МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра Комп'ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
комп'ютерних систем та мереж

_____(Жуков І.А.)

« ____ » _____ 2021 р.

ДИПЛОМНИЙ ПРОЕКТ

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"БАКАЛАВР"

Тема: Економні структури локальних обчислювальних мереж медичного призначення

Виконавець: Авер'янова А.І.

Керівник: Печурін М.К.

Нормоконтролер: Журавель С.В.

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютерних систем та мереж
Напрям (спеціальність) 123 "Комп'ютерна інженерія"
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем та мереж

_____(Жуков І.А.)

« ____ » _____ 2021 р.

З А В Д А Н Н Я
на виконання дипломного проекту

Авер'янової Алли Ігорівни
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема проекту (роботи): Економні структури локальних обчислювальних мереж медичного призначення
затверджена наказом ректора від " 26 " квітня 2021 року № 648/ст.

2.Термін виконання проекту (роботи): з 24.05.2020 до 20.06.2020

3.Вихідні дані до проекту (роботи): 1) структури ЛОМ медичного призначення; 2) метод вибору програмно-апаратних засобів розглядається *Analytic Hierarchy Process (AHP)*; 3) методи реалізації *GREoverIPSec.*

4.Зміст пояснювальної записки (перелік питань, що підлягають розробці):
провести системний аналіз економних структур локальних обчислювальних мереж медичного призначення.; провести програмно-апаратних засобів для створення економних структур локальних обчислювальних мереж медичного призначення з подальшим вибором обладнання.; провести планування та втілення економної структури лом для медичних потреб.

5.Перелік обов'язкового графічного матеріалу:
Презентація *PowerPoint:* постановка задачі; моделі досліджуваної системи; графічні результати дослідження; висновки

6. Календарний план

№ п/п	Етапи виконання дипломного проекту	Термін виконання етапів	Примітка
1.	Ознайомлення з постановкою задачі	26.05.2021	
2.	Огляд літератури	28.05.2021	
3.	Розробка розділу: провести системний аналіз економних структур локальних обчислювальних мереж медичного призначення.	31.05.2021	
4.	Розробка розділу: провести програмно-апаратних засобів для створення економних структур локальних обчислювальних мереж медичного призначення з подальшим вибором обладнання.	01.06.2021	
5.	Розробка розділу: провести планування та втілення економної структури лом для медичних потреб.	03.06.2021	
6.	Оформлення пояснювальної записки	04.06.2021	
7.	Оформлення графічної частини	09.06.2021	
8.	Передача документації в ЕК	11.06.2021	
9.	Захист бакалаврської атестаційної роботи	16.06.2021	

7. Дата отримання завдання «25» травня 2021 р.

Керівник дипломного проекту Печурін М.К.
(підпис)

Завдання прийняв до виконання Авер'янова А.І.
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту “Економні структури локальних обчислювальних мереж медичного призначення”: 65 с., 37 рис., 3 таблиці, 47 літературних джерел, 1 додаток.

Мета дипломного проекту – дослідження способів побудови соціальних комп’ютерних мереж з вибором та побудовою економної структури ЛОМ медичного призначення.

Об’єкт проектування – окальна обчислювальна мережа медичного призначення.

Предмет проектування – методи побудови економних структур локальних обчислювальних мереж медичного призначення.

Метод проектування – визначення основних методів побудови ЛОМ медичного призначення.

Прогнози припущення щодо розвитку об’єкта дослідження – запропоновані методи побудови ЛОМ медичного призначення можуть бути використані при побудові реальних локальних обчислювальних мереж підприємств будь-якого типу та розміру.

Результати дипломного проектування рекомендується використовувати при розробці нових ЛОМ медичного призначення.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

IP	-	*Internet Protocol*
OSI	-	*The **Open Systems Interconnection** model*
IEEE	-	*The Institute of Electrical and Electronics Engineers*
TCP	-	*Transmission Control Protocol*
MAC	-	*Media Access Control*
LLC	-	*Logical Link Control*
ISO	-	*The International Organization for Standardization*
ANSI	-	*The American National Standards Institute*
ITU	-	*The International Telecommunication Union*
EIA/TIA	-	*The Electronics Industry Alliance/Telecommunications Industry Association*
ЛОМ	-	Локальна обчислювальна мережа
WI-FI	-	*Wireless Fidelity*
ДССЗЗІ	-	Державна служба спеціального зв'язку та захисту інформації України
L2VPN	-	*Layer2 VPN*
VLAN	-	*Virtual Local Area Network*
PWE3	-	*pseudo-wire*
MPLS	-	*MultIProtocol Label Switching*
VPLS	-	*Virtual Private LAN Service*
L3VPN	-	*Layer3 VPN*
GRE	-	*Generic Routing Encapsulation*
IPSec	-	*IP Security*
VTI	-	*Virtual Tunnel Interface*
DMVN	-	*Dynamic MultIPoint VPN*
VPN	-	*Virtual Private Network*
HDLC	-	*High-Level Data Link Control*
AHP	-	*Analytic Hierarchy Process*

HPE	-	*Hewlett Packard Enterprise*
ОС	-	Операційна система
MTBF	-	*Mean time between failures*
NAT	-	*Network Address Translation*
ACL	-	*Access Control List*
SNMP	-	*Simple Network Management Protocol*
ESP	-	*Electronic Stability Program*

ВСТУП

Актуальність.

На сьогодні одним із найбільш важливих показників для будь-якої медичної установи, включаючи аптеки, в Україні є вартість побудови та обслуговування інформаційної компьютерної локальної мережі. Станом на 2021 рік у зв'язку з подіями пов'язаними з епідемією *COVID-19* велика частина бюджету медичних установ направлена на боротьбу із захворюванням. Таким чином на інші потреби орагнізації, в тому числі побудову і обслуговування ЛОМ, залишається досить мала частина бюджету.

Беручи до уваги наведене вище, є підстави вважати, що тема дипломної роботи є новою та актуальною.

Метою дипломної роботи є дослідження способів побудови соціальних комп'ютерних мереж з вибором та побудовою економної структури ЛОМ медичного призначення.

Досягнення мети потребує розв'язання таких задач:

- Системний аналіз економних структур локальних обчислювальних мереж медичного призначення.
- Огляд структур локальних обчислювальних мереж.
- Визначення проблеми створення економних структур локальних обчислювальних мереж медичного призначення. З вибором критерія ефективності структури мережі.
- Оцінка та вибір структури лом медичного призначення.
- Вибір програмно-апаратних засобів для створення економних структур локальних обчислювальних мереж медичного призначення.
- Способи вибору типу програмно-апаратних засобів побудови економних структур ЛОМ медичного призначення з розробкою схеми структурного алгоритму вибору.
- Огляд обладнання для створення ЛОМ з вибором обладнання з

урахуванням обраних показників.

- Розробка економної структури ЛОМ для медичних потреб.
- Розробка схеми мережевої інфраструктури на прикладі мережі аптек розміщеної по м. Києву.
- Реалізація схеми ЛОМ на базі обраного обладнання та програмних засобів.

Об'єкт дослідження: локальна обчислювальна мережа медичного призначення.

Предмет дослідження: методи побудови економних структур локальних обчислювальних мереж медичного призначення.

Галузь застосування. Результати дипломної роботи можуть бути використані в галузі комп'ютерних мереж, зокрема в сучасних інформаційно-комунікаційних системах та мережах для підвищення ефективності застосування комплексних систем та окремих засобів побудови економних локальних обчислювальних мереж.

Новизна. Систематизовано сучасні методи побудови ЛОМ для інформаційно-комунікаційних мереж як соціального, так і програмно-апаратного типів.

Практична цінність полягає у тому, що запропоновані методи побудови ЛОМ медичного призначення можуть бути використані при побудові реальних локальних обчислювальних мереж підприємств будь-якого типу та розміру.

Апробація роботи. Основні результати роботи апробовано на реальній інфраструктурі Приватного Підприємства «ТЕХЕКСПЕРТ», рекомендації щодо вдосконалення впроваджено в практичну діяльність підприємства, про що надано відповідну довідку.

Структура та обсяг дипломної роботи.

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків загальним обсягом робота складає 65 сторінок, має 37 рисунків, 3 таблиці та 1 додаток. Список використаних джерел містить 47 найменувань і займає 4 сторінки

РОЗДІЛ 1. СИСТЕМНИЙ АНАЛІЗ ЕКОНОМНИХ СТРУКТУР ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ МЕДИЧНОГО ПРИЗНАЧЕННЯ.

1.1. Огляд структур локальних обчислювальних мереж

Комп’ютерна мережа (Computer Network) – це система зв’язку, що складеться мінімум з двох пристроїв (мережеве обладнання, комп’ютери, *IP* телефони тощо). Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали.[1]

Основна частина мереж, що існують на момент даного дослідження, функціонує за принципами еталонної мережевої моделі *OSI*, яка прийнята як міжнародний стандарт для мережних комунікацій у 1984 році Інститутом інженерів з електротехніки та електроніки (*IEEE*)[2] (Рис. 1.1.1 Модель *OSI*). За рекомендаціями світових лідерів за постачанням мережевого обладнання модель *OSI* класифікована як занадто складна[3], тому на практиці на сьогодні використовують більш просту та практичну модель – стек протоколів *TCP/IP* (Рис.1.1.2)

Модель *OSI* має 7 рівнів: прикладний (*Application*), рівень представлення (*Presentation*), сеансовий (*Session*), транспортний (*Transport*), мережевий (*Network*), канальний (*Data Link*), фізичний (*Physical*).

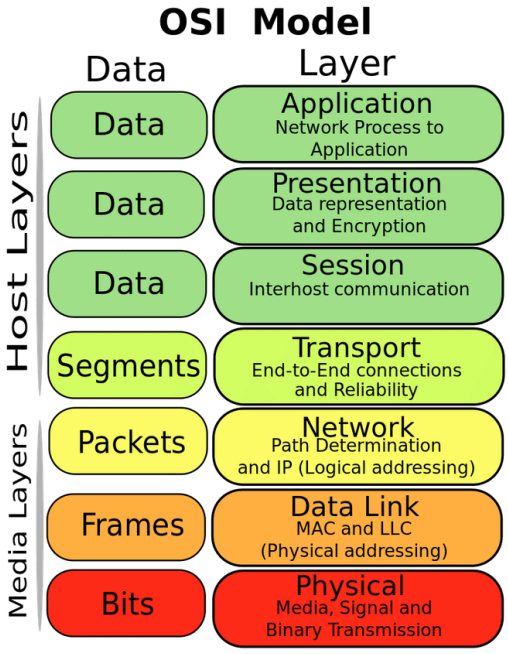

Рис. 1.1.1. Мережева модель *OSI*[10]

- Прикладний рівень (*Application layer*) визначається як 7-й рівень моделі, і забезпечує взаємодію мережі й користувача. На даному рівні забезпечується доступ між прикладним програмами користувача та мережевими службами. Прикладами такої взаємодії є обробники запитів до баз даних, доступ до файлів, пересилання електронної пошти.
- Рівень представлення (*Presentation layer*). На рівні представлення відбувається перевірка даних і їх перетворення для подальшої сумісності з комунікаційними ресурсами. Рівень відповідає за перетворення протоколів і кодування/декодування даних.
- Сеансовий рівень (*Session layer*) керує з'єднаннями між комп'ютерами, створенням/завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу.
- Транспортний рівень (*Transport layer*) визначається як 4-й рівень моделі *OSI*, що призначений для передачі та доставки даних від одного точки до іншої без помилок, втрат і дублювання.

- Мережевий рівень (*Network layer*) визначається 3-й рівень мережевої моделі *OSI*. Даний рівень необхідний для визначення шляху передачі даних. Відповідає за трансляцію логічних адрес й імен у фізичні, визначення найкоротших маршрутів, комутацію й маршрутизацію пакетів, відстеження неполадок і заторів у мережі.
- Канальний рівень (*Data Link layer*) призначений для забезпечення взаємодії мереж на фізичному рівні й контролю за помилками, які можуть виникнути. Специфікація *IEEE 802*[4] поділяє цей рівень на 2 підрівня — *MAC* (*Media Access Control*) регулює доступ до поділюваного фізичного середовища, *LLC* (*Logical Link Control*) забезпечує обслуговування мережного рівня.
- Фізичний рівень (*Physical layer*) останній рівень моделі, що призначений для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів у кабель і відповідно їхній прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. Технології фізичного рівня визначаються стандартами, що розробляються такими організаціями: *The International Organization for Standardization (ISO)*[5], *The Institute of Electrical and Electronics Engineers (IEEE)*[6], *The American National Standards Institute (ANSI)[7]*, *The International Telecommunication Union (ITU)*[8], *The Electronics Industry Alliance/Telecommunications Industry Association (EIA/TIA)*[9] тощо.

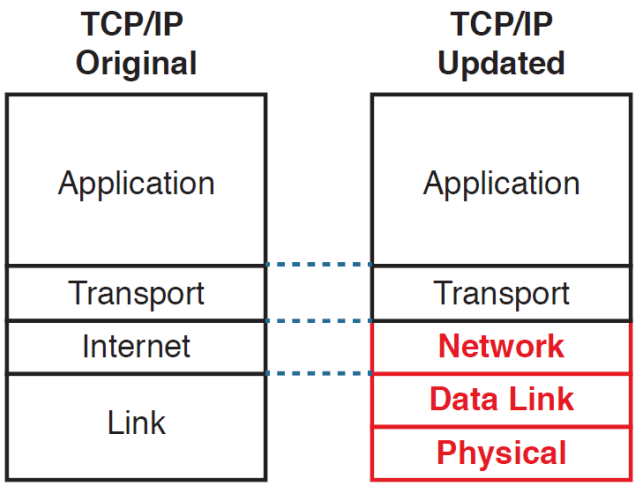

Рис. 1.1.2. Модель *TCP/IP*[10]

Стек протоколів *TCP/IP*, *TCP/IP*-модель — набір протоколів мережі Інтернет. Це систематизований стек протоколів, що поділяється на чотири рівні, які корелюються з еталонною моделлю *OSI*.

Модель *TCP/IP* має 4 абстрактних рівня: прикладний (*Application*), транспортний (*Transport*), міжмережевий (*Internet*) та рівень доступу до середовища передачі (Канальный – *Link*). [11]

- *Application* - прикладний рівень. Протоколи прикладного рівня описують, як саме додатки взаємодіють між собою.
- *Transport* - транспортний рівень. На ньому відбувається установка з'єднань між прикладними рівнями на різних комп'ютерах, управління потоком і корекція помилок.
- *Network* - мережевий рівень. Забезпечує адресацію і маршрутизацію.
- *Data-Link* - канальний рівень. Забезпечує установку з'єднання між безпосередньо з'єднаними пристроями і забезпечує виявлення помилок при передачі.
- *Physical* - забезпечує фізичне з'єднання між мережевими пристроями.

На Рис.1.1.3 приведено порівняння моделей *OSI* та *TCP/IP*. За функціями прикладний рівень моделі *TCP/IP* відповідає комбінації рівнів 5, 6, 7 моделі *OSI*, але варто зазначити, що модель *TCP/IP* не має окремих сеансового рівня та рівня представлення. Транспортний рівень *TCP/IP* аналогічний транспортному рівню моделі *OSI*, але також часткового охоплює функції сеансового рівня. Рівень доступу до даних моделі *TCP/IP* поєднує у собі канальний та фізичний рівні моделі *OSI*.

Порівнюючи ці дві моделі можна сказати, що модель *OSI* - концептуальна модель, що описує кожну взаємодію при передачі даних, в той час як модель *TCP/IP* створена для вирішення конкретних задач. Модель *OSI* не залежить від протоколів, що використовуються, на противагу тому, як *TCP/IP* заснована на стандартних протоколах.

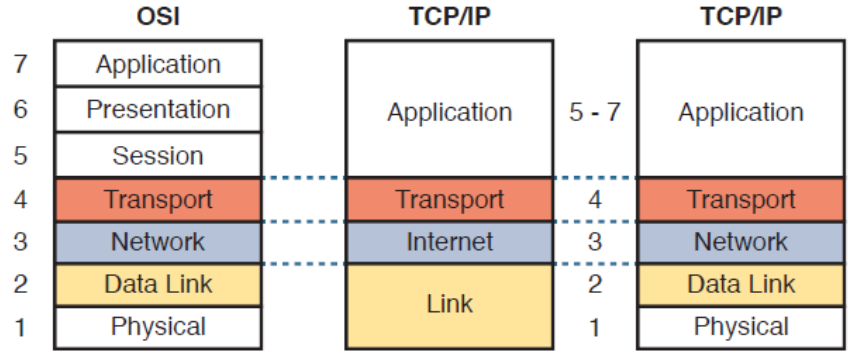

Рис. 1.1.3. Порівняння моделі *OSI* і *TCP/IP*.[10]

Рекомендаційні матеріали, що розроблені світовими лідерам з розробки протоколів, стандартів, а також з постачання мережевого програмного та апаратного забезпечення (*Cisco, HP*) визначають локальну обчислювальну мережу (ЛОМ)[3] як комп'ютерну мережу для обмеженого кола користувачів, що об'єднує комп'ютери в одному приміщенні або в рамках одного підприємства. Домашні мережі та мережі невеликих офісів часто складаються з декількох комп'ютерів і

суміщеного комутатора/маршрутизатора/бездротової точки доступу. Приклад локальної мережі представлений на рис. 1.1.3.

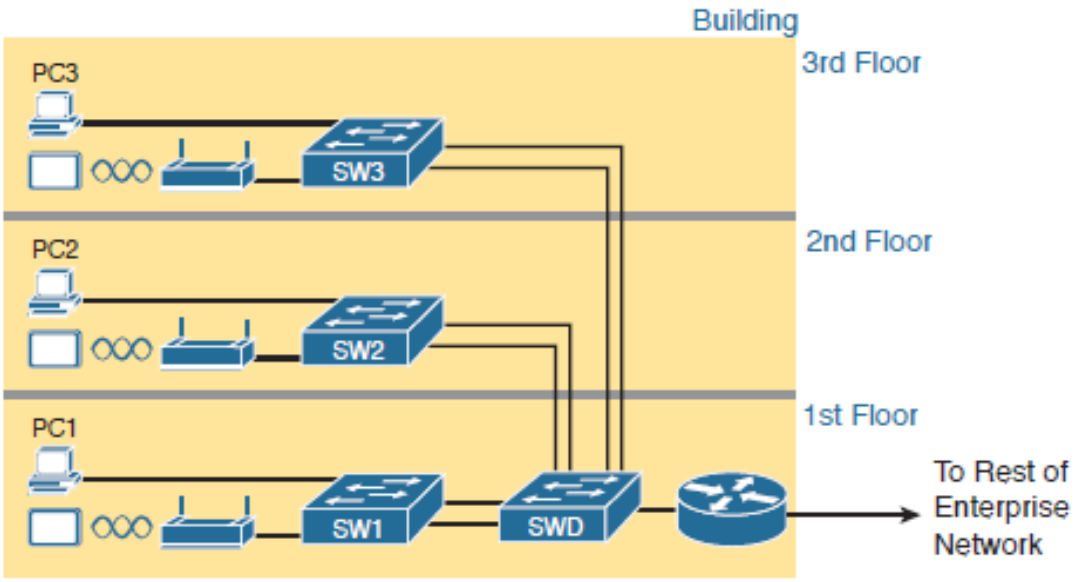

Рис. 1.1.4. Приклад ЛОМ підприємства[10]

Поняття ЛОМ може розглядатися не тільки в рамках одного офісу. Наприклад, існує мережа аптек, яка складається з кількох офісів географічно розміщених у різних кінцях міста. По відношенню корпоративної мережі до всього Інтернету, ця мережа вважається локальною.

Постає питання з'єднання між собою в одну ЛОМ певної кількості географічно розміщених офісів. На сьогодні, є безліч варіантів для вирішення цієї проблеми на будь-який вибір, залежно від бюджету, рівня безпеки та відмостійкості.

Розглянемо найбільш популярні структури для створення ЛОМ підприємства.

Перша структура. В даному випадку для зв'язку у мережі будується фізичний канал. Для цього можуть бути використані такі методи:

- *Ethernet*. За допомогою витої пари. Якісну передачу даних за такого методу можливо досягнути на відстані до 100 метрів, тобто така мережа має розташовуватися безпосередньо в рамках одного географічного розташування. Швидкість передачі даних в такій мережі досягатиме, згідно з групами стандартів *IEEE 802.3* (*Ethernet*) 1 Гбіт/с.[12]
- *WI-FI – IEEE 802.11x*.[13] Даний метод так само розраховано на використання при відносно невеликих відстанях радіусом 50-100м, окрім випадків використання надпотужних антен, використання яких потребує окремої реєстрації та дозволу ДССЗЗІ.[14] За стандартом *802.11a*, що працює на частоті 5ГГц, а також *802.11g*, що працює на частості 2,4ГГц, максимальна швидкість передачі даних складає 54 Мбіт/с. На сьогодні широко застосовується стандарт *802.11n*, що може забезпечити швидкість передачі даних 320 Мбіт/с.
- Оптоволоконне з'єднання. Найбільш оптимальним варіантом фізичного з'єднання географічно розподілених офісів є використання оптоволоконного з'єднання. Швидкість передачі даних в такій мережі досягає 1Гб/с. [15] Відстань, яку може покрити оптоволоконне з'єднання, коливається від декількох кілометрів до сотень. Проте головним недоліком є необхідність узгодження прокладання кабелю, задіяння кваліфікованого персоналу для побудування та обслуговування.

Друга структура. Оренда каналу у постачальника послуг доступу до мережі Інтернет. Даний метод більш дієвий, якщо необхідно об'єднати в одну мережу офіси, що знаходять на великій відстані. В даній структурі також існує кілька варіантів реалізації.

- Постачальник послуг виділяє в оренду власний канал фізичного зв'язку. Тобто, нівелюється необхідність побудування та обслуговування власного каналу, що знижує фінансові, економічні та виробничі затрати. Через виділений постачальником канал можливо пропускати будь-який трафік, що не обмежується чинним законодавством та/чи постачальником послуг.

• *L2VPN*. Даний спосіб відрізняється від попереднього лише тим, що трафік буде маршрутизовано через активне обладнання постачальника послуг, що може спричинити обмеження за швидкістю. Даний спосіб використовує специфікації другого (канального) рівня моделі *TCP/IP*, а саме:

- Використання *VLAN* – провайдер надає окремий *VLAN* [19] між офісами.
- *PWE3* – використання типів з'єднання, що побудовані за принципом «Точка-Точка». Всі передані фрейми без змін доставляються до віддаленої точки. Коли фрейм приходить на маршрутизатор постачальника послуг, він інкапсулюється в *PDU* вищого рівня, як правило, це пакет *MPLS*. *MPLS* (англ. *MultIProtocol Label Switching* — багатопротокольна комутація за мітками) [16] представляє собою механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів. *MPLS* працює на рівні, який можна було б розташувати між другим (канальним) і третім (мережевим) рівнями моделі *OSI*, і тому його, зазвичай, називають протоколом другого з половиною рівня (2,5-рівень).
- *VPLS* (Віртуальна приватна мережа) - симуляція локальної мережі. При даній технології мережа постачальника послуг виступає в ролі абстрактного комутатора для мережі Замовника. [18]

• *L3VPN* [17]. Дана структура буде функціонувати на третьому (мережевому) рівні. Мережа постачальника послуг виступає в ролі маршрутизатора для клієнта. Єдине, що необхідно виконати клієнту – налаштування *IP* адрес на своїх точках, а за маршрутизацію відповідає постачальник. Функціонування даної структури можливо забезпечити за допомогою технологій *GRE, IPSec, MPLS*.

Третя структура. Ця структура полягає у побудові тунелю через публічну мережу. У більшості випадків цей метод є найбільш економічно вигідним і

простим. Для цього необхідно отримати від постачальника послуг статичні зовнішні (т.з. «білі») адреси на точках і обладнання. Для реалізації даної структури можуть бути використані наступні технології: *GRE, IPSec, GRE over IPSec, VTI, DMVN.*

Virtual Tunnel Interface (VTI) використовується як альтернатива політиці *VPN*, тунель *VPN* може бути створений між одноранговими мережами з налаштованими інтерфейсами віртуального тунелю.[20] Дана технологія підтримує *VPN*[21] на основі маршруту з профілями *IPSec*, прикріпленими до кінця кожного тунелю, дозволяє використання динамічних або статичних маршрутів.

Dynamic MultIPoint VPN (*DMVPN*) [22] - це програмне рішення безпеки *Cisco IOS®* для побудови масштабованих корпоративних *VPN*, що підтримують розподілені програми, такі як голос та відео (Рисунок 1.1.5).

Cisco DMVPN широко використовується для поєднання підключення до галузі, телемережі та екстрамережі. Основні переваги включають:

- Повномережеве підключення на вимогу з простою конфігурацією концентратора та спиці
- Автоматичне спрацьовування захисту *IP* (*IPSec*) для побудови тунелю *IPSec*
- Розгортання "*Zero-touch*"[23] для додавання віддалених сайтів
- Знижена затримка та економія смуги пропускання

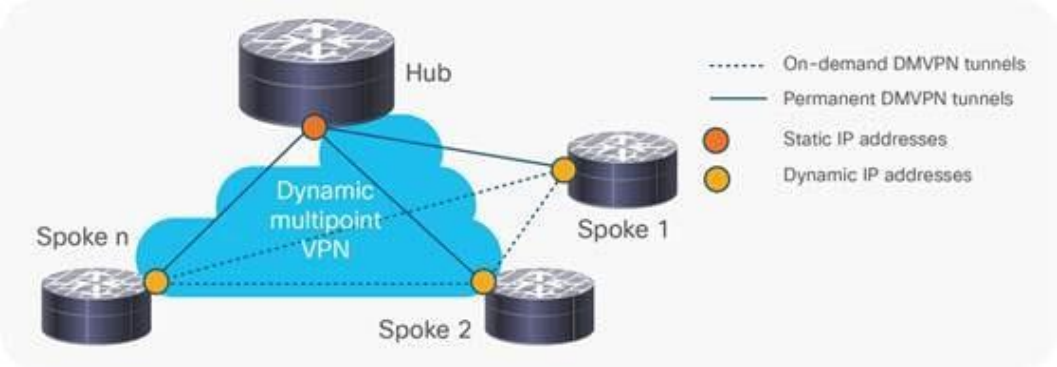

Рис. 1.1.5. *Cisco Dynamic MultIPoint VPN* [22]

Технології *GRE, IPSec, GRE* over *IPSec* мають ключове значення для даного дослідження, тому детально будуть розглянуті далі за текстом.

1.2. Визначення проблеми створення економних структур локальних обчислювальних мереж медичного призначення. з вибором критерія ефективності структури мережі.

В контексті медичного призначення, а також з урахуванням фінансово-економічного становища цільового користувача та/або замовника локальних обчислювальних, а також інформаційно-комунікаційних мереж, можливо визначити наступні чинники, що в подальшому будуть використані при формуванні визначення проблеми створення таких структур, а також допоможуть у виборі головного та додаткових критеріїв ефективності структури мережі:

1. Побудована структура локальної обчислювальної мережі має бути реалізована в умовах мінімально можливих фінансових, економічних та виробничих вкладень

2. Побудована структура локальної обчислювальної мережі має бути простою у використанні, обслуговуванні та дрібному ремонті персоналом, що не має спеціалізованої освіти у випадку критичності відновлення функціонування окремих елементів мережі

3. Структура локальної обчислювальної мережі має бути організована з урахуванням загальних технологічних та теоретичних принципів відмовостійкості програмного, апаратного та програмно-апаратного комплексів

4. Структура локальної обчислювальної мережі має бути організована з урахуванням загальних принципів інформаційної та кібербезпеки. Побудована мережа має бути в достатній мірі безпечною та ураховувати необхідність збереження цілісності, доступності і конфіденційності інформації

5. Незважаючи на необхідність максимальної економності, побудована структура локальної обчислювальної мережі має бути достатньо ефективною, забезпечувати необхідну пропускну здатність каналів, необхідну швидкість мережевого з’єднання в усіх вузлах мережі та інші аспекти ефективності мережі

Приймаючи до уваги вищезазначені чинники, можливо визначити головну проблему створення економних структур локальних обчислювальних мереж медичного призначення наступним чином: **структура локальної обчислювальної мережі, в першу чергу, має бути недорогою у побудуванні, ремонті та обслуговуванні, однак даний факт має бути реалізовано без шкоди ефективності та безпечності в рамках кожної окремої мережі.**

В таблиці 1.2.1. визначено пріоритети та вагові коефіцієнти кожного з визначених чинників при формуванні рекомендацій щодо вибору обладнання та програмного комплексу при побудові ЛОМ.

Таблиця 1.2.1.

Пріоритети та вагові коефіцієнти критеріїв для побудови ЛОМ

П/п	Чинник	Ваговий коефіцієнт
1	Мінімальність фінансових та виробничих вкладень	0.5000
2	Надійність та відмовостійкість	0.2500
3	Забезпечення безпеки інформації	0.1250
4	Простота використання та обслуговування	0.0650
5	Швидкість з’єднання та пропускна спроможність	0.0600

1.3.Оцінка та вибір структури ЛОМ медичного призначення.

Для вибору ЛОМ медичного призначення необхідно визначити основні вимоги медичних установ до мережі.

Перш за все, найбільш важливим показником для будь-якої медичної установи, включаючи аптеки, в Україні є вартість побудови та обслуговування мережі. Враховуючи події пов'язані з епідемією *COVID-19*[24][25] практично весь бюджет медичних установ направлений на боротьбу із захворюванням, а, отже, питання вартості стоїть дуже гостро.

Другим важливим показником ЛОМ медичного призначення це відмовостійкість. Медична інфраструктура вважається критично важливою[26], а тому, забезпечення відмовостійкості є одним із головних пріоритетів.

Третім не менш важливим критерієм є забезпечення безпечної передачі даних та захист від несанкціонованого доступу, оскільки в базах даних медичних установ зберігається дуже велика кількість конфіденційної інформації пацієнтів, клієнтів аптек тощо.

Також немало важливим критерієм є простота реалізації, оскільки це допоможе зберегти фінансові та економічні активи Замовника (в даному випадку мережі аптек) та виробничі затрати.

Отже, таким чином, враховуючи всі вище наведені фактори, є можливим виділити 4 критерії, за якими буде обрано структуру майбутньої ЛОМ: економічність, простота реалізації, відмостійкість та безпека передачі даних. За кожним критерієм є необхідним проведення оцінювання за 5-бальною шкалою та складання порівняльної таблиці 1.3.1. За результатами даних активностей та методів дослідження є можливим проведення вибору найбільш ефективної структури ЛОМ.

Перша структура:

- Економічність. Перша структура визначається як фізичне з'єднання компонентів мережі. Прокладати кабелі між будівлями, а тим паче між географічно розділеними офісами дуже дорого. Наприклад, середня ціна за метр

оптоволоконного кабелю, що прокладається в грунт/каналізацію складає 24 грн.за 1 метр., якщо враховувати мінімальні та максимальні фінансові вкладення, рівні яких визначено основними постачальниками даного матеріального ресурсу. Отже, щоб прокласти кабель на відстань умовно 7 км до наступного офісу/аптеки необхідно витратити 168000,00 грн. без урахування фінансових та виробничих витрат на проведення монтажних робіт та подальшого обслуговування. Враховуючи всі вищезазначені аспекти, найбільш доцільним результатом з питання даного критерію буде – 1 бал

- Простота реалізації. Для забезпечення зв'язку та створення локальної мережі між офісами, що географічно розподілені у різних кінцях міста, в даному випадку доведеться прокладати кабель через усе місто. Це може створити певні труднощі, оскільки потребує пошук підрядника, а також потребує врахування географічних особливості міста, через які може виникнути проблема прокладання найбільш оптимального шляху тощо. Враховуючи всі вищезазначені аспекти, найбільш доцільним результатом з питання даного критерію буде - 1 бал.
- Відмостійкість. Мережа, що з'єднана фізично із великою вірогідністю матиме достатній запас надійності у найближчий перспективі. Але не можна виключати той факт, що у місті часто проводяться ремонтні/дорожні роботи, у ході яких є велика вірогідність пошкодження кабелів. Тому на основі викладеного доцільною оцінкою буде - 4 бали.
- Безпека даних. Мережа має достатній у даному випадку рівень захисту середи передачі даних, оскільки більша частина трафіку проходить в середині ЛОМ без виходу у Інтернет. На основі цього доцільною оцінкою буде - 5 балів.

Друга структура:

- Економічність. Дана структура більш економна ніж така, що представлена в попередньому пункті, оскілки постачальних послуг доступу до Інтернет позбавляє Замовника від необхідності прокладати фізичний канал між офісами самостійно. Проте, послуга такого роду, за Законом України «про

телекомунікаційні послуги»[27], може бути надана лише на комерційній основі в окремому порядку. Враховуючи всі вищезазначені аспекти, найбільш доцільним результатом з питання даного критерію буде - 4 бали

• Простота реалізації. Розглядаючи питання простоти реалізації даної структури з точки зору Замовника, то дана технологія потребує мінімальних налаштувань зі сторони користувача на основі інструкцій вказаних постачальником послуг. Основуючись на вищевикладеному доцільною оцінкою буде - 5 балів

• Відмовостійкість. Відмова системи, що реалізовано за другою структурою, можливо лише за несправного обладнання зі сторони Замовника, або через проблеми зі сторони постачальника послуг. При цьому, якщо проблема виникла через вину провайдера, то останній відшкодовує збитки спричинені простоєм у роботі. Враховуючи всі вищезазначені аспекти, найбільш доцільним результатом з питання даного критерію буде - 4 бали

• Безпека даних. Оскільки постачальник послуг виділяє Замовнику окремий канал передачі даних, то до цього каналу не матиме доступу основна частина сторонніх осіб. Також враховуючи можливе використання таких технологій як *IPSec* дозволяє шифрувати дані, які передаються каналом, що також значно підвищує безпеку з'єднання. Враховуючи всі вищезазначені аспекти, найбільш доцільним результатом з питання даного критерію буде - 5 балів.

Третя структура:

• Економічність. Суть даного методу полягає у тому, що всі з'єднання створюються через Інтернет. Отже, єдине, що має бути у користувача це т.з. «білі» адреси офісів отримані від постачальника послуг доступу до Інтернет. В даному випадку рівень фінансових витрат на забезпечення послуги доступу до Інтернет мінімальний. Тому доцільною оцінкою для даної структури буде - 5 балів.

• Простота реалізації. Для реалізації даного методу використовуються такі технології, як *GRE*, *IPSec*, *GRE* over *IPSec*. Їх налаштування не викличе труднощів

у технічних фахівців компанії. Найбільш доцільним результатом з питання даного критерію буде - 5 балів

• Відмовостійкість. Аналогічно попередньому випадку відмова системи може виникнути лише за несправності обладнання Замовника, або за відсутності доступу до Інтернет. Найбільш доцільним результатом з питання даного критерію буде - 4 бали

• Безпека даних. З точки зору безпеки передачі даних даний метод поступається попереднім двум описаним вище, оскільки весь трафік передається через Інтернет, проте за допомогою такої технології як *GRE* over *IPSec* стає можливим створити окремий зашифрований канал передачі даних, який практично неможливо зламати. Враховуючи всі вищезазначені аспекти, найбільш доцільним результатом з питання даного критерію буде - 4 бали.

Таблиця 1.3.1.

Порівняльна таблиця структур ЛОМ

№	Економічність	Простота реалізації	Відмостійкість	Безпека даних	Загалом
1	1	1	4	5	11
2	3	5	4	5	17
3	5	5	4	4	**18**

За результатами проведеного оцінювання структур ЛОМ за показником економічності найбільш ефективною буде третя структура. Друга структура більш безпечна, проте потребує вищих матеріальних витрат. Найменш ефективною для великих корпоративних мереж виявляється перша структура, оскільки потребує найбільше фінансово-матеріальних витрат. Тому для подальшої роботи в даному дослідженні буде використана структура номер 3.

Надалі у роботі буде використана технологія *GRE* over *IPSec*, тому розглянемо її більш детально.

VPN між сайтами з *IPSec*

«*VPN* «від сайту до сайту» означає, що два корпоративні сайти створюють тунель *VPN*, шифруючи та надсилаючи дані між двома пристроями. Один набір правил для створення *VPN* від сайту до сайту визначається *IPSec*.

IPSec - це архітектура або структура служб безпеки для *IP*-мереж. Сама назва не є абревіатурою, а скоріше назвою, що походить від назви *RFC*, що визначає її (*RFC 4301*, Архітектура безпеки для Інтернет-протоколу), більш загально називається *IP* Security або *IPSec*. *IPSec* визначає, як два пристрої, обидва з яких підключаються до Інтернету, можуть досягти основних цілей *VPN*: конфіденційність, автентифікація, цілісність даних та антивідтворення. *IPSec* не визначає лише один спосіб реалізації *VPN*, замість цього дозволяє кілька різних варіантів протоколів для кожної функції *VPN*.

Одна із сильних сторон технології *IPSec* полягає в тому, що її роль як архітектури дозволяє їй розширюватися та змінюватися з часом у міру вдосконалення окремих функцій безпеки. цьому розділі показано, як дві кінцеві точки *IPSec* шифрують дані та додають заголовки *IPSec VPN* до зашифрованих даних.

Ідея шифрування *IPSec* може здатися лякаючою, але якщо проігнорувати математику - шифрування *IPSec* не надто складно зрозуміти. Шифрування *IPSec* використовує пару алгоритмів шифрування, які, по суті, є математичними формулами, щоб задовольнити пару вимог. По-перше, дві математичні формули - це узгоджений набір:

- Один, щоб приховати (зашифрувати) дані
- Інший - повторне створення (розшифрування) вихідних даних на основі зашифрованих даних

Окрім цих дещо очевидних функцій, дві математичні формули були обрані таким чином, що якщо зловмисник перехоплює зашифрований текст, але не має секретного пароля (який називається ключем шифрування), розшифрувати один

пакет буде важко. Крім того, формули також вибираються таким чином, що якщо зловмисник випадково розшифрував один пакет, ця інформація не дасть зловмисникові жодних переваг при дешифруванні інших пакетів. Процес шифрування даних для *IPSec VPN* працює загалом, як показано на рис.1.3.1. Варто звернути увагу, що ключ шифрування також відомий як ключ сеансу, спільний ключ або спільний ключ сеансу. » [28]

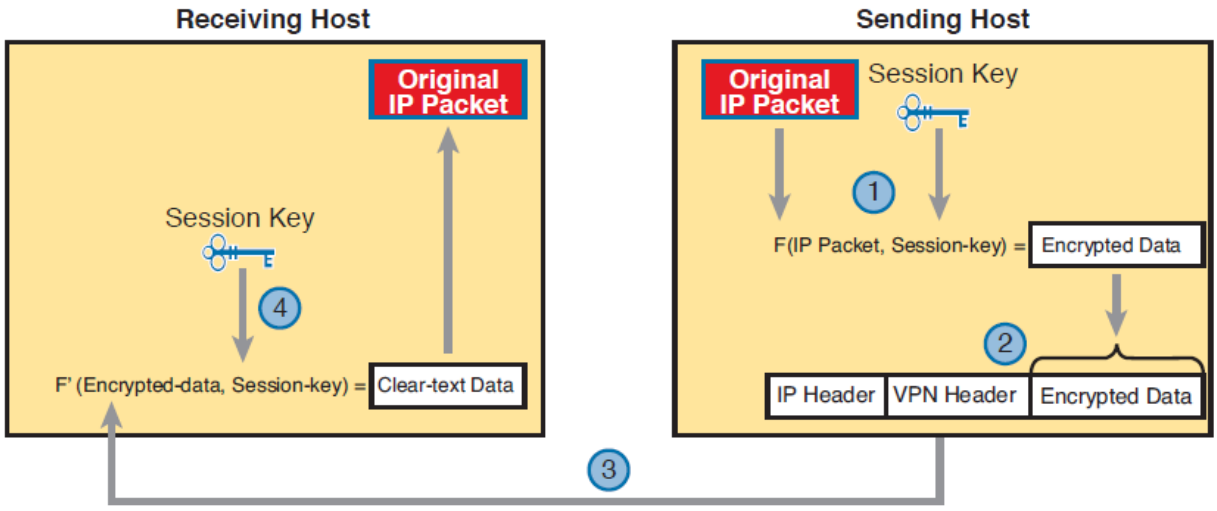

Рис.1.3.1. Основний процес шифрування *IPSec*[28]

«Чотири кроки, що показані на малюнку:

1. Надсилаючий пристрій *VPN* подає вихідний пакет і ключ сеансу у формулу шифрування, обчислюючи зашифровані дані.

2. Відправляючий пристрій інкапсулює зашифровані дані в пакет, який включає новий заголовок *IP* та заголовок *VPN*.

3. Надсилаючий пристрій надсилає цей новий пакет на пристрій *VPN* призначення

4. Приймаючий пристрій *VPN* запускає відповідну формулу дешифрування, використовуючи зашифровані дані та ключ сеансу - те саме

значення ключа, що було використано на надсилаючому пристрої *VPN* - для розшифрування даних.»[28]

Концепція *GRE* тунелю описана нижче:

«В даному розділі розглядається один тип тунелю *IP*: загальна інкапсуляція маршрутизації (*GRE*). *GRE*, визначений у *RFC 2784*, визначає додатковий заголовок, що використовується *GRE* для виконання тунелювання, разом з новим заголовком *IP*, який інкапсулює вихідний пакет. Два маршрутизатори працюють разом, з відповідними налаштуваннями конфігурації, для створення *IP*-тунелю *GRE*. Потім можна додати конфігурацію *IPSec* для шифрування трафіку.

Коли між двома маршрутизаторами існує тунель *GRE*, тунель працює майже як послідовне з'єднання для пересилання пакетів. При використанні послідовних фізичних інтерфейсів хост надсилає пакет за *IP*-адресою призначення, інкапсулює пакет у протокол лінії передачі даних, що використовується на з'єднанні. При використанні фізичних послідовних інтерфейсів мережа не потребує шифрування даних за допомогою *VPN*.

GRE створює концепцію, яка працює так само, як послідовий інтерфейс, принаймні з огляду до *IP*-маршрутизації. Замість послідовного зв'язку із послідовними інтерфейсами маршрутизатори використовують віртуальні інтерфейси, що називаються тунельними інтерфейсами. Два маршрутизатори мають *IP*-адреси на своїх інтерфейсах тунелю і знаходяться в одній підмережі. На малюнку 1.3.2 наведено приклад, коли послідовне посилання замінено на інтерфейси віртуального тунелю.

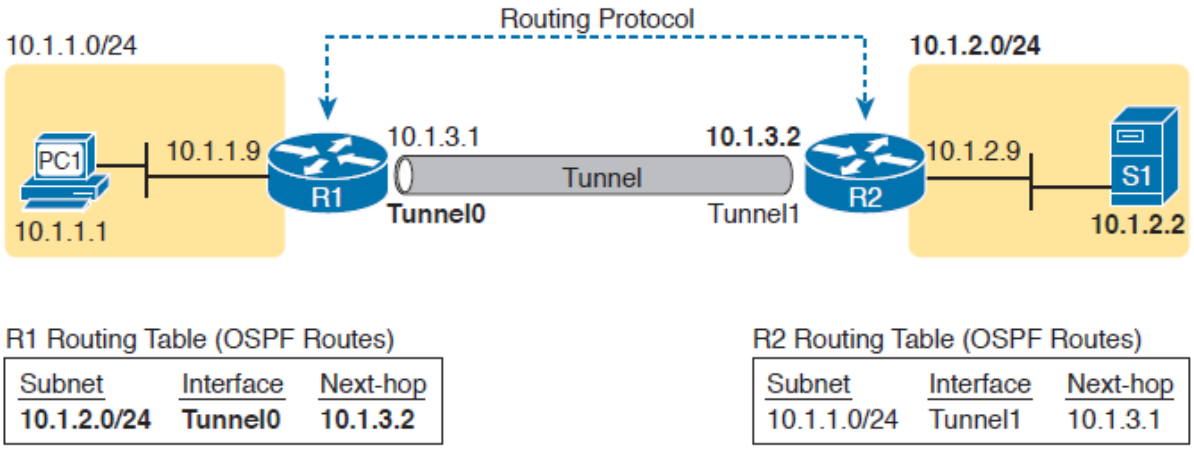

Рис.1.3.2. Заміна послідовного з'єднання на *IP*-тунель[28]

На даний момент тунель виглядає як ще одне з'єднання в захищеній частині мережі. *IP*-адреси тунелю надходять із захищеної корпоративної мережі. Маршрутизатори інкапсулюють оригінальний пакет всередині заголовка тунелю, який замінює заголовок *HDLC* послідовного з'єднання. І маршрутизатори навіть матимуть маршрути, в яких інтерфейси тунелю (у цьому випадку *Tunnel0* та *Tunnel1*) перераховані як вихідні інтерфейси.

Щоб скористатися тунелем *GRE*, маршрутизатори обробляють його як будь-яке інше з'єднання з топологією «точка-точка». Маршрутизатори мають адреси *IPv4* у тій самій підмережі. Маршрутизатори використовують протокол маршрутизації, щоб стати сусідами та обмінятися маршрутами через тунель. А маршрути, вивчені через тунель, перелічують інтерфейс тунелю як вихідний інтерфейс, а *IP*-адреса інтерфейсу тунельного маршрутизатора сусіднього маршрутизатора є наступним маршрутизатором. Тунель може існувати через будь-яку *IP*-мережу. Тунель створюється за допомогою *IP*-мережі для пересилання оригіналу пакетів, тому будь-яка *IP*-мережа між маршрутизаторами *R1* та *R2* дозволить тунелю існувати.»[28]

GRE over *IPSec*

«Хоча *IPSec* забезпечує безпечний метод тунелювання даних через *IP*-мережу, він має обмеження. *IPSec* не підтримує трансляцію *IP* або багатоадресну передачу *IP*, запобігаючи використанню протоколів, які покладаються на ці функції, наприклад протоколи маршрутизації. *IPSec* також не підтримує використання багатопротокольного трафіку.

Загальна інкапсуляція маршрутів (*GRE*) - це протокол, який може використовуватися для «перенесення» інших пасажирських протоколів, таких як широкомовне передавання *IP*-адреси або багатоадресна передача *IP*-адрес, а також протоколів, що не належать до *IP*. Використання тунелів *GRE* спільно з *IPSec* забезпечує можливість запуску протоколу маршрутизації, багатоадресної передачі *IP* (*IP*mc) або багатопротокольного трафіку через мережу між головними апаратами та філіями.

GRE також дозволяє приватну адресацію. Без запуску тунельного протоколу всі кінцеві станції повинні отримувати адреси із зареєстрованими *IP*-адресами. Шляхом інкапсуляції пакету *IP* у протоколі тунелювання можна використовувати приватний адресний простір.»[29]

Висновки до розділу

У даному розділі було проведено системний аналіз економних структур локальних обчислювальних мереж медичного призначення. Виконана оцінка та вибір структури ЛОМ медичного призначення.

Результатами системного аналізу було визначено три основі структури побудови ЛОМ медичного призначення, а саме: побудова фізичного каналу між географічно розподіленими об’єктами, оренда каналу зв’язку постачальника послуг доступу до Інтернет, побудова *VPN*-мережі на основі *IPSec, GRE over IPSec.* В рамках даної дипломної роботи найбільш фінансово доцільним методом на основі проведеного аналізу виявилася структура з побудовою *VPN*-мережі через Інтернет.

РОЗДІЛ 2.
ВИБІР ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ДЛЯ СТВОРЕННЯ ЕКОНОМНИХ СТРУКТУР ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ МЕДИЧНОГО ПРИЗНАЧЕННЯ

2.1. Способи вибору типу програмно-апаратних засобів побудови економних структур ЛОМ медичного призначення з розробкою схеми структурного алгоритму вибору.

В рамках даного дипломного дослідження зі створення ЛОМ медичного призначення як метод вибору програмно-апаратних засобів розглядається *Analytic Hierarchy Process (AHP)*[30] - метод для організації і аналізу складних рішень, що базується на математиці та психології. Метод був розроблений в 1970-х роках Томасом Л. Сааті.

Суть даного способу полягає у точному підході для кількісної оцінки ваги критеріїв прийняття рішень. Для оцінки відносної величини факторів за допомогою парних порівнянь використовується досвід окремих експертів. Кожен з респондентів повинен порівняти відносну важливість між двома пунктами відповідно до спеціально розробленої анкети (хоча більшість опитувань прийняли п'ятибальну шкалу Лікерта, анкета *AHP* становить від 1 до 9)[31]

AHP метод розроблений з метою полегшення пошуку рішення задач, що виникають, з найбільшою відповідністю цілям, які постають у проекті. Він допомагає побудувати основу для структурування проблеми прийняття рішень,

для представлення та кількісної оцінки її елементів, для зв'язку цих елементів із загальними цілями та для оцінки альтернативних рішень.

AHP використовує ієрархічний підхід до задачі, тобто за допомогою цього методу велику задачу розкладають на кілька під задач із певними критеріями. Кожну з цих задач можливо проаналізувати окремо. Елементи ієрархії можуть стосуватися будь-якого аспекту проблеми прийняття рішення — матеріального чи нематеріального, ретельно виміряного або грубо оціненого, добре або погано зрозумілого — будь-чого, що стосується відповідного рішення.

Після того, як ієрархія побудована, особи, що приймають рішення, систематично оцінюють різні її елементи, порівнюючи їх один з одним попарно, з огляду на їх вплив на елемент над ними в ієрархії. Здійснюючи порівняння, особи, що приймають рішення, можуть використовувати конкретні дані про елементи, але вони, як правило, використовують свої судження щодо відносного значення та важливості елементів. Суть *AHP* полягає в тому, що при проведенні оцінок можна використовувати кваліфіковані людські судження, а не лише основну інформацію.[32]

AHP перетворює ці оцінки на числові значення, які можна обробити та порівняти протягом усього періоду розрішення проблеми. Числова вага або пріоритет виводиться для кожного елемента ієрархії, що дозволяє порівнювати між собою різні та часто неспівставні елементи раціональним та послідовним способом. Ця можливість відрізняє *AHP* від інших методів прийняття рішень.

На завершальному етапі процесу обчислюються числові пріоритети для кожної з альтернатив рішення. Ці цифри відображають відносну здатність альтернатив досягти цілі прийняття рішення, тому вони дозволяють прямо розглянути різні напрямки дій.

Процедура використання *AHP*:[33]

- Позначення ієрархії

На початку роботи необхідно позначити проблему у вигляді ієрархічної структури, яка представляє собою т.з. «перевернуте дерево». В основі даної ієрархічної структури повинна стояти мета, яку необхідно досягти, або проблема, яку необхідно вирішити. Наступним шаром стануть критерії - параметри, величина яких впливає на підсумкове рішення. Критерії можуть поділятися на субкритерії. Далі мають бути присутні альтернативи досягнення мети. Для кожної з цих альтернатив має бути можливим визначення абсолютного або відносного значення кожного з критеріїв. Таким чином, ієрархія дозволяє розкласти складну проблему на частини, що дозволяє зрозуміти складність і багатогранність майбутнього вибору. Елементами ієрархії можуть бути як матеріальні, так і нематеріальні показники, як кількісні, так і якісні фактори.

- Розстановка пріоритетів

Для розстановки критеріїв необхідно попарно порівняти всі критерії, за допомогою яких в наступному кроці буде проводитися порівняння наявних альтернатив. Результатом даного етапу стане створення матриці пріоритетів. Сума питомих ваг субкритеріїв дорівнює критеріям.

- Порівняння альтернатив

Наступним етапом після розстановки пріоритетів стане порівняння альтернатив на основі інформації про відносну вагу кожного із критеріїв.

- Перевірка на узгодженість

У випадку, коли метод *AHP* використовується групою осіб необхідно використовувати середнє значення персональних оцінок кожного учасника. Для цього дуже важливим фактором визначається узгодженість оцінок усіх осіб.

- Прийняття підсумкового рішення

На основі результатів попарного порівняння альтернатив і визначення відносної ваги усіх виставлених критеріїв стає можливим розрахувати оцінку кожної з альтернатив. На підставі оцінок буде прийнято підсумкове рішення.

Приклад найпростішої ієрархії *AHP* для вибору лідера наведено на рис.2.1.1. У даній моделі є одна мета, три кандидати та чотири критерії вибору серед них.

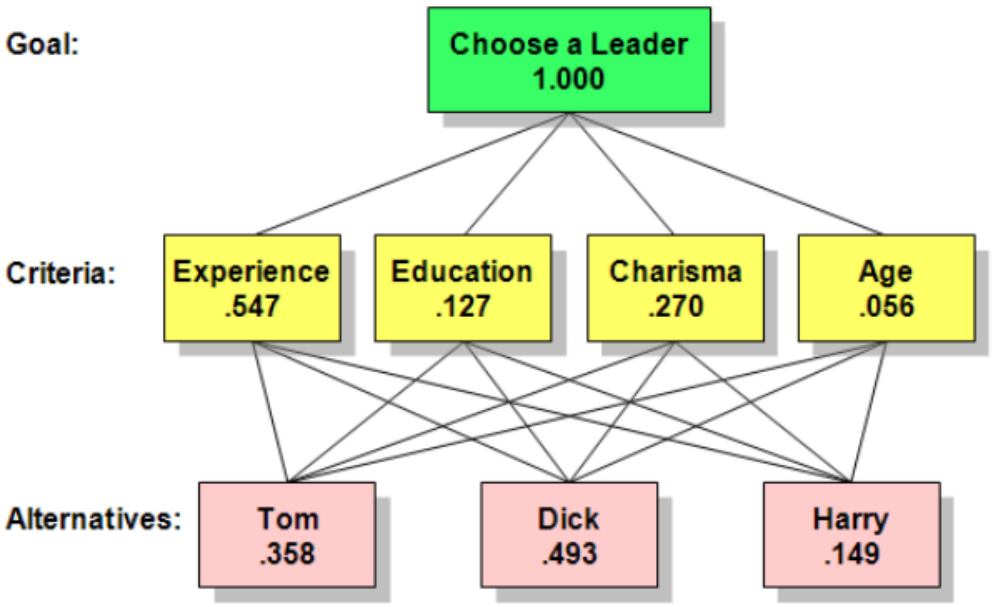

Рис. 2.1.1. Ієрархія *AHP* для вибору лідера.[34]

Проблемою, що вимагає вирішення та розв'язується за допомогою результатів даного дипломного дослідження, є підбір обладнання для роботи в ЛОМ медичного призначення.

Визначеними критеріями є:

- Мінімізація фінансових вкладень в організацію та підтримку функціональності мережі
- Надійність та відмовостійкість
- Забезпечення інформаційної та кібербезпеки
- Простота організації, конфігурації та підтримки функціональності мережі
- Швидкодійність та пропускна спроможність мережі

Альтернативами вибору в даній ситуації є обладнання певних вендорів. Коефіцієнти, що необхідні для вибору, будуть базуватися на відповідності критеріям, що зазначені у попередньому абзаці. Альтернативами вибору є:

- *Cisco*

- *HPE FlexNetwork*
- *MikroTik*
- *Linux-based PC*

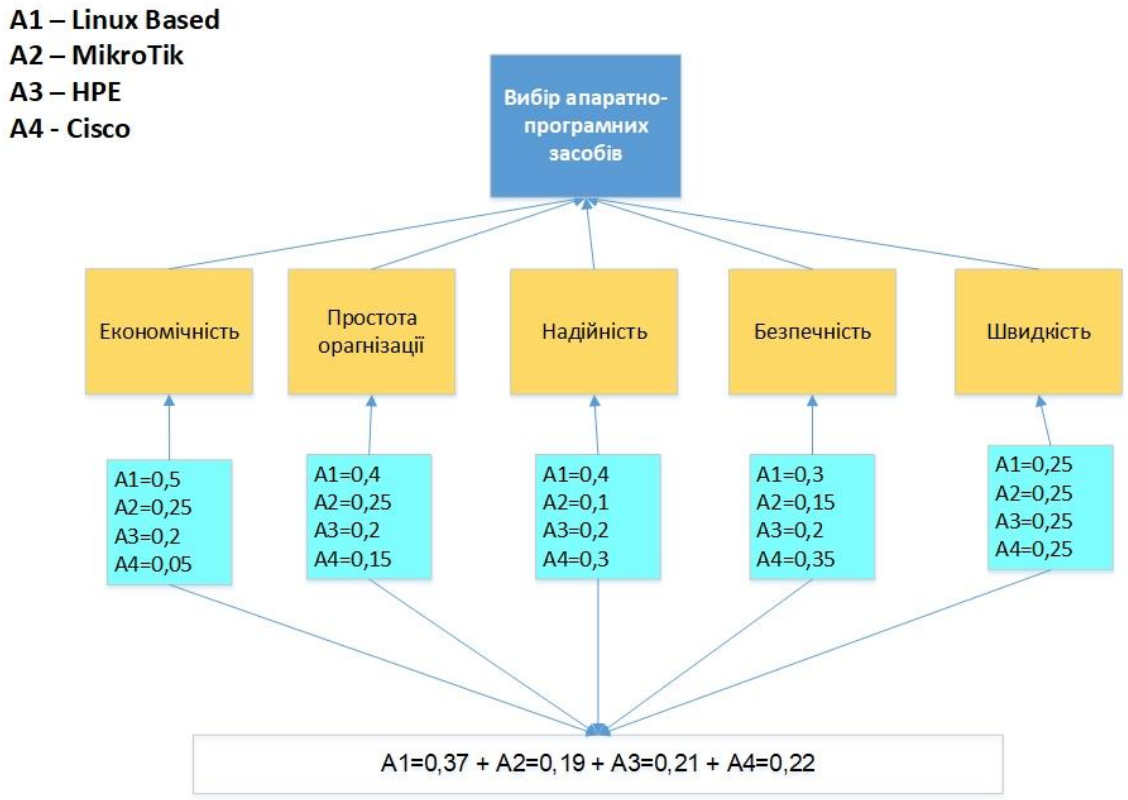

Рис. 2.1.2. Схема алгоритму вибору апартно-програмних засобів для побудови ЛОМ медичного призначення.

2.2. Огляд обладнання для створення ЛОМ з вибором обладнання з урахуванням обраних показників.

Для побудови корпоративної мережі на світовому ринку представлена велика кількість мережевого обладнання від провідних вендорів: *Cisco[3]*, *Hewlett Packard Enterprise (HPE)[35]*, *MikroTik[36]* та інші.

Компанія *Cisco* представляє декілька лінійок маршрутизаторів для мереж будь-якого типу та розміру: для агреграції глобального мережі, для постачальників послуг мережі Інтернет, промислові, віртуальні, для малого бізнесу.

В рамках даного дипломного дослідження буде розглянута серія маршрутизаторів *Cisco ASR 920 Series Aggregation Services Router*. Маршрутизатори служб агрегації *Cisco ASR 920* пропонують повний і масштабований набір служб *VPN* рівня 2 і рівня 3 у компактному пакеті. Вони мають невеликий форм-фактор — стандарт, що задає габаритні розміри технічного виробу, а також описує додаткові сукупності його технічних параметрів, наприклад форму, типи додаткових елементів розміщуваних в/на пристрої, їх положення та орієнтацію.[37] Вони також пропонують високу пропускну здатність та низьке енергоспоживання, ідеально підходять для мобільного зворотного зв'язку, бізнес-послуг та житлових програм для передачі голосу, відео та даних. Для виконання проекту розглянута модель *Cisco ASR 920-4SZ-A Router*. (Рис. 2.2.1)

Рис.2.2.1. Cisco ASR 920-4SZ-A Router

Однією з альтернатив *Cisco* буде розглянута серія маршрутизаторів *HPE FlexNetwork MSR1000 Router Series*. Маршрутизатори цієї серії забезпечують високопродуктивну маршрутизацію зі швидкістю до 500 тис. пакетів/с для невеликих філій в економічному модульному форм-факторі. Завдяки вбудованим функціям маршрутизації, комутації та безпеки, а також підтримки протоколу *SIP* без додаткового ліцензування ці маршрутизатори допоможуть прискорити надання послуг і спростити управління корпоративною глобальною мережею. Завдяки ОС *Comware v7* і зручною модульної конструкції пристрою *MSR1000*

гарантують високу продуктивність і поліпшені служби, а також надають різні варіанти підключення. Вони забезпечують гнучке управління середовищами невеликих філій на основі відкритих стандартів і надійний захист інвестицій за рахунок зниження капітальних і експлуатаційних витрат.[38] Для виконання проекту обрана модель *HPE FlexNetwork MSR1002 4* (Рис. 2.2.2)

Рис. 2.2.2 HPE Flex*Network* MSR1002 4

Другою альтернативою буде використання роутерів *MikroTik*. На разі *MikroTik* один із світових лідерів, що пропонує апаратне та програмне забезпечення для підключення до Інтернету в більшості країн світу. Ними була створена спеціальна програмна система *RouterOS*, яка забезпечує широку стабільність, управління та гнучкість для всіх видів інтерфейсів даних та маршрутизації. В рамках даної дипломної роботи буде розглянута модель *CCR1016-12S-1S+* [39] (Рис.2.2.3).

Рис. 2.2.3 *MikroTik CCR1016-12S-1S+*

Останнім варіантом вибору, що було розглянуто в даному дипломному дослідженні є використання x86-64 сумісних персональних комп’ютерів із встановленою операційною систему із сімейства *GNU Linux.*

Розглянемо кожну з альтернатив детально за обраними критеріями: мінімізація фінансових вкладень в організацію та підтримку функціональності мережі; надійність та відмовостійкість; забезпечення інформаційної та кібербезпеки; простота організації, конфігурації та підтримки функціональності мережі; швидкодійність та пропускна спроможність мережі.

Cisco ASR 920-4SZ-A Router: [40]

- Вартість: 90551,36грн. (Туті далі з прив'язкою до курсу національної валюти за 04.06.2021)
- Відмовостійкість: тут і надалі даний критерій оцінюється за показником *MTBF* (англ. *Mean time between failures, MTBF* — відношення сумарного наробітку відновлюваного об'єкта до математичного сподівання числа його відмов протягом цього наробітку[41] тобто показує, який наробіток (переважно у годинах) у середньому припадає на одну відмову (скор. наробіток на відмову).) – 301480год.
- Безпека: Вразливість в логіці, яка обробляє контроль доступу до одного з апаратних компонентів у власному впровадженні *Secure Boot* від *Cisco*, може дозволити автентифікованому локальному зловмиснику написати змінений образ прошивки на компонент. Ця вразливість зачіпає кілька продуктів *Cisco*, які підтримують апаратну функціональність безпечного завантаження. [42]
- Простота організації: наявність великої спільноти *Cisco*, що допомагає у пошуку вирішення проблем з налаштуванням; наявність великої кількості керівництв користувача із установки та налаштування, що полегшить реалізацію.
- Пропускна спроможність: на найвужчій ділянці мережі складає 1Гігабіт, на найширшій – 10 Гігабіт.

HPE FlexNetwork MSR1002 4 [43]

- Вартість: 27247,36грн.
- Відмовостійкість: *MTBF* – 1 205 299 год.
- Безпека: Вбудовані функції безпеки з апаратним шифруванням, брандмауером, *NAT* та *VPN*; обмежує доступ до команд критичної конфігурації; пропонує кілька рівнів привілеїв із захистом паролем; *ACL* забезпечують доступ через *telnet* та *SNMP*; локальні та віддалені можливості системного журналу дозволяють реєструвати весь доступ. Система контролю доступу контролера доступу терміналу *(TACACS* +); Надає інструмент автентифікації за допомогою *TCP* із шифруванням повного запиту автентифікації, забезпечуючи додатковий захист.
- Простота організації: Підтримує автоматичне розгортання *USB*-диска та автоматичне розгортання *3G SMS*; Інформаційний центр забезпечує центральне сховище інформації про систему та мережу; об'єднує всі журнали, пастки та інформацію про налагодження, що генеруються системою, та підтримує їх у порядку важкості; виводить мережеву інформацію на кілька каналів на основі визначених користувачем правил; наявність великої кількості керівництв користувача із установки та налаштування, що полегшить реалізацію.
- Пропускна спроможність: на найвужчій ділянці мережі складає 1Гігабіт, на найширшій – 10 Гігабіт.

MikroTik CCR1016-12S-1S+ **[39]**

- Вартість: 16212,45грн.
- Відмовостійкість: *MTBF* – 200 000 год.
- Безпека: Вбудовані функції безпеки з апаратним шифруванням, брандмауером, *NAT* та *VPN*; пропонує кілька рівнів привілеїв із захистом паролем; *ACL*; локальні та віддалені можливості системного журналу дозволяють реєструвати весь доступ.

• Простота організації: підтримує управління через *Web*-інтерфейс; наявні неповні керівництва користувача.

• Пропускна спроможність: на найвужчій ділянці мережі складає 1Гігабіт, на найширшій – 10 Гігабіт.

Linux Based Station

• Вартість: ОС – вільне програмне забезпечення безкоштовно. Вартість залежить лише від зборки робочої станції.

• Відмовостійкість: в середньому *MTBF* для робочої станції складає – 87658 год.

• Безпека: ОС *Linux* надає широкий інструментарій для підтримання безпеки системи; підтримує протоколи *IPSEC, GRE* та інші для побудови безпечної корпоративної мережі.

• Простота організації: ОС *Linux* можливо впровадити практично на будь-якому апаратному забезпечені, що робить його універсальним інструментом.

• Пропускна спроможність: даний показник залежить від характеристик обраної робочої станції.

На основі вищеописаного методу вибору *AHP* та характеристик обраного для дослідження обладнання, для побудови економної структури ЛОМ в рамках даного дипломного проекту найбільш доцільним програмно-апаратним засобом буде робоча станцій на ОС *Linux*.

Висновки до розділу

В даному розділі було проведено огляд способів вибору типу програмно-апаратних засобів побудови економних структур ЛОМ медичного призначення з розробкою схеми структурного алгоритму вибору.

В результаті огляду способів вибору у даному дослідженні був використаний *AHP* метод, на основі якого було вибрано програмно-апаратні засоби побудови економних структур ЛОМ медичного призначення. Обраними

програмно-апаратними засобами стали *Linux Based Station*, що є найбільш доцільними з урахуванням показника економічності. Оскільки, варість даного засобу залежить виключно від обраної робочої станції; за рівнем безпеки *Linux* надає широкий інструментарій для підтримання безпечного використання мережі; а за простотою організації ОС *Linux* можливо впровадити практично на будь-якому апаратному забезпечені, що робить його універсальним інструментом.

РОЗДІЛ 3 РОЗРОБКА ЕКОНОМНОЇ СТРУКТУРИ ЛОМ ДЛЯ МЕДИЧНИХ ПОТРЕБ

3.1. Розробка схеми мережевої інфраструктури на прикладі мережі аптек розміщеної по м. Києву.

Нехай у місті Київ існує мережа аптек. У складі мережі знаходиться 3 філії та центральний офіс. У Таблиці 3.1.1. наведено географічне розміщення кожного об’єкта.

Таблиця 3.1.1.

Георграфічне розміщення об’єктів мережі

Об’єкт	Адреса
Аптека 1	м. Київ, вул. Тулузи, 3Б
Аптека 2	м. Київ, пр. Володимира Маяковського, 60/10
Аптека 3	м. Київ, пр. Валерія Лобановського, 196
Центральний офіс	м. Київ, вул. Басейна, 10 (Палац Спорту)

На рис.3.1.1 наведено географічне розташування аптек на карті. Фото з супутника. [44]

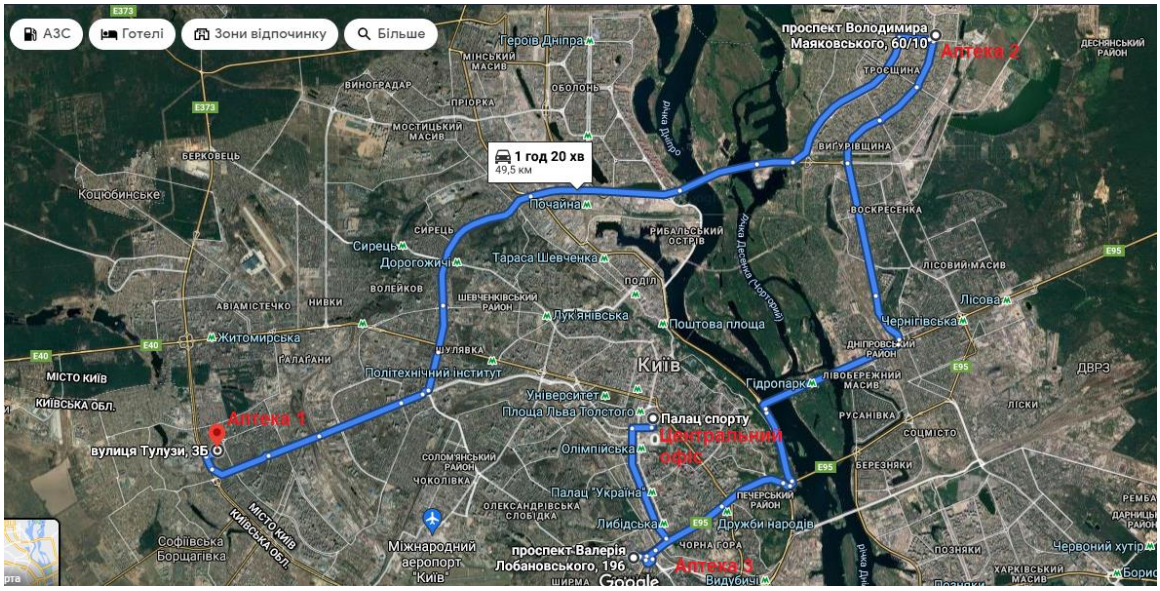

Рис. 3.1.1. Географічне розміщення мережі аптек на карті

Завданням даного дипломного дослідження є розробка методу логічного поєднання аптек в цілісну локальну обчислювальну мережу. Для цього буде використана третя структура побудови ЛОМ (п.1.3), тобто створення *VPN* з'єднання між об'єктами.

Початковий стан мережі схематично зображений на рис. 3.1.2. Кожна аптека має свою власну внутрішню адресацію та зв'язок з Інтернет через постачальника послуг.

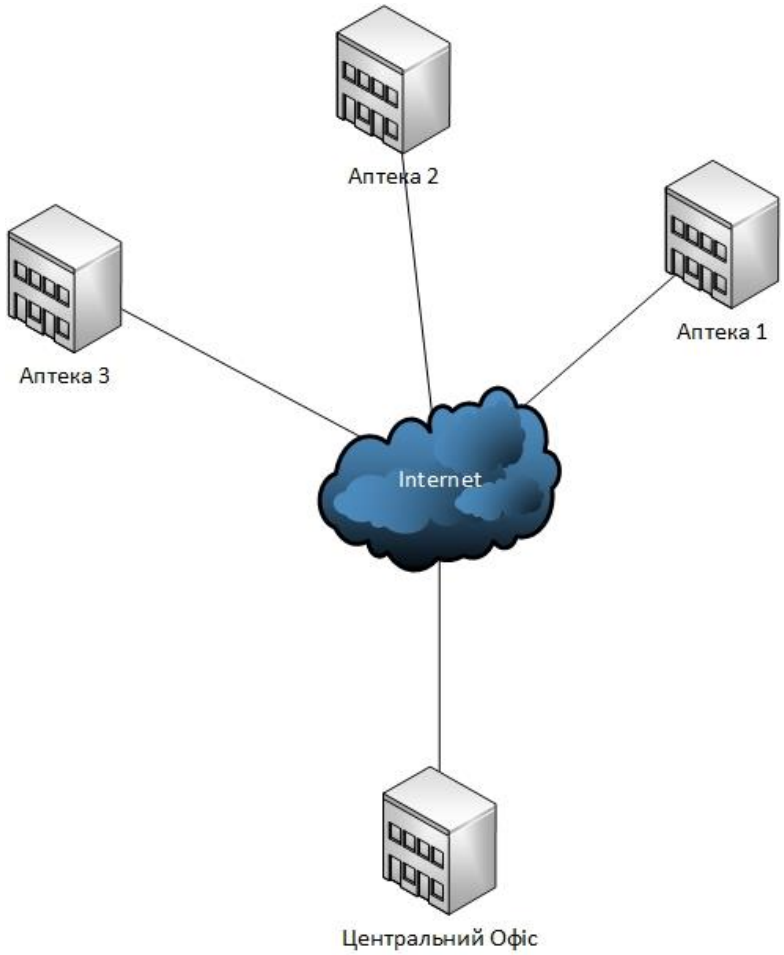

Рис.3.1.2. Початкова схема мережі

Схема побудови *VPN* представлена на рис. 3.1.3. За даною схемою у кожній аптеці встановлений маршрутизатор, який і буде поєднуючою ланкою з іншими компонентами мережі. В рамках даного дослідження реалізація комп'ютерною мережі та обладнання поза маршрутизаторами не має значення, тому на схемі на представлена.

Кожен маршрутизатор поєднаний з іншим за топологією *mesh* – «кожний із кожним»[45]. Між аптеками побудовані тунелі *GRE over IPSec*. Пунктирною лінію позначені *GRE*-тунелі між об'єктами та їх адресація у мережі. Товстою синьою лінією позначений канал зв'язку з постачальником послуг доступу до Інтернет.

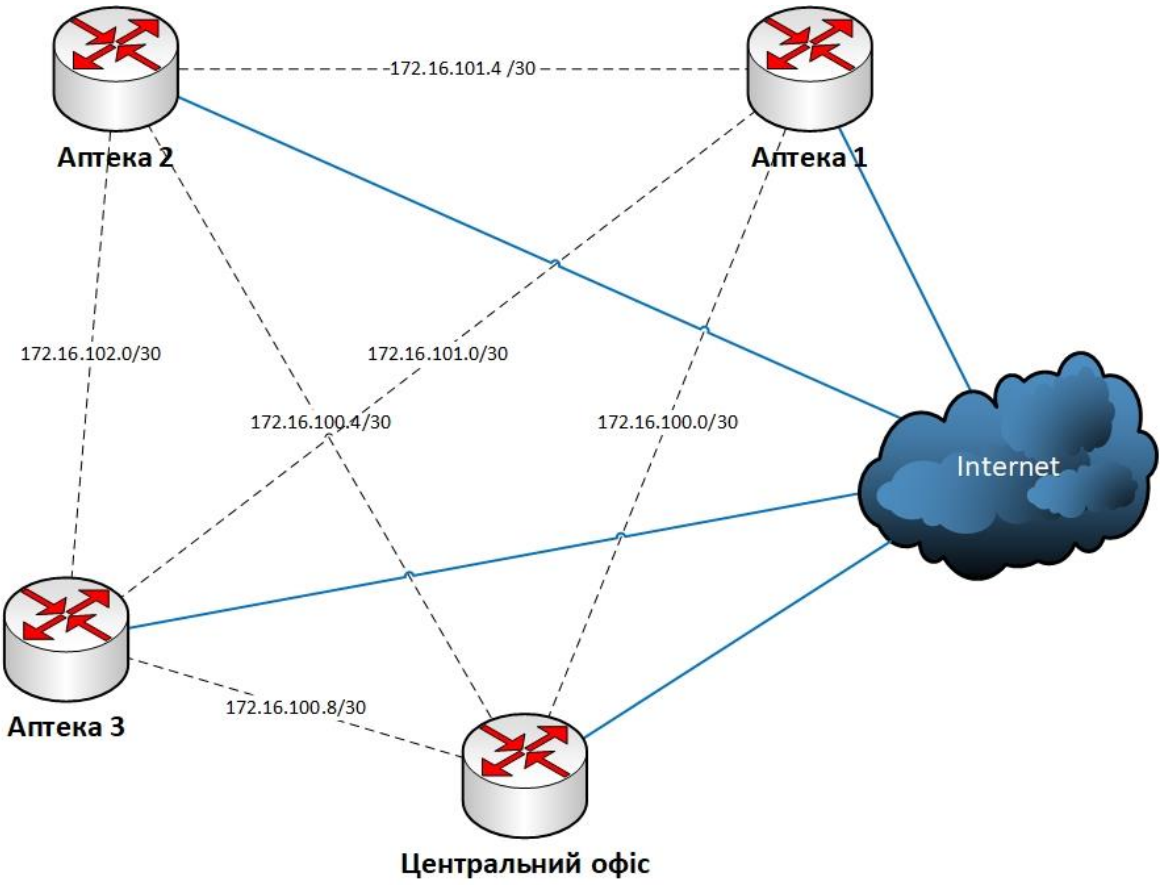

Рис. 3.1.4. Схема *VPN*-з'єднань.

Нехай дана мережа аптек використовує послуги одного постачальника доступу до Інтернет для кожної філії. Постачальник послуг використовує мережу з наступною адресацією: 172.19.22.0/24.

Адресація присвоєна аптекам наведена в таблиці 3.1.2.

Таблиця 3.2.1

Адресація об’єктів мережі

Об’єкт	Публічна адреса	Шлюз постачальника	Внутрішня адреса	*VLAN* аптеки
Аптека 1	172.19.22.113	172.19.22.1	10.10.10.1/24	10
Аптека 2	172.19.22.114	172.19.22.1	10.10.20.1/24	20
Аптека 3	172.19.22.112	172.19.22.1	10.10.30.1/24	30
Центральний офіс	172.19.22.130	172.19.22.1	10.10.100.1/24	10

Результатом правильно побудованих *GRE* over *IPSec* тунелів має бути наявність повного зв’язку між усіма об’єктами за внутрішніми адресами.

3.2. Реалізація схеми ЛОМ на базі обраного обладнання та програмних засобів.

У пунктах 1.3 і 2.2 було обрано, що реалізація ЛОМ в даному дипломному дослідженні засновується на побудові *VPN GRE* over *IPSec* на основі *Linux Based Station*.

Налаштування мережі буде виконуватися за наступним алгоритмом:

1. Перевірка ОС на наявність оновлень та їх встановлення за необхідності.
2. Встановлення пакетів мережевого адміністрування мережі.
3. Налаштування ОС в режимі маршрутизатора.
4. Налаштування адресації мережі на маршрутизаторах.
5. Налаштування *GRE* тунелів між аптеками.
6. Налаштування *IPSec* між аптеками.
7. Перевірка працездатності.

Інструменти використані для реалізації даного дипломного дослідження: *SuperPuTTY* [46] (Рис. 3.2.1) – це програма на базі графічного інтерфейсу користувача (*GUI*), яка в основному використовується для управління вкладками для клієнта *PuTTY SSH,* що є емулятором терміналу з відкритим кодом; використання віртувальних машин із встановленою ОС *Debian 10* [47].

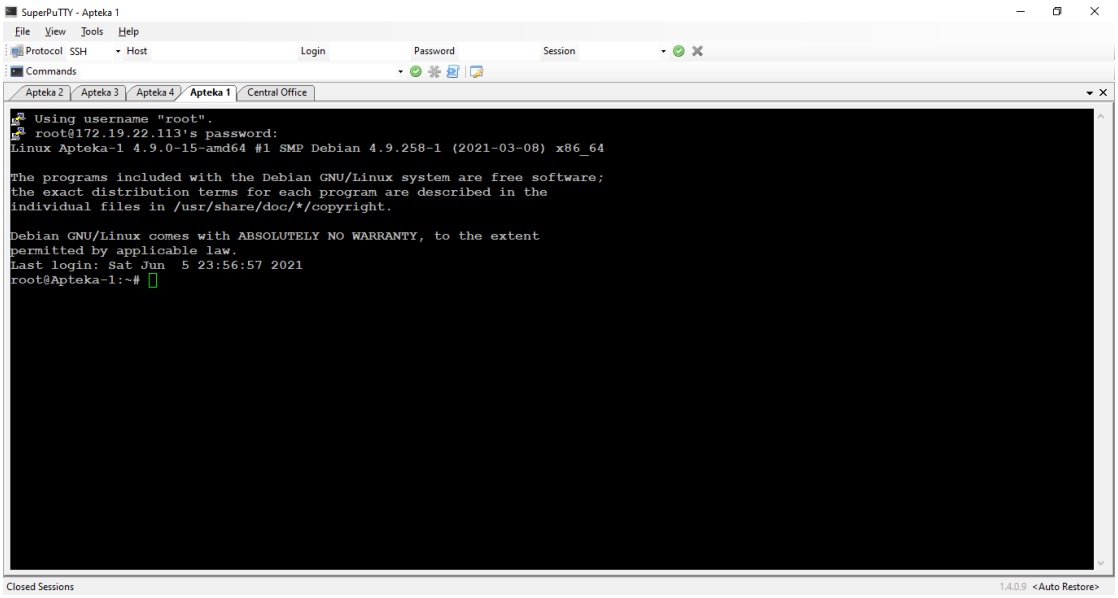

Рис. 3.2.1 Термінал *SuperPuTTY*

Налаштування Аптека 1.

1. Перевірка ОС на наявність оновлень та їх встановлення за необхідності.

Перевірка ОС на наявність оновлень самої системи та встановлений у ній пакетів виконується за допомогою команди: *apt-get update*. Оновлення системи виконується командою *apt-get upgrade*. Результат виконання команд наведено на рис. 3.2.2.

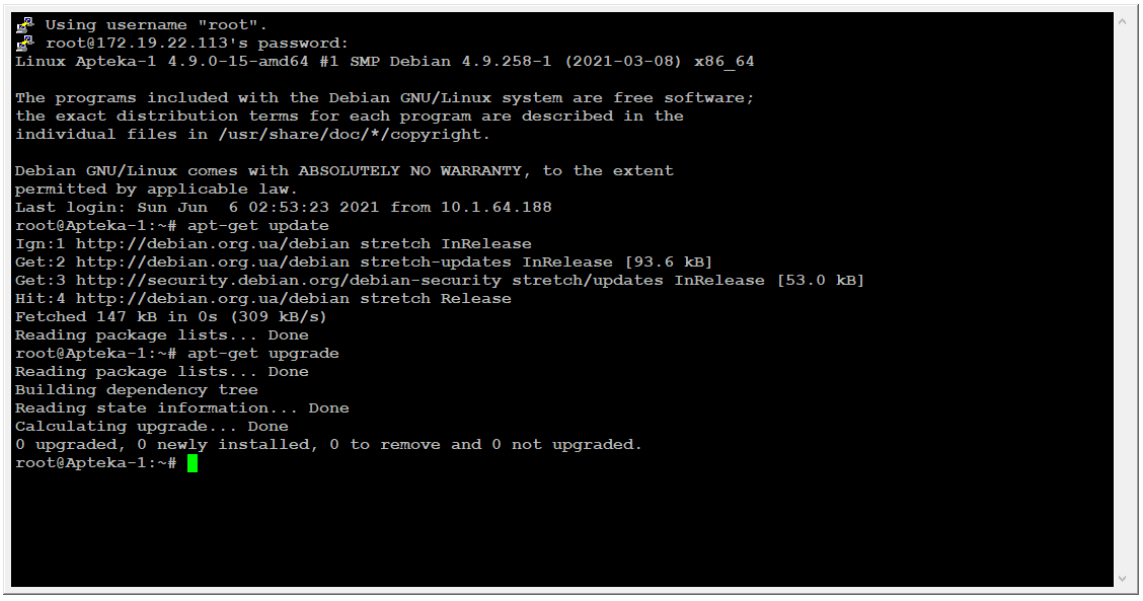

Рис. 3.2.2. Виконання команд оновлення ОС Аптеки 1.

2. Встановлення пакетів мережевого адміністрування мережі.

В ОС *Linux* необхідні для даного дипломного дослідження утиліти за замовчуванням не встановлені. Тому, перш за все, необхідно виконати встановлення таких пакетів:

- *net-tools, VLAN* – для мережевого адміністрування
- *strongswan* – утиліта для реалізації *OpenSource IPSec*.

Встановлення цих утиліт виконується за допомогою наступних команд: *apt-get install net-tools, apt-get install VLAN, apt-get install strongswang*. Виконання процесу встановлення наведено на Рис. 3.2.3. - 3.2.5

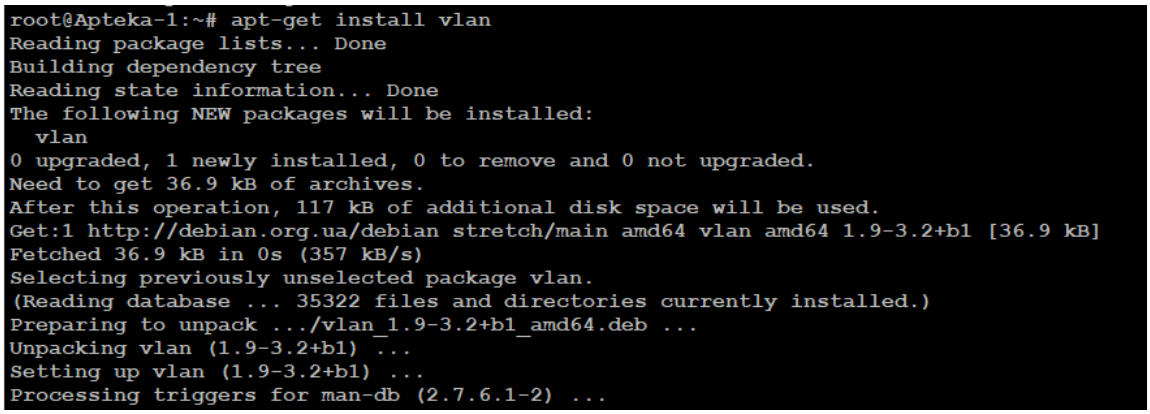

Рис. 3.2.3. Встановлення утиліти *VLAN* Аптека 1

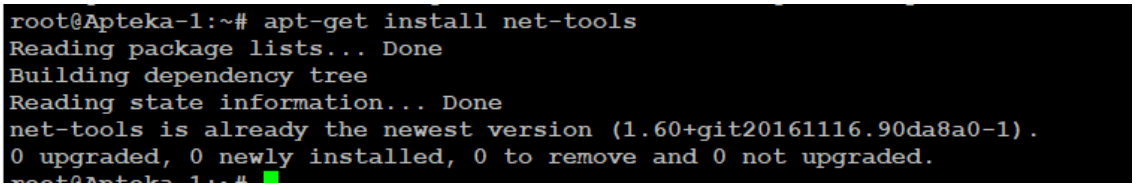

Рис. 3.2.4.Встановлення мережевих утиліт Аптека 1

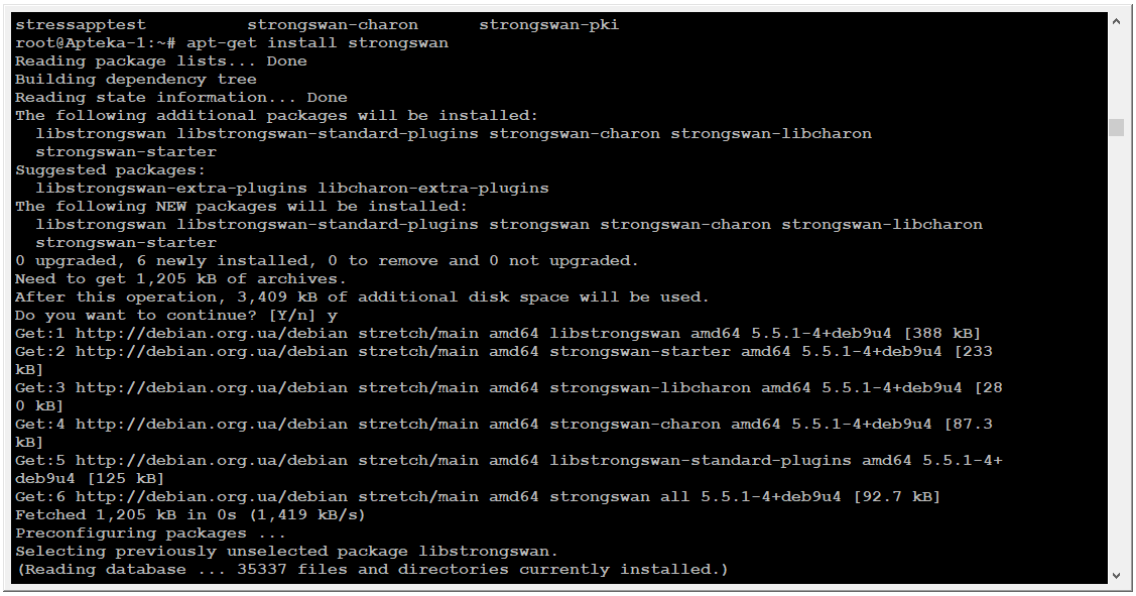

Рис. 3.2.5. Встановлення утиліти *strongswan* Аптека 1

3. Налаштування ОС в режимі маршрутизатора.

Для того, щоб Debian почав працювати в режимі маршрутизатора необхідно увімкнути пересилку пакетів. Для цього необхідно виконати команду: *sysctl net.IPv4.IP_forward=1*. Рис.3.2.6

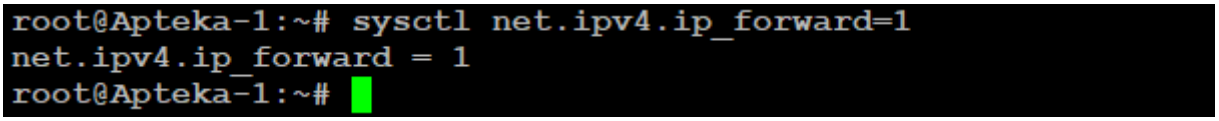

Рис. 3.2.6. Ввімкнення пересилки пакетів Аптека 1.

4. Налаштування адресації мережі на маршрутизаторах.

Налаштування адресації виконується у файлі */etc/Network/interfaces*. На рис.3.2.7 представлено налаштування публічної адреси та внутрішньої адреси мережі.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

#eth0
auto eth0
iface eth0 inet static
address 172.19.22.113
netmask 255.255.255.0
gateway 172.19.22.1
dns-nameservers 8.8.8.8 1.1.1.1

auto vlan10
iface vlan10 inet static
        address 10.10.10.1
        netmask 255.255.255.0
        vlan-raw-device eth0

```

Рис. 3.2.7. Налаштування адресації Аптека 1

Після того як налаштування *VLAN* було занесено у конфігураційний файл необхідно активувати *VLAN* інтерфейс за допомогою команд *vconfig add eth0 10 / ifup VLAN10*.

```
root@Apteka-1:~# vconfig add eth0 10
Added VLAN with VID == 10 to IF -:eth0:-
root@Apteka-1:~# ifup vlan10
Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan/config
root@Apteka-1:~#
```

Рис. 3.2.8. Включення *VLAN* інтерфейсу Аптека 1

Перевірити чи виконання виконалося успішно необхідно за допомогою команди *ifconfig*. У виводі команди *ifconfig* має з’явитися *VLAN* інтерфейс *VLAN*10 із адресацією, що була задана у файлі конфігурації.

```
root@Apteka-1:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.22.113  netmask 255.255.255.0  broadcast 172.19.22.255
        inet6 fe80::215:5dff:fe60:9936  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:60:99:36  txqueuelen 1000  (Ethernet)
        RX packets 237  bytes 20598 (20.1 KiB)
        RX errors 0  dropped 3  overruns 0  frame 0
        TX packets 78  bytes 9581 (9.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vlan10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.1  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::215:5dff:fe60:9936  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:60:99:36  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 968 (968.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рис. 3.2.9. Перевірка підключення *VLAN* інтерфейсу Аптека 1

5. Налаштування *GRE* тунелів між аптеками.

Налаштування *GRE* тунелів виконується у файлі */etc/Network/interfaces*. Рис. 3.2.10. У файлі було виконано налаштування трьох тунельних інтерфейсів по одному на кожну аптеку.

```
25
26
27 #to Apteka2
28 auto A2
29 iface A2 inet static
30         address 172.16.101.5
31         netmask 255.255.255.252
32         pre-up iptunnel add A2 mode gre local 172.19.22.113 remote 172.19.22.114 ttl 255
33         post-up ip route add 10.10.20.0/24 via 172.16.101.6
34         up ip link set A2 mtu 1400 up
35         post-down iptunnel del A2
36
37 #to Apteka3
38 auto A3
39 iface A3 inet static
40         address 172.16.101.1
41         netmask 255.255.255.252
42         pre-up iptunnel add A3 mode gre local 172.19.22.113 remote 172.19.22.112 ttl 255
43         post-up ip route add 10.10.30.0/24 via 172.16.101.2
44         up ip link set A3 mtu 1400 up
45         post-down iptunnel del A3
46
47 #to Central Office
48 auto CO
49 iface CO inet static
50         address 172.16.100.2
51         netmask 255.255.255.252
52         pre-up iptunnel add CO mode gre local 172.19.22.113 remote 172.19.22.130 ttl 255
53         post-up ip route add 10.10.100.0/24 via 172.16.100.1
54         up ip link set CO mtu 1400 up
55         post-down iptunnel del CO
56
                                                                25,0-1        96%
```

Рис. 3.2.10. Налаштування тунельних інтерфейсів Аптека 1

Тунелям присвоєна адресація за /30 маскою, що дозволяє вмістити у собі лише 2 хоста. Локальним та віддаленим адресами треба вказати публічні адреси аптек. Команда *post-up IP route add 10.10.30.0/24 via 172.16.101.2* додає маршрут до внутрішньої мережі аптеки на другому боці тунелю.

6. Налаштування *IPSec* між аптеками.

Налаштування служби *IPSec* відбувається у файлах */etc/IPSec.conf* і */etc/IPSec.secret*. Рис. 3.2.11 - 3.2.13.

У файлі необхідно задати значення: *charondebug = "all" і uniqueids = yes.*

- *config setup* - вказує загальну інформацію про конфігурацію для *IPSec*, яка застосовується до всіх з'єднань.
- *charondebug* - визначає, скільки вихідних даних налагодження Charon має бути зареєстровано.
- *uniqueids* - вказує, чи повинен конкретний ідентифікатор учасника залишатися унікальним.

```
1 # ipsec.conf - strongSwan IPsec configuration file
2
3 # basic configuration
4
5 config setup
6     # strictcrlpolicy=yes
7     charondebug = "all"
8     uniqueids = yes
9
```

Рис. 3.2.11. Налаштування значень *config setup.*

```
64 #CO
65 conn CO
66         ikelifetime=8h
67         keylife=1h
68         type=tunnel
69         authby=secret
70         left=172.19.22.113
71         leftprotoport=47
72         right=172.19.22.130
73         rightprotoport=47
74         ike=aes256-sha256-modp1024
75         esp=aes256-sha1-modp1024
76         keyexchange=ikev1
77         auto=start
78
79
80
81
```

Рис. 3.2.12. Налаштування з’єднань

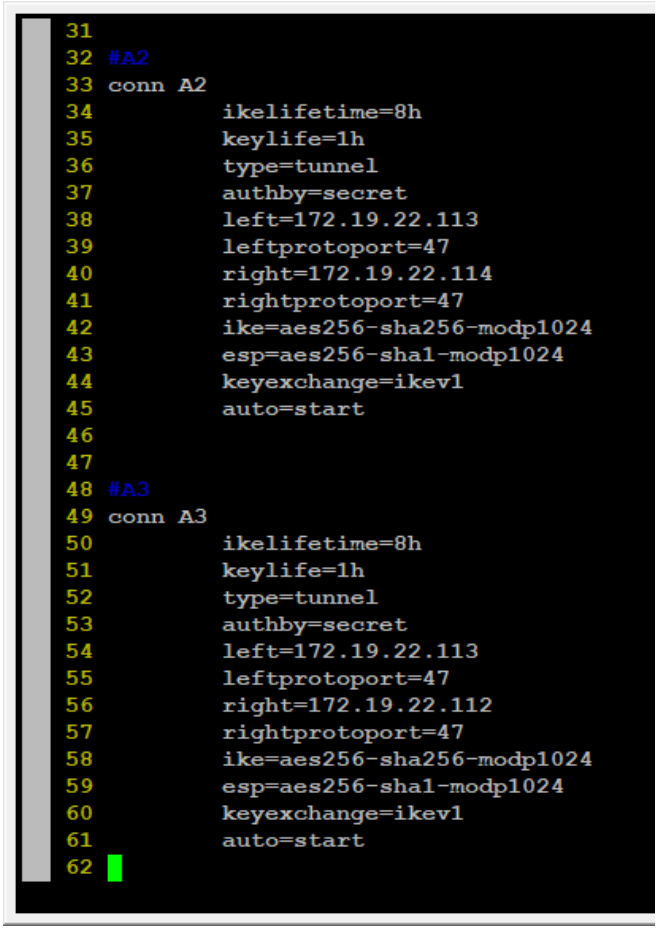

Рис. 3.2.13. Налаштування з’єднань

— *type* - визначає тип з'єднання.

— *auto* - як обробляти з'єднання при запуску або перезапуску *IPSec*.

— *keyexchange* - визначає версію протоколу IKE

— *authby* - визначає, як однорангові вузли повинні аутентифицировать один одного.

— *left* - визначає *IP*-адресу інтерфейсу публічної мережі лівого учасника.

— *leftsubnet* - вказує приватну підмережа позаду лівого учасника.

— *right* - вказує *IP*-адреса загальнодоступного мережевого інтерфейсу правого учасника.

— *rightsubnet* - вказує приватну підмережа позаду лівого учасника.

— *ike* - визначає список використовуваних алгоритмів шифрування / аутентифікації IKE / ISAKMP SA. Ви можете додати список через кому.

— *esp* - визначає список алгоритмів шифрування / аутентифікації ESP, які будуть використовуватися для з'єднання.

— *ikelifetime* - вказує, як довго має тривати канал ключів з'єднання до повторного погодження.

— *lifetime* визначає, як довго має тривати конкретний екземпляр з'єднання, від успішного узгодження до закінчення терміну дії.

Налаштування файлу */etc/IPSec.secret*. представлено на рис. 3.2.14

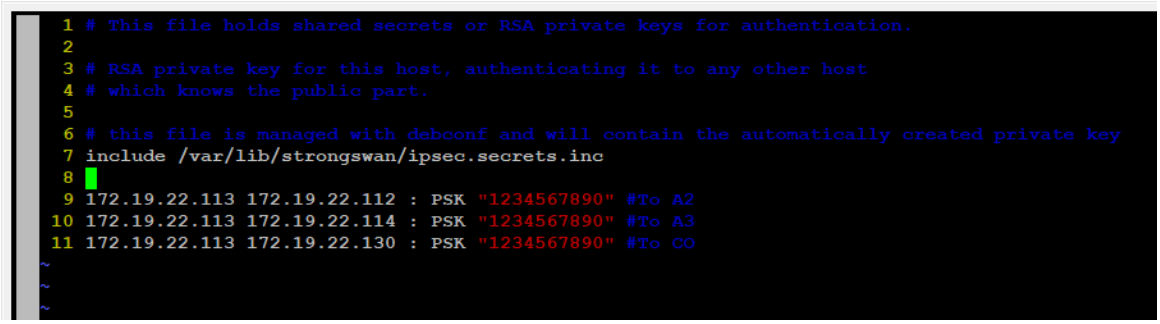

Рис. 3.2.14. Налаштування *PSK* для тимчасової аутентифікації

Аналогічні налаштування мають бути на інших аптеках. Зміст файлів конфігурації Аптеки 1, Аптеки 2, Аптеки 3, Центрального офісу наведено в Додатку А.

7. Перевірка працездатності.

Для перевірки працездатності тунелів *GRE over IPSEC* необхідно ввести команду *IPSec statusall*. Яка покаже стан усіх з’єднань, а також спробувати провести пінгування внутрішніх підмереж.

Аптека 1.

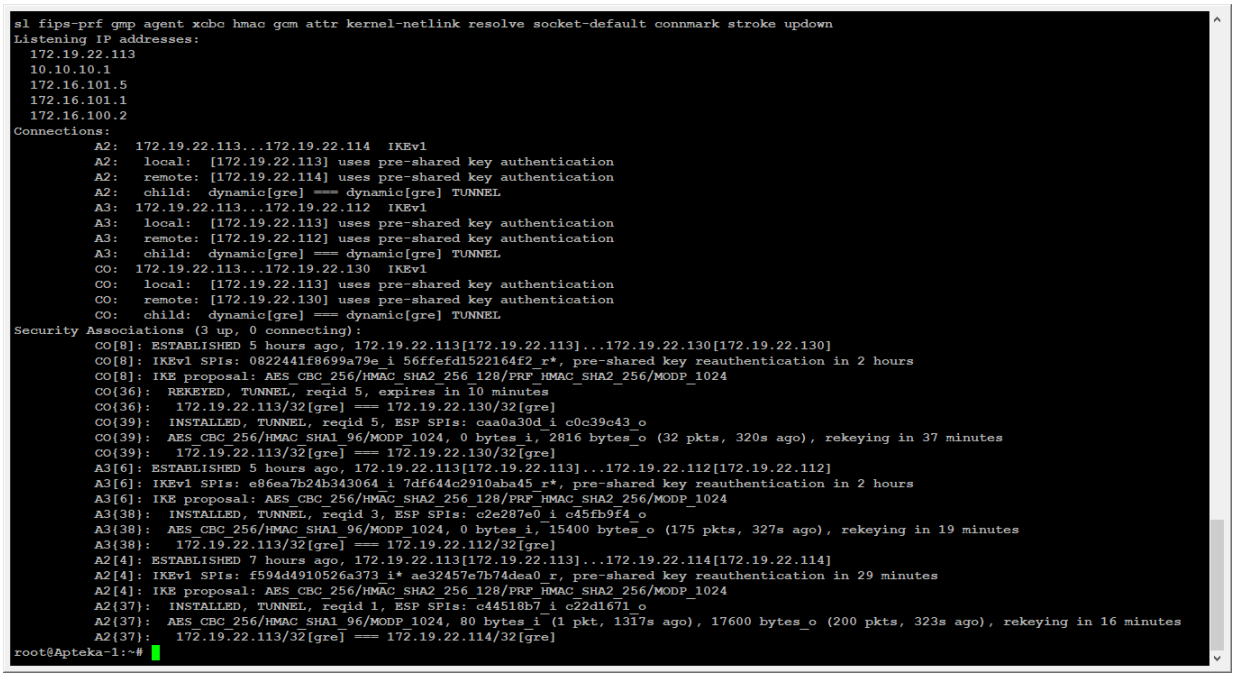

Рис. 3.2.15. Стан *GRE* over *IPSEC* з'єднань

```
root@Apteka-1:~# ping 10.10.20.1
PING 10.10.20.1 (10.10.20.1) 56(84) bytes of data.
64 bytes from 10.10.20.1: icmp_seq=1 ttl=64 time=0.528 ms
64 bytes from 10.10.20.1: icmp_seq=2 ttl=64 time=0.361 ms
^C
--- 10.10.20.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.361/0.444/0.528/0.086 ms
root@Apteka-1:~# ping 10.10.30.1
PING 10.10.30.1 (10.10.30.1) 56(84) bytes of data.
64 bytes from 10.10.30.1: icmp_seq=1 ttl=64 time=0.560 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.953 ms
^C
--- 10.10.30.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.560/0.756/0.953/0.198 ms
root@Apteka-1:~# ping 10.10.100.1
PING 10.10.100.1 (10.10.100.1) 56(84) bytes of data.
64 bytes from 10.10.100.1: icmp_seq=1 ttl=64 time=0.743 ms
64 bytes from 10.10.100.1: icmp_seq=2 ttl=64 time=0.621 ms
64 bytes from 10.10.100.1: icmp_seq=3 ttl=64 time=0.624 ms
^C
--- 10.10.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.621/0.662/0.743/0.064 ms
root@Apteka-1:~#
```

Рис. 3.2.17. Пінгування внутрішніх мереж за тунелями

Аптека 2

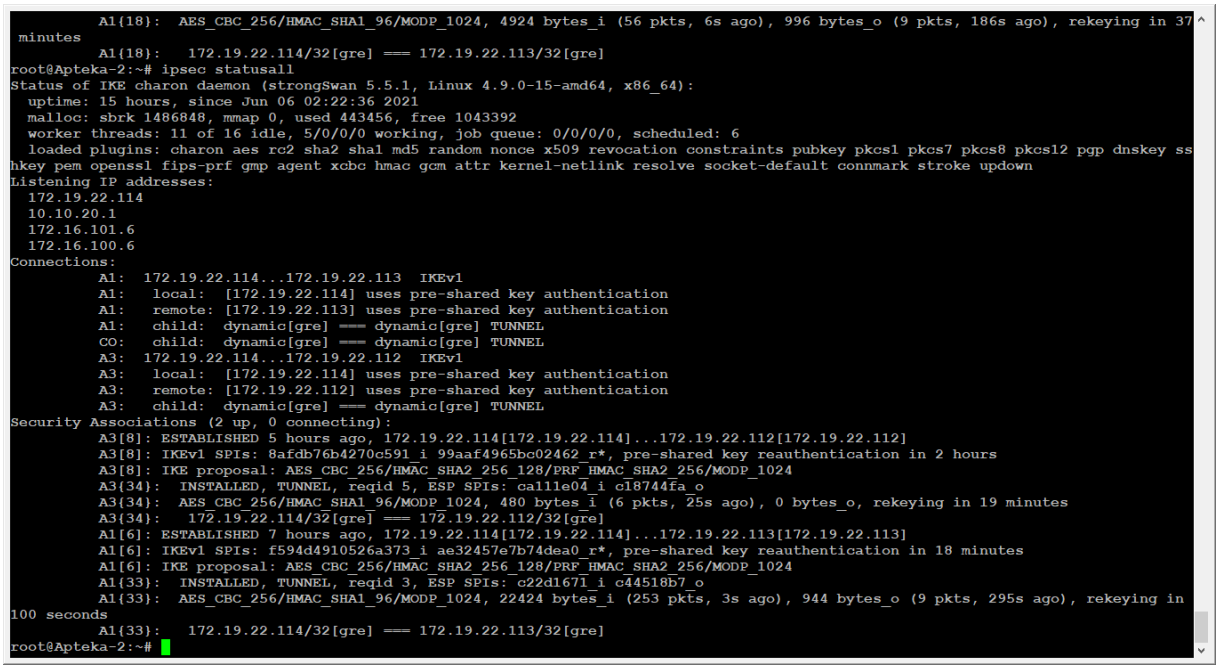

Рис. 3.2.18. Стан *GRE* over *IPSEC* з'єднань

```
root@Apteka-2:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.667 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.759 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.500 ms
^C
--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.500/0.642/0.759/0.107 ms
root@Apteka-2:~# ping 10.10.30.1
PING 10.10.30.1 (10.10.30.1) 56(84) bytes of data.
64 bytes from 10.10.30.1: icmp_seq=1 ttl=64 time=0.560 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.953 ms
^C
--- 10.10.30.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.560/0.756/0.953/0.198 ms
root@Apteka-2:~# ping 10.10.100.1
PING 10.10.100.1 (10.10.100.1) 56(84) bytes of data.
64 bytes from 10.10.100.1: icmp_seq=1 ttl=64 time=0.992 ms
64 bytes from 10.10.100.1: icmp_seq=2 ttl=64 time=0.480 ms
64 bytes from 10.10.100.1: icmp_seq=3 ttl=64 time=0.665 ms
64 bytes from 10.10.100.1: icmp_seq=4 ttl=64 time=0.761 ms
^C
--- 10.10.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3046ms
rtt min/avg/max/mdev = 0.480/0.724/0.992/0.186 ms
root@Apteka-2:~#
```

Рис. 3.2.19. Пінгування внутрішніх мереж за тунелями

Аптека 3

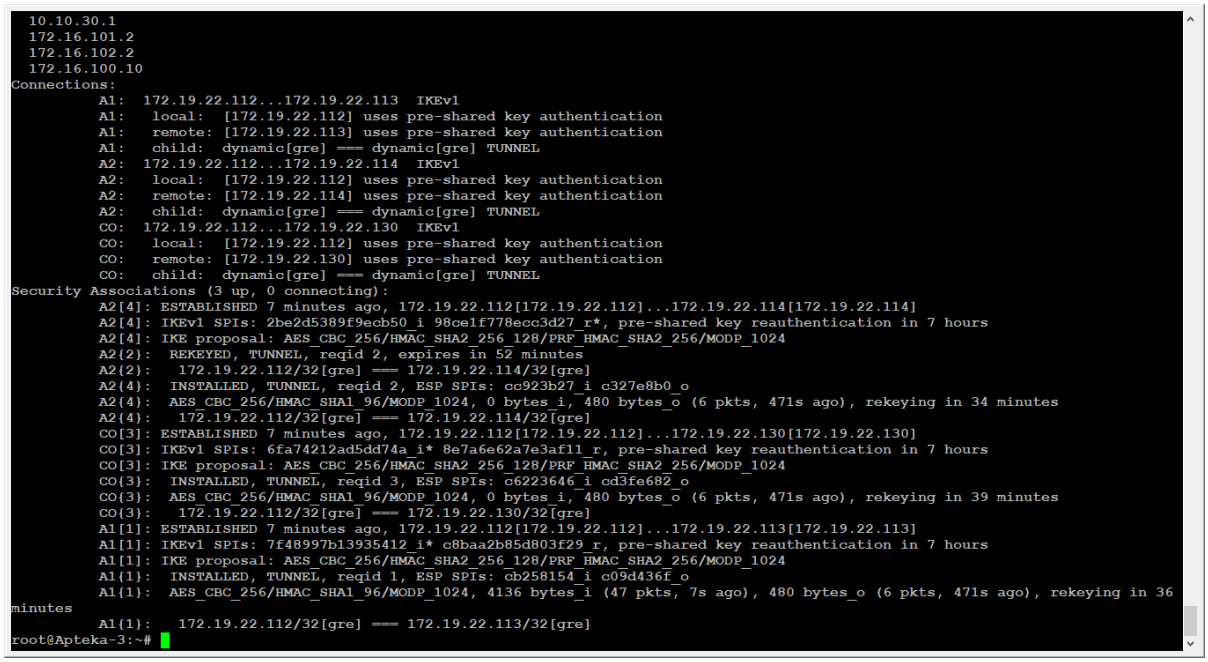

Рис. 3.2.20. Стан *GRE* over *IPSEC* з'єднань

```
root@Apteka-3:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.658 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.415 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.716 ms
^C
--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.415/0.596/0.716/0.131 ms
root@Apteka-3:~# ping 10.10.20.1
PING 10.10.20.1 (10.10.20.1) 56(84) bytes of data.
64 bytes from 10.10.20.1: icmp_seq=1 ttl=64 time=0.528 ms
64 bytes from 10.10.20.1: icmp_seq=2 ttl=64 time=0.361 ms
^C
--- 10.10.20.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.361/0.444/0.528/0.086 ms
root@Apteka-3:~# ping 10.10.100.1
PING 10.10.100.1 (10.10.100.1) 56(84) bytes of data.
64 bytes from 10.10.100.1: icmp_seq=1 ttl=64 time=0.507 ms
64 bytes from 10.10.100.1: icmp_seq=2 ttl=64 time=0.685 ms
64 bytes from 10.10.100.1: icmp_seq=3 ttl=64 time=0.310 ms
64 bytes from 10.10.100.1: icmp_seq=4 ttl=64 time=1.22 ms
^C
--- 10.10.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.310/0.682/1.226/0.340 ms
root@Apteka-3:~#
```

Рис. 3.2.21. Пінгування внутрішніх мереж за тунелями

Центральний офіс

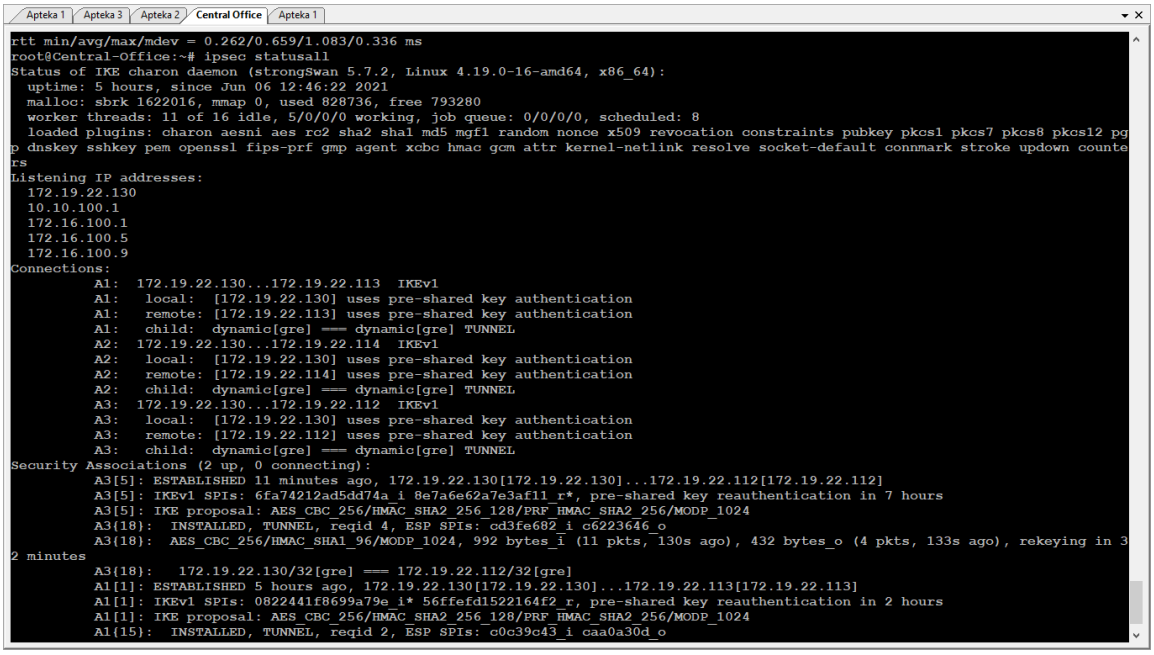

Рис. 3.2.22. Стан *GRE* over *IPSEC* з'єднань

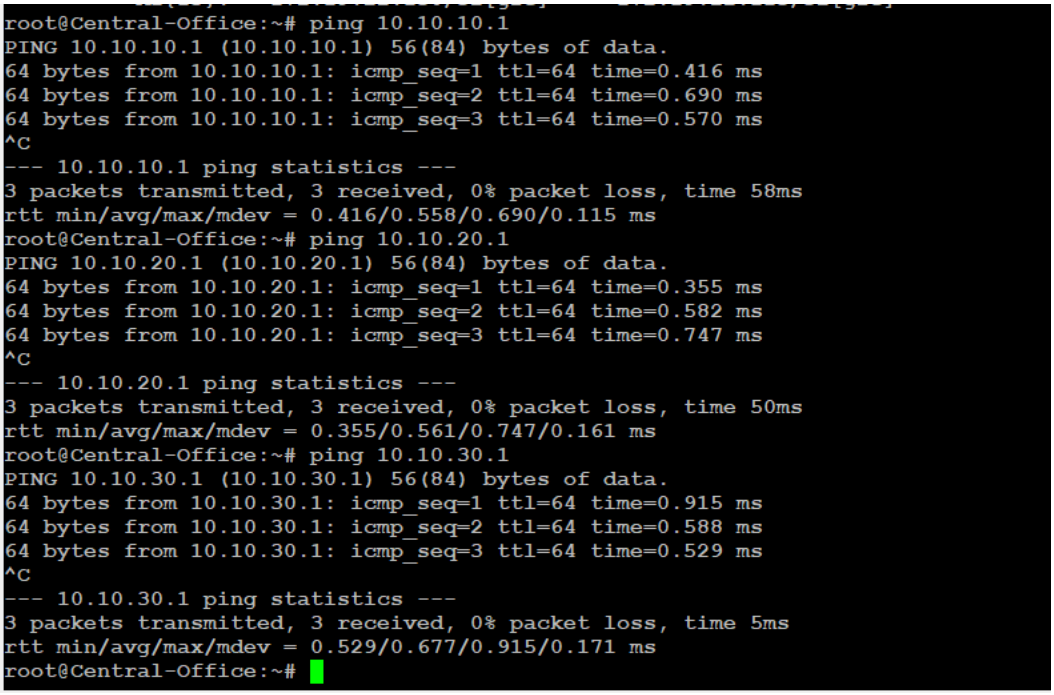

Рис. 3.2.23. Пінгування внутрішніх мереж за тунелями

Висновки до розділу

В даному розділі було проведена розробка схеми мережевої інфраструктури на прикладі мережі аптек розміщеної по м. Києву. Головним завданням даного розділу було створення ЛОМ за допомгою побудови *VPN*-з'єднань між аптеками на основі *GRE over IPSec.*

В результаті викоання цього розділу були налаштовані тунелі *GRE over IPSec* між маршрутизаторами аптек, що дало змогу об'єднати локальні мережі кожної аптеки в цілісну корпоративну ЛОМ.

Врахувоючи вищесказане, можна вважати мету даного дипломного проекту досягнутою.

ВИСНОВКИ

Метою даного дипломного дослідження було дослідження способів побудови соціальних комп'ютерних мереж з вибором та побудовою економної структури ЛОМ медичного призначення.

Для досягнення мети було розв'язано такі задачі:

1. Проведено системний аналіз економних структур локальних обчислювальних мереж медичного призначення. Оцінка та вибір структури ЛОМ медичного призначення.

У ході аналізу було визначено три основі структури побудови ЛОМ медичного призначення, а саме: побудова фізичного каналу між географічно розподіленими об'єктами, оренда каналу зв'язку постачальника послуг доступу до Інтернет, побудова *VPN*-мережі на основі *IPSec*, *GRE* over *IPSec*. В рамках даної дипломної роботи найбільш фінансово доцільним методом на основі проведеного аналізу виявилася структура з побудова *VPN*-мережі через Інтернет.

2. Проведено огляд способів вибору типу програмно-апаратних засобів побудови економних структур ЛОМ медичного призначення з розробкою схеми структурного алгоритму вибору.

В результаті огляду способів вибору у даному дослідженні був використаний *AHP* метод, на основі якого було вибрано програмно-апаратні засоби побудови економних структур ЛОМ медичного призначення. Обраними програмно-апаратними засобами стали *Linux Based Station*, що є найбільш доцільними з урахуванням показника економічності. Оскільки, варість даного засобу залежить виключно від обраної робочої станції; за рівнем безпеки *Linux* надає широкий інструментарій для підтримання безпечного використання мережі; а за простотою організації ОС *Linux* можливо впровадити практично на будь-якому апаратному забезпечені, що робить його універсальним інструментом.

3. Проведена розробка схеми мережевої інфраструктури на прикладі мережі аптек розміщеної по м. Києву. Та її повна реалізація на базі обраного обладнання та програмних засобів.

В результаті виконання цього розділу були налаштовані тунелі *GRE over IPSec* між маршрутизаторами аптек, що дало змогу об’єднати локальні мережі кожної аптеки в цілісну корпоративну ЛОМ.

Враховуючи усі вищевикладене, мету даної дипломної роботи можна вважати досягнутою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.https://ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky_Kuzmenko_Org_Komp_merej.pdf

2. https://standards.*IEEE*.org/standard/802_3-2018.html

3. https://www.cisco.com/

4. https://www.*IEEE*802.org/

5. https://www.iso.org/ru/home.html

6. https://www.*IEEE*.org/

7. https://www.ansi.org/

8. https://www.itu.int/ru/Pages/default.aspx

9. https://tiaonline.org/what-we-do/standards/

10. CCNA Routing and Switching ICND2 200-105 Official Cert Guide, WENDELL ODOM, CCIE No. 1624 with contributing author SCOTT HOGG, CCIE No. 5133

11. Кручинин, С. В. (2015). Стеки сетевых технологий *TCP/IP* и *OSI*/ISO. Вопросы науки, 3, 145-147.

12. https://standards.*IEEE*.org/standard/802_3-2018.html

13. https://www.*IEEE*802.org/11/

14. https://c*IP*.gov.ua/ua/docs

15. https://standards.globalspec.com/std/1404447/*IEEE*-1682

16. http://www.ciscopress.ru/books/5-8459-0633-4.html

17. El Mghazli, Y., Nadeau, T. D., Boucadair, M., Chan, K. H., & Gonguet, A. (2005). Framework for *layer* 3 virtual private *Network*s (l3*VPN*) operations and management. RFC4176.

18. Kompella, K., & Rekhter, Y. (2007). Virtual private LAN service (*VPLS*) using BGP for auto-discovery and signaling (p. 27). RFC 4761, January.

19. Yamasaki, Y., Miyamoto, Y., Yamato, J., Goto, H., & Sone, H. (2011, July). Flexible access management system for campus *VLAN* based on OpenFlow. In 2011 *IEEE*/*IP*SJ International Symp*OSI*um on *Application*s and the Internet (pp. 347-351). *IEEE*.

20.https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/*VPN*/asa-97-*VPN*-config/*VPN*-vti.pdf

21. Ferguson, P., & Huston, G. (1998). What is a *VPN*?.

22.https://www.cisco.com/c/en/us/products/collateral/security/dynamic-mult*IP*oint-*VPN*-dm*VPN*/data_sheet_c78-468520.html

23. Benzaid, C., & Taleb, T. (2020). AI-driven zero touch *Network* and service management in 5G and beyond: Challenges and research directions. *IEEE Network*, 34(2), 186-194.

24.https://www.president.gov.ua/news/volodimir-zelenskij-pidpisav-zmini-do-derzhbyudzhetu-na-2020-60725

25. https://www.president.gov.ua/documents/decrees

26. https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

27. https://www.kmu.gov.ua/npas/19834263

28. CCNA Routing and Switching ICND2 200-105 Official Cert Guide, WENDELL ODOM, CCIE No. 1624 with contributing author SCOTT HOGG, CCIE No. 5133, c.393-396

29.https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_*GRE_IPSec*/P2P_*GRE*/2_p2p*GRE*_Phase2.html

30. Teknomo, K. (2006). Analytic hierarchy process (*AHP*) tutorial. Revoledu. com, 1-20.

31. Li, R. Y. M., Chau, K. W., & Zeng, F. F. (2019). Ranking of risks for existing and new building works. Sustainability, 11(10), 2863.

32. Saaty, T. L. (2008). Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of

intangible factors the analytic hierarchy/*Network* process. RACSAM-Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas, 102(2), 251-318.

33. Fogliatto, F. S., & Albin, S. L. (2003). An *AHP*-based procedure for sensory data collection and analysis in quality and reliability *Application*s. Food Quality and Preference, 14(5-6), 375-385.

34.https://commons.wikimedia.org/wiki/File:*AHP*Hierarchy1.1Russian.png#/media/Файл:*AHP*Hierarchy1.1Russian.png

35. https://www.hpe.com/us/en/home.html

36. https://www.mikrotik.ua/

37. Кремень, В. Г., & Биков, В. Ю. (2014). Інноваційні завдання сучасного етапу інформатизації освіти. Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми, (37), 3-15.

38. https://buy.hpe.com/ru/ru/*Network*ing/routers/modular-ethernet-routers/msr-modular-products/hpe-flex*Network*-msr1000-router-series/hpe-flex*Network*-msr1002-4-ac-router/p/JG875A

39. https://mikrotik.com/product/CCR1016-12S-1Splus

40.https://www.cisco.com/c/en/us/products/collateral/routers/asr-920-series-ag*GRE*gation-services-router/datasheet-c78-732103.html

41. Шайдурова, К. А. (2019). Гарантований порядок доставки повідомлень в хмарних системах (Master's thesis, КПІ ім. Ігоря Сікорського).

42.https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20190513-secureboot.html

43. https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c04121295

44. https://www.google.com/maps

45. Зацепин, Э. С. (2015). Характеристики протоколов в mesh-сетях. Моделирование, оптимизация и информационные технологии, (1), 11-11.

46. https://www.puttygen.com/superputty

47. https://www.debian.org/index.ru.html

Додаток А

Зміст конфігураційних файлів маршрутизатора Аптека-1:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

#eth0
auto eth0
iface eth0 inet static
address 172.19.22.113
netmask 255.255.255.0
gateway 172.19.22.1
dns-nameservers 8.8.8.8 1.1.1.1

auto vlan10
iface vlan10 inet static
        address 10.10.10.1
        netmask 255.255.255.0
        vlan-raw-device eth0

#to Apteka2
auto A2
iface A2 inet static
        address 172.16.101.5
        netmask 255.255.255.252
        pre-up iptunnel add A2 mode gre local 172.19.22.113 remote 172.19.22.114
ttl 255
        post-up ip route add 10.10.20.0/24 via 172.16.101.6
        up ip link set A2 mtu 1400 up
        post-down iptunnel del A2

#to Apteka3
auto A3
iface A3 inet static
        address 172.16.101.1
        netmask 255.255.255.252
```

```
        pre-up iptunnel add A3 mode gre local 172.19.22.113 remote 172.19.22.112
ttl 255
        post-up ip route add 10.10.30.0/24 via 172.16.101.2
        up ip link set A3 mtu 1400 up
        post-down iptunnel del A3

#to Central Office
auto CO
iface CO inet static
        address 172.16.100.2
        netmask 255.255.255.252
        pre-up iptunnel add CO mode gre local 172.19.22.113 remote 172.19.22.130
ttl 255
        post-up ip route add 10.10.100.0/24 via 172.16.100.1
        up ip link set CO mtu 1400 up
        post-down iptunnel del CO

# ipsec.conf - strongSwan IPsec configuration file
# basic configuration

config setup
     #strictcrlpolicy=yes
     charondebug = "all"
     uniqueids = yes

# Add connections here.

#A2
conn A2
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.113
        leftprotoport=47
        right=172.19.22.114
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

#A3
conn A3
        ikelifetime=8h
        keylife=1h
```

```
        type=tunnel
        authby=secret
        left=172.19.22.113
        leftprotoport=47
        right=172.19.22.112
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

#CO
conn CO
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.113
        leftprotoport=47
        right=172.19.22.130
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

include /var/lib/strongswan/ipsec.conf.inc

# This file holds shared secrets or RSA private keys for authentication.
# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created
private key
include /var/lib/strongswan/ipsec.secrets.inc

172.19.22.113 172.19.22.112 : PSK "1234567890" #To A3
172.19.22.113 172.19.22.114 : PSK "1234567890" #To A2
172.19.22.113 172.19.22.130 : PSK "1234567890" #To CO
```

Зміст конфігураційних файлів маршрутизатора Аптека-2:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
```

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

#eth0
auto eth0
iface eth0 inet static
address 172.19.22.114
netmask 255.255.255.0
gateway 172.19.22.1
nameservers 8.8.8.8 1.1.1.1

auto vlan20
iface vlan20 inet static
        address 10.10.20.1
        netmask 255.255.255.0
        vlan-raw-device eth0

#to Apteka1
auto A1
iface A1 inet static
        address 172.16.101.6
        netmask 255.255.255.252
        pre-up iptunnel add A1 mode gre local 172.19.22.114 remote 172.19.22.113
ttl 255
        post-up ip route add 10.10.10.0/24 via 172.16.101.5
        up ip link set A1 mtu 1400 up
        post-down iptunnel del A1

#to Apteka3
auto A3
iface A3 inet static
        address 172.16.102.1
        netmask 255.255.255.252
        pre-up iptunnel add A1 mode gre local 172.19.22.114 remote 172.19.22.112
ttl 255
        post-up ip route add 10.10.30.0/24 via 172.16.102.2
        up ip link set A3 mtu 1400 up
        post-down iptunnel del A3

#to CO
auto CO
```

```
iface CO inet static
        address 172.16.100.6
        netmask 255.255.255.252
        pre-up iptunnel add CO mode gre local 172.19.22.114 remote 172.19.22.130
ttl 255
        post-up ip route add 10.10.100.0/24 via 172.16.100.5
        up ip link set CO mtu 1400 up
        post-down iptunnel del CO


# ipsec.conf - strongSwan IPsec configuration file

# basic configuration
config setup
     #strictcrlpolicy=yes
     uniqueids = yes
     charondebug = "all"

# Add connections here.

#A1
conn A1
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.114
        leftprotoport=47
        right=172.19.22.113
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

#A3
conn A3
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.114
        leftprotoport=47
        right=172.19.22.112
        rightprotoport=47
        ike=aes256-sha256-modp1024
```

```
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

#CO
conn CO
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.114
        leftprotoport=47
        right=172.19.22.113
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

include /var/lib/strongswan/ipsec.conf.inc

# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created
private key
include /var/lib/strongswan/ipsec.secrets.inc

172.19.22.114 172.19.22.113 : PSK "1234567890" #to A1
172.19.22.114 172.19.22.112 : PSK "1234567890" #to A3
172.19.22.114 172.19.22.130 : PSK "1234567890" #to CO
```

Зміст конфігураційних файлів маршрутизатора Аптека-3:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface

#eth0
auto eth0
iface eth0 inet static
address 172.19.22.112
netmask 255.255.255.0
gateway 172.19.22.1
dns-nameservers 8.8.8.8 1.1.1.1

auto vlan30
iface vlan30 inet static
        address 10.10.30.1
        netmask 255.255.255.0
        vlan-raw-device eth0

#to A1
auto A1
iface A1 inet static
        address 172.16.101.2
        netmask 255.255.255.252
        pre-up iptunnel add A1 mode gre local 172.19.22.112 remote 172.19.22.113
ttl 255
        post-up ip route add 10.10.10.0/24 via 172.16.101.1
        up ip link set A1 mtu 1400 up
        post-down iptunnel del A1

#to A2
auto A2
iface A2 inet static
        address 172.16.102.2
        netmask 255.255.255.252
        pre-up iptunnel add A2 mode gre local 172.19.22.112 remote 172.19.22.114
ttl 255
        post-up ip route add 10.10.20.0/24 via 172.16.102.1
        up ip link set A2 mtu 1400 up
        post-down iptunnel del A2

#to CO
auto CO
iface CO inet static
        address 172.16.100.10
        netmask 255.255.255.252
        pre-up iptunnel add CO mode gre local 172.19.22.112 remote 172.19.22.130
ttl 255
        post-up ip route add 10.10.100.0/24 via 172.16.100.9
```

```
        up ip link set CO mtu 1400 up
        post-down iptunnel del CO

# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
      # strictcrlpolicy=yes
      uniqueids = yes
      charondebug = "all"

# Add connections here.

# Sample VPN connections

#A1
conn A1
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.112
        leftprotoport=47
        right=172.19.22.113
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

#A2
conn A2
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.112
        leftprotoport=47
        right=172.19.22.114
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start
```

```
#CO
conn CO
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.112
        leftprotoport=47
        right=172.19.22.130
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

include /var/lib/strongswan/ipsec.conf.inc

# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created
private key
include /var/lib/strongswan/ipsec.secrets.inc

172.19.22.112 172.19.22.113 : PSK "1234567890"
172.19.22.112 172.19.22.114 : PSK "1234567890"
172.19.22.112 172.19.22.130 : PSK "1234567890"
```

Зміст конфігураційних файлів маршрутизатора Центральний-офіс:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 172.19.22.130/24
    gateway 172.19.22.1
```

```
    # dns-* options are implemented by the resolvconf package, if installed
    dns-nameservers 8.8.8.8 1.1.1.1

auto vlan100
iface vlan100 inet static
        address 10.10.100.1
        netmask 255.255.255.0
        vlan-raw-device eth0

#to Central Office
auto A1
iface A1 inet static
        address 172.16.100.1
        netmask 255.255.255.252
        pre-up iptunnel add A1 mode gre local 172.19.22.130 remote 172.19.22.113
ttl 255
        post-up ip route add 10.10.10.0/24 via 172.16.100.2
        up ip link set A1 mtu 1400 up
        post-down iptunnel del A1

#to Apteka2
auto A2
iface A2 inet static
        address 172.16.100.5
        netmask 255.255.255.252
        pre-up iptunnel add A2 mode gre local 172.19.22.130 remote 172.19.22.114
ttl 255
        post-up ip route add 10.10.20.0/24 via 172.16.100.6
        up ip link set A2 mtu 1400 up
        post-down iptunnel del A2

#to Apteka3
auto A3
iface A3 inet static
        address 172.16.100.9
        netmask 255.255.255.252
        pre-up iptunnel add A3 mode gre local 172.19.22.130 remote 172.19.22.112
ttl 255
        post-up ip route add 10.10.30.0/24 via 172.16.100.10
        up ip link set A3 mtu 1400 up
        post-down iptunnel del A3

# ipsec.conf - strongSwan IPsec configuration file
# basic configuration

config setup
```

```
    # strictcrlpolicy=yes
    charondebug = "all"
    uniqueids = yes

# Add connections here.

#CO
conn A1
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.130
        leftprotoport=47
        right=172.19.22.113
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

#A2
conn A2
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.130
        leftprotoport=47
        right=172.19.22.114
        rightprotoport=47
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

#A3
conn A3
        ikelifetime=8h
        keylife=1h
        type=tunnel
        authby=secret
        left=172.19.22.130
        leftprotoport=47
        right=172.19.22.112
        rightprotoport=47
```

```
        ike=aes256-sha256-modp1024
        esp=aes256-sha1-modp1024
        keyexchange=ikev1
        auto=start

include /var/lib/strongswan/ipsec.conf.inc

# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created
private key
include /var/lib/strongswan/ipsec.secrets.inc

172.19.22.130 172.19.22.113 : PSK "1234567890" #To A1
172.19.22.130 172.19.22.114 : PSK "1234567890" #To A2
172.19.22.130 172.19.22.112 : PSK "1234567890" #To A3
```