

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр

Освітній рівень

Мультисервісна мережа приватного підприємства

Назва теми

КвРТР.2019018.01.017.ПЗ

Галузь знань 17 «Електроніка та телекомунікації»

Шифр, назва

Спеціальність 172 «Телекомунікації та радіотехніка»

Шифр, назва

Освітня програма «Телекомунікації та інформаційно-комунікаційні технології»

Назва

Виконав:

студент IV курсу, група ТР1-19-1



Підпис

Кирил ШЕПТИЦЬКИЙ

Ім'я, ПРІЗВИЩЕ

Керівник

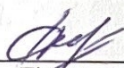


Підпис, дата

Микола ФЕДУЛА

Ім'я, ПРІЗВИЩЕ

Нормоконтролер



Підпис, дата

Людмила КОРЕЦЬКА

Ім'я, ПРІЗВИЩЕ

До захисту допускаю:

зав. кафедри автоматизації  
та комп'ютерно-інтегрованих  
технологій



Підпис, дата

Валерій МАРТИНЮК

Ім'я, ПРІЗВИЩЕ

« 24 » червня 2023 р.

Хмельницький 2023

Хмельницький національний університет

Факультет інформаційних технологій

Кафедра автоматизації, комп'ютерно-інтегрованих технологій та  
робототехніки

Освітній рівень перший (бакалаврський)

Галузь знань 17 – Електроніка та телекомунікації

Спеціальність 172 – Телекомунікації та радіотехніка

Освітня-професійна програма Телекомунікації та інформаційно-комунікаційні  
технології

ЗАТВЕРДЖУЮ

Зав. кафедрою АКІТ та Р  
С.В. Мерашон  
«01» 02 2023р.

## ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шептицький Кирил Юрійович

1 Тема роботи: Автоматизація процесу опалення електричною котельнею  
керівник роботи Федула М. В., к.т.н., доцент

Затверджено наказом по університету від «01» березня 2023р. №5.

2 Строк подання студентом роботи на кафедру: 03.06.2023р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування





4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ.  
Аналіз існуючих інфокомуникаційних технологій та огляд об'єктів групи  
приватного підприємства. Проектування мультисервісної мережі приватного  
підприємства. Моделювання мультисервісної мережі приватного підприємства.  
Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) 1.  
Схема організації зв'язку Хмельницького філіалу. 2. Схема мереж зв'язку  
приватного підприємства офісів «Sigma Software». 3. Схема реалізації мережі  
зв'язку VPN

Завдання отримав Мер

Керівник Са

### Консультанти розділів кваліфікаційної роботи

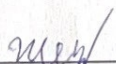
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Антиплагіат	Федула М.В., доцент кафедри АКІТтаР		
Нормоконтроль	Корецька Л.О., доцент кафедри АКІТтаР		

7. Дата видачі завдання « 01 » 02 2023 р.

### КАЛЕНДАРНИЙ ПЛАН


№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Вступ	15.02.2023р.	Виконано
2	Огляд літературних джерел, аналіз сучасного стану завдання	15.03.2023р.	Виконано
3	Основна частина	10.04.2023р.	Виконано
4	Проектування мультисервісної мережі приватного підприємства	10.05.2023р.	Виконано
5	Висновки	15.05.2023р.	Виконано
6	Оформлення пояснювальної записки до кваліфікаційної роботи	25.05.2023р.	Виконано
7	Оформлення креслень, презентаційних матеріалів	1.06.2023р.	Виконано

Студент

  
Підпис

Кирил ШЕПТИЦЬКИЙ  
Ім'я, прізвище

Керівник роботи

  
Підпис

Микола ФЕДУЛА  
Ім'я, прізвище

## АНОТАЦІЯ

Тема кваліфікаційної роботи: «Мультисервісна мережа приватного підприємства».

Автор роботи: Шептицький Кирил Юрійович.

Керівник роботи: Федула Микола Васильович.

Пояснювальна записка: 62 с., 14 рис., 7 табл., 47 джерел.

Графічна частина: 3 креслення.

МУЛЬТИСЕРВІСНА МЕРЕЖА ПРИВАТНОГО ПІДПРИЄМСТВА,  
ІНФОРМАЦІЙНА БЕЗПЕКА, МАРШРУТИЗАТОР, СКАНЕРИ, ПРИНТЕРИ,  
КАМЕРИ, ПЕРСОНАЛЬНІ КОМП'ЮТЕРИ, ІР-ТЕЛЕФОНІЯ.

Метою роботи є проектування, розробка та програмно-апаратне забезпечення мультисервісної мережі Хмельницького філіалу приватного підприємства.

У цій роботі проведено проектування інфраструктури мультисервісної мережі, вибір технологій та обладнання, налаштування мережевих пристроїв, а також розробку стратегій забезпечення ІБ. Здійснено дослідження процедури керування та моніторингу, щоб забезпечити ефективну роботу мультисервісної мережі між офісами приватного підприємства (компанії «Sigma Software»). Запропоновано ефективні рішення та стратегії для досягнення мети створення надійної, безпечної та ефективної мультисервісної мережі між офісами приватного підприємства (компанії «Sigma Software»).

24.06.2023  
дата

Метт  
Підпис

## ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ.....	4
ВСТУП.....	6
1 АНАЛІЗ ІСНУЮЧИХ ІНФОКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ОГЛЯД ОБ'ЄКТІВ ГРУПИ ПРИВАТНОГО ПІДПРИЄМСТВА.....	7
1.1. Загальні відомості про інформаційно-телекомунікаційні мережі .....	7
1.2. Класифікація мультисервісних мереж.....	10
1.3. Постановка задачі на проектування мультисервісної мережі приватного підприємства.....	11
1.4. Архітектура мультисервісної мережі приватного підприємства.....	14
1.5. Технології передачі даних в мультисервісних мережах.....	17
1.6. Висновки до першого розділу.....	19
2 ПРОЕКТУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ПРИВАТНОГО ПІДПРИЄМСТВА .....	21
2.1. Вимоги до мультисервісної мережі приватного підприємства.....	21
2.2. Розробка структурної схеми організації зв'язку мультисервісної мережі приватного підприємства.....	22
2.3. Розрахунок навантаження для мультисервісної мережі приватного підприємства .....	22
2.4. Апаратно-програмні засоби для мультисервісної мережі приватного підприємства.....	33
2.5. Висновки до другого розділу .....	44
3 МОДЕЛЮВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ПРИВАТНОГО ПІДПРИЄМСТВА.....	46
3.1. Модель схеми зв'язку групи компаній приватного підприємства.....	46

					КвРТР.2019018.01.017.ПЗ		
Вип.	Аркуш	№ Докум.	Підпис	Дата	Мультисервісна мережа приватного підприємства Пояснювальна записка		
Розробив		Шептицький К.Ю.	<i>ШШ</i>	26.08.23			
Перевірив		Федула М.В.	<i>МВ</i>	16.06.24	Літера	Аркуш	Аркушів
						2	62
Р. контр.		Корещька Л.О.	<i>ЛК</i>	16.08.23	ХНУ, гр. ТР1-19-1		
Затв.		Мартишок В.В.	<i>ВМ</i>	27.06.23			

3.2. Розробка плану IP-адресації для мультисервісної мережі приватного підприємства.....	47
3.3. Модель мультисервісної мережі приватного підприємства в середовищі CiscoPacketTracer.....	49
3.4. Висновки до третього розділу.....	56
ВИСНОВКИ.....	57
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	58
ДОДАТОК А Схема організації зв'язку Хмельницького філіалу.....	64
ДОДАТОК Б Схема мереж зв'язку приватного підприємства офісів «Sigma Software».....	65
ДОДАТОК В Схема реалізації сегмента мереж зв'язку VPN.....	66

## СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АММПП - Архітектура мультисервісної мережі приватного підприємства

ІБ – інформаційна безпека

ІКП – Інфокомунікаційна платформа

ІТМ- Інформаційна телекомунікаційна мережа

КВР - Кваліфікаційна робота

КМЗ – корпоративні мережі зв'язку

ЛМЗ – локальна мережа зв'язку

МЗ – мережі зв'язку

МСМПП - Мультисервісна мережа приватного підприємства

ОС – операційна система

ПП – приватне підприємство

СЗ – системи зв'язку

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		4

## ВСТУП

У сучасному телекомунікаційному світі планування МЗ відіграє важливу роль. Планування територіального розташування МЗ дозволяє забезпечити їх розвиток. Останнім часом в світі телекомунікацій спостерігається збільшений інтерес до віртуальних приватних МЗ (VPN). Це обумовлено необхідністю зниження витрат на утримання КМЗ завдяки більш дешевому підключенню віддалених офісів та віддалених користувачів через МЗ Інтернет. При порівнянні вартості послуг з'єднання декількох МЗ через Інтернет можна помітити суттєву різницю в вартості. Однак необхідно відзначити, що при об'єднанні ЛМЗ через Інтернет виникає питання про ІБ передачі даних, тому виникла необхідність створення механізмів, що дозволяють забезпечити конфіденційність та цілісність переданої інформації. МЗ, побудовані на базі таких механізмів, отримали назву "віртуальні приватні мережі" - VPN. Переваги технології VPN полягають у тому, що організація віддаленого доступу здійснюється не через телефонну лінію, а через Інтернет, що набагато дешевше та краще.

У даному проекті для розробки МСМПП пропонується використання технології VPN, що дозволяє реалізувати ІБ СЗ між різними підрозділами ПП. За допомогою VPN забезпечується ІБ передачі даних між філіями та центральним офісом ПП (компанії «Sigma Software»), а також доступ до важливої інформації з будь-якої точки світу. Однією з головних метою проекту є покращення процесу обміну інформацією та взаємодії між підрозділами ПП (компанії «Sigma Software») та його партнерами та клієнтами. Для цього необхідно розробити ІКП, яка забезпечить ефективний та безпечний обмін даними, а також забезпечить необхідний рівень комунікації між підрозділами ПП.

У КвР проведено проектування інфраструктури МЗ, вибір технологій та обладнання, налаштування мережевих пристроїв, а також розробку стратегій забезпечення ІБ. Здійснено дослідження процедури керування та моніторингу, щоб забезпечити ефективну роботу МЗ між офісами ПП (компанії «Sigma Software»).

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		5

Запропоновано ефективні рішення та стратегії для досягнення мети створення надійної, безпечної та ефективної МЗ між офісами ПП (компанії «Sigma Software»).

*Мета роботи:* проектування, розробка та програмно-апаратне забезпечення мультисервісної мережі Хмельницького філіалу приватного підприємства.

*Об'єкт дослідження:* процес програмного, апаратного, інформаційного забезпечення мультисервісної мережі Хмельницького філіалу приватного підприємства.

*Предмет дослідження:* параметри та характеристики мультисервісної мережі Хмельницького філіалу приватного підприємства.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		6

# 1. АНАЛІЗ ІСНУЮЧИХ ІНФОКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ОГЛЯД ОБ'ЄКТІВ ГРУПИ ПРИВАТНОГО ПІДПРИЄМСТВА

## 1.1. Загальні відомості про інформаційно-телекомунікаційні мережі

У ПП (компанії «Sigma Software») функціонує КМЗ, яка має на меті забезпечити зв'язок між різними відділеннями та підрозділами компанії. КМЗ в цьому контексті є територіально розподіленою і об'єднує офіси та структури, які знаходяться на значній відстані один від одного. Вузли КМЗ розташовуються у різних містах.

Варто зазначити, що принципи, за якими будується МСМПП, досить відрізняються від принципів створення ЛМЗ. Однією з головних відмінностей є використання орендованих ліній зв'язку для забезпечення територіально розподіленої МЗ. У ПП (компанії «Sigma Software») КМЗ не надає послуг іншим організаціям чи користувачам, вона призначена лише для внутрішнього використання [1].

З урахуванням швидкого розвитку телекомунікаційних технологій, МЗ ПП (компанії «Sigma Software») в Україні потребує покращення та модернізації. З появою нових підрозділів та зростанням обсягу переданої інформації, необхідно забезпечити безпечну передачу конфіденційних даних. МЗ, створена значний час тому, не відповідає сучасним вимогам. Тому постає необхідність у наданні філіям ПП (компанії «Sigma Software») сучасних інфокомунікаційних послуг та технологій, а також можливості управління інформаційними та іншими ресурсами з головного офісу компанії, який розташований у місті Харків. Таким чином, проектування транспортної МЗ для ПП (компанії «Sigma Software»), є актуальним завданням. У ПП (компанії «Sigma Software») функціонують декілька відділень, розташованих по всій Україні:

1. Харків, вулиця Академіка Проскури 1, - Головний офіс об'єднує різні відділи та команди, забезпечуючи їх ефективну координацію та спільну мету. Тут

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		7

не лише відбуваються зустрічі та брифінги, але й стимулюються інтелектуальні дебати, надихаючі ідеї та креативні розмірковування. Головний офіс також є місцем, де проводяться інноваційні дослідження та розробки, спрямовані на пошук нових технологій та рішень для клієнтів. – Приблизна кількість абонентів: ~450.

2. Львів, вулиця Наукова 7д, - розташований поза головним офісом, цей підрозділ має менш просторе приміщення, ніж попереднє. Це середовище сприяє об'єднанню різних команд та відділів, створюючи сприятливу атмосферу для співпраці та постійного розвитку, тобто тут проводяться зустрічі, брифінги, інтелектуальні дебати та народжуються ідеї, спрямовані на проведення інноваційних досліджень та розробок. – Приблизна кількість абонентів: ~300.

3. Хмельницький.
4. Київ.
5. Одеса.
6. Дніпро.
7. Черкаси.
8. Чернівці.
9. Івано-Франківськ.
10. Луцьк.
11. Полтава.
12. Суми.
13. Тернопіль.
14. Ужгород.
15. Вінниця.

Проект МСМПП для ПП (компанії «Sigma Software») має на меті забезпечити безпечну та ефективну комунікацію між усіма відділеннями, тобто розширення (збільшення масштабування) мережі на тричі є вигідним рішенням з наступних причин: збільшення мережі дозволить забезпечити безпечний обмін даними між усіма відділеннями «Sigma Software», зменшуючи ризик втрати або підміни даних. Нова МЗ забезпечить більш ефективну комунікацію між усіма

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		8

відділеннями, що дозволить співробітникам працювати швидше та ефективніше. Збільшення мережі дозволить «Sigma Software» надавати більш якісні та ефективні послуги своїм клієнтам у всіх регіонах, що підвищить задоволеність клієнтів та зміцнить їх лояльність до компанії. Розширення МЗ для ПП (компанії «Sigma Software») є вигідним рішенням, яке дозволить покращити якість надання послуг та забезпечить більш безпечну та ефективну роботу в цілому [2].



Рисунок 1.1 - Місце знаходження офісів ПП «Sigma Software»

На рисунку 1.1 показано локацію ПП, тобто офісів компанії «Sigma Software», яка складається в загалом з 15 офісів та приблизно 3200 абонентів, для яких в проекті має бути передбачено надання наступних послуг: IP телефонія, бездротовий Wi-Fi доступ, IP-камери відеоспостереження та доступ в Інтернет [3].

## 1.2 Класифікація мультисервісних мереж

Мультисервісна мережа (МСМ) - це мережа, яка здатна передавати голос, відео-зображення та дані на базі єдиної інфраструктури, де основною метою розвитку МСМ є зниження вартості володіння, підтримка складних мультимедійних застосунків та розширення функціональних можливостей мережевого обладнання МСМ [4].

Для створення середовища МСМПП з інтеграцією ІР-телефонії, необхідно врахувати наступні аспекти: забезпечення МСМ з можливістю подальшого розвитку без значних інвестицій, така прозора інтеграція технологій ІР-телефонії, зберігаючи функціональність наявних рішень у сфері традиційної телефонії, надає можливість забезпечення безпеки мережі (з врахуванням інформаційної безпеки) шляхом створення захищених каналів передачі даних та запобігання несанкціонованому доступу.

Переваги МСМПП включають зменшення витрат на міжміський та міжнародний зв'язок, низькі вимоги до кваліфікації персоналу, простоту підключення нових філій до МСМ та використання пропускну здатності наявних наземних каналів МСМ.

У цьому проекті МСМ було вибрано продукти MikroTik та Cisco для створення інтелектуальної мережевої інфраструктури МСМПП, яка підтримує основні сервіси КМЗ, такі як передача даних та голосу, безпека, мережеве управління та гарантія якості сервісу, а канали передачі можуть бути традиційними наземними лініями зв'язку або цифровими каналами Frame Relay, які орендуються у оператора зв'язку.

Основні компоненти мультисервісної КМЗ включають ІР-телефони, підключені до локальної мережі кожного офісу МСМ, які надають традиційні функції телефонів та нові функції для МСМ; сервер, що керує телефонними з'єднаннями та надає додаткові послуги ІР-телефонії; голосові шлюзи для підключення до існуючих телефонних систем; комутатори, необхідні для підключення активних мережевих пристроїв, таких як робочі станції, ІР-телефони

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		10

та сервери. Побудова МСМ дозволить забезпечити надійність та безпеку передачі інформації, а також масштабованість мережі та послуг, тобто керованість КМЗ, а також готовність до впровадження нових послуг та додатків для МСМ, що призводить до того, що вибір обладнання та постачальника послуг варто здійснювати з урахуванням цих важливих параметрів МСМ [5].

### 1.3 Постановка задачі на проектування мультисервісної мережі приватного підприємства

Транспортна МЗ - це сукупність ресурсів, що забезпечують функції транспортування в ІТМ, яка охоплює системи передачі та відповідні засоби контролю, оперативного перемикавання, резервування та керування МСМ. У проєктованій мережі транспортна МЗ є сегментом між ядром МЗ, розташованим у м. Харків, та підмережами офісів.

Для побудови розподілених мереж МСМ часто використовується віртуальна приватна МЗ (VPN). Віртуальні приватні МЗ є підключеннями "точка-точка" у приватній або публічній МЗ, наприклад, Інтернеті. VPN-клієнт використовує спеціальні протоколи на основі TCP/IP МЗ, відомі як тунельні протоколи, для віртуального з'єднання з VPN-сервером у МЗ. При стандартному використанні VPN клієнт ініціює віртуальне "точка-точка" з'єднання через МЗ Інтернет з сервером віддаленого доступу МЗ. Сервер віддаленого доступу МЗ перевіряє автентичність ініціюючої сторони та передає дані через МЗ між VPN-клієнтом та приватною МЗ організації [6].

Для емуляції "точка-точка" каналу МЗ до даних додається заголовок (інкапсуляція), цей заголовок містить маршрутизаційну інформацію, яка забезпечує проходження даних МЗ, як через загальну МЗ або публічну МЗ до кінцевої точки. Для емуляції каналу ПП та забезпечення конфіденційності, дані МЗ шифруються. Пакети даних МЗ, перехоплені в спільній або публічній МЗ, не можуть бути розшифровані без шифрувального ключа, тобто таке зашифроване та

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		11

інкапсульоване з'єднання в МЗ, через яке передаються приватні дані, називається VPN-підключенням МЗ [7].

Існує два типи VPN-підключень МЗ:

1. VPN-підключення МЗ віддаленого доступу - дозволяє користувачам працювати з дому або в дорозі, отримуючи доступ до сервера МЗ ПП через інфраструктуру громадської МЗ. З точки зору користувача, VPN-підключення МЗ є "точка-точка" з'єднанням між комп'ютером (VPN-клієнтом) та сервером організації МЗ ПП. Реальна інфраструктура загальної або публічної МЗ не має значення, оскільки дані передаються так, ніби вони проходять через виділений приватний канал.

2. VPN-підключення типу "мережа-мережа" - дозволяє організаціям створювати маршрутизовані з'єднання між окремими офісами МЗ (або між іншими організаціями) через публічну МЗ, забезпечуючи безпеку зв'язку. Маршрутизоване VPN-підключення через Інтернет логічно подібне до виділеного каналу глобальної мережі (WAN). У випадку, коли МЗ з'єднані через Інтернет, маршрутизатор переадресовує пакети до іншого маршрутизатора через VPN-підключення. З точки зору маршрутизаторів, VPN-підключення працює як канал передачі рівня, а VPN-підключення типу "мережа-мережа" з'єднує два сегменти приватної МЗ. VPN-сервер забезпечує маршрутизоване підключення до МЗ, до якої він прикріплений. Викликаючий маршрутизатор (VPN-клієнт) пройшов автентифікацію на відповідному маршрутизаторі (VPN-сервері), а в процесі взаємної автентифікації маршрутизатор, що відповідає, перевіряє автентичність викликаючого маршрутизатора. При VPN-підключенні типу "мережа-мережа" пакети, які передаються через VPN-з'єднання будь-яким з маршрутизаторів, зазвичай не формуються на маршрутизаторах [8].

*Властивості підключення VPN МЗ.* Підключення VPN, що використовують протоколи PPTP, L2TP/IPsec та SSTP, мають наступні властивості:

1. Інкапсуляція МЗ: підключення VPN використовує інкапсуляцію МЗ для упакування телекомунікаційних даних в захищений тунель, а це означає, що

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		12

дані передаються в зашифрованій формі через загальну або публічну МЗ, забезпечуючи їх безпеку та приватність.

2. Перевірка справжності МЗ: VPN-підключення включають механізми перевірки справжності, які забезпечують, що тільки правомірні користувачі та пристрої можуть отримати доступ до МЗ. Це допомагає запобігти несанкціонованому доступу та зберегти безпеку МЗ.

3. Шифрування даних МЗ: Підключення VPN використовують шифрування для захисту переданих даних в МЗ від несанкціонованого доступу. Дані МЗ, що передаються через VPN, шифруються з використанням спеціальних алгоритмів, що робить їх незрозумілими для незаконних користувачів, які можуть перехоплювати дані в МЗ. Такі властивості підключення VPN допомагають забезпечити безпеку, приватність та надійність передачі даних МЗ через віртуальну приватну МЗ.

*Інкапсуляція МЗ:* технологія VPN забезпечує інкапсуляцію приватних даних МЗ у заголовки, що містить інформацію про маршрутизацію для передачі цих даних через транзитну МЗ [9].

*Перевірка автентичності МЗ:* існує три форми автентифікації для підключення VPN МЗ.

1. Перевірка автентичності МЗ на рівні користувача за допомогою протоколу PPP: при встановленні VPN-підключення МЗ, VPN-сервер перевіряє автентичність VPN-клієнта МЗ на рівні користувача за допомогою протоколу PPP та перевіряє, чи має VPN-клієнт необхідну авторизацію, і у випадку взаємної автентифікації, VPN-клієнт також перевіряє автентичність VPN-сервера для захисту від комп'ютерів (інфокомунікаційних систем), що видають себе за сервери VPN для МЗ.

2. Перевірка автентичності на рівні комп'ютера (інфокомунікаційних систем) за допомогою протоколу IKE: для встановлення з'єднання в МЗ IPsec VPN, VPN-клієнт та VPN-сервер використовують протокол IKE МЗ для обміну сертифікатами комп'ютерів (інфокомунікаційних систем) або переднім ключем, у таких (обох) випадках VPN-клієнт та VPN-сервер МЗ перевіряють автентичність

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		13

одне одного тільки на рівні комп'ютера (інфокомунікаційних систем), і далі рекомендується використовувати аутентифікацію з використанням сертифіката комп'ютера (інфокомунікаційних систем) для більшої безпеки МЗ.

3. Перевірка справжності джерела даних МЗ та забезпечення цілісності її даних: для переконання, що дані МЗ, надіслані через VPN-підключення, походять від іншої сторони VPN-підключення і не змінилися, дані МЗ містять контрольну суму шифрування, засновану на ключі шифрування, відомому лише відправнику та одержувачу МЗ, а перевірка справжності джерела даних МЗ та забезпечення цілісності даних МЗ доступні лише для підключень L2TP/IPsec.

4. *Шифрування даних:* для забезпечення конфіденційності даних МЗ під час їх передачі через загальну або публічну транзитну МЗ вони шифруються відправником і розшифровуються одержувачем МЗ, а ефективність процесу шифрування та розшифрування МЗ забезпечується використанням спільного ключа шифрування між відправником та одержувачем МЗ. Зміст перехоплених пакетів МЗ, надісланих через VPN-підключення до транзитної МЗ, може бути розпізнаний лише власниками спільного ключа.

Довжина ключа шифрування є важливим параметром безпеки МЗ. Визначення ключа шифрування може використовувати обчислювальну техніку для МЗ, однак, збільшення розміру ключів шифрування вимагає більшої обчислювальної потужності МЗ та часу для виконання обчислень МЗ, тому для забезпечення конфіденційності рекомендується використовувати найбільшу можливу довжину ключа.

#### 1.4 Архітектура мультисервісної мережі приватного підприємства

АММПП включає різноманітні складові та компоненти, які грають важливу роль у забезпеченні ефективної та надійної роботи мережі, а саме основні елементи такої архітектури МЗ включають сервери, комутатори, маршрутизатори, пристрої безпеки та інші засоби МЗ. Розглянемо кожен з цих елементів більш детально.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		14

Сервери є одним із ключових компонентів МСМПП, і вони відповідають за забезпечення обробки даних МЗ та надання різноманітних сервісів МЗ, таких як електронна пошта, файлообмін, веб-сервери та бази даних МЗ. Сервери МЗ можуть бути фізичними машинами або віртуальними машинами, що працюють на фізичних серверах МЗ [9].

Комутатори МЗ є мережевими пристроями, які використовуються для пересилання даних між пристроями в МЗ, і вони відіграють важливу роль у забезпеченні швидкого та ефективного обміну даними МЗ, а також між різними вузлами МЗ. Комутатори МЗ можуть мати різну кількість портів і можуть бути управляючими або неуправляючими [10].

Маршрутизатори МЗ також є важливими компонентами МСМПП. Вони відповідають за передачу даних між різними сегментами МЗ, вибір найкоротшого шляху для передачі пакетів даних МЗ та забезпечення безпеки МЗ, і контролю трафіку МЗ. Маршрутизатори МЗ можуть підтримувати різні протоколи маршрутизації, такі як OSPF, BGP або EIGRP, що дозволяє ефективно керувати трафіком МЗ.

Пристрої безпеки МЗ, такі як мережеві брандмауери, інтрузійні виявлення та запобігання (IDS/IPS) та віртуальні приватні МЗ (VPN), відіграють критичну роль у забезпеченні безпеки МСМПП. Вони допомагають управляти (керувати) доступом до мережевих ресурсів МЗ, виявляти та запобігати потенційним загрозам безпеки МЗ, а також забезпечувати конфіденційність даних МЗ, переданих через МЗ.

Крім основних компонентів МЗ, існують інші складові архітектури МСМПП, такі як мережеві кабелі, бездротові точки доступу, пристрої для моніторингу та керування МЗ, системи резервного копіювання та відновлення даних МЗ тощо. Всі ці компоненти МЗ співпрацюють між собою, щоб створити ефективну та надійну МЗ, яка задовольняє потреби приватного підприємства.

Загалом, АММПП вимагає уважного розгляду кожної складової та компонента МЗ, щоб забезпечити оптимальну продуктивність МЗ, безпеку та доступність мережевих сервісів МЗ. Конкретний вибір компонентів МЗ та їх

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		15

конфігурація залежить від потреб підприємства, його розміру та специфіки бізнесу. Професійне проектування та налагодження архітектури МСМ є важливим етапом для забезпечення успішної роботи МЗ приватного підприємства [11].

АММПП також може включати інші компоненти МЗ, які сприяють оптимізації функціональності та продуктивності МЗ. Одним з таких компонентів МЗ є мережеві сховища даних або NAS (Network-Attached Storage). NAS МЗ дозволяє централізовано зберігати дані МЗ та надавати доступ до них різним користувачам і пристроям в МЗ. Воно може бути оснащено великою ємністю дискового простору і має можливість резервного копіювання даних МЗ для забезпечення безпеки і надійності інформації МЗ.

Іншим важливим елементом архітектури є система моніторингу МЗ. Ця система включає в себе спеціальне програмне забезпечення МЗ, яке надає можливість відстежувати роботу мережевих компонентів МЗ, аналізувати мережевий трафік МЗ і виявляти проблеми або відхилення від норми МЗ. Моніторинг МЗ допомагає оперативно виявляти та усувати неполадки, покращувати продуктивність МЗ та забезпечувати високий рівень надійності і доступності мережевих послуг для користувачів МЗ.

Успішне функціонування МСМПП також потребує правильного планування IP-адресного простору МЗ. Ефективне управління IP-адресами є важливою складовою архітектури МЗ, особливо в умовах зростаючого числа підключених пристроїв і послуг для МЗ. Застосування методів розподілу та керування IP-адресами МЗ, таких як DHCP (Dynamic Host Configuration Protocol) і IPAM (IP Address Management), дозволяє для МЗ забезпечити ефективне використання IP-ресурсів і уникнути конфліктів адрес в МЗ [12].

Необхідно також звернути увагу на впровадження віртуалізації в архітектурі МЗ. Віртуалізація дозволяє розділити ресурси МЗ на логічні окремість, що сприяє ефективному використанню фізичних ресурсів МЗ, забезпечує гнучкість, масштабованість та забезпечує ізольоване середовище МЗ, тобто для різних послуг і додатків.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		16

Крім того, важливо забезпечити належну захист МЗ та інформації. Для цього використовуються різноманітні пристрої та методи МЗ, такі як файрволи, антивіруси, системи виявлення та запобігання вторгнень (IDS/IPS), шифрування даних МЗ та аутентифікаційні механізми МЗ. Захист МЗ від зовнішніх загроз та зловмисного програмного забезпечення є критично важливим завданням для забезпечення безпеки МЗ та конфіденційності інформації ПП [13].

Всі ці складові та компоненти архітектури МСМПП взаємодіють між собою, створюючи цілісну та динамічну інфраструктуру МЗ. Правильне проектування, розгортання та налагодження такої МЗ є важливими етапами, які вимагають компетентності та досвіду в галузі мережевих технологій (проектування МЗ). Забезпечення надійності, продуктивності та безпеки МЗ є основними пріоритетами для будь-якого ПП, і вірна АММПП грає важливу роль у досягненні цих цілей.

### 1.5 Технології передачі даних в мультисервісних мережах

Технології передачі даних в МСМПП відіграють важливу роль у забезпеченні ефективної комунікації та передачі різноманітних типів даних МЗ у сучасному світі. У цьому тексті розглянемо декілька ключових технологій, які дозволяють забезпечити передачу даних у МСМПП.

Однією з найпоширеніших технологій є комутація пакетів в МЗ. У МСМПП, що підтримують комутацію пакетів МЗ, дані розбиваються на пакети, кожен з яких містить заголовок з необхідною інформацією для маршрутизації в МЗ та призначення. Цей підхід дозволяє ефективно використовувати ресурси МЗ та забезпечити передачу різних типів даних в МЗ, таких як голос, відео, текст та інші, в одній МЗ [14].

Ще однією важливою технологією є комутація каналів в МЗ. У МСМПП, що використовують комутацію каналів МЗ, встановлюється постійний зв'язок між відправником і одержувачем на протязі всього сеансу передачі даних МЗ. Це особливо важливо для реалізації послідовної передачі даних в МЗ, де забезпечується гарантована пропускна здатність МЗ та низька її затримка.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		17

Комутація каналів в МЗ широко використовується в мультимедійних додатках та відеоконференціях [15].

Мережевий протокол MPLS (Multiprotocol Label Switching) в МЗ є ще однією важливою технологією передачі даних в МСМПП. Він дозволяє швидку маршрутизацію пакетів в МЗ за допомогою міток, які додаються до пакетів на рівні мережевого протоколу МЗ. MPLS забезпечує можливість встановлення віртуальних приватних мереж (VPN) МЗ та керування якістю обслуговування (Quality of Service), що робить його ефективним рішенням в МЗ для передачі різних типів даних у МСМПП.

Окрім вищезгаданих технологій МЗ, варто згадати про Ethernet. Це широко використовувана технологія МЗ, що дозволяє передавати дані по локальній МЗ. Ethernet забезпечує високу швидкість передачі даних МЗ і широкий спектр застосувань, включаючи передачу голосу, відео та інших типів даних у МСМПП.

Технології передачі даних в МСМПП постійно розвиваються, і виникають нові інноваційні рішення для проектування МЗ. Наприклад, Software-Defined Networking (SDN) дозволяє централізовано керувати в МЗ мережевими ресурсами та надавати послуги різного типу в МСМПП [16].

Узагальнюючи, технології передачі даних в МЗ, такі як комутація пакетів, комутація каналів, MPLS, Ethernet та інші, грають важливу роль у розвитку МСМ. Ці технології забезпечують ефективну та надійну передачу різних типів даних МЗ, розвиваються та вдосконалюються для задоволення зростаючих потреб користувачів у сфері комунікацій та обміну даними в МЗ [17].

Однак, розвиток технологій передачі даних в МСМПП не зупиняється на досягнутому. В сучасному світі, де швидкість та надійність є критичними факторами МЗ, постійно виникають нові інноваційні рішення для поліпшення передачі даних в МЗ.

Однією з таких технологій МЗ є Network Function Virtualization (NFV), яка дозволяє розділити функції мережевого обладнання МЗ від апаратного забезпечення МЗ і виконувати їх на віртуальних серверах МЗ. Це дозволяє

спростити конфігурацію та керування МЗ, а також забезпечити більшу гнучкість та масштабованість МСМ.

Одним з актуальних напрямків МСМ є так звана Internet of Things (IoT) - Інтернет речей. Ця технологія передбачає підключення різних пристроїв до МЗ, від домашньої техніки до автомобілів, до МЗ з метою обміну даними та взаємодії. Для успішної реалізації Інтернету речей необхідні високошвидкісні МЗ з низькою затримкою та високою стійкістю.

Також, в сучасних МСМПП все більшою популярністю користується технологія Software-Defined Wide Area Network (SD-WAN) для МЗ. Вона дозволяє підключати різні географічно розподілені МЗ та керувати ними централізовано з використанням програмного забезпечення. SD-WAN для МЗ забезпечує більшу гнучкість та ефективність в управлінні її мережевими ресурсами (для МСМ), а також поліпшує якість обслуговування МЗ та забезпечує безпеку передачі даних [18].

Розвиток технологій передачі даних у МСМПП також відбувається у напрямку впровадження штучного інтелекту (AI) та машинного навчання (Machine Learning). Ці технології дозволяють МЗ аналізувати та оптимізувати трафік, передбачати збої та адаптуватися до змінних умов МЗ. Вони допомагають підвищити продуктивність МЗ та забезпечити кращу якість обслуговування для користувачів МЗ.

У майбутньому розвиток МСМ буде спрямований на поєднання цих технологій та впровадження нових концепцій МЗ, таких як 5G мобільні МЗ, квантові МЗ та блокчейн. Це дозволить створити ще більш потужні та гнучкі мультисервісні МЗ, які задовольняють потреби сучасного світу комунікацій та обміну даними в МЗ [19].

## 1.6 Висновки до першого розділу

Компанія "Sigma Software" (ПП) має розташовані відділення по всій Україні, але головний офіс у Харкові на вулиці Академіка Проскури 1 виступає

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		19

центральною точкою ПП, яка об'єднує різні відділи та команди. Головний офіс гарантує ефективну координацію та спільну мету всіх підрозділів ПП компанії "Sigma Software".

МСМ пропонують концепцію створення єдиної інфраструктури МЗ, що може передавати голос, відео-зображення та дані. Це допомагає знизити вартість володіння та підтримки складних процесів передачі даних в МЗ.

Для розробки МСМПП необхідно чітко визначити його потреби та вимоги до МЗ, врахувати особливості об'єктів компанії. АММПП включає основні компоненти, такі як сервери, комутатори, маршрутизатори та інші елементи МЗ. Крім того, використовуються інші компоненти МЗ, наприклад, мережеві кабелі, бездротові точки доступу та системи резервного копіювання та відновлення даних в МЗ. Усі ці компоненти МЗ взаємодіють між собою для створення ефективною та надійною МЗ, яка повністю задовольняє потреби ПП.

Технології передачі даних в МСМПП відіграють важливу роль у забезпеченні ефективною комунікації та передачі різних типів даних МЗ. Один з найпоширеніших підходів - це комутація пакетів в МЗ, яка дозволяє оптимально використовувати ресурси МЗ та забезпечує передачу голосу, відео, тексту та інших типів даних в одному каналі МЗ.

Розвиток технологій передачі даних в МЗ продовжується, і нові розробки, наприклад, Software-Defined Networking (SDN) для МЗ, дають можливість централізовано керувати мережевими ресурсами МЗ та надавати різноманітні послуги у МСМПП. Використання таких інновацій для МЗ допомагає досягти ще більшої ефективності та гнучкості у керуванні МЗ [19].

Отже, розробка МСМ для приватних підприємств, зокрема компанії "Sigma Software", є актуальним та перспективним завданням, оскільки це сприяє ефективному об'єднанню команд в МЗ та підтримці різних типів передачі даних МЗ. Застосування новітніх технологій в МЗ та врахування особливостей ПП допомагає створити ефективну та надійну МЗ, яка відповідає потребам і вимогам ПП.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		20

## 2. ПРОЕКТУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ПРИВАТНОГО ПІДПРИЄМСТВА

### 2.1 Вимоги до мультисервісної мережі приватного підприємства

Для проектування МСМ доступу в офісах ПП "Sigma Software" необхідно вибрати обладнання МЗ та описати умови створення зв'язку в МЗ.

В якості виробника комунікаційного обладнання для створення МСМ ПП, було обрано дві компанії, які на сьогоднішній день є одними з провідних гравців на ринку розробки телекомунікаційного обладнання та МЗ, і відома своєю надійністю та якістю продукції, а саме MikroTik та Cisco [20].

Прийнято рішення використати наступне обладнання для МСМ:

1. Маршрутизатор МСМПП середнього офісу MikroTik RB1100AHx4.
2. Маршрутизатор МСМПП середнього офісу MikroTik CCR1036-12G-4S.
3. Комутатор МСМПП MikroTik CRS328-24P-4S+RM.
4. VoIP шлюз для МСМПП Cisco SPA112.
5. Платформа для МСМПП Cisco ME 3400E.
6. IP-телефон до МСМПП серії Cisco 7841.
7. Відеокамери до МСМПП АНД.
8. Принтер для МСМПП.
9. Сканер для МСМПП.
10. Точка доступу WiFi для МСМПП.
11. Персональний комп'ютер МСМПП.
12. Ноутбук МСМПП.

2.2 Розробка структурної схеми організації зв'язку мультисервісної мережі приватного підприємства

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		21

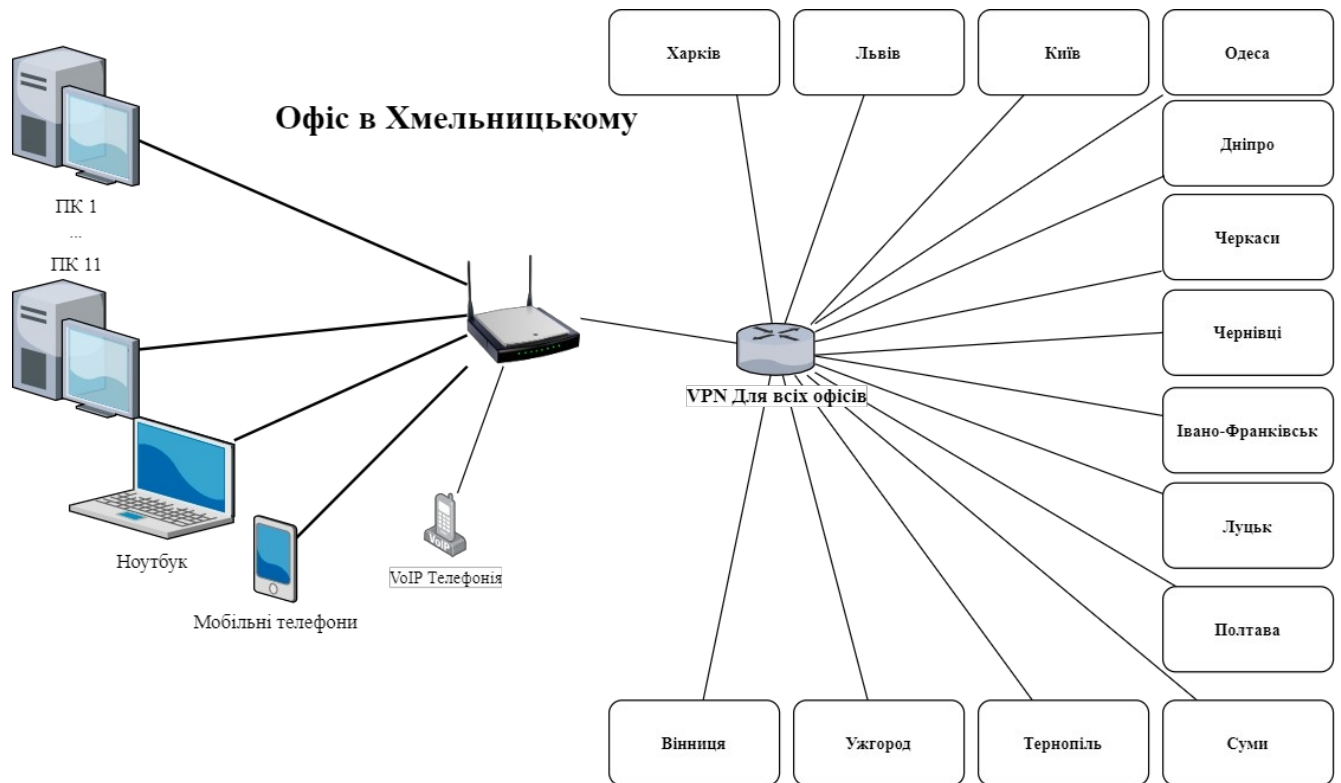


Рисунок 2.1 - Схема організації зв'язку МСМПП Хмельницького філіалу

На цьому рисунку основним компонентом МЗ є платформа Cisco ME 3400E, яка включає в себе маршрутизатор МЗ головного офісу та VoIP шлюз МЗ. Ця платформа розташована на майданчику філії в Харкові МЗ. Вона відповідає за забезпечення з'єднання МЗ з загальнодоступною МЗ та з маршрутизатором середнього офісу МЗ, що розташований на майданчику по вулиці Академіка Проскури 1. Крім того, платформа забезпечує з'єднання МЗ з іншими філіями за допомогою МЗ VPN. Нижче наведено детальний опис обладнання МЗ та його характеристики.

### 2.3 Розрахунок навантаження для мультисервісної мережі приватного підприємства

Для розрахунку навантажень МЗ використовувалися офіси розташовані у Харкові та Львові. Кількість абонентів МЗ в цих офісах складала приблизно 450 та 300 відповідно. У проєктованій МЗ основну пропускну здатність МЗ займали

послуги IP-телефонії, передачі даних всередині МЗ, IPTV та доступ до глобального Інтернету (послуги Triple Play). Для інших послуг необхідна менша пропускна здатність МЗ [21]. З урахуванням цього, розраховувалася необхідна пропускна здатність МЗ для послуг Triple Play, а також враховувався додатковий резерв МЗ для інших послуг. Для правильної оцінки характеристик МЗ та розрахунку необхідної пропускної здатності МЗ для комплексної послуги Triple Play використовуються параметри МЗ, що базуються на статистичних даних МЗ, адаптованих до ринку зв'язку. Проектована МСМПП повинна бути надійною і не перевантаженою, тому всі розрахунки трафіку МЗ проводяться для години з найбільшим навантаженням МЗ, а саме для одного оптичного мережного вузла МЗ.

Для надання послуги IP-телефонії в МЗ необхідно розрахувати потрібну пропускну здатність МЗ. Для цього маємо наступні вихідні дані МЗ:

1. Кількість джерел навантаження МЗ - абоненти, які використовують термінали SIP та підключаються до пакетної МЗ за допомогою мультисервісного абонентського концентратора МЗ. Кількість абонентів МЗ для розрахунку складає 450 та 300 відповідно.
2. Тип кодека МЗ, який планується використовувати - G.729A.
3. Довжина заголовка IP-пакета МЗ - 58 байт.

Необхідний транспортний ресурс МЗ для передачі телефонного трафіку МЗ в пакетній МЗ на концентраторі визначається таким чином:

$$U_{\text{користності}} = \frac{t_{\text{звучання голосу}} \cdot v_{\text{кодування}}}{8 \text{ біт/байт}} \quad (2.1)$$

де  $t_{\text{звучання голосу}}$  – час звучання голосу (мс),  $v_{\text{кодування}}$  – швидкість кодування мовного сигналу (Кбіт/с)

Ці параметри МЗ відображають характеристики використовуваного кодека для МЗ. У даному випадку, для кодека МЗ G.729A, швидкість кодування становить 8 кбіт/с, а час звучання голосу - 20 мс.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		23

$$Y_{\text{кор.}} = \frac{20 \cdot 8}{8} = 20 \text{ байт}$$

Розмір заголовка кожного пакета в МЗ складає 58 байтів. Отже, загальний розмір голосового пакета в МЗ буде:

$$V_{\text{пакета}} = L_{\text{Eth}} + L_{\text{IP}} + L_{\text{UDP}} + L_{\text{RTP}} + Y_{\text{кор.}} - \text{байт} \quad (2.2)$$

де  $L_{\text{Eth}}$ ,  $L_{\text{IP}}$ ,  $L_{\text{UDP}}$ ,  $L_{\text{RTP}}$  - довжина заголовків протоколів МЗ Ethernet, IP, UDP, RTP відповідно (у байтах),  $Y_{\text{кор.}}$  - корисне навантаження голосового пакета МЗ (у байтах).

$$V_{\text{пакета}} = 14 + 20 + 8 + 16 + 20 = 78 \text{ байт}$$

Використання кодека в МЗ G.729А дозволяє передавати через шлюз 50 пакетів на секунду. Враховуючи це, смуга пропускання МЗ для одного виклику визначається за допомогою такої формули:

$$\text{ППр}_1 = V_{\text{пакета}} \cdot 8 \text{ біт/байт} \cdot 50_{\text{pps}}, \text{ Кбіт/секунду}, \quad (2.3)$$

де розмір голосового пакета МЗ позначається як  $V_{\text{пакета}}$  і вимірюється в байтах.

$$\text{ППр}_1 = 78 \cdot 8 \cdot 50 = 30 \text{ Кбіт/секунду}.$$

У проєктованій МЗ, а саме мультисервісній комутаційній системі (МСС) розгортається точка присутності з наявністю 450 та 300 голосових портів. За допомогою засобів МЗ придушення пауз можливо стиснути звичайний голосовий виклик приблизно на 50 відсотків (за консервативною оцінкою – 30%). Враховуючи ці дані, необхідна смуга пропускання МЗ -WAN для нашої точки присутності буде:

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		24

$$\text{ППр}_{WAN} = \text{ППр}_1 \cdot N_{SIP} \cdot VAD = 30\text{Кбіт/секунду}. \quad (2.4)$$

де  $\text{ППр}_1$  - смуга пропускання МЗ одного виклику (кбіт/с),  $N_{SIP}$  - кількість голосових портів МЗ у точці присутності (шт),  $VAD$  (Voice Activity Detection) - коефіцієнт механізму виявлення активності голосу МЗ (0,7).

$$\text{ППр}_{WAN} = 30 \cdot 450 \cdot 0,7 = 9450\text{біт/секунду}.$$

$$\text{ППр}_{WAN} = 30 \cdot 300 \cdot 0,7 = 6300\text{біт/секунду}.$$

Результати можуть відрізнятися, якщо були використані інші методи кодування/декодування (CODEC) в МЗ або якщо змінилася середня тривалість викликів. Крім того, тип використовуваної програми може також вплинути на кінцевий результат МЗ. Наприклад, у випадку передачі музики абоненту в МЗ, який очікує відповіді оператора, можуть бути обмежені можливості використання засобів придушення пауз [22].

МЗ та передачі даних призначені для спільного доступу користувачів до ресурсів комп'ютерів (інфокомунікаційних систем). В якості виробника комунікаційного обладнання для МЗ, таких як додатки, файли, принтери та інше, а також для передачі мультимедійного трафіку в МЗ. Трафік, що генерується цими традиційними послугами МЗ, має свої особливості та відрізняється від трафіку повідомлень у телефонних МЗ чи кабельних телевізійних МЗ. Трафік комп'ютерних даних МЗ характеризується нерівномірною інтенсивністю надходження повідомлень до МЗ [23]. Коефіцієнт пульсації трафіку окремого користувача МЗ, який визначається відношенням середньої інтенсивності обміну даними до максимально можливої, може досягати значень 1:50 або навіть 1:100. Однак, якщо кількість абонентів, обслуговуваних комутаторами МЗ, є достатньо великою, то пульсації окремих абонентів МЗ розподіляються в часі відповідно до закону великих чисел, і піки їх активності не збігаються. Це призводить до значного зниження коефіцієнта пульсації в МЗ на головних каналах передачі даних. Загалом, в годину найбільшого навантаження МЗ буде активними лише певна частина

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		25

абонентів (активні абоненти) МЗ, які передають дані. Навіть під час піку навантаження кількість активних абонентів МЗ може змінюватися, тому для їх обліку використовується п'ятихвилинний часовий інтервал всередині години найбільшого навантаження МЗ, і максимальна кількість активних абонентів МЗ протягом цього періоду визначається параметром Data Average Activity Factor (DAAF) МЗ. Таким чином, кількість активних абонентів МЗ буде розраховуватися на основі DAAF та буде становити

$$AS = TS * DAAF \text{ абонентів} \quad (2.5)$$

де  $TS$  - кількість абонентів МЗ на одному мережевому вузлі,  $DAAF$  - відсоток абонентів МЗ, які перебувають у мережі найбільшого навантаження (ЧНН).

$$AS = (450/9.4) * 0.9 = 43 \text{ абонента}$$

$$AS = (300/6.3) * 0.9 = 43 \text{ абонента}$$

Абоненти МЗ іноді передають і приймають дані, і, як правило, обсяг переданих даних в МЗ значно менший за обсяг прийнятих даних МЗ. Метою КвР є забезпечення заявленої пропускної здатності МЗ для кожного її абонента. Для досягнення цієї мети, необхідно визначити середню пропускну здатність МЗ, яка забезпечить нормальну роботу користувачів МЗ [24]. Зокрема, проведемо розрахунок середньої пропускної здатності МЗ для прийому даних:

$$BDDA = (AS * ADBS) * (1 + OHD), \text{ Мбіт/с}, \quad (2.6)$$

де  $AS$  представляє кількість активних абонентів МЗ (аб),  $ADBS$  означає середню швидкість прийому даних МЗ (в Мбіт/с), а  $OHD$  вказує на відношення довжини заголовка IP пакета МЗ до його загальної довжини вхідного потоку МЗ.

$$BDDA = (43 * 2) * (1 + 0,1) = 94,6 \text{ Мбіт/с}$$

$$BDDA = (43 * 2) * (1 + 0,1) = 94,6 \text{ Мбіт/с}$$

Середня пропускна здатність передачі даних МЗ

$$BUDA = (AS * AUBS) * (1 + OHU), \text{ Мбіт/с}, \quad (2.7)$$

де AS представляє кількість активних абонентів МЗ (аб), AUBS означає середню швидкість передачі даних МЗ (в Мбіт/с), а OHU вказує на відношення довжини заголовка IP пакета МЗ до його загальної довжини у вихідному потоці МЗ.

$$BUDA = (43 * 0,5) * (1 + 0,15) = 24,725 \text{ Мбіт/с}$$

$$BUDA = (43 * 0,5) * (1 + 0,15) = 24,725 \text{ Мбіт/с}$$

Пікова пропускна здатність МЗ визначається кількістю абонентів МЗ, які одночасно передають або приймають дані протягом короткого проміжку часу. Коефіцієнт Data Peak Activity Factor (DPAF) МЗ визначається кількістю таких абонентів МЗ під час години з найбільшим навантаженням [25]. Цей коефіцієнт відображає ступінь активності абонентів МЗ під час пікового навантаження і є важливим фактором при визначенні пропускної здатності МЗ.

$$PS = AS * DPAF, \text{ аб}, \quad (2.8)$$

де DPAF (Data Peak Activity Factor) МЗ - це відсоток абонентів МЗ, які одночасно здійснюють передачу або отримання даних протягом короткого проміжку часу. Цей показник відображає ступінь активності абонентів МЗ під час пікового навантаження МЗ і має велике значення при визначенні пропускної здатності МЗ. Чим вищий відсоток DPAF в МЗ, тим більша кількість абонентів МЗ зайнята передачею або отриманням даних МЗ одночасно, що впливає на необхідну пропускну здатність МЗ.

$$PS = 43 * 0,7 = 30 \text{ абонентів МЗ}$$

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		27

$$PS = 43 * 0,7 = 30 \text{ абонентів МЗ}$$

Пікова пропускна здатність МЗ вимірюється протягом короткого проміжку часу, зазвичай однієї секунди, і вона є необхідною для прийому та передачі даних МЗ в той момент, коли декілька користувачів МЗ одночасно здійснюють передачу або отримання даних через МЗ [26]. Щоб забезпечити плавну роботу МЗ, необхідно визначити пікову пропускну здатність МЗ для прийому даних протягом години, коли спостерігається найбільше навантаження МЗ:

$$BDDP = (PS * PDBS) * (1 + OHD), \text{ Мбіт/с}, \quad (2.9)$$

де PDBS - пікова швидкість прийому даних, Мбіт/с.

$$BDDP = (30 * 3) * (1 + 0,1) = 99 \text{ Мбіт/с}$$

$$BDDP = (30 * 3) * (1 + 0,1) = 99 \text{ Мбіт/с}$$

Пікова пропускна здатність МЗ для передачі даних у ЧПН визначається протягом короткого проміжку часу, зазвичай однієї секунди, і вона є необхідною для ефективної передачі даних МЗ в той самий момент, коли кілька користувачів МЗ одночасно активно використовують МЗ [27]. Забезпечення оптимальної пропускної здатності МЗ у ЧПН дозволяє забезпечити швидку та безперебійну передачу даних МЗ, задовольняючи потреби користувачів МЗ та забезпечуючи ефективне використання мережних ресурсів МЗ:

$$BUDP = (PS * PUBS) * (1 + OHU), \text{ Мбіт/с}, \quad (2.10)$$

де PUBS - це пікова швидкість передачі даних МЗ, вимірювана у Мбіт/с.

$$BUDP = (30 * 1,5) * (1 + 0,15) = 51,75 \text{ Мбіт/с}$$

$$BUDP = (30 * 1,5) * (1 + 0,15) = 51,75 \text{ Мбіт/с}$$

При розрахунку МЗ встановлено, що пікова пропускна здатність МЗ для передачі даних перевищує середню пропускну здатність МЗ [27]. Це означає, що в певні моменти часу в МЗ відбувається інтенсивна передача даних, що перевищує середнє навантаження МЗ.

При проектуванні МСМ важливо враховувати максимальне значення пропускної здатності МЗ, яке включає як пікові, так і середні значення МЗ. Це необхідно для запобігання перевантаження МСМ та забезпечення її надійної роботи в умовах збільшеного трафіку МЗ [28]. Підбираючи максимальне значення смуги пропускання МЗ, гарантується, що МЗ зможе ефективно обробляти навантаження МЗ навіть в пікові періоди, забезпечуючи задану якість обслуговування МЗ.

$$BDD = \text{Max} [BDDA; BDDP], \text{ Мбіт/с}, \quad (2.11)$$

$$BDU = \text{Max} [BUDA; BUDP], \text{ Мбіт/с}, \quad (2.12)$$

де BDD – пропускна здатність МЗ для прийому даних (Мбіт/с), BDU – пропускна здатність передачі даних МЗ, [Мбіт/с].

$$BDD = \text{Max} [94,6; 99] = 99 \text{ Мбіт/с},$$

$$BDU = \text{Max} [24,725; 51,75] = 51,75 \text{ Мбіт/с}$$

$$BDD = \text{Max} [94,6; 99] = 99 \text{ Мбіт/с},$$

$$BDU = \text{Max} [24,725; 51,75] = 51,75 \text{ Мбіт/с}$$

Загальна пропускна здатність МЗ для прийому та передачі даних, необхідна для нормального функціонування в МЗ оптичного мережного вузла, і складе

$$BD = BDD + BDU, \text{ Мбіт/с}, \quad (2.13)$$

де BDD – максимальна пропускна спроможність МЗ прийому даних, (Мбіт/с), BDU – максимальна пропускна здатність МЗ передачі даних, (Мбіт/с).

$$BD = 99 + 51,75 = 150,75 \text{ Мбіт/с}$$

Отже, передачі даних між абонентами МЗ одному мережевому вузлі МЗ у Києві необхідна смуга пропускання 150,75 Мбіт/с.

$$BD = 99 + 51,75 = 150,75 \text{ Мбіт/с}$$

Виходить, що для передачі даних між абонентами МЗ до одного мережевого вузла у Вишневому також необхідна смуга пропускання МЗ 150,75 Мбіт/с.

При розрахунку параметрів проекрованої МСМПП, враховано наступні вихідні дані:

- Тільки 10% від загальної кількості користувачів МЗ можуть одночасно перебувати в МЗ.
- З цих 10%, 20% спостерігається протягом години найбільшого навантаження (ЧПН).
- З цих 20%, лише 25% здійснюють передачу даних в МЗ.

Ці дані є ключовими для нашого розрахунку та проектування МСМПП. Визначимо кількість активних користувачів МЗ, що працюють на середній швидкості за формулою:

$$N_{act\ subser} = NHP * DP * DAAF, \text{ аб,} \quad (2.14)$$

У формулі використовуються наступні позначення: NHP, що означає загальну кількість абонентів МЗ, що користуватимуться проективною МСМПП; DP, що вказує на характеристику проникнення трафіку даних в МСМПП; та DAAF, що є фактором активності МСМПП [29].

$$N_{act\ subser} = 450 * 0,1 * 0,2 = 9 \text{ абонентів}$$

$$N_{act\ subser} = 300 * 0,1 * 0,2 = 6 \text{ абонентів}$$

Далі розраховується кількість абонентів МЗ, які одночасно приймають і передають дані в МЗ, використовуючи наступну формулу:

$$Peak_{subser} = NHP * DP * DPeakAF, \text{ аб} \quad (2.15)$$

$$Peak_{subser} = 450 * 0,1 * 0,1 = 4 \text{ абонента}$$

$$Peak_{subser} = 300 * 0,1 * 0,1 = 3 \text{ абонента}$$

Для визначення необхідної пропускної здатності МЗ, яка потрібна для середнього і пікового трафіку МЗ, розраховується пропускна здатність в ЧНН для висхідного і низхідного трафіку МЗ, а потім обрати максимальне значення серед них.

$$BWDA (N BWA) (OH) = act\ subser * per\ subser * 1+, \text{ Мбіт/с}, \quad (2.16)$$

$$BWDPeak (Peak BWP) (OH) = subser * per\ subser * 1+, \text{ Мбіт/с}. \quad (2.17)$$

У формулі використовуються наступні позначення:  $BWA_{per\ subser}$ , що означає середню пропускну здатність МЗ, що припадає на одного абонента МЗ (1800 кбіт/с);  $BWP_{per\ subser}$  – пікову пропускну здатність на одного абонента МЗ (4000 кбіт/с);  $OH$  – відношення довжини заголовка до довжини пакета МЗ (0,1).

$$BWDA = (9 * 1800) * (1 + 0,1) = 17,4, \text{ Мбіт/с},$$

$$BWDA = (6 * 1800) * (1 + 0,1) = 11,6 \text{ Мбіт/с}$$

$$BWDPeak = (4 * 4000) * (1 + 0,1) = 17,2, \text{ Мбіт/с}$$

$$BWDPeak = (3 * 4000) * (1 + 0,1) = 12,9, \text{ Мбіт/с}$$

Для визначення необхідної смуги пропускання МЗ, в якій максимальне значення буде враховане, порівнюємо пікову та середню пропускну здатність МЗ та оберемо більше з них:

$$BWData = \text{MAX}[BWDA; BWDPeak], \text{ Мбіт/с} \quad (2.18)$$

$$BWData = \text{MAX}[17,4; 17,2] = 17,4 \text{ Мбіт/с}$$

$$BWData = \text{MAX}[11,6; 12,9] = 12,9 \text{ Мбіт/с}$$

У такий спосіб, з метою забезпечення доступу до глобальної МЗ Інтернет, необхідно мати пропускну здатність МЗ проєктованого вузла у Харкові, яка становить 17,4 Мбіт/с, тоді як у Львові ця пропускну здатність МЗ має складати 12,9 Мбіт/с.

Загальна пропускну здатність МЗ вузла для кожного офісу буде розраховуватись наступним чином:

$$\text{ППр Triple play} = \text{ППрWAN} + \text{BD} + \text{BWData}, \text{ Мбіт/с}, \quad (2.19)$$

Зараз між місцями випуску та прийому контенту МЗ намагаються зберегти баланс на вузлі доступу так, щоб не виникало вузьких місць, а під час розподілу ширини пропускання МЗ [29] між послугами МЗ враховують різні фактори, такі як ППрWAN, яке відображає пропускну спроможність для трафіку ІР телефонії МЗ в Мбіт/с, АВ, що відповідає пропускну здатності МЗ для відеопотоків в Мбіт/с, ВD - пропускну здатності для трафіку даних МЗ в Мбіт/с та BWData, яка визначає пропускну спроможність МЗ для надання послуг доступу до МЗ Інтернет в Мбіт/с.

$$\text{ППр Triple play} = 21,231 + 178,2 + 48,4 = 247,831 \text{ Мбіт/с}$$

$$\text{ППр Triple play} = 21,231 + 178,2 + 48,4 = 247,831 \text{ Мбіт/с}$$

## 2.4 Апаратно-програмні засоби для мультисервісної мережі приватного підприємства

Віртуальна приватна мережа МСМПП (VPN) надає можливість забезпечити безпечний та зашифрований віддалений доступ до різноманітних філій МЗ з будь-якого місця [30]. Шляхом використання різних профілів VPN МСМПП можна налаштувати з'єднання для різноманітних типів пристроїв МЗ, включаючи комп'ютери МЗ, ноутбуки, смартфони, планшети та інші пристрої МЗ. У представленій таблиці 2.1. наведена докладна інформація про підтримувані типи з'єднань для кожної з платформ МЗ, що дозволяє вибрати оптимальний метод підключення залежно від потреб та характеристик кожного пристрою МЗ.

Таблиця 2.1. - Список можливостей VPN МСМПП

Тип підключення МСМПП	iOS и Mac OS X для МЗ	Android для МЗ	Windows 8.1 для МЗ	Windows RT для МЗ	Windows RT 8.1 для МЗ	Windows Phone 8.1 для МЗ	Windows 10 Desktop и Mobile для МЗ
Cisco AnyConnect	Так	Так	Ні	Ні	Ні	Так (OMA-URI)	Так (OMA-URI)
Pulse Secure	Так	Так	Так	Ні	Так	Так	Так
F5 Edge Client	Так	Так	Так	Ні	Так	Так	Так

Dell SonicWALL Mobile Connect	Так	Так	Так	Ні	Так	Так	Так
CheckPoint Mobile VPN	Так	Так	Так	Ні	Так	Так	Так
Microsoft SSL (SSTP)	Ні	Ні	Так	Так	Так	Ні	Ні
Microsoft Automatic	Ні	Ні	Так	Так	Так	Ні	Так (OMA-URI)
IKEv2	Так (налаштовувалась політика)	Ні	Так (OMA-URI)	Так (OMA-URI)	Так (OMA-URI)	Так (OMA-URI)	Так (OMA-URI)
PPTP	Так (налаштовувалась політика)	Ні	Так (OMA-URI)	Так (OMA-URI)	Так (OMA-URI)	Ні	Так (OMA-URI)

Для забезпечення віддаленого доступу до МЗ необхідно мати комп'ютери (інфокомунікаційні системи) з двома мережевими підключеннями в МЗ: до публічної МЗ і до захищеної МЗ. На даному ПП планується використання операційної системи Windows Server 2008, яка надає функції маршрутизації в МЗ та віддаленого доступу. Коли клієнтський комп'ютер (інфокомунікаційна система)

підключається до віртуальної приватної МЗ (VPN), обидва комп'ютери будуть шифрувати всі передані між ними дані в МЗ [31].

*Підбір необхідного обладнання МЗ:* Для побудови МЗ було обрано сучасне телекомунікаційне обладнання, яке відповідає сучасним тенденціям у світі телекомунікацій. Корпоративні маршрутизатори МЗ, призначені для використання корпоративними користувачами, забезпечують нормальне функціонування МЗ. Для цих цілей вибрано компанії MikroTik та Cisco, їхні маршрутизатори МЗ володіють широким спектром функціональних можливостей, які відповідають потребам сучасних ПП. Вони забезпечують стабільну та безпечну передачу даних МЗ, забезпечуючи високу продуктивність і масштабованість МЗ. Корпоративні маршрутизатори МЗ від MikroTik та Cisco є надійними партнерами для ПП, які прагнуть забезпечити ефективну роботу своєї МЗ [32].

MikroTik RB1100AHx4 є потужним маршрутизатором МЗ з 13 GE портами, який працює на процесорі Annapurna Alpine AL21400 з чотирма ядрами Cortex A15, тактовою частотою 1.4 ГГц кожне, такі маршрутизатори для МЗ забезпечують максимальну пропускну спроможність МЗ до 7.5 Гбіт/с, що дозволяє швидко обробляти великі обсяги даних МЗ [33].

Одним з переваг MikroTik RB1100AHx4 для МЗ є підтримка апаратного прискорення IPsec з можливістю досягнення швидкості МЗ до 2.2 Гбіт/с з AES128. Це забезпечує безпечну і швидку передачу даних МЗ за допомогою шифрування.

Також маршрутизатор МЗ оснащений слотом для microSD, що дозволяє розширити його пам'ять зберігання і забезпечити зручне зберігання даних в МЗ. Крім того, пристрій має порт RS2321, що дозволяє підключати гарнітуру або інші зовнішні пристрої МЗ для комунікації та управління [34].

Завдяки своїм потужним характеристикам для МЗ і розширеним можливостям, MikroTik RB1100AHx4 в МЗ є надійним вибором для вимогливих МЗ і забезпечує стабільну роботу та швидкість передачі даних в МЗ. і у сучасних мережевих середовищах.

MikroTik RB1100AHx4 МЗ також пропонує розширений набір функцій, включаючи інтегрований маршрутизатор МЗ, фаїрвол, VPN-сервер МЗ та інші

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		35

можливості для ефективного керування МЗ. Цей маршрутизатор МЗ також підтримує різні протоколи маршрутизації і мережеві стандарти в МСМПП, забезпечуючи сумісність з різноманітними пристроями та системами МСМПП.

Загалом, MikroTik RB1100AHx4 МЗ є потужним і надійним маршрутизатором, який відповідає вимогам високошвидкісних МЗ і забезпечує стабільну та безпечну передачу даних МЗ. Він є ідеальним вибором для організацій і ПП, які потребують надійного і ефективного мережевого обладнання в МСМПП.

Його характеристики в зручному вигляді представлені у таблиці 2.2.

Таблиця 2.2. - Характеристики маршрутизатора МСМПП MikroTik RB1100AHx4

Характеристика	Значення
Архітектура маршрутизатора МСМПП	ARM 32bit
CPU маршрутизатора МСМПП	AL21400
Кількість ядер CPU маршрутизатора МСМПП	4
Номінальна частота CPU маршрутизатора МСМПП	1.4 ГГц
Модель комутатора маршрутизатора МСМПП	RTL8367
Розміри маршрутизатора МСМПП	443 x 148 x 44 мм
Ліцензія RouterOS маршрутизатора МСМПП	6
ОС маршрутизатора МСМПП	RouterOS
Розмір ОЗП маршрутизатора МСМПП	1 ГБ
Розмір пам'яті маршрутизатора МСМПП	128 МБ
Тип пам'яті маршрутизатора МСМПП	NAND
Кількість АС входів маршрутизатора МСМПП	2
Кількість DC входів маршрутизатора МСМПП	2 (2-контактний термінал, PoE-IN)
Вхідна напруга 2-контактного терміналу маршрутизатора МСМПП	-48, 12-57 В
Максимальне споживання енергії маршрутизатора МСМПП	20 Вт

Тип охолодження маршрутизатора МСМПП	Пасивне
PoE in маршрутизатора МСМПП	802.3af/at
Вхідна напруга PoE in маршрутизатора МСМПП	20-57 В
Кількість GE портів маршрутизатора МСМПП	13
Тип карти пам'яті маршрутизатора МСМПП	microSD
Карти пам'яті маршрутизатора МСМПП	1
Порт для гарнітури маршрутизатора МСМПП	RS232
Апаратне прискорення IPsec маршрутизатора МСМПП	Так

Маршрутизатор МСМПП середнього офісу MikroTik CCR1036-12G-4S. MikroTik CCR1036-12G-4S МСМПП є потужним маршрутизатором МЗ з 12 GE портами і 4 SFP портами, призначеним для високопродуктивних МЗ. Цей маршрутизатор МЗ використовує процесор Tile 36 core з тактовою частотою 1.2 ГГц на кожному ядрі, що забезпечує високу продуктивність та максимальну пропускну спроможність МСМПП до 16 Гбіт/с. Додатково, пристрій підтримує апаратне прискорення в МСМПП IPsec з AES128, що дозволяє досягти швидкості МЗ до 3.2 Гбіт/с.

MikroTik CCR1036-12G-4S МЗ має вбудований слот для microSD, що дозволяє розширити обсяг пам'яті для зберігання даних в МЗ. Також наявний порт RJ45 для підключення гарнітури та інших пристроїв в МЗ, що спрощує управління та налагодження маршрутизатора МСМПП [35].

Цей маршрутизатор МСМПП володіє надійними характеристиками, включаючи 12 GE портів для швидкого та стабільного підключення пристроїв МЗ, а також 4 SFP портів для підключення оптичних модулів МЗ. Ліцензія RouterOS надає розширені можливості управління та налаштування МЗ.

Маршрутизатор МСМПП, завдяки своїм потужним характеристикам та розширеним функціональним можливостям, є ідеальним рішенням для високопродуктивних МЗ, де важлива швидкість, надійність та розширені

можливості управління МЗ. Застосування такого маршрутизатора МСМПП дозволяє забезпечити ефективне та стабільне функціонування МЗ з високою пропускнуою спроможністю.

Таблиця 2.3. - Характеристики маршрутизатора МСМПП MikroTik CCR1036-12G-4S

Характеристика	Значення
Архітектура маршрутизатора МСМПП	TILE
CPU маршрутизатора МСМПП	TLR4-03680
Кількість ядер CPU маршрутизатора МСМПП	36
Номінальна частота CPU маршрутизатора МСМПП	1.2 ГГц
Розміри маршрутизатора МСМПП	443 x 193 x 44 мм
Ліцензія RouterOS маршрутизатора МСМПП	6
ОС маршрутизатора МСМПП	RouterOS
Розмір ОЗП маршрутизатора МСМПП	4 ГБ
Розмір пам'яті маршрутизатора МСМПП	1 ГБ
Тип пам'яті маршрутизатора МСМПП	NAND
Кількість АС входів маршрутизатора МСМПП	2
Діапазон АС входу маршрутизатора МСМПП	100-240 В
Максимальне споживання енергії маршрутизатора МСМПП	60 Вт
Тип охолодження маршрутизатора МСМПП	2 вентилятори
Кількість GE портів маршрутизатора МСМПП	12
SFP DDMI маршрутизатора МСМПП	Так
Кількість SFP портів маршрутизатора МСМПП	4
Порт для гарнітури маршрутизатора МСМПП	RJ45
Кількість USB портів маршрутизатора МСМПП	1
USB Power Reset маршрутизатора МСМПП	Так
Тип слоту USB маршрутизатора МСМПП	USB type A
Максимальний струм USB (А) маршрутизатора МСМПП	1

Вип.	Аркуш	№ Докум.	Підпис	Дата

КвРТР.2019018.01.017.ПЗ

Арк.

38

Карти пам'яті маршрутизатора МСМПП	microSD
Апаратне прискорення IPsec маршрутизатора МСМПП	Так

Комутатор МЗ MikroTik CRS328-24P-4S+RM - це сучасний комутатор МЗ з 24 GE портами і 4 SFP+ портами, який може задовольнити різні потреби в МСМПП. Ви можете використовувати його як звичайний комутатор для МСМПП з операційною системою SwOS або як потужний маршрутизатор МЗ з операційною системою RouterOS. Зручною функцією є можливість швидко перемикатися між цими двома операційними системами за допомогою спеціальної кнопки або налаштувань RouterBOOT.

Одним з ключових переваг комутатора МЗ є гнучкість в плані живлення. Ви можете жити ваше обладнання МЗ, що підтримує PoE, за допомогою різних методів МЗ, таких як Passive PoE для МЗ, low voltage PoE для МЗ, 802.3af/at для МЗ (Type 1 "PoE" / Type 2 "PoE+") з автоматичним визначенням. Підтримується передача в МСМПП PoE-Out через режим В піни (4,5+) (7,8-). Кожен порт комутатора МЗ може надавати до 30 Вт високої напруги або 26 Вт низької напруги. Крім того, комутатор МЗ має вбудований блок живлення 100-240 В АС 500 Вт, який споживає до 44 Вт, забезпечуючи гарантовану потужність 450 Вт (3x150 Вт на кожному 8 Ethernet портів) для живлення обладнання МЗ, що підтримує PoE.

Щодо продуктивності, цей комутатор МСМПП оснащений процесором ARM 32bit з тактовою частотою 800 МГц і 512 МБ оперативної пам'яті. Він підтримує апаратне прискорення для МЗ IPsec і може досягати пропускної спроможності МЗ до 16 Гбіт/с. Також є слот для карти пам'яті microSD і порт RJ45 для консольного доступу. На передній панелі комутатора МЗ розміщений LCD-екран, який відображає статус пристрою МЗ і дозволяє налаштовувати параметри МСМПП [36].

MikroTik CRS328-24P-4S+RM МСМПП - це надійний комутатор МЗ з розширеним функціоналом і доступною ціною, тобто ви можете використовувати його для будь-яких завдань, пов'язаних з комутацією або маршрутизацією МЗ.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		39

Також ви можете використовувати переваги для МЗ операційних систем RouterOS або SwOS, в залежності від вашого сценарію використання МСМПП [37].

Таблиця 2.4. - Характеристики комутатора МСМПП MikroTik CRS328-24P-4S+RM

<b>Характеристика</b>	<b>Значення</b>
Архітектура комутатора МСМПП	ARM 32bit
CPU комутатора МСМПП	98DX3236
Кількість ядер CPU комутатора МСМПП	1
Номінальна частота CPU комутатора МСМПП	800 МГц
Модель комутатора МСМПП	98DX3236
Розміри комутатора МСМПП	443 x 300 x 44 мм
Ліцензія RouterOS комутатора МСМПП	5
ОС комутатора МСМПП	RouterOS / SwitchOS (Dual boot)
Розмір ОЗП комутатора МСМПП	512 МБ
Розмір пам'яті комутатора МСМПП	16 МБ
Тип пам'яті комутатора МСМПП	FLASH
Кількість АС входів комутатора МСМПП	1
Діапазон АС входу комутатора МСМПП	100-240 В
Максимальне споживання енергії комутатора МСМПП	494 Вт
Максимальне споживання енергії без додатків комутатора МСМПП	44 Вт
Тип охолодження комутатора МСМПП	2 вентилятори
Кількість GE портів комутатора МСМПП	24
SFP DDMI комутатора МСМПП	Так
Кількість SFP+ портів комутатора МСМПП	4
Порт для гарнітури комутатора МСМПП	RJ45
Карти пам'яті комутатора МСМПП	microSD

Платформа МСМПП Cisco ME 3400E - це комутатори МЗ доступу до Ethernet наступного покоління для сервіс-провайдерів, які пропонують високу доступність МЗ і гнучкість послуг МЗ для бізнес-доступу до Carrier Ethernet. Вони базуються на широко використовуваних комутаторах МЗ доступу Cisco ME 3400 Series Ethernet і допомагають сервіс-провайдерам МЗ надавати чотири ключові атрибути, які необхідні для послуг МЗ, а саме Carrier Ethernet наступного покоління МЗ: доступність, гнучкість, керованість і безпека МЗ [38].

Серія Cisco ME 3400E МСМПП включає три моделі для МЗ, які розширюють можливості комутації МЗ і забезпечують різноманітні опції для різних вимог МЗ і їх сценаріїв використання. Перша модель для МЗ, Cisco ME 3400EG-12CS, оснащена 12 двоцільними портами (10/100/1000 і SFP), а також чотирма SFP-портами підключення, і двома слотами для змінних блоків живлення і вентилятора. Ця модель для МЗ є ідеальним вибором для сервіс-провайдерів, які потребують великої кількості портів і гнучкості в налаштуванні живлення МЗ.

Друга модель для МЗ, Cisco ME 3400EG-2CS, має два двоцільні порти (10/100/1000 і SFP), два SFP-порти підключення і вбудований блок живлення АС. Цей комутатор МСМПП є ідеальним рішенням для середніх розмірів МЗ, які потребують надійного живлення і невеликої кількості портів.

Третя модель МЗ, Cisco ME 3400E-24TS, має 24 порти Ethernet 10/100, два двоцільні порти (10/100/1000 і SFP) підключення і два слоти для змінних блоків живлення і вентилятора. Цей комутатор МСМПП ідеально підходить для великих мереж, які вимагають багато портів і високої пропускної здатності МЗ [39].

Обидві моделі комутаторів МСМПП, Cisco ME 3400EG-12CS і Cisco ME 3400E-24TS, пропонують два різних види програмного забезпечення (ПЗ для МСМПП) Cisco IOS: METROACCESS і METROIPACCESS. Вид ПЗ METROACCESS має розширені функції QoS для МСМПП, обмеження швидкості, надійне управління мультикастом і комплексні функції безпеки МЗ, і він підходить для сервіс-провайдерів МЗ, які пропонують послуги Carrier Ethernet з підтримкою різних рівнів якості обслуговування МСМПП. Вид ПЗ МСМПП METROIPACCESS, з іншого боку, надає розширені функції шару 3, такі як

підтримка розширених протоколів IP-маршрутизації МСМПП, Multi-VRF CE та PBR. Цей вид ПЗ підходить для МЗ, які потребують просунутих функцій маршрутизації та сегментації МЗ [40].

Всі моделі для МСМПП Cisco ME 3400E мають компактний дизайн форм-фактору 1 rack unit, що забезпечує зручну установку в стійку, тобто вони також підтримують відмінну пропускну здатність МЗ комутації - до 32 Gbps, що дозволяє обробляти великий обсяг даних МСМПП з високою швидкістю пересилання до 26 Mpps. Крім того, комутатори МСМПП мають велику таблицю MAC-адресів з розміром 8 000 записів для МСМПП, що дозволяє ефективно обробляти трафік великих МЗ.

Для МСМПП Cisco ME 3400E - це ідеальний вибір для сервіс-провайдерів МЗ, які прагнуть підвищити якість і надійність своїх послуг Carrier Ethernet. Завдяки широким можливостям комутації МЗ, різноманітним опціям живлення і розширеним функціям програмного забезпечення для МЗ Cisco IOS, ці комутатори МЗ забезпечують гнучкість і ефективність в будь-якому середовищі МЗ.

Таблиця 2.5. - Характеристики платформи для МСМПП Cisco ME 3400E

Характеристика	Значення
Кількість мережевих портів платформи для МСМПП	12x 1 Gigabit Ethernet Combo (SFP/RJ-45)
Кількість портів підключення платформи для МСМПП	4x 1 Gigabit Ethernet SFP
Кількість портів керування платформи для МСМПП	1x Console RJ-45, 1x Fast Ethernet Management, 4x External Alarm Input Contacts
Кількість блоків живлення платформи для МСМПП	ME34X-PWR-AC Power Supply / Fan Module
Пропускна здатність комутатора платформи для МСМПП	32 Gbps

Швидкість пересилання платформи для МСМПП	26 Mpps
Розмір таблиці MAC-адрес платформи для МСМПП	8,000
Кріплення до стійки платформи для МСМПП	Включено (1 rack unit)

У місті Хмельницький існує філія компанії ПП «Sigma Software». Для неї було створено схему МЗ, в якому було використано наступне обладнання, подане у таблиці 2.6.

Таблиця 2.6. Технологічне обладнання МСМПП для Хмельницького філіалу

Назва обладнання	Кількість, шт.
Платформа Cisco ME 3400E МСМПП	1
Маршрутизатор МСМПП малого офісу MikroTik CCR1036-12G-4S	1
Комутатор МСМПП на 24 порти MikroTik CRS328-24P-4S+RM	2
Камера відеонагляду АHD МСМПП	4
Принтер МСМПП HP LaserJet Enterprise M806dn	2
Персональний комп'ютер МСМПП	11
ІР-телефон МСМПП	2
Точка доступу МСМПП	2

При вході у офіс ПП можна побачити платформу МЗ Cisco ME 3400Е, яка використовується для мережевих потреб ПП. Поруч з нею розташований маршрутизатор МЗ малого офісу ПП MikroTik CCR1036-12G-4S, який забезпечує маршрутизацію даних у МЗ.

Для забезпечення комутації даних МЗ та забезпечення підключення до МЗ розміщені комутатори МЗ на 24 порти MikroTik CRS328-24P-4S+RM. Всього в офісі є два таких комутатори МСМПП.

Для забезпечення безпеки МЗ та спостереження в офісі ПП встановлено камери відеонагляду АHD. Всього у офісі ПП є чотири камери, які допомагають контролювати безпеку приміщення через МСМПП.

Офіс ПП також має два принтери HP LaserJet Enterprise M806dn для друку документів та матеріалів компанії, враховуючи друк через МЗ.

Для роботи співробітників в офісі ПП є 24 персональних комп'ютери (інфокомунікаційні системи), які використовуються для виконання різних завдань та роботи з програмним забезпеченням МСМПП.

Крім того, у офісі ПП є два IP-телефони МЗ та дві точки доступу МЗ для бездротового підключення до МЗ Інтернет.

Також в офісі ПП є один сканер, який використовується для цифровізації та збереження документів у електронному вигляді 41[[]].

## 2.5 Висновки до другого розділу

Визначено основні вимоги до МСМПП, такі як надійність, швидкодія, безпека та можливості для розширення МЗ. У другому розділі для МСМПП було проведено дослідження ряд технологій та архітектур МЗ, що дозволяють створити оптимальний варіант МЗ для даного приватного підприємства.

Створені різні варіанти програмно-апаратних засобів для структурних схем МСМПП та проведено їх обґрунтування. В результаті було запропоновано

оптимальну структуру МСМПП, яка дозволяє задовольняти всі вимоги до МСМПП та забезпечувати її ефективну роботу.

Проведено розрахунки МСМПП необхідної пропускної здатності МЗ для послуг Triple Play та додаткового резерву для інших послуг МЗ. Для цього використано дані про кількість абонентів МЗ у розташованих у Харкові та Львові офісах ПП. Результатом розрахунків стала оптимальна пропускна здатність МСМПП, яка дозволяє задовольняти потреби користувачів МЗ у послугах Triple Play та інших послугах МЗ, що надаються в МСМ приватного підприємства.

Розглянуто розробку сценарію МСМПП через технологію VPN для забезпечення безпечного та зашифрованого віддаленого доступу в МЗ до різноманітних філій МЗ з будь-якого місця. У таблиці наведена докладна інформація про платформи МЗ, якими можна користуватися для налаштування з'єднань для різноманітних типів пристроїв МСМПП, включаючи комп'ютери МЗ, ноутбуки, смартфони, планшети та інші пристрої МЗ. Отже, приділено увагу безпеці та доступності МСМПП для користувача.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		45

### 3 МОДЕЛЮВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ПРИВАТНОГО ПІДПРИЄМСТВА

#### 3.1. Модель схеми зв'язку групи компаній приватного підприємства

З метою аналізу структури МСМПП "Sigma Software" та організації МЗ VPN між філіями компанії, було прийнято рішення про створення моделі МЗ з використанням програми 10-Strike для моделювання МСМПП.

Ця програма надає можливість створити схему МСМПП, виявити мережеві пристрої та розмістити їх на схемі МСМПП, а також автоматично побудувати зв'язки між комутаторами МСМПП, якщо вони підтримують протокол SNMP для МСМПП.

Крім того, в комплекті з програмою є мережеві інструменти для моніторингу МСМПП, які допомагають розробити більш детальну схему МЗ для КМЗ та магістралі.

У комплекті з програмою 10-Strike доступні наступні інструменти для моделювання МСМПП:

- 10-Strike LANState: програма для адміністрування та моніторингу МЗ.
- 10-Strike Network File Search: програма для пошуку файлів у локальних МЗ та на FTP-серверах.
- 10-Strike Connection Monitor: програма для відстеження та контролю підключень до МЗ комп'ютерів.

Ці інструменти допомагають забезпечити ефективне управління МСМПП, моніторинг та пошук файлів в МСМПП, а також відстеження підключень до ресурсів МЗ.

Для створення МЗ VPN використовувалася програма Cisco Packet Tracer, це програмне середовище надає зручні можливості для організації МСМПП VPN на базі обладнання, яке доступне в бібліотеці компонентів програми.

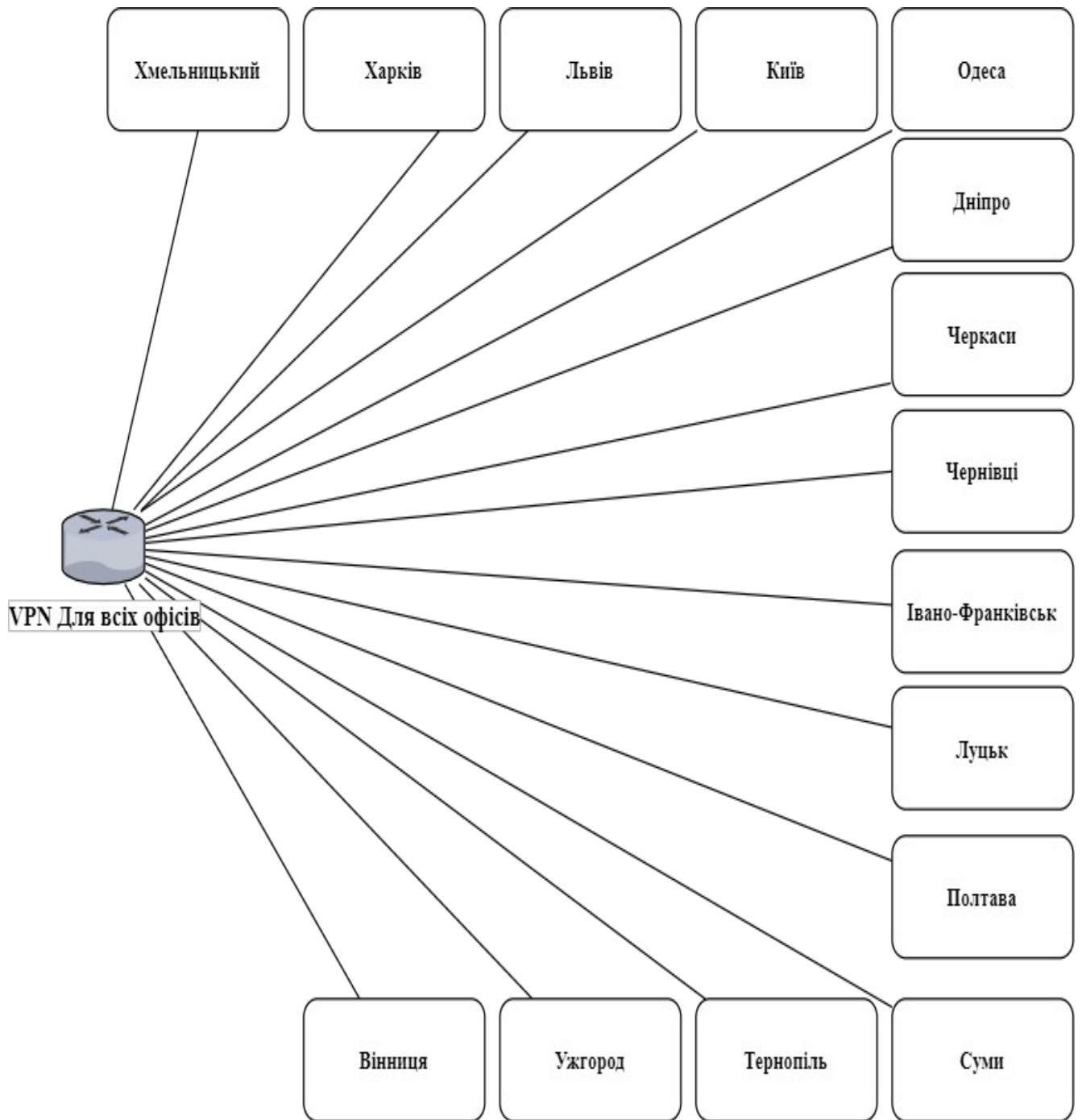


Рисунок 3.1 Схема МЗ ПП офісів «Sigma Software»

### 3.2. Розробка плану IP-адресації для мультисервісної мережі приватного підприємства

Для реалізації проекту МЗ VPN необхідно присвоїти кожному маршрутизатору МЗ, що належить до МСМПП, свою унікальну IP-адресу. В

таблиці 3.1. наведено план IP-адресації МСМПП, який використовуватиметься для цього проекту.

Таблиця 3.1. - План IP-адресації МСМПП

<b>Назва міста МСМПП</b>	<b>IP-адреса МСМПП</b>
Головний офіс Харків МСМПП	77.0.0.1
Львів МСМПП	77.1.0.1
Київ МСМПП	77.2.0.1
Одеса МСМПП	77.3.0.1
Дніпро МСМПП	77.4.0.1
Черкаси МСМПП	77.5.0.1
Чернівці МСМПП	77.6.0.1
Івано-Франківськ МСМПП	77.7.0.1

Вип.	Аркуш	№ Докум.	Підпис	Дата

КвРТР.2019018.01.017.ПЗ

Арк.

48

Луцьк МСМПП	77.8.0.1
Полтава МСМПП	77.9.0.1
Суми МСМПП	77.10.0.1
Тернопіль МСМПП	77.11.0.1
Ужгород МСМПП	77.12.0.1
Вінниця МСМПП	77.13.0.1
Хмельницький МСМПП	77.14.0.1

### 3.3 Модель мультисервісної мережі приватного підприємства в середовищі CiscoPacketTracer

Спочатку були налаштовані комп'ютери (та інфокомунікаційні системи) МСМПП для головного офісу та філії. Для кожного комп'ютера (та інфокомунікаційної системи) МСМПП була призначена окрема IP-адресація. Приклад моделювання МСМПП для двох вузлів МЗ, тобто схема реалізація сегменту МЗ VPN представлено на рисунку 3.2, а на рисунках 3.3-3.12 наведено IP-адресація МСМПП для м.Харків та м.Львів.

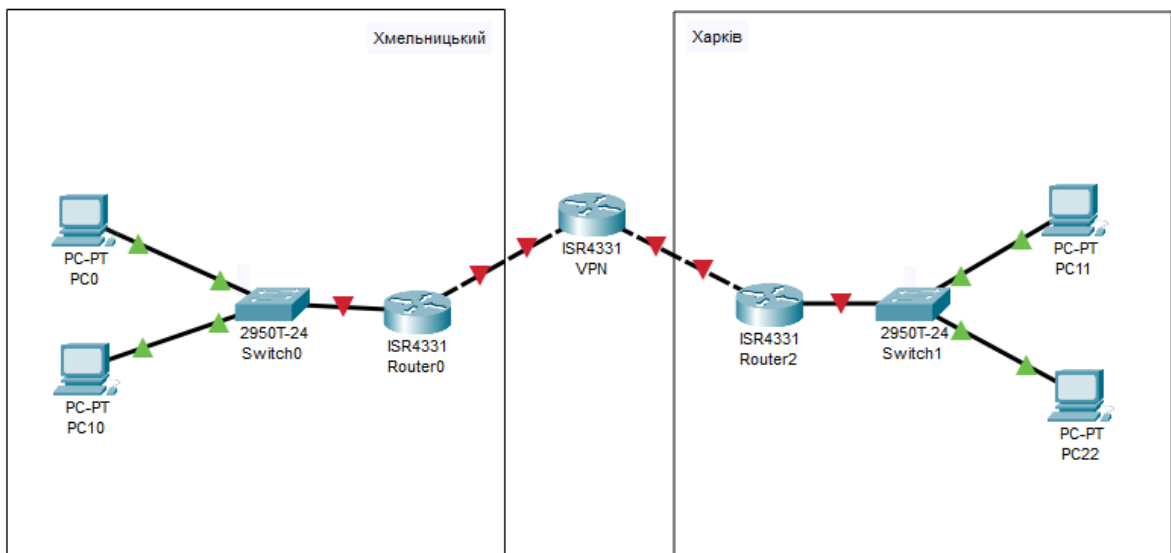


Рисунок 3.2 – Схема реалізації сегмента МЗ VPN

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.3 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса в Харкові (частина 1)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.4 – Присвоєння комп'ютеру МСМПП ІР-адреси для офіса в Харкові  
(частина 2)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.5 – Присвоєння комп'ютеру МСМПП ІР-адреси для офіса в Харкові  
(частина 3)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.6 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса в Харкові  
(частина 4)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.7 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса в Харкові  
(частина 5)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.8 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса в Харкові  
(частина б)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.9 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса  
Львів (частина 1)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.10 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса Львів (частина 2)

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Gateway/DNS IPv4

DHCP

Static

Default Gateway

DNS Server

Рисунок 3.11 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса Львів (частина 3)

The image contains two identical-looking configuration windows for 'Gateway/DNS IPv4'. Both windows have the 'Static' radio button selected. The top window has 'Default Gateway' set to 77.1.0.8 and 'DNS Server' set to 255.255.255.0. The bottom window has 'Default Gateway' set to 77.1.0.9 and 'DNS Server' set to 255.255.255.0.

Рисунок 3.12 – Присвоєння комп'ютеру МСМПП IP-адреси для офіса Львів (частина 4)

Надалі були здійснені основні налаштування маршрутизатора МСМПП. Приклад було продемонстровано на маршрутизаторі МСМПП - R1. Спочатку було встановлено ім'я для маршрутизатора МСМПП, вимкнено пошук DNS МЗ і увімкнено пароль для привілейованого режиму МСМПП. Далі було виконано налаштування консолі МЗ, встановлено пароль для входу і ввімкнено запит пароля перед доступом до консолі МЗ. Потім було перейдено до режиму МСМПП – telnet, і так само встановлено та увімкнено пароль для входу, щоб забезпечити роботу МСМПП, було необхідно увімкнути інтерфейси МЗ і призначити їм IP-адресу та відповідну маску [42]. Наступним кроком для МСМПП було перевірено стан всіх інтерфейсів, а також надано їм відповідні (для МСМПП) конфігураційні параметри. Після цього було налаштовано маршрутизацію МСМПП для забезпечення передачі пакетів між мережевими сегментами МЗ. Крім того, було встановлено правила фільтрації на маршрутизаторі МЗ, щоб забезпечити безпеку МЗ. Після завершення цих кроків маршрутизатор МСМПП був налаштований до використання у

функціональній МЗ. Такі самі дії були проведені на двох інших маршрутизаторах МСМПП, а наступним кроком було налаштовано VPN МЗ [43].

Процес налаштування віртуальної приватної МЗ включає кілька етапів:

1. Етап першої фази МСМПП: створено політику ІБ crypto isakmp з policy 1, в якій вказані алгоритм шифрування МСМПП 3des, алгоритм хешування МЗ md5, тип аутентифікації МЗ pre-share та алгоритм обміну ключами в МСМПП pre-share group 2.

Ці параметри МСМПП необхідні для встановлення ініційного тунелю isakmp, через який передаються параметри в МСМПП основного тунелю ipsec.

2. Етап налаштування ключа аутентифікації та бенкету МСМПП: було налаштовано в МЗ pre-share key і вказано в МЗ IP-адресу бенкету, яким є маршрутизатор філії ПП.

Секретний ключ ПП має назву "bababooue", а адресою бенкету є зовнішня IP-адреса МЗ роутера філії - 77.1.1.1.

3. Етап другої фази МСМПП: встановлено параметри МЗ, необхідні для побудови ipsec тунелю, такі як ім'я, алгоритм шифрування та алгоритм хешування.

4. Етап визначення трафіку МСМПП, який потрібно зашифрувати: створено access-list, який визначає, який трафік МЗ буде передаватися через VPN тунель МЗ. Вказано IP-адресу МЗ центрального офісу ПП та філії, і щоб уникнути неправильного NAT-у трафіку МСМПП, спочатку був визначений заборонений трафік МЗ, а потім - всі інші типи трафіку МЗ, які можна трансформувати в МСМПП [44].

5. Етап створення криптокарти та прив'язки до інтерфейсу МСМПП: було створено криптокарту СМАР 10 з прив'язкою до зовнішньої адреси маршрутизатора МСМПП центрального офісу ПП [45].

Вказано access-list в МСМПП і прив'язано його до інтерфейсу FastEthernet 0/0, таким чином, використання VPN в МСМПП (компанії «Sigma Software») дозволить уникнути необхідності будувати власну транспортну інфраструктуру МЗ та знизить вартість оплати за виділений канал МЗ.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		56

### 3.4 Висновки до третього розділу

Розглянуто модель схеми МСМПП для групи компаній приватного підприємства. У цьому розділі наведено детальний опис структури МЗ, яка включає в себе локальну мережу (LAN) МСМПП, бездротову мережу (WLAN) МСМПП та віртуальну приватну МЗ (VPN). Отже, було надано увагу оптимальності та ефективності МСМ та її інфраструктурі для групи компаній ПП.

Розроблено план IP-адресації МСМПП для кожного маршрутизатора МЗ, що входить до складу МЗ VPN. У цьому плані вказано, які IP-адреси МСМПП будуть використовуватись у цьому проєкті. Згідно з цим планом, кожен маршрутизатор МЗ отримає свою унікальну IP-адресу. Таким чином, надано особливу увагу правильному та ефективному присвоєнню IP-адрес в МЗ для кожного маршрутизатора у МСМПП [46].

Для створення та налаштування МСМПП підходить середовище моделювання МЗ Cisco Packet Tracer, за допомогою якого було проведено опис процесу налаштування комп'ютерів (інфокомунікаційних систем) для головного офісу ПП та філії, а також призначення окремих IP-адрес в МЗ для кожного комп'ютера. Було досягнуто коректного налаштування з підвищеною ефективністю та налагодження МСМ інфраструктури приватного підприємства, використовуючи сучасні інструментальні засоби МЗ [47].

## ВИСНОВКИ

МСМПП - компанії "Sigma Software" має розташовані відділення по всій Україні, з головним офісом у Харкові, а головний офіс є центральною точкою МЗ, яка об'єднує різні відділи та команди.

Технології передачі даних в МСМПП відіграють важливу роль для забезпечення ефективної комунікації МЗ ПП та передачі різних типів даних у ній. Розробка МСМПП потребує чіткого визначення потреб та вимог до МЗ, включаючи сервери, комутатори, маршрутизатори та інші компоненти МЗ.

Використання новітніх технологій в МСМПП, таких як Software-Defined Networking (SDN), допомагає досягти ефективності та гнучкості у керуванні МЗ.

Розробка МСМПП є актуальним завданням, оскільки сприяє ефективному об'єднанню команд та підтримці різних типів передачі даних. Пропускна здатність та безпека МСМПП також мають велике значення.

Розглянуті різні аспекти структурної схеми МСМПП та розроблено план IP-адресації для маршрутизаторів у МСМПП. Cisco Packet Tracer є оптимальним варіантом використовувати її для моделювання та налаштування МСМПП.

					КвРТР.2019018.01.017.ПЗ	Арк.
Вип.	Аркуш	№ Докум.	Підпис	Дата		58

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. John Evans та Clarence Filsfils. Deploying IP and MPLS QoS for Multiservice Networks / John Evans та Clarence Filsfils. – Сан-Дієго: Morgan Kaufmann, 2007. – 576 с.
2. Jim Durkin та ін. Building Multiservice Transport Networks / Jim Durkin та ін. – Індіанаполіс: Cisco Press, 2010. – 576 с.
3. Robert Wood. Next-Generation Network Services / Robert Wood. – Індіанаполіс: Cisco Press, 2005. – 408 с.
4. Mehmet Toy. IP-Based Next-Generation Wireless Networks / Mehmet Toy. – Нью-Йорк: Wiley, 2013. – 336 с.
5. Syed A. Ahson та Mohammad Ilyas (ред.). Cloud Computing and Software Services / Syed A. Ahson та Mohammad Ilyas (ред.). – Бока-Ратон: CRC Press, 2010. – 472 с.
6. Thomas D. Nadeau та Ken Gray. SDN: Software Defined Networks / Thomas D. Nadeau та Ken Gray. – Себастополь: O'Reilly Media, 2013. – 384 с.
7. Olivier Hersent, David Gurle та Jean-Pierre Petit. IP Telephony: Deploying Voice-over-IP Protocols / Olivier Hersent, David Gurle та Jean-Pierre Petit. – Чічестер: Wiley, 2005. – 384 с.
8. Rajiv Ramaswami, Kumar N. Sivarajan та Galen H. Sasaki. Optical Networks: A Practical Perspective / Rajiv Ramaswami, Kumar N. Sivarajan та Galen H. Sasaki. – Сан-Дієго: Morgan Kaufmann, 2010. – 928 с.
9. Adrian Farrel та Igor Bryskin (ред.). GMPLS: Architecture and Applications / Adrian Farrel та Igor Bryskin (ред.). – Сан-Дієго: Morgan Kaufmann, 2006. – 400 с.
10. Daniel Minoli та Emma Minoli (ред.). Delivering Voice over IP Networks / Daniel Minoli та Emma Minoli (ред.). – Нью-Йорк: Wiley, 2002. – 544 с.
11. Daniel Collins та Clint Smith (ред.). Carrier Grade Voice over IP / Daniel Collins та Clint Smith (ред.). – Нью-Йорк: McGraw-Hill Education, 2013. – 656 с.

12. Kevin Wallace та Michael Valentine (ред.). CCNA Voice Study Guide / Kevin Wallace та Michael Valentine (ред.). – Індіанаполіс: Sybex, 2010. – 648 с.
13. William Stallings (ред.). Data and Computer Communications / William Stallings (ред.). – Бостон: Pearson Education, 2013. – 912 с.
14. Behrouz A Forouzan (ред.). Data Communications and Networking / Behrouz A Forouzan (ред.). – Нью-Йорк: McGraw-Hill Education, 2012. – 1264 с.
15. James F Kurose та Keith W Ross (ред.). Computer Networking: A Top-Down Approach / James F Kurose та Keith W Ross (ред.). – Бостон: Pearson Education, 2012. – 864 с.
16. Larry L Peterson та Bruce S Davie (ред.). Computer Networks: A Systems Approach / Larry L Peterson та Bruce S Davie (ред.). – Сан-Дієго: Morgan Kaufmann, 2011 – 920 с.
17. Andrew S Tanenbaum та David J Wetherall (ред.). Computer Networks / Andrew S Tanenbaum та David J Wetherall (ред.). – Бостон: Pearson Education, 2011 – 960 с.
18. Uyles Black (ред.). MPLS and Label Switching Networks / Uyles Black (ред.). – Нью-Йорк: Prentice Hall, 2013. – 384 с.
19. Vivek Alwayn (ред.). Advanced MPLS Design and Implementation / Vivek Alwayn (ред.). – Індіанаполіс: Cisco Press, 2001. – 400 с.
20. Bruce S Davie та Adrian Farrel (ред.). MPLS: Next Steps / Bruce S Davie та Adrian Farrel (ред.). – Сан-Дієго: Morgan Kaufmann, 2008. – 464 с.
21. Daniel Minoli (ред.). Voice Over MPLS: Planning and Designing Networks / Daniel Minoli (ред.). – Нью-Йорк: McGraw-Hill Education, 2002. – 400 с.
22. Daniel Minoli (ред.). IP Multicast with Applications to IPTV and Mobile DVB-H / Daniel Minoli (ред.). – Чічестер: Wiley, 2008. – 304 с.
23. Amitabh Kumar (ред.). Mobile Broadcasting with WiMAX / Amitabh Kumar (ред.). – Амстердам: Elsevier, 2008. – 456 с.
24. Syed A Ahson та Mohammad Ilyas (ред.). WiMAX Standards and Security / Syed A Ahson та Mohammad Ilyas (ред.). – Бока-Ратон: CRC Press, 2007. – 552 с.

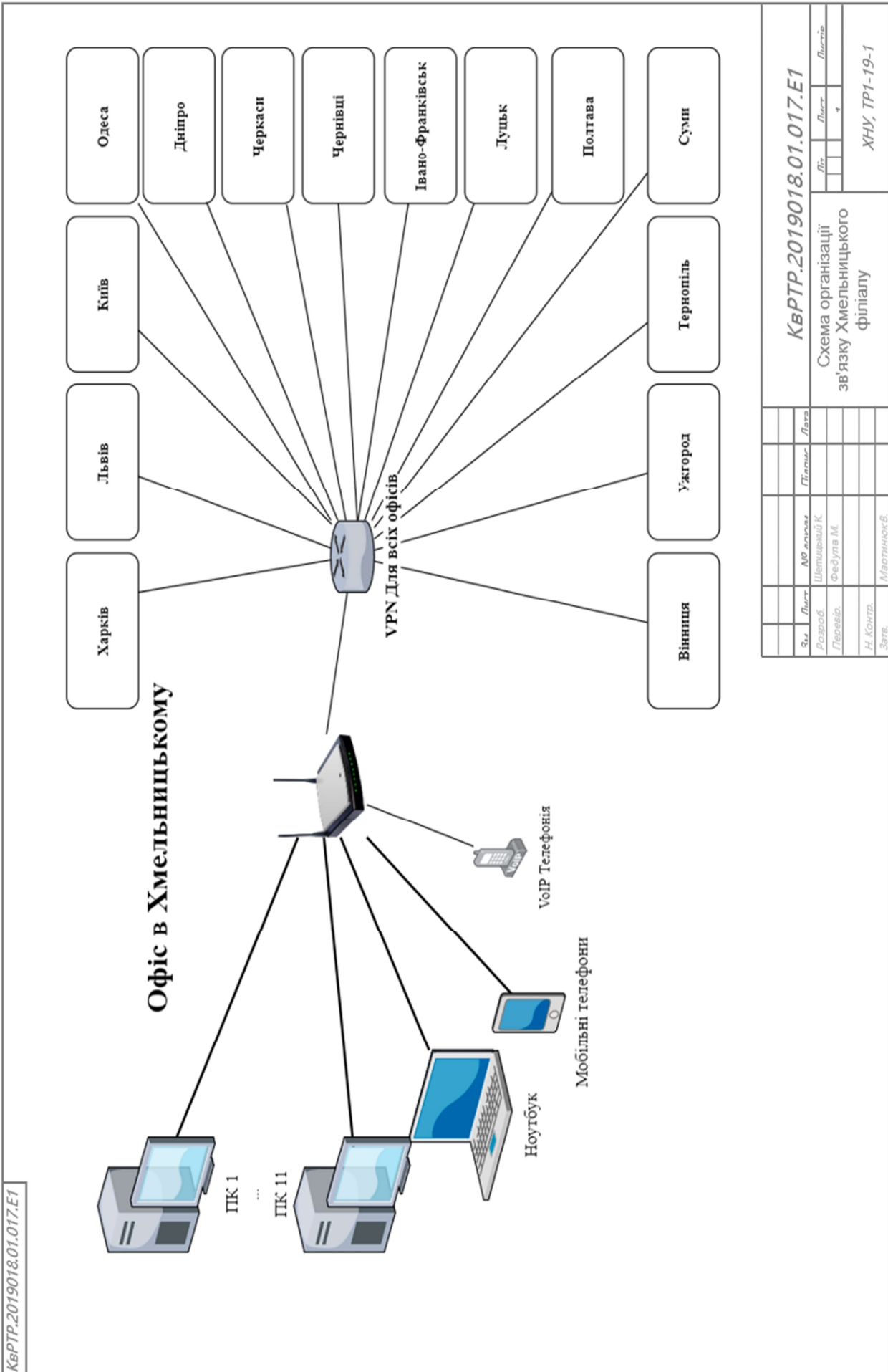
25. Jeffrey G Andrews, Arunabha Ghosh та Rias Muhamed (ред.). Fundamentals of WiMAX / Jeffrey G Andrews, Arunabha Ghosh та Rias Muhamed (ред.). – Нью-Йорк: Prentice Hall, 2007. – 496 с.
26. Clint Smith та John Meyer (ред.). 4G Wireless Networks / Clint Smith та John Meyer (ред.). – Нью-Йорк: McGraw-Hill Education, 2011. – 352 с.
27. Frank Ohrtman (ред.). Wi-Fi Handbook: Building 802.11b Wireless Networks / Frank Ohrtman (ред.). – Нью-Йорк: McGraw-Hill Education, 2003. – 400 с.
28. Matthew S Gast (ред.). 802.11 Wireless Networks: The Definitive Guide / Matthew S Gast (ред.). – Себастополь: O'Reilly Media, 2005. – 656 с.
29. Jim Geier (ред.). Wireless LANs / Jim Geier (ред.). – Індіанаполіс: Sams Publishing, 2001 – 608 с.
30. Daniel Collins та Clint Smith (ред.). Carrier Grade Voice over IP / Daniel Collins та Clint Smith (ред.). – Нью-Йорк: McGraw-Hill Education, 2013 – 656 с.
31. Olivier Hersent, David Gurle та Jean-Pierre Petit. IP Telephony: Deploying Voice-over-IP Protocols / Olivier Hersent, David Gurle та Jean-Pierre Petit. – Чічестер: Wiley, 2005 – 384 с.
32. Kevin Wallace та Michael Valentine (ред.). CCNA Voice Study Guide / Kevin Wallace та Michael Valentine (ред.). – Індіанаполіс: Sybex, 2010 – 648 с.
33. William Stallings (ред.). Data and Computer Communications / William Stallings (ред.) – Бостон: Pearson Education, 2013 – 912 с.
34. Behrouz A Forouzan (ред.). Data Communications and Networking / Behrouz A Forouzan (ред.) – Нью-Йорк: McGraw-Hill Education, 2012 – 1264 с.
35. James F Kurose та Keith W Ross (ред.). Computer Networking: A Top-Down Approach / James F Kurose та Keith W Ross (ред.) – Бостон: Pearson Education, 2012 – 864 с.
36. Larry L Peterson та Bruce S Davie (ред.). Computer Networks: A Systems Approach / Larry L Peterson та Bruce S Davie (ред.) – Сан-Дієго: Morgan Kaufmann, 2011 – 920 с.

37. Andrew S Tanenbaum та David J Wetherall (ред.). Computer Networks / Andrew S Tanenbaum та David J Wetherall (ред.) – Бостон: Pearson Education, 2011 – 960 с.
38. Vivek Alwayn (ред.). Advanced MPLS Design and Implementation / Vivek Alwayn (ред.) – Індіанаполіс: Cisco Press, 2001 – 400 с.
39. Bruce S Davie та Adrian Farrel (ред.). MPLS: Next Steps / Bruce S Davie та Adrian Farrel (ред.) – Сан-Дієго: Morgan Kaufmann, 2008 – 464 с.
40. Daniel Minoli (ред.). Voice Over MPLS: Planning and Designing Networks / Daniel Minoli (ред.) – Нью-Йорк: McGraw-Hill Education, 2002 – 400 с.
41. Daniel Minoli (ред.). IP Multicast with Applications to IPTV and Mobile DVB-H / Daniel Minoli (ред.) – Чічестер: Wiley, 2008 – 304 с.
42. Amitabh Kumar (ред.). Mobile Broadcasting with WiMAX / Amitabh Kumar (ред.) – Амстердам: Elsevier, 2008 – 456 с.
43. Syed A Ahson та Mohammad Ilyas (ред.). WiMAX Standards and Security / Syed A Ahson та Mohammad Ilyas (ред.) – Бока-Ратон: CRC Press, 2007 – 552 с.
44. Jeffrey G Andrews, Arunabha Ghosh та Rias Muhamed (ред.). Fundamentals of WiMAX / Jeffrey G Andrews, Arunabha Ghosh та Rias Muhamed (ред.) – Нью-Йорк: Prentice Hall, 2007 – 496 с.
45. Clint Smith та John Meyer (ред.). 4G Wireless Networks / Clint Smith та John Meyer (ред.) – Нью-Йорк: McGraw-Hill Education, 2011 – 352 с.
46. Frank Ohrtman (ред.). Wi-Fi Handbook: Building 802.11b Wireless Networks / Frank Ohrtman (ред.) – Нью-Йорк: McGraw-Hill Education, 2003 – 400 с.
47. Matthew S Gast (ред.). 802.11 Wireless Networks: The Definitive Guide / Matthew S Gast (ред.) – Себастополь: O'Reilly Media, 2005 – 656 с.

# Додатки

# Додаток А

## Схема організації зв'язку Хмельницького філіалу



КвРТР\_2019018.01.017.E1

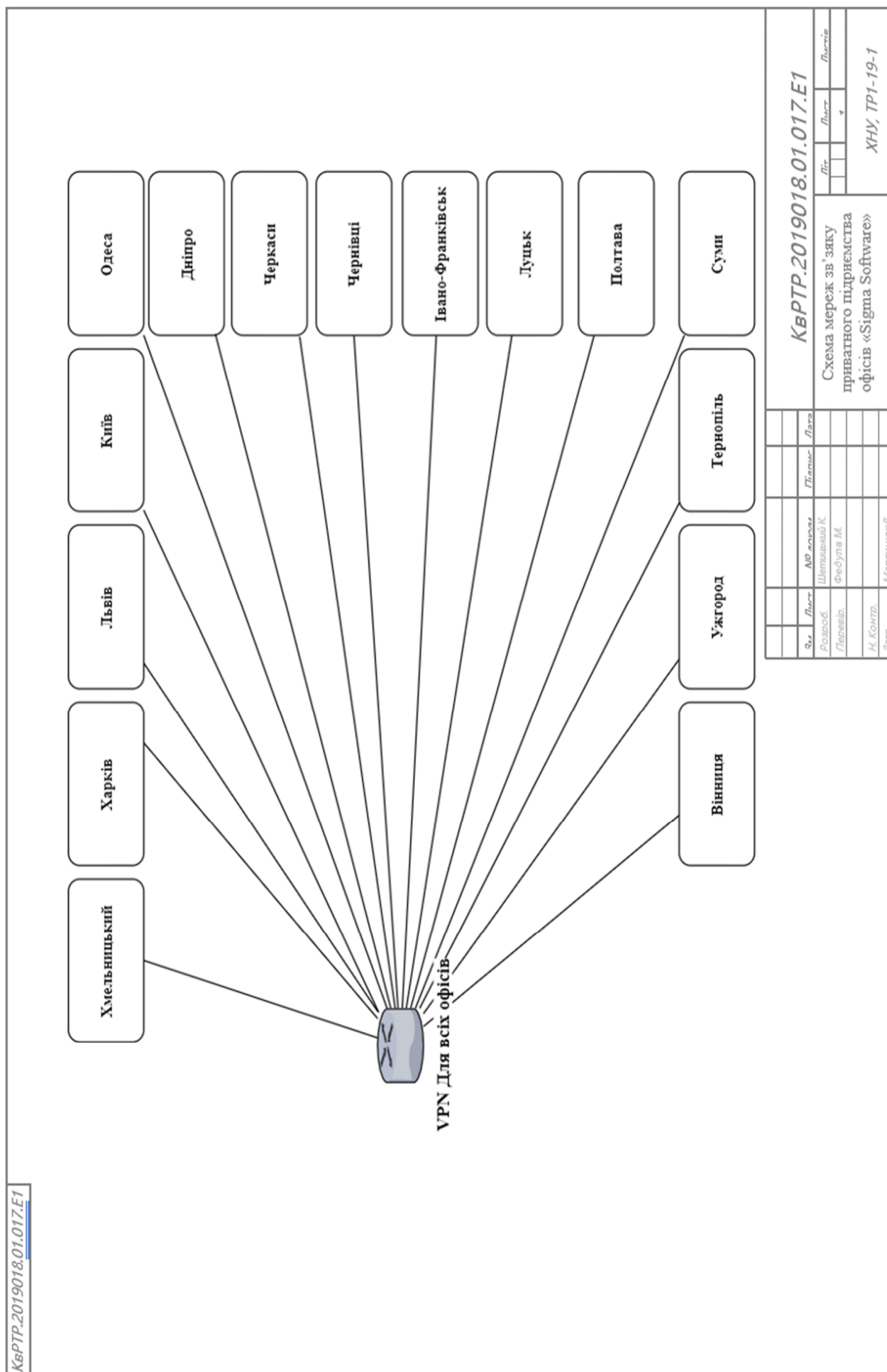
КвРТР_2019018.01.017.E1		Лист	Лист	Лист	Лист
З.	Лист	Лист	Лист	Лист	Лист
Розроб.	Штецький К.				
Лесев.	Федула М.				
Н.Контр.	Мартинюк В.				
Затв.					

Схема організації зв'язку Хмельницького філіалу

ХНУ, ТР1-19-1

## Додаток Б

### Схема мереж зв'язку приватного підприємства офісів «Sigma Software»





Ім'я користувача:  
Кафедра АКІТІТК

ID перевірки:  
1015687842

Дата перевірки:  
24.06.2023 21:43:12 EEST

Тип перевірки:  
Doc vs Internet + Library

Дата звіту:  
24.06.2023 21:47:35 EEST

ID користувача:  
100005862

Назва документа: Шептицький

Кількість сторінок: 57 Кількість слів: 11073 Кількість символів: 78235 Розмір файлу: 850.91 KB ID файлу: 1015331809

1189 слів позначені як "вилучені" та не враховуються у підрахунку слів

## 0.63% Схожість

Найбільша схожість: 0.24% з Інтернет-джерелом ([http://elartu.tntu.edu.ua/bitstream/lib/33694/2/Dyplom\\_Lyzun\\_V\\_2020..](http://elartu.tntu.edu.ua/bitstream/lib/33694/2/Dyplom_Lyzun_V_2020..))

0.63% Джерела з Інтернету

30

Сторінка 59

Не знайдено джерел з Бібліотеки

## 0% Цитат

Не знайдено жодних цитат

Не знайдено жодних посилань

## 0.01% Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

Немає вилучених Інтернет-джерел

0.01% Вилученого тексту з Бібліотеки

15

Сторінка 59

## Модифікації

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

Замінені символи

22

**Anti-Plagiarism v-15.257****Максимальне співпадіння з одним документом 0.0%****Словники перевірки: en\_US, ru\_RU, ua\_UA. Помилки в документах: 16%**

ID: 118017 Назва: БКР Мультисервісна мережа приватного підприємства Додано в БД: 2023-06-24 Автора: Кирил ШЕПТИЦЬКИЙ Керівники: Микола ФЕДУЛА Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	67712	524	389 (1%)	6 (1%)

## Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Шептицький Кирил Юрійович

Тема: Мультисервісна мережа приватного підприємства

Спеціальність: 172 «Телекомунікації та радіотехніка»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 62

1. Короткий зміст роботи та прийнятих рішень: спроєктовано мультисервісну мережу приватного підприємства
2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню
3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі кваліфікаційної роботи проведено проектування інфраструктури мереж зв'язку, вибір технологій та обладнання, налаштування мережевих пристроїв, а також розробку стратегій забезпечення інформаційної безпеки. Здійснено дослідження процедури керування та моніторингу, щоб забезпечити ефективну роботу мереж зв'язку між офісами компанії «Sigma Software». У другому розділі розроблено принцип роботи та розглянуто функції мультисервісної мережі приватного підприємства. Розвиток технологій, як SDN, дозволяє централізовано керувати мережевими ресурсами та надавати різноманітні послуги. Розробка мережі зв'язку для компанії "Sigma Software" є актуальним завданням, що сприяє ефективному об'єднанню команд та підтримці різних типів передачі даних. У третьому розділі наведено детальний опис структури мереж зв'язку, яка включає в себе локальну мережу (LAN) мультисервісної мережі приватного підприємства, бездротову мережу (WLAN) мультисервісної мережі приватного підприємства та віртуальну приватну мережу зв'язку (VPN). Отже, було надано увагу оптимальності та ефективності мережі зв'язку та її інфраструктурі для групи компаній приватного підприємства. Розроблено план IP-адресації мультисервісної мережі приватного підприємства для кожного маршрутизатора мереж зв'язку, що входить до складу мереж зв'язку VPN. У цьому плані вказано, які IP-адреси мультисервісної мережі приватного підприємства будуть використовуватись у цьому проекті. Згідно з цим планом, кожен маршрутизатор мереж зв'язку отримає свою унікальну IP-адресу. Таким чином, надано особливу увагу правильному та ефективному присвоєнню IP-адрес в мережах зв'язку для кожного маршрутизатора у мультисервісній мережі приватного підприємства.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: у роботі недостатньо уваги приділяється огляду підвищення масштабованості у подальшому використанні для мультисервісної мережі приватного підприємства

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації

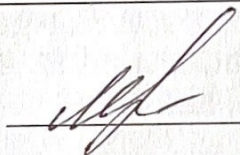
7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: відсутні

9. Оцінка дипломної роботи: добре (4,25/В)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) к. т. н. доцент  
коф. ТМІТ Мішан Віктор Володимирович

“26” 06 2023 р.

 (підпис)

**РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ  
КАФЕДРИ АВТОМАТИЗАЦІЇ, КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ ТА  
РОБОТОТЕХНІКИ  
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ**

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

Назва: Мультисервісна мережа приватного підприємства

Автор: Шептицький Кирил Юрійович

Спеціальність: 172 – Телекомунікації та радіотехніка

Освітня програма: Освітньо-професійна програма «Телекомунікації та інформаційно-комунікаційні технології»

Науковий керівник: Федула Микола Васильович, кандидат технічних наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. 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. 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 письмової роботи та ідентичності друкованої й електронної 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 (наступного року) після 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) у тексті кваліфікаційної роботи системами перевірки на плагіат виявлено схожість з деякими документами в частині загальноживаних обов'язкових словосполучень у стандартних бланках (титулка, відомість документів), у структурі змісту, назвах розділів/підрозділів тощо, у назвах публікацій у переліку джерел посилання;

2) усі запозичення є фрагментарними або мають належним чином оформленні посилання;

3) виявлені модифікації тексту не впливають на відсоток схожості.




Сумарний обсяг всіх запозичень, визначений системою виявлення збігів ідентичності/схожості, складає 0,67% і адресується до 45 джерел, що, з урахуванням наведених обґрунтувань, відповідає характеру теми і свідчить на користь кваліфікаційної роботи.

Дата 24.06.2023р.

Завідувач кафедри

Гарант освітньої програми

Керівник кваліфікаційної роботи

  
\_\_\_\_\_  
  
\_\_\_\_\_  
  
\_\_\_\_\_

Валерій МАРТИНЮК

Денис МАКАРИШКІН

Микола ФЕДУЛА