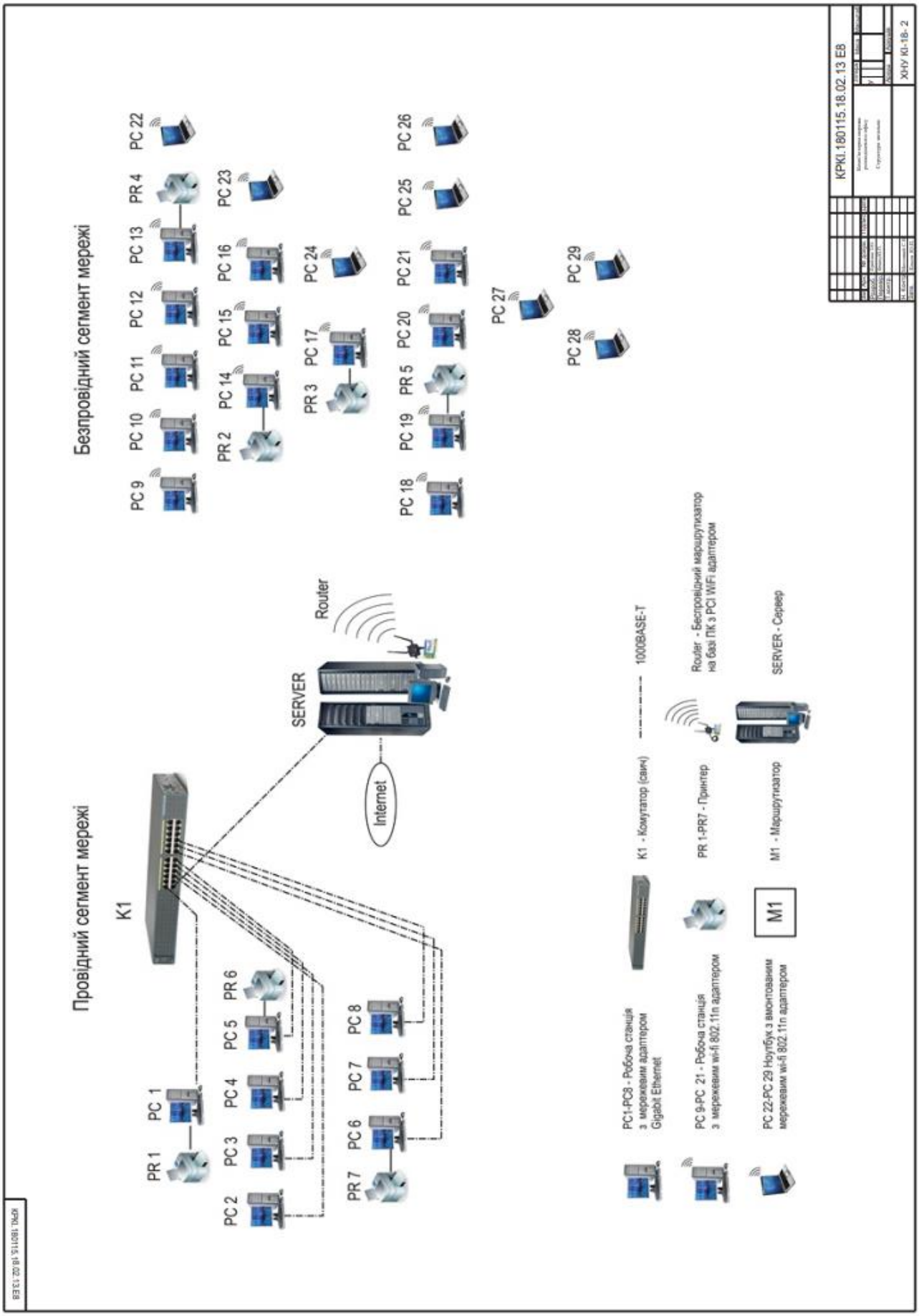
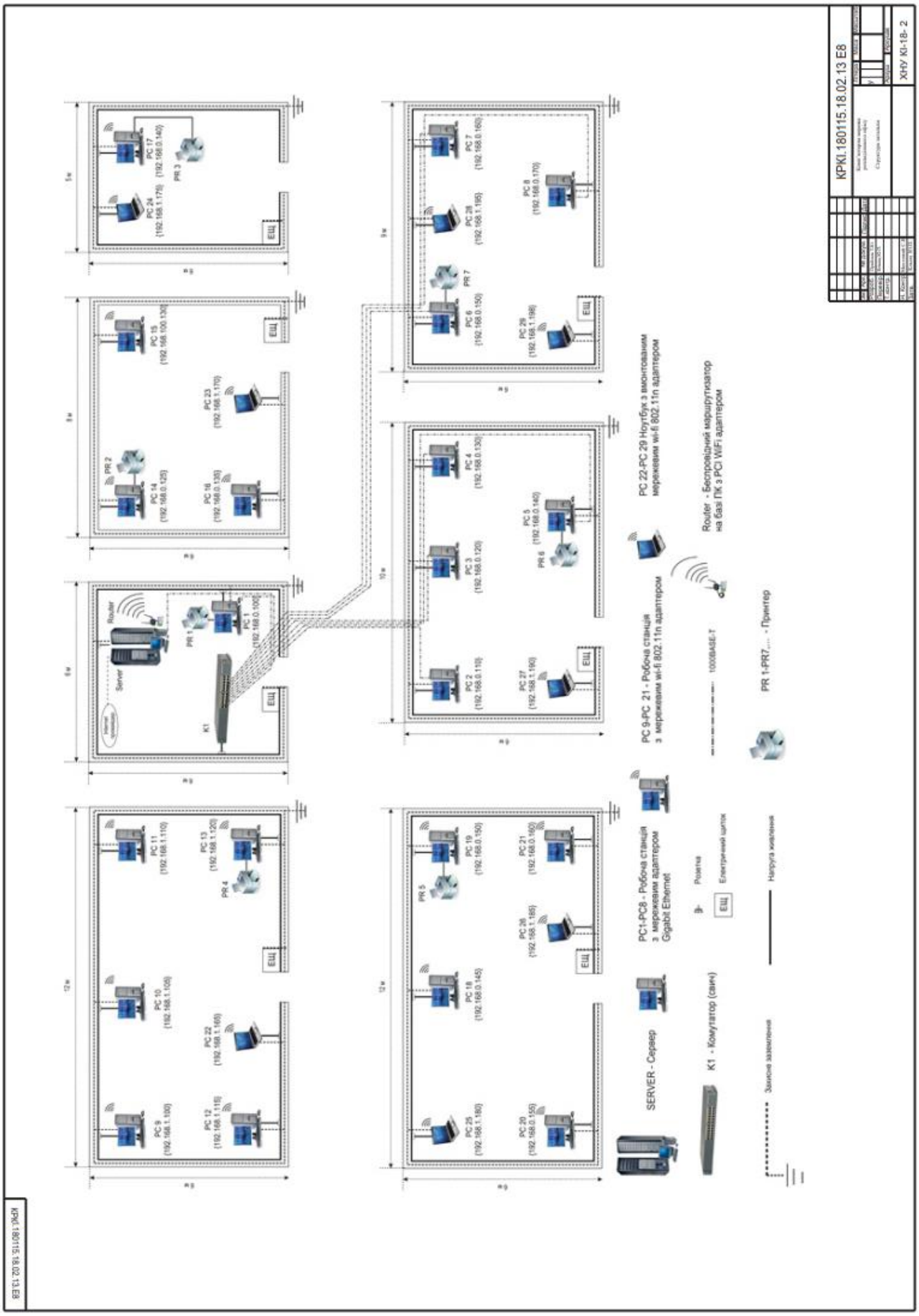
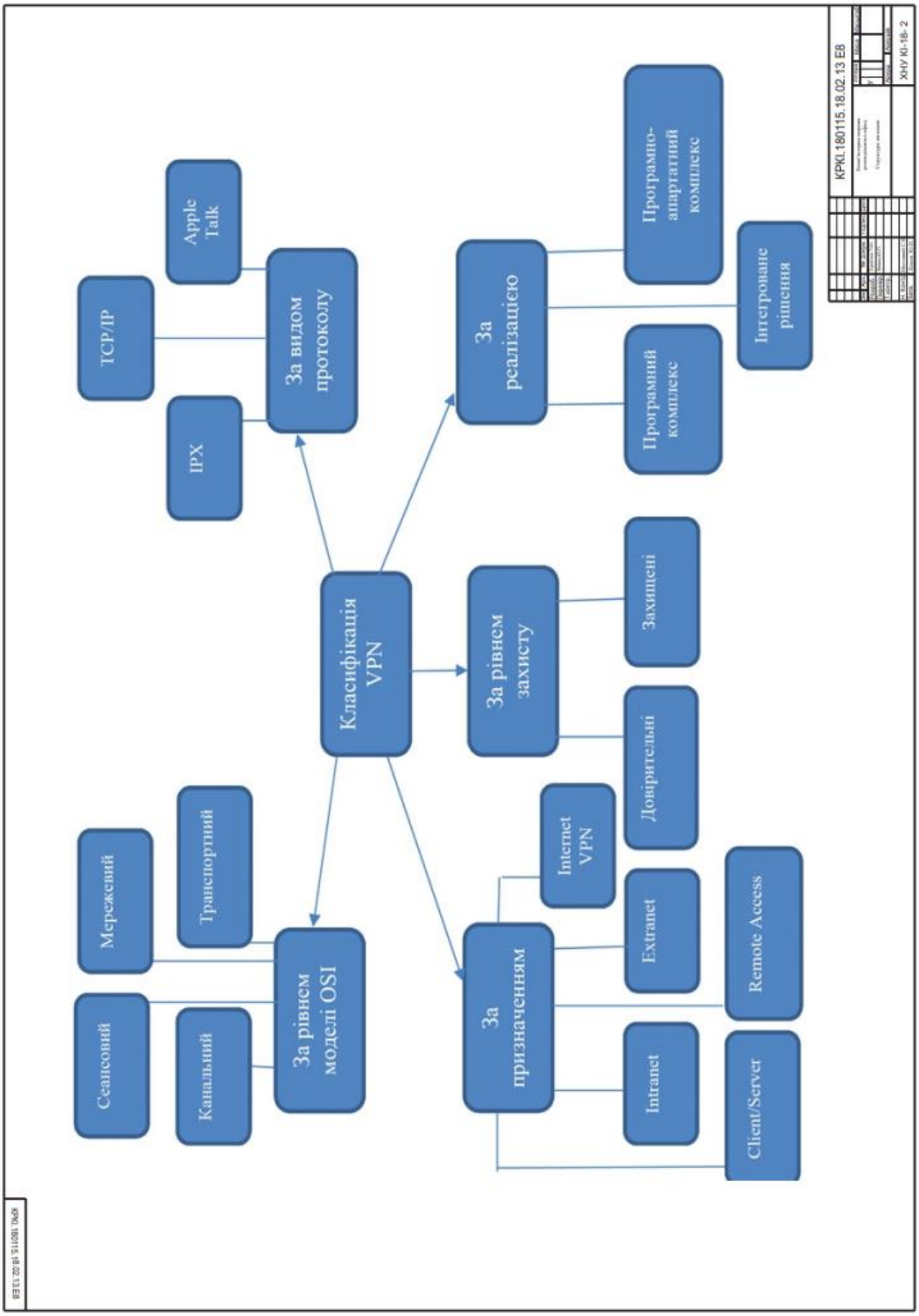


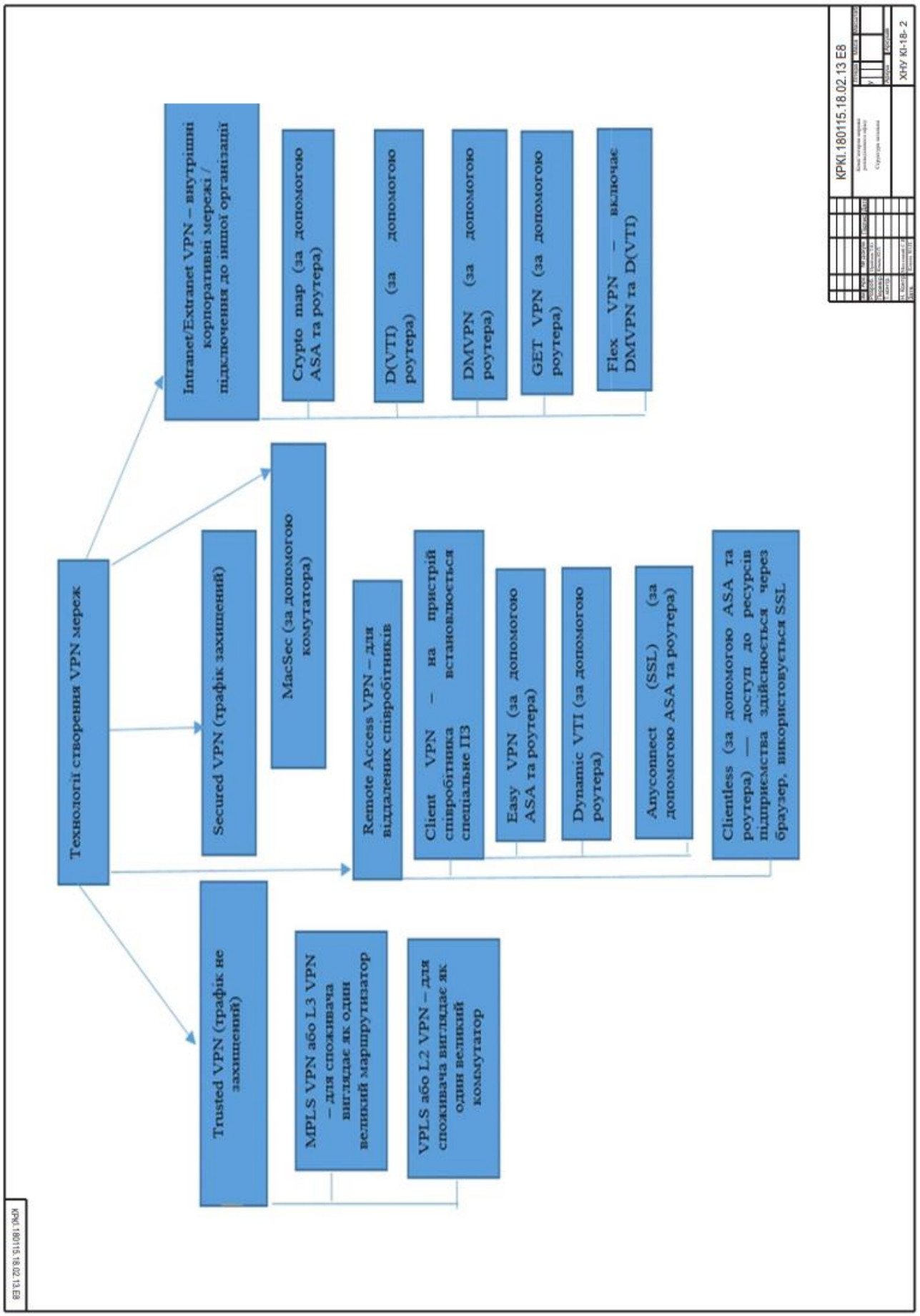
Схема розташування комп'ютерів у мереж



Класифікація віртуальних мереж



Технології створення віртуальних мереж



Додаток Б

Налаштування маршрутизатора і комутаторів

Для налаштування динамічної маршрутизації потрібно ввести такі команди:

R1(config)#router rip // налаштування rip

R1(config-router)#version 2 // вибираємо версію rip.

R1(config-router)#network 192.168.1.0 // записуємо адреси під мереж підключених безпосередньо до маршрутизатора

R1(config-router)#exit R1(config)#exit // виходимо

R1#write // зберігаємо конфігурації.

В результаті ми буде мати такі налаштування маршрутизатора:

interface GigabitEthernet0/0

no ip address

interface GigabitEthernet1/0

no ip address interface GigabitEthernet1/0.210

encapsulation dot1Q 210

interface GigabitEthernet1/0.211

encapsulation dot1Q 211

ip address 192.168.211.200 255.255.255.0 interface GigabitEthernet1/0.214

encapsulation dot1Q 214 ip address 192.168.214.200 255.255.255.0 interface GigabitEthernet1/0.315

encapsulation dot1Q 315

no ip address interface GigabitEthernet1/0.317

encapsulation dot1Q 3179

no ip address

interface GigabitEthernet1/0.320

encapsulation dot1Q 320

no ip address interface GigabitEthernet2/0

no ip address interface GigabitEthernet3/0

no ip address

shutdown

interface GigabitEthernet4/0 ip address 192.168.4.1 255.255.255.0 interface GigabitEthernet5/0

ip address 192.168.5.1 255.255.255.0

interface GigabitEthernet6/0

ip address 192.168.6.1 255.255.255.0

interface GigabitEthernet7/0

ip address 192.168.22.1 255.255.255.0

duplex auto speed auto

interface GigabitEthernet8/0

ip address 192.168.3.1 255.255.255.0

duplex auto speed auto interface GigabitEthernet8/0.

115 encapsulation dot1Q 315

ip address 192.168.115.200 255.255.255.0

interface GigabitEthernet8/0.117

encapsulation dot1Q 117

ip address 192.168.117.200 255.255.255.0

interface GigabitEthernet8/0.120

encapsulation dot1Q 320

ip address 192.168.120.200 255.255.255.0

interface GigabitEthernet8/0.320

no ip address interface GigabitEthernet8/0.324

encapsulation dot1Q 324

ip address 192.168.124.200 255.255.255.0

interface GigabitEthernet9/0

no ip address duplex

auto speed auto interface GigabitEthernet9/0.2

encapsulation dot1Q 21

ip address 192.168.1.222 255.255.255.0

interface GigabitEthernet9/0.22

encapsulation dot1Q 22

ip address 192.168.122.200 255.255.255.0

interface GigabitEthernet9/0.27

encapsulation dot1Q 27

ip address 192.168.27.200 255.255.255.0

router rip version 2 network 192.168.0.0

network 192.168.4.0 network 192.168.22.0

Налаштування комутатора виконується так само як і маршрутизатор з допомогою консольного кабелю і програми huperterminal.

Для початку налаштовуємо пароль на вхід:

Sw1#conf t

Sw1(config)#line VTY 0 4

Sw1(config-line)#

login Sw1(config-line)#pssword

Sw1(config-line)#exit

Sw1(config)#exit

Для створення vlan вводимо такі команди:

Sw1 (config)#interface GigabitEthernet0/1

вибір порту який буде налаштовуватися

Sw1 (config-if)#switchport access vlan 21 установка номеру VLAN вибраного порту

Sw1 (config-if)#exit Sw1 (config)#interface GigabitEthernet0/2

Sw1 (config-if)#switchport access vlan 22

Sw1 (config-if)#exit

Налаштування портів для зв’язку між комутаторами і маршрутизаторами.

Для зв’язку між різними підмережами на комутаторах порти які безпосередньо підключенні до маршрутизатора порт налаштовується в режимі trunk це дозволить всім підмережам даного маршрутизатора здійснювати передачу даних через даний порт.

Наприклад:

Sw1 (config)#interface GigabitEthernet0/2

Sw1 (config-if)#switchport trunk

В результаті отримуємо такі налаштування:

Налаштування комутатора SW_1

spanning-tree mode pvst interface FastEthernet0/1

switchport access vlan 21

switchport mode access interface FastEthernet0/2

switchport access vlan 22

interface FastEthernet0/3

switchport access vlan 22

interface FastEthernet0/4

switchport access vlan 22

interface FastEthernet0/5

switchport access vlan 22

interface FastEthernet0/6

switchport access vlan 22

interface FastEthernet0/7

switchport access vlan 22

interface FastEthernet0/8

switchport access vlan 27

interface FastEthernet0/9

switchport access vlan 27

interface FastEthernet0/10

switchport access vlan 27

interface FastEthernet0/11

switchport access vlan 210

interface FastEthernet0/12

switchport access vlan 210

interface FastEthernet0/13

switchport access vlan 210

interface GigabitEthernet0/1

switchport mode trunk

interface GigabitEthernet0/2

switchport mode trunk

interface Vlan1

Налаштування комутатора SW_2

spanning-tree mode pvst

interface GigabitEthernet0/1

switchport mode trunk

interface GigabitEthernet1/1

switchport access vlan 21

interface GigabitEthernet2/1

switchport access vlan 210

interface GigabitEthernet3/1

switchport access vlan 210

interface GigabitEthernet4/1

switchport access vlan 211

interface GigabitEthernet5/1

switchport access vlan 211

interface GigabitEthernet6/1

switchport access vlan 211

switchport access vlan 214

interface Vlan1 no ip address

shutdown

line con 0

line vty 0 4

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 8%**

ID: 104748 Название: Комп'ютерна мережа розподіленого офісу Добавлено в БД: 2022-06-08 Авторы: Приймак Тарас Юрійович Руководители: Кльоц Ю.П. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	111322	705	2803 (3%)	39 (6%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1011504775

Дата перевірки:
08.06.2022 12:58:28 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
08.06.2022 13:25:34 EEST

ID користувача:
100008300

Назва документа: **Плагіат Кваліфакаційна робота 2022 Приймак КІ-18-2**

Кількість сторінок: **63** Кількість слів: **17170** Кількість символів: **122490** Розмір файлу: **6.16 MB** ID файлу: **1011379835**

5.92%
Схожість

Найбільша схожість: **2.41%** з джерелом з Бібліотеки (ID файлу: **1008248163**)

0.44% Джерела з Інтернету	31	Сторінка 65
5.8% Джерела з Бібліотеки	82	Сторінка 65

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	7

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

Направляється студент Приймак Тарас Юрійович (прізвище, ім'я, по батькові) на захист дипломного проєкту (роботи)

за спеціальністю 123 - Комп'ютерна інженерія

На тему: Комп'ютерна мережа розподіленого офісу

Дипломний проєкт (робота), рецензія і довідка про перевірку на плагіат додаються.

Декан факультету _____ О. Савенко (підпис) (ім'я, прізвище)

ДОВІДКА УСПІШНОСТІ

Приймак Т. Ю. за період навчання на факультеті інформаційних технологій з 2018 по 2022 роки повністю виконав навчальний план спеціальності з таким розподілом оцінок за:
національною шкалою: відмінно 0,00 %, добре 0,00 %, задовільно 100,00.
шкалою ЄКТС: A 0,00 %, B 0,00 %, C 4,35 %, D 2,17 %, E 93,48 %.

Методист факультету _____ Т. Пакуш (підпис) (ім'я, прізвище)

ВИСНОВОК КЕРІВНИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ) ТА ОБГРУНТУВАННЯ ОЦІНКИ

Студент Студент Приймак Т. Ю завдання на дипломне проектування виконав з зауваженнями

Оцінка дипломного проєкту (роботи) загальна оцінка задовільно

Керівник дипломного проєкту _____ Клюх Ю.Н. (підпис) (ім'я, прізвище)

"16" 06 2022 р.

ВИСНОВОК КАФЕДРИ ПРО ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ)

Дипломний проєкт (роботу) розглянуто. Студент Приймак Т. Ю. допускається до захисту цього проєкту (роботи) в екзаменаційній комісії.

Завідувач кафедри кібербезпеки (назва)

_____ Клюх Ю.Н. (підпис, ім'я, прізвище)

"16" 06 2022 р.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Приймака Тараса Юрійовича
ПІБ здобувача вищої освіти

студента ФІТ, 4 курсу, групи КІ-18-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

6.06.2022
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджусмо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Комп'ютерна мережа розподіленого офісу

Автор: Приймак Тарас Юрійович

Галузь знань *12 «Інформаційні технології»*

Спеціальність: 123 – *«Комп'ютерна інженерія»*

Освітня програма: *«Комп'ютерна інженерія»*

Науковий керівник: Кльоц Юрій Павлович, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання роботи та ідентичності версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-30 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано послідовності кодів, які є вхідними даними до великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає % і адресується до першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру роботи і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Ю.П. Кльоц

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

Дата: 01.06.2022

Гарант ОП С.М. Лисенко