Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Алгоритми маршрутизації в анонімних мережах

(тема)

Виконав:

студент II курсу, групи КСМзм-23-1

Чепурна І.С.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Комп'ютерні системи та мережі
(повна назва освітньої програми)

Керівник: доц. Ткачов В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Чепурній Ірині Сергіївні
(прізвище, ім'я, по батькові)

1. Тема роботи Алгоритми маршрутизації в анонімних мережах

затверджена наказом по університету від "13" листопада 2024 р. № 189Стз

2. Термін подання студентом роботи до екзаменаційної комісії 20 січня 2025 р.

3. Вхідні дані до роботи
Існуючі статичні, динамічні та гібридні алгоритми маршрутизації в комп'ютерних мережах. Протоколи маршрутизації
Оверлейні мережі, зокрема VPN, TOR, Gnutella, Bittorent

4. Перелік питань, що потрібно опрацювати у роботі
Анонімні мережі
Технології віртуалізації з використанням платформи Proxmox
Налаштування віддаленого доступу у мережах TOR, Freenet, peer–to–peer
Налаштування віддаленого доступу за допомогою VPN
Передача еластичних та нееластичних даних в анонімних мережах

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 15 Слайдів презентації Power Point

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Розділи I,II	14.11.2024 – 01.12.2024	
2	Розділ III–V	01.12.2024 – 14.12.2024	
3	Проведення експериментальних досліджень	01.12.2024 – 20.12.2024	
4	Оформлення пояснювальної записки	21.12.2024 – 28.12.2024	
5	Оформлення презентації	29.12.2024 – 04.01.2025	
6	Подання кваліфікаційної роботи керівникові	04.01.2025	
7	Подання кваліфікаційної роботи на рецензу-	05.01.2025	
	вання		

Дата видачі завдання 13 листопада 2024 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Ткачов В.М
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 113 с., 24 рис., 7 табл., 2 дод., 90 джерел.

АНОНІМНА МЕРЕЖА, ОВЕРЛЕЙНА МЕРЕЖА, VPN, МАРШРУТИЗАЦІЯ.

Актуальність застосування анонімних комп'ютерних мереж при передачі даних через глобальні комп'ютерні мережі, на кшталт, мережі Інтернет, обумовлена зростаючим попитом на рішення, які гарантують високий рівень захисту даних та забезпечують цілісність інформації, особливо на тлі зростання загроз і ризиків витоку комерційних даних. Метою кваліфікаційної роботи є дослідження основних алгоритмів маршрутизації в анонімних комп'ютерних мережах з метою розробки рекомендацій щодо їх застосування при передачі даних з мінімальними затримками. В кваліфікаційній роботі розглянуто основні алгоритми маршрутизації, які базуються на використанні статичних, динамічних та гібридних методів маршрутизації, та які можуть бути застосовані для передачі даних у анонімних мережах, як різновиді оверлейних комп’ютерних мереж.

У ході виконання кваліфікаційної роботи було проведено порівняльний аналіз деяких алгоритмів маршрутизації, з огляду їх швидкодії при побудові маршрутів передачі даних в анонімних мережах. Показано, що досяжність високого рівня анонімності можливе шляхом використанням технологій багатошарового шифрування даних. Це можливе за рахунок комбінацій існуючих технологій віртуалізації побудови динамічних вузлів анонімної мережі, основних принципів функціонування оверлейних мереж та сучасних підходів у створенні прикордонних вузлів для синергії традиційних та оверлейних мереж.

ABSTRACT

Master`s Thesis: 113 pages, 24 figures, 7 tables, 2 appendices, 90 sources.

ANONYMOUS NETWORK, OVERLAY NETWORK, VPN, ROUTING.

The relevance of using anonymous computer networks when transferring data through global computer networks, such as the Internet, is due to the growing demand for solutions that guarantee a high level of data protection and ensure the integrity of information, especially against the background of growing threats and risks of commercial data leakage . The purpose of the qualification work is to study the main routing algorithms in anonymous computer networks in order to develop recommendations for their use in data transmission with minimal delays. In the qualifying work, the main routing algorithms are considered, which are based on the use of static, dynamic and hybrid routing methods, and which can be applied for data transmission in anonymous networks, as a type of overlay computer networks.

In the course of the qualification work, a comparative analysis of some routing algorithms was carried out, in view of their speed when building data transmission routes in anonymous networks, data transmission. It is shown that the achievement of a high level of anonymity is possible through the use of multilayer data encryption technologies. This is possible due to the combination of existing virtualization technologies for the construction of dynamic nodes of an anonymous network, the basic principles of the functioning of overlay networks and modern approaches in creating border nodes for the synergy of traditional and overlay networks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОЗУ – оперативна пам’ять (англ., Random Access Memory)

ПЗ – прикладне програмне забезпечення (англ., Application Software)

ПК – персональний комп’ютер (англ., Personal Computer)

5G – п’яте покоління мобільного зв’язку (англ., Fifth Generation)

AES – стандарт шифрування даних (англ., Advanced Encryption Standard)

AODV – протокол маршруту на вимогу (англ., Ad hoc On–Demand Distance Vector)

AS – автономна система (англ., Autonomous System)

AWS – хмарна платформа Amazon (англ., Amazon Web Services)

BDR – резервний маршрутизатор (англ., Backup Designated Router)

BGP – протокол прикордонного шлюзу (англ., Border Gateway Protocol)

BSD – операційна система на базі Unix (англ., Berkeley Software Distribution)

DDoS – розподілені атаки відмови в обслуговуванні (англ., Distributed Denial of Service)

DES – стандарт шифрування даних (англ., Data Encryption Standard)

DHT – децентралізована хеш-таблиця (англ., Distributed Hash Table)

DoS – атака «відмова в обслуговуванні» (англ., Denial of Service)

DR – призначений маршрутизатор (англ., Designated Router)

DSR – динамічна маршрутизація джерела (англ., Dynamic Source Routing)

DVA – алгоритми дистанційно-векторного типу (англ, Distance Vector Algorithms)

EGP – зовнішній протокол шлюзу (англ., Exterior Gateway Protocol)

EIGRP – вдосконалений внутрішній протокол шлюзу (англ., Enhanced

Interior Gateway Routing Protocol)

GRE – загальна інкапсуляція маршруту (англ., Generic Routing Encapsulation)

GUI – графічний інтерфейс користувача (англ., Graphical User Interface)

HMAC – код аутентифікації повідомлень на основі хешу (англ., Hash–based Message Authentication Code)

HSRP – протокол гарячого резервування маршрутизаторів (англ., Hot Standby Router Protocol)

HTTP – протокол передачі гіпертексту (англ., HyperText Transfer Protocol)

I2P – невидимий інтернет-проєкт (англ., Invisible Internet Project)

ICMP – протокол повідомлень про помилки в мережі (англ., Internet Control Message Protocol)

IDEA – алгоритм шифрування даних (англ., International Data Encryption Algorithm)

IKEv2 – версія 2 обміну ключами в Інтернеті (англ., Internet Key Exchange version 2)

IoT – Інтернет речей (англ., Internet of Things)

IP – протокол Інтернету (англ., Internet Protocol)

IP – телефонія IP-телефонія (англ., Internet Protocol Telephony)

IPSec – протокол безпеки Інтернету (англ., Internet Protocol Security)

IS–IS – протокол маршрутизації від системи до системи (англ., Intermediate System to Intermediate System)

L2TP – ротокол тунелювання другого рівня (англ., Layer 2 Tunneling Protocol)

LAN – локальна мережа (англ., Local Area Network)

LSA – алгоритм стану з’язків (англ., Link State Algorithms)

MANETs – мобільні ad hoc мережі (англ, Mobile Ad hoc Networks)

MITM – атака типу «людина посередині» (англ., Man–In–The–Middle)

MPLS – багатопротокольне комутаційне маркування (англ., Multiprotocol Label Switching)

NAT – механізм трансляції адрес (англ., Network Address Translation)

NFV – віртуалізація мережних функцій (англ., Network Function Virtualization)

OSI – модель взаємодії відкритих систем (англ., Open Systems Interconnection)

OSPF – відкритий протокол найкоротшого шляху (англ., Open Shortest Path First)

OTP – одноразові паролі (англ., One-Time Password)

P2P – однорангові мережі (англ., Peer-to-Peer)

QoS – якість обслуговування (англ., Quality of Service)

RIP – протокол маршрутизації інформації (англ., Routing Information Protocol)

RRAS – служба маршрутизації та віддаленого доступу (англ., Routing and Remote Access Service)

RSA – криптографічний алгоритм RSA (англ., Rivest-Shamir-Adleman)

SDN – програмно–керовані мережі (англ., Software-Defined Networking)

SPF – алгоритм найкоротшого шляху (англ., Shortest Path First)

SSH – протокол захищеного доступу (англ., Secure Shell)

SSL – протокол захищених сокетів (англ., Secure Sockets Layer)

SSTP – протокол безпечного тунелювання Microsoft (англ., Secure Socket Tunneling Protocol)

TCP – протокол керування передачею (англ., Transmission Control Protocol)

TLS – захист транспортного рівня (англ., Transport Layer Security)

TTL – час життя пакета (англ., Time To Live)

UDP – протокол дейтаграм користувача (англ., User Datagram Protocol)

VLAN – віртуальні локальні мережі (англ., Virtual Local Area Network)

VLSM – змінна довжина маски підмережі (англ., Variable Length Subnet Mask)

VM – віртуальна машина (англ., Virtual Machine)

VoIP – голос через IP (англ., Voice over Internet Protocol)

VPN – віртуальна приватна мережа (англ., Virtual Private Network)

VRRP – протокол резервування маршрутизаторів (англ., Virtual Router Redundancy Protocol)

VXLAN – віртуальна розширювана локальна мережа (англ., Virtual Extensible LAN)

WAN – глобальна мережа (англ., Wide Area Network)

Wi–Fi – бездротова технологія передачі даних (англ., Wireless Fidelity).

ZRP – протокол зон маршрутизації (англ., Zone Routing Protocol)

ВСТУП

Питання забезпечення конфіденційності та цілісності даних під час передачі через загальнодоступні мережі стає дедалі актуальнішим в сучасному світі цифрових технологій. Це стимулює розвиток оверлейних мереж та інших методів анонімізації. Зростання ринку цифрових послуг, збільшення попиту на віддалену роботу та вдосконалення технологій передачі даних також супроводжується зростанням кількості кіберзагроз та ризиків витоку інформації.

Використання оверлейних мереж стає дедалі розповсюдженим. Вони надають можливість забезпечити високу швидкість передачі даних та високий рівень захисту інформації від несанкціонованого доступу та витоку інформації. Шифрування даних та передача інформації ізольованими мережами та тунелями набуває широкого поширення в корпоративних комп'ютерних мережах. Маршрутизація є ключовим елементом комп'ютерних мереж, яка забезпечує вибір та побудову оптимального шляху для передачі даних від відправника до одержувача. Застосування спеціалізованих протоколів, шифрування та обфускації даних, технологій віртуалізації забезпечує конфіденційність користувачів та підвищений рівень захисту та цілісності даних в анонімних мережах. Саме тому, в порівнянні з маршрутизацією у відкритих мережах, попередня обробка та вибір маршрутів передачі даних в таких мережах має свої особливості. Підвищений рівень безпеки під час обміну даними в мережах вимагає глибокого аналізу та розробки алгоритмів маршрутизації, які також забезпечують належну продуктивність та відмовостійкість корпоративних комп’ютерних мереж.

Використання обраних або комбінованих методів маршрутизації, зокрема динамічних, статичних або гібридних, дозволяє адаптувати процес передачі даних до потреб користувачів мережі, враховуючи вимоги до продуктивності, ризики перехоплення або несанкціонованого доступу до

інформації. Саме тому аналіз та дослідження алгоритмів, які ефективно поєднують різні методи маршрутизації з механізмами обфускації, дозволяє значно підвищити рівень безпеки корпоративних комп’ютерних мереж, зберігаючи при цьому високу швидкість та надійність передачі даних.

Дана кваліфікаційна робота присвячена дослідженню основних алгоритмів маршрутизації в анонімних оверлейних мережах. Метою роботи є аналіз принципів роботи та впровадження цих алгоритмів для забезпечення високого рівня безпеки в залежності від сценаріїв використання корпоративної комп’ютерної мережі. Особливу увагу буде приділено порівнянню різних підходів до маршрутизації для забезпечення анонімності та ефективності в корпоративних комп'ютерних мережах.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність використання анонімних мереж

Питання захисту конфіденційності та безпеки передачі даних в сучасному світі є найактуальнішими через зростання цифрових загроз, стрімкого розвитку електронної комерції та електронних послуг, підвищений попит на захист особистої інформації [1].

Анонімні мережі створюють конфіденційне середовище для комунікацій, забезпечуючи захист особистих даних користувачів. Від несанкціонованого доступу та спостереження приховуються не лише ідентичність відправників та одержувачів, але й метадані та маршрути передачі даних [2]. Вони використовуються для безпечного перегляду веб–сторінок, обміну інформацією, проведення фінансових транзакцій, знижуючи ризики злому або витоку даних [3]. Це надає вагому переваги анонімним мережам в сучасному цифровому суспільстві, де пріоритетом стає захист персональних даних.

До основних переваг анонімних мереж відносяться захист конфіденційності користувачів, стійкість до кіберзагроз, зниження ризиків витоку даних, перехоплення та порушення цілісності інформації. Проте вони теж мають недоліки, зокрема збільшення затримки та зниження швидкості передачі даних в порівнянні з відкритими мережами, що обумовлено архітектурою, додатковими налаштуваннями безпеки та особливостями маршрутизації [4, 5]. Також до недоліків анонімних мереж відносять технічні складнощі налаштувань та застосування додаткового програмного забезпечення, які призводять до збільшення навантаження на апаратні ресурси. Крім цього, можливе впровадження кримінальної відповідальності при використанні таких мереж для протиправних дій [6, 7].

Досягнення оптимального балансу між швидкодією та забезпеченням високого рівня безпеки даних в сучасниxx корпоративних комп'ютерних мережах залишається актуальним завданням для науковців та мережних адміністраторів. Воєнні конфлікти, глобальні локдауни та економічна конкуренція стимулюють попит на організацію віддалених та захищених комунікацій. Тому сучасні дослідження зосереджені на розробці нових технологій та методів, які забезпечують надійну роботу комп'ютерних мереж при збереженні високої рівня продуктивності, відмовостійкості, безпеки та цілісності даних.

Автори наукових робіт приділяють особливу увагу впровадженню технологій віртуалізації, розподілених мережних систем, вдосконаленню алгоритмів маршрутизації для відкритого та захищеного трафіку, розвитку протоколів тунелювання, які задовольняють вимогам до підвищення ефективності передачі даних, резильєнтності мереж в умовах перевантажень, передачі даних з різною пропускною здатністю, забезпечення стійкості мережі до атак, а також інтеграції цих рішень в сучасних корпоративних комп'ютерних мережах в умовах підвищеного рівня безпеки та конфіденційності даних.

Так, в роботі «Дослідження технологій тунелювання в сучасних комп'ютерних мережах» було проведено аналіз протоколів тунелювання для забезпечення конфіденційного зв'язку, зокрема OpenVPN, IPSec, L2TP + IPSec та EoIP + IPSec. Результати дослідження показали, що протокол OpenVPN використовує апаратне шифрування даних, проте використання цього протоколу для тунелювання завдає значно нижчого навантаження на центральний процесор в порівнянні з іншими протоколами, зокрема IPSec [8].

Також в роботі «Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment» автори зазначають, що VPN та оверлейні мережі постають як високонадійні технології, які задовольняють вимогам безпечної та надійної інфраструктури. Вони забезпечують економічну ефективність щодо простору та часу. Основні

відмінності між різними типами оверлейних мереж, включно з VPN, полягають в методах до забезпечення безпеки, архітектури та керування потоком даних у загальнодоступних мережах. Наприклад, наскрізне шифрування даних в оверлейній мережі TOR забезпечує безпеку даних через загальнодоступну мережу. Водночас VPN забезпечують безпеку даних шляхом тунелювання, створюючи захищений віртуальний канал між кінцевими точками. Крім того, у дослідженні зазначено, що платформа для віртуалізації Proxmox VE покращує керування центральним процесором за допомогою різних методів, використовуючи віртуальні машини або контейнери, які можуть використовуватися для побудови інфраструктури оверлейних мереж завдяки застосуванню апаратних розширень віртуалізації, таких як Intel VT-x та AMD-V. В цій роботі також зазначено, що середовища віртуалізації, такі як Proxmox, забезпечують масштабованість та гнучкість мережі, завдяки можливості утримувати більшу кількість вузлів без впливу на продуктивність, проте керування централізованими тунелями та залежність від апаратних ресурсів обмежує застосування VPN у великих мережах [9].

В дослідженні «Технології анонімних мереж» автори наводять огляд існуючих анонімних мереж, зокрема TOR, Freenet, I2P, де застосовуються динамічні методи маршрутизації в децентралізованих мережах. Дослідники підкреслюють, що застосування динамічних протоколів OSPF, BGP та RIP найкраще підходить до невеликих та середніх мереж, оскільки може викликати затримки при передачі даних. Це пов’язано з витратами обчислювальних ресурсів на пошук оптимальних маршрутів. В дослідженні зазначено, що описані мережі не забезпечують високої швидкості передачі даних та повної анонімності користувачів. Також для забезпечення повної анонімності слід використовувати додаткове програмне забезпечення та мати високий рівень технічних навичок з адміністрування мереж [10].

В роботах «Analysis of peer-to-peer network protocols» та «Аналіз тенденцій розвитку пірингових мереж» авторами розглянуто концепцію

пірингової мережі, проаналізовано ряд поширених протоколів однорангових мереж, виявлено особливості, переваги та сфери застосування кожного з протоколів. Також було проаналізовано основні вразливості протоколів пірингових мереж, серед яких особливу увагу приділено BitTorrent, Gnutella, Tox, Skype та Ethereum. Концепція пірингової (P2P) мережі була вперше використана в 1969 р. В дослідженні P2P розглядається як мережний протокол, який забезпечує створення та взаємодію мережі однорангових вузлів. В піринговых мережах використовують протоколи стеку TCP/IP для передачі даних. Автори зазначають, що вибір протоколу залежить від сценарію використання пірингової мережі – для обміну файлами або для блокчейну застосовуються різні протоколи. Наразі не існує будь-якого універсального протоколу обміну даними в корпоративній комп'ютерній мережі, ось чому неможливо передбачити всі потенційні вразливості та створити універсальний захист від усіх типів атак. Виявлення вразливостей та особливостей реалізації кожного протоколу є актуальним завданням для науковців та стимулом подальших досліджень в цьому напрямі.

В цих дослідженнях також було проаналізовано протоколи обміну файлами BitTorrent та Gnutella, які дозволяють користувачам розповсюджувати аудіо-, відео- та текстові файли через децентралізовану мережу. Недоліком використання клієнтського забезпечення BitTorrent є можливість отримання файлів зі шкідливим програмним забезпеченням, яке можуть бути доступним через завантаження в одноранговій мережі [11, 12].

Попри високу відмовостійкість та інші переваги протоколу Gnutella, такі пірінгові мережі залишаються вразливими до атак, зокрема DDoS, невірного оновлення та пошуку маршруту, що може призвести до витоку інформації та несанкціонованого доступу до даних користувачів [13].

Таким чином, поглиблений аналіз і вдосконалення сучасних технологій та алгоритмів маршрутизації в анонімних мережах є важливим для забезпечення безпеки та конфіденційності передачі даних, що є ключовим фактором розвитку сучасних мережних інфраструктур. Проте, динамічні

методи маршрутизації, які застосовуються в мережах типу TOR та Freenet, а також гібридні підходи в піринговых мережах, потребують подальшого вдосконалення для підвищення ефективності в умовах зростаючих навантажень та нових кіберзагроз. Дослідження також підкреслюють переваги VPN та оверлейних мереж як надійних та економічно ефективних рішень для побудови безпечної інфраструктури. Важливість динамічних методів маршрутизації та децентралізації для підвищення стійкості та анонімності передачі даних підтверджується успішністю однорангових моделей у забезпеченні безпечного обміну інформацією.

На основі вищевикладеного, завданням для майбутніх досліджень є аналіз та оптимізація існуючих алгоритмів маршрутизації в анонімних оверлейних мережах, які забезпечують високу продуктивність та максимальний рівень захисту даних, особливо в умовах децентралізованих та однорангових моделей корпоративних комп’ютерних мереж.

1.2 Постановка задачі

Мета кваліфікаційної роботи полягає в дослідженні сучасних алгоритмів маршрутизації в анонімних мережах в умовах забезпечення високого рівня безпеки, конфіденційності та ефективності передачі даних.

Основним завданням кваліфікаційної роботи є проведення аналізу та дослідження алгоритмів маршрутизації, зокрема статичних, динамічних та гібридних методів, в оверлейних мережах, а саме в мережах TOR та Gnutella, а також застосуванні VPN-тунелів для захищеної передачі даних.

Основна увага в роботі зосереджена на оцінці ключових параметрів передачі даних різної пропускної здатності в умовах підвищеного рівня безпеки та цілісності даних при передачі в корпоративних комп’ютерних мережах обраними методами маршрутизації.

1.3 Особливості функціонування анонімних комп'ютерних мереж

Для захисту корпоративної інформації від несанкціонованого доступу, сучасних кіберзагроз та зниження ризику витоку інформації в корпоративних комп’ютерних мережах дедалі частіше використовують основні переваги та принципи організації анонімних мереж, серед яких складні алгоритми маршрутизації та шифрування, що дозволяють приховати ідентичність користувачів та маршрути передачі даних. Поряд з перевагами, вони мають низку технічних обмежень, зокрема зниження продуктивності та значні затримки під час передачі інформації, що потребує вдосконалення існуючих рішень. Оптимізація ключових параметрів анонімних мереж дозволить досягти рівня продуктивності відкритих мереж, при цьому зберігаючи високий рівень конфіденційності та безпеки даних.

Специфіка функціонування анонімних мереж враховує різні параметри, що впливають на рівень безпеки та ефективність передачі даних. Анонімні мережі класифікують за різними параметрами, зокрема архітектурою, рівнем анонімності, призначенням тощо.

В анонімних мережах найчастіше застосовуються клієнт–серверна та децентралізована моделі мережної архітектури. В клієнт-серверній моделі всі підключення здійснюються через центральний сервер, що дозволяє централізовано контролювати доступ до ресурсів мережі. В децентралізованих мережах кожен вузол може виступати водночас сервером та клієнтом. Така архітектура забезпечує підвищений рівень анонімності, оскільки немає централізованої точки контролю [14].

В мережній інфраструктурі застосовуються наступні підходи до забезпечення анонімності:

1. Використання оверлейних мереж, які забезпечують додатковий рівень безпеки та конфіденційності при передачі даних через незалежну інфраструктуру, що ускладнює аналіз і перехоплення трафіка. Цей підхід застосовується у VPN та в мережних інфраструктурах з використанням

гіпервізорів, зокрема VMware, Citrix (Xen), платформах віртуалізації, зокрема Proxmox, або в хмарних середовищах [15].

Вони забезпечують гнучкість та масштабованість у налаштуванні корпоративних мереж, дозволяючи створювати окремі сегменти з різними рівнями доступу та безпеки. Технологія контейнеризації, яка застосовується в оверлейних мережах, дозволяє зменшити навантаження на апаратні ресурси, що важливо для великих мережних інфраструктур. Також контейнеризація спрощує масштабування мережних ресурсів та автоматизацію процесів без втрати контролю над безпекою [16].

Застосування технологій NFV дозволяє переносити функції фізичної мережної інфраструктури у віртуальне середовище, що надає можливості масштабувати та швидко адаптувати мережну інфраструктуру до нових вимог. Технології NFV дозволяють реалізувати мережне обладнання, зокрема, маршрутизатори, брандмауери або балансувальники навантаження, в віртуальних машинах або в контейнерах, що значно спрощує управління мережею та знижує операційні витрати [17].

2. Застосування шифрування трафіку, яке є ключовим механізмом забезпечення безпеки передачі даних. Шифрування вмісту переданих пакетів інформації відбувається через використання поширених криптографічних алгоритмів, зокрема AES, IDEA, Blowfish, Twofish, DES. Такий вид захисту даних застосовують у різних сферах діяльності людини – від онлайн–банкінга до передачі особистих даних через електронну пошту [18].

3. Використання багаторівневої маршрутизації через ланцюг проміжних серверів дозволяє приховати ідентифікаційні дані відправника та одержувача, а також маршрут передачі даних. На кожному вузлі маршруту здійснюється заміна IP-адреси попереднього вузла на IP-адресу наступного вузла. Додаткове шифрування вмісту переданих пакетів на кожному етапі маршрутизації, яке реалізовано в “цибулевій” маршрутизації мережі TOR унеможливлює відстеження відправника та одержувача даних, забезпечуючи при цьому найвищий рівень конфіденційності та захисту інформації [19].

4. Використання підміни IP-адреси користувача є поширеним методом маскування реальної IP-адреси користувача. Такий принцип також застосовується в роботі каскаду проксі–серверів або VPN-ланцюгів [20]. Це дозволяє обходити географічні обмеження та отримувати доступ до контенту, що може бути заблокованим у певних регіонах.

5. Застосування механізму «змішування» трафіку передбачає перемішування пакетів даних та затримку їх передачі з метою ускладнення відстеження трафіку. Цей підхід дозволяє знизити ризик виявлення даних користувача та його місцезнаходження [21].

6. Використання децентралізованих мереж, зокрема I2P, TOR та Freenet, дозволяють користувачам безпечно обмінюватися інформацією через розподілену систему вузлів [22].

7. Застосування анонімних профілів та псевдонімів використовуються для обмеження збору особистих даних користувача та відстеження його активності. Такі методи часто застосовують користувачі в соціальних мережах, форумах або електронній комерції [23].

8. Використання короткотривалих сесій до мережних ресурсів або веб-ресурсів мінімізують ризики виявлення активності користувача протягом часу спостереження, таким чином знижуючи ймовірність ідентифікації користувача та виявлення його місцезнаходження [24].

Псевдоніми та короткочасні сесії використовуються для захисту особистих даних користувача під час його індивідуального доступу до веб-ресурсів. Проте підміна IP-адрес, шифрування, використання анонімних децентралізованих мереж або побудова сегментів оверлейних мереж є технічними методами анонімізації, які можуть бути використані в корпоративних комп’ютерних мережах. для забезпечення високого рівня захисту даних, збереження цілісності інформації та мінімізації ризиків витоку або перехоплення інформації.

Незважаючи на перелічені переваги методів анонімізації існують суттєві недоліки, зокрема зниження ефективності, високі затримки при

передачі даних, що підтверджені численними науковими дослідженнями в цьому напрямі. Додаткове шифрування на кожному вузлі «цибулевої» маршрутизації призводять до значних затримок передачі даних. Так само в піринговых мережах високі затримки через помилки в побудові та оновленні маршрутів спричиняють зниження ефективності децентралізованих мереж. Обмеження апаратних ресурсів фізичної інфраструктури, яка є основою оверлейних сегментів теж є вагомим фактором зниження ефективності анонімних мереж.

Постановка задачі кваліфікаційної роботи полягає в дослідженні та аналізі існуючих методів маршрутизації, зокрема статичних, динамічних та гібридних методів. Аналіз особливостей функціонування анонімних мереж вказує на необхідність глибокого аналізу методів маршрутизації, зокрема дослідження ключових параметрів передачі даних в корпоративних мережах при передачі трафіку різної пропускної здатності.

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ ТРАДИЦІЙНИХ АЛГОРИТМІВ МАРШРУТИЗАЦІЇ ТА АЛГОРИТМІВ МАРШРУТИЗАЦІЇ В АНОНІМНИХ МЕРЕЖАХ

Маршрутизація є ключовим процесом, який визначає маршрут передачі інформації від джерела до одержувача. Маршрутизація відбувається на мережному рівні моделі OSI, де маршрут формується на основі аналізу стану мережних пристроїв та параметрів потоку даних [25]. Алгоритми маршрутизації повинні враховувати можливі перевантаження та адаптацію до змін в мережі для забезпечення стабільності та неперервності передачі даних.

Основні принципи маршрутизації є універсальними для різних видів комутації, але найбільша варіативність спостерігається в мережах з пакетною передачею даних (рисунок 2.1) [26].

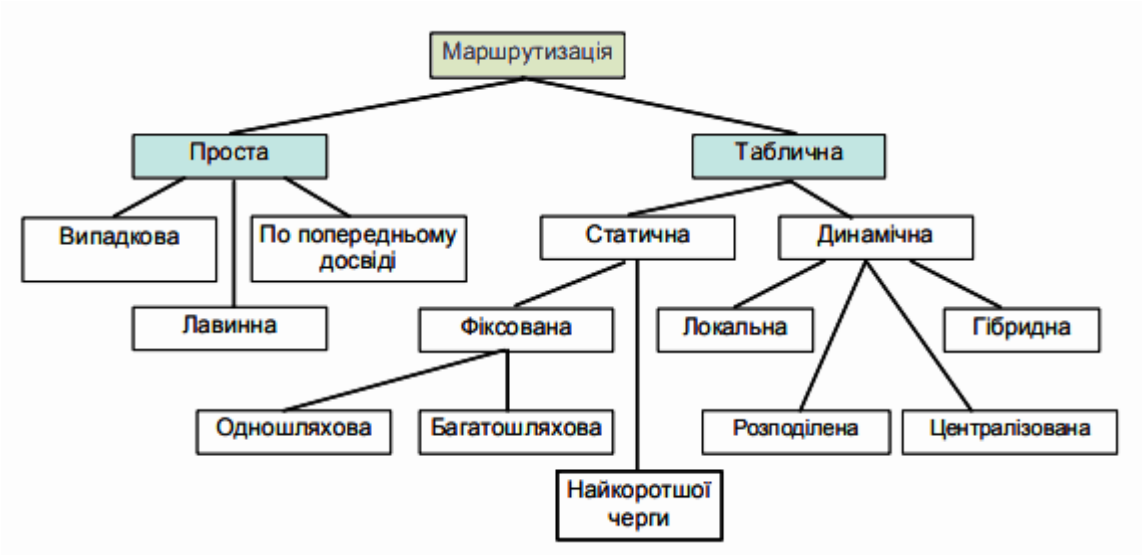


Рисунок 2.1 – Методи маршрутизації в мережах передачі даних

Алгоритми табличної маршрутизації поділяються на дві основні групи: покрокова маршрутизація та маршрутизація від джерела.

Покрокова маршрутизація характеризується тим, що кожен вузол самостійно приймає рішення до якого наступного вузлу відправити пакет, тобто самостійно визначає наступний вузол передачі даних. Головним чинником, який впливає на вибір наступного вузла є інформація про доступні маршрути, яка зберігається в таблиці маршрутизації кожного вузла передачі – маршрутизаторі. Критеріями вибору маршруту можуть бути кількість проміжних вузлів до кінцевого вузла одержувача, затримка передачі пакетів, пропускна здатність вузла або каналу зв'язку.

Крім покрокової маршрутизації існує маршрутизація від джерела, що базується на алгоритмі Форда – Фалкерсона, в якій маршрут будується від кінцевого вузлу одержувача – IP-адреса пункту призначення задається в заголовку пакету. Надалі всі проміжні вузли дотримуються цього визначеного маршруту передачі пакету. Маршрутизація від джерела наразі є найбільш використовуваним методом передачі даних, оскільки за таким маршрутом найлегше контролювати реальний маршрут пакетів, а також це ускладнює несанкціонований доступ до зміни маршруту. Такий метод маршрутизації відповідає роботі мереж з комутацією каналів або мереж з використанням віртуальних каналів передачі [27].

Проста маршрутизація може здійснюватися за відсутності таблиць маршрутизації та без участі спеціальних протоколів. Така маршрутизація, в свою чергу, поділяється на види: випадкова, лавинна та за попереднім досвідом.

Випадкова маршрутизація передбачає відправку пакету в будь-якому напрямі, крім того, звідки пакет надійшов. Лавинна маршрутизація може застосовуватися в разі, коли розмноження пакетів є припустимим, та здійснює розповсюдження пакетів в усіх напрямках, крім того, звідки пакети надходять. Маршрутизація за попереднім досвідом здійснюється в разі, коли маршрутизатор "запам'ятовує" напрямки, якими було надіслано та успішно доставлено пакети. Проте проста маршрутизація застосовується обмежено в мережах TCP/IP, оскільки не є характерною для таких мереж.

В анонімних мережах маршрутизація враховує вимоги щодо збереження конфіденційності маршруту та захисту переданих даних. Саме тому, в таких мережах застосовують схожі методи маршрутизації, які забезпечують підвищений рівень безпеки передачі даних та маршрутів передачі, а також приховування ідентифікаційних даних джерел та одержувача.

Мережі з відкритим трафіком, як відомо, для передачі даних використовують протокол IP, проте він не гарантує захисту переданих даних. Таким чином, дані, що передаються за протоколом IP можуть бути підроблені або перехоплені, що обумовлюється структурою протоколу [27].

Оверлейні мережі забезпечують додатковий захист маршрутів та ідентифікаційних даних користувачів, що дозволяє гарантувати захист переданих даних в порівнянні з протоколом IP. Такі мережі функціонують як логічна надбудова поверх фізичної інфраструктури, що дозволяє створювати захищені канали або окремі сегменти для обміну даними. Оверлейні мережі забезпечують додатковий рівень абстракції, що сприяє інтеграції різних мережних середовищ, зменшуючи складність управління, підвищуючи масштабованість та ефективну передачу даних в корпоративних мережах. Основними характеристиками оверлейних мереж є ізольованість, модульний підхід, гнучкість архітектури та здатність підтримувати різноманітні протоколи, що забезпечують роботу корпоративної мережі, безпеку та роботу різноманітних сервісів, забезпечуючи вимоги та потреби користувачів. Слід зазначити, що модульний підхід дозволяє адаптувати використання мережних ресурсів до кількості та ролей користувачів, а також до зміни протоколів, які забезпечують роботу та взаємодію з сервісами корпоративної мережі. Ізольованість в оверлейних мережах досягається через формування окремих сегментів або інших структур мережної інфраструктури за допомогою використання віртуальних машин або контейнерів, що також надає додатковий рівень захисту мережній інфраструктурі. Такий підхід забезпечує побудову розвиненої архітектури, яка здатна функціонувати незалежно від фізичної інфраструктури [28].

Розробка та експлуатація великомасштабних розподілених сервісів без внесення змін в основні мережні протоколи є ще однією з переваг оверлейних мереж. Проте недоліком цих мереж є підвищені витрати при передачі інформації через додатковий рівень обробки пакетів або використання неефективних маршрутів [29].

Оверлейні мережі широко застосовуються для побудови розвиненої архітектури Інтернету речей (IoT), особливо промислового IoT, та мобільних мереж покоління 5G. Вони забезпечують організацію неперервного бездротового зв’язку між великою кількістю пристроїв, що сприяє автоматизації та інтеграції різноманітних систем. Однією з переваг оверлейних мереж є інтеграція з фізичними мережами, що дозволяє забезпечити безшовну взаємодію між фізичною інфраструктурою та віртуалізованими ресурсами. Вони також сприяють реалізації концепцій інтелектуальних систем, які використовують для автоматичного налаштування, управління та оптимізації ресурсів, що дозволяє знизити затримки передачі даних та забезпечити відмовостійкість - ключових аспектів продуктивності сучасної мережної інфраструктури [30, 31].

Оверлейні мережі також використовуються для дослідження, розробки та тестування нових протоколів, створення та експлуатації нових сервісів та додатків. Вони можуть бути застосовані в разі неможливості використання традиційної мережної інфраструктури. Оверлейні мережі використовуються для організації розподілених обчислень, зокрема для зберігання та обміну інформацією [32], в розробці та оптимізації алгоритмів маршрутизації з підвищеними вимогами до якості обслуговування, відмовостійкості та забезпечення високого рівня безпеки та цілісності інформації [33-35].

Оверлейні мережі за своєю архітектурою поділяються на централізовані та децентралізовані. В централізованих оверлейних мережах маршрутизація здійснюється з одного центрального вузла, що є ефективним для невеликих мереж. Такий підхід забезпечує надійність системи завдяки стабільній роботі

центрального вузла, який визначає напрямок маршрутів. Проте децентралізована архітектура забезпечує більшу відмовостійкість [36].

Децентралізований підхід, навпаки, передбачає, що кожен вузол самостійно приймає рішення щодо маршруту пакетів. Така схема підвищує стійкість та гнучкість мережі, оскільки відмова одного вузла не впливає на загальну працездатність [37].

Побудова оверлейної мережі може включати застосування NFV – віртуалізованих мережних пристроїв, зокрема маршрутизаторів, комутаторів, фаєрволів тощо [38]. Застосування гіпервізорів, зокрема VMware, VirtualBox, Citrix, платформ віртуалізації, зокрема Proxmox, Openstack, а також хмарних середовищ від провідних постачальників хмарних обчислень, а саме AWS, Microsoft Azure, Oracle та Google Cloud дозволяє створювати віртуальні машини та контейнери, які застосовуються для побудови оверлейних мереж. Це дозволяє створювати багаторівневі мережні структури, навіть в умовах обмежених апаратних ресурсів, забезпечувати ізольованість віртуальних середовищ, що сприяє безпеці та захисту фізичної інфраструктури, а також дозволяє спростити адміністрування таких мереж [39].

Також для організації віртуальних мереж застосовуються інші технології, зокрема організація або сегментація за допомогою VLAN та Virtual Extensible LAN (VXLAN), створення VPN-тунелів, та кластеризація, яка застосовує інструменти Docker або Kubernetes, інтегровані засоби управління, зокрема в платформі Proxmox, для управління та розгортання кластерів на основі контейнерів [40].

VLAN дозволяє об’єднувати пристрої в логічні підмережі в межах фізичної мережі. Саме тому функціонування VLAN відрізняється від загальної концепції віртуалізації, зважаючи на те, що VLAN також забезпечують сегментацію мережі, але діють на канальному рівні мережної моделі OSI. VXLAN застосовується в гіпервізорах для створення логічних мереж та організовується за принципом VLAN. Також VXLAN

використовуються для побудови масштабних віртуальних мереж, зокрема в мережах провайдерів та дата-центрах.

Побудова VPN ґрунтується на створенні віртуального захищеного каналу зв'язку між мережними вузлами. Віртуальні тунелі використовуються для забезпечення конфіденційності, цілісності та автентичності даних, які передаються через загальнодоступні мережі. Поряд з відомими протоколами VPN–тунелювання, зокрема OpenVPN, IPSec, Wireguard, також використовуються технології Generic Routing Encapsulation (GRE) та Multiprotocol Label Switching (MPLS).

Технологія GRE використовується для об’єднання різних VLAN або мережних сегментів. MPLS теж застосовується в мережах провайдерів та масштабованих мережах підприємств, забезпечуючи пріоритезацію трафіку. Проте MPLS вимагає додаткової конфігурації та застосовується в мережах зі складною топологією.

Технологія програмно–визначеної мережі (SDN) забезпечує управління всіма ресурсами через програмне забезпечення, при цьому відокремлюючи площину керування від площини даних. Такий підхід дозволяє адмініструвати мережну архітектуру, а саме забезпечити гнучке та динамічне налаштування топології та маршрутизації відповідно до трафіку даних, дозволяючи динамічно реагувати на зміни навантаження та забезпечувати оптимальні маршрути для передачі даних [41].

Вибір структури оверлейної мережі визначається вимогами користувачів та функціями мережі, а також підходами та технологіями, які використовуються для забезпечення функціоналу таких мереж. З'єднання між вузлами реалізується на логічному рівні, при цьому вузли можуть мати різноманітні функції, зокрема зберігання, обробки та передачі даних. В оверлейних мережах, так само як в фізичних мережах, застосовуються механізми маршрутизації, які включають статичні, динамічні та гібридні підходи.

2.1 Алгоритми статичної маршрутизації

Статична або неадаптивна маршрутизація передбачає використання фіксованих маршрутів для передачі даних в мережі. Вони базуються на заздалегідь визначених маршрутах в таблицях маршрутизації, які налаштовуються адміністраторами мережі. Статичну (фіксовану) маршрутизацію застосовують в мережах з невеликою кількістю вузлів (рисунок 2.2). При фіксованій маршрутизації використовується централізований алгоритм, який передбачає, що в мережі є виділений маршрутизатор, який обробляє інформацію про топологію мережі та доступні маршрути. Такий маршрутизатор може бути єдиним пристроєм в невеликій мережі. В мережах з великою кількістю вузлів, де може використовуватися ряд маршрутизаторів, кожен з маршрутизаторів буде обслуговувати визначений сегмент мережі, а маршрутизатори на рівня ядра виконують роль центральних вузлів мережі. Маршрутизатор на рівні ядра створює таблиці для всіх мар-шрутизаторів та розсилає їх, щоб передача пакетів здійснювалася за принципом покрокової маршрутизації. Також він може організовувати маршру-тизацію від джерела, коли дані маршрутизації розсилаються кінцевим вузлам і прикордонним маршрутизаторам.

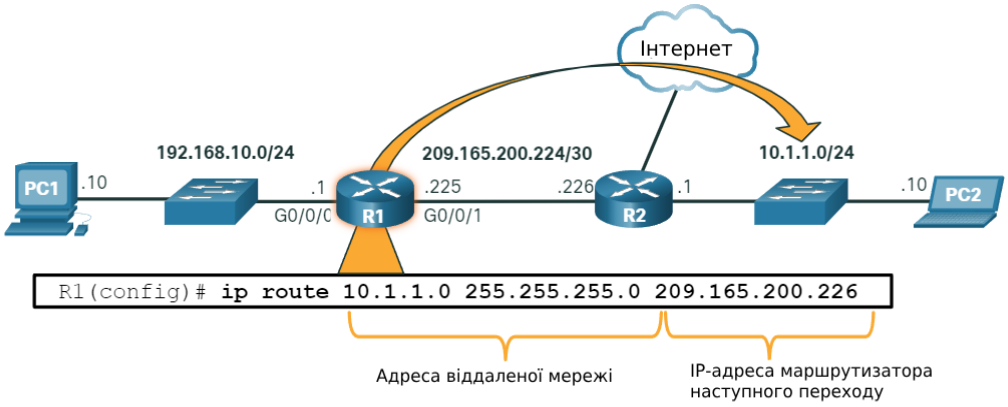


Рисунок 2.2 – Приклад статичної маршрутизації

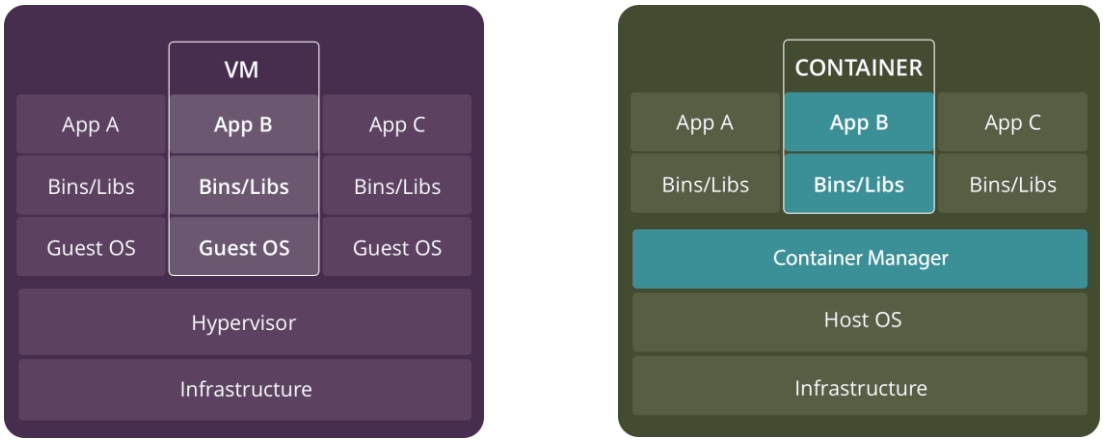
Такий алгоритм побудови маршрутизації в межах мережі забезпечує стабільність передачі даних, проте має ряд недоліків. По-перше, головним недоліком статичної маршрутизації є нездатність до адаптації до змін в мережі, які можуть виникати через вихід з ладу окремих вузлів, що може зробити недоступними окремі локальні мережі або сегмент великої корпоративної мережі. По-друге, через налаштування таблиць маршрутизації вручну адміністраторами існує ризик помилкових налаштувань, що може спричинити відмову окремого вузла через перевантаження, що також зробить недоступними локальну мережу або окремий сегмент мережі [42].

Попри обмеження, статичні методи можуть застосовуватися в корпоративних середовищах, де мережний трафік та топологія є стабільними та передбачуваними [28]. Найчастіше ці методи використовують при з'єднанні однієї локальної мережі, сегментів великої корпоративної комп'ютерної мережі або налаштуванні локальної мережі до виходу до глобального інтернету. Саме в такому випадку використання статичних методів маршрутизації є найефективнішим, оскільки статичні адреси надаються прикордонним маршрутизаторам, шлюзу локальної мережі, що значно зменшує навантаження на пристрої маршрутизації та знижує затримку в передачі даних. При цьому організація локальної мережі спрощується та зменшуються помилки при налаштуванні [43].

Використання статичної маршрутизації в мережах з високими вимогами до низької затримки, зокрема при передачі потокових даних в режимі реального часу, дозволяє забезпечити передбачувану ефективність завдяки фіксованим маршрутам передачі пакетів, що знижує потребу в регулярному оновленні таблиць маршрутизації та загальне навантаження на мережу [43].

Налаштування оверлейних мереж, зокрема з використанням VPN-тунелів або віртуальних машин і контейнерів передбачають використання статичної маршрутизації, що дозволяє точно визначити маршрути передачі даних між віддаленими вузлами або окремими сегментами корпоративних

мереж. Такий підхід забезпечує стабільність та безпеку з'єднань, а також ізоляцію окремих мереж або сегментів в захищених корпоративних середовищах. При використанні контейнерів для організації мережної інфраструктури статичні маршрути дозволяють спростити взаємодію між контейнерами та мережними вузлами, знижуючи навантаження на ресурси системи та покращуючи продуктивність мережі (рисунок 2.3) [44].



а) б)

Рисунок 2.3 – Схема порівняння архітектур віртуальної машини та контейнера на прикладі платформи Proxmox:
а) віртуальна машина; б) контейнер

Для побудови VPN-тунелю доцільно використовувати віртуальні машини або контейнери, які розгорнуті за допомогою платформ віртуалізації або хмарних середовищ. Такий підхід забезпечує додатковий рівень захисту, можливість масштабування фізичної інфраструктури, зниження апаратних ресурсів та ізоляцію окремих сегментів мереж від несанкціонованого доступу. Процес побудови VPN-тунелю передбачає створення зашифрованого каналу, який дозволяє користувачам передавати дані, приховуючи їх від сторонніх спостерігачів та забезпечуючи захист від атак типа MITM («людина посередині») (рисунок 2.4).

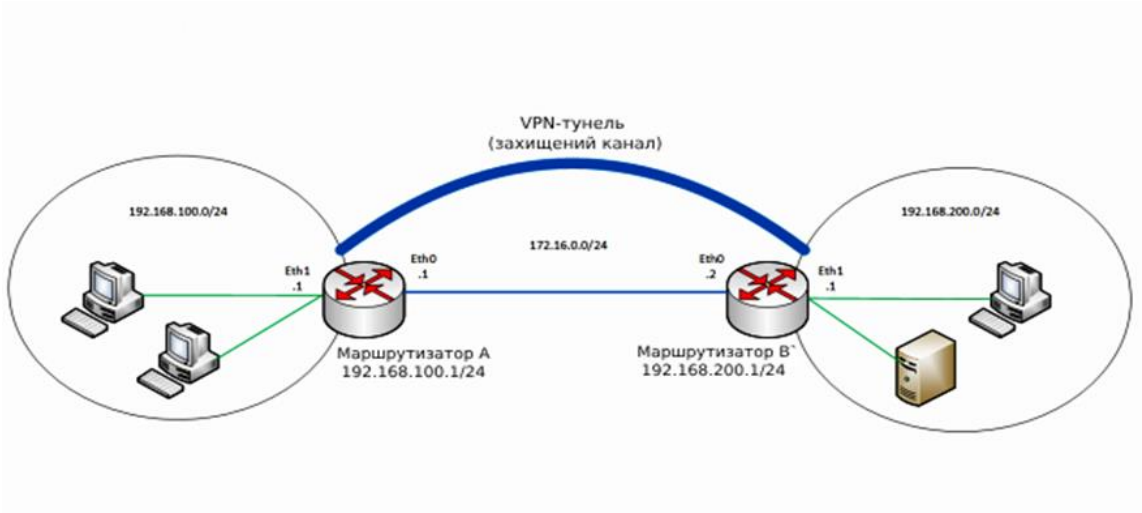


Рисунок 2.4 – Схема побудови VPN-тунелю

VPN-тунелі забезпечують захищену передачу інформації через загальнодоступні мережі. Це реалізується шляхом інкапсуляції мережних пакетів одного протоколу в пакети іншого, що забезпечує конфіденційність та цілісність даних при передачі через відкриті мережі. Створення віртуальних тунелів базується на використанні різних протоколів тунелювання, кожен з яких має свої особливості:

- IPSec – це стек протоколів для забезпечення захисту даних, які передаються за протоколом IP, та працює на мережному рівні моделі OSI. Часто протокол IPSec використовують в комбінації з іншими протоколами. Наприклад, в комбінації з IKEv2 – протоколом тунелювання, який розроблено компаніями Microsoft та Cisco. Найчастіше така комбінація використовується для підключень в операційних системах Windows, macOS та iOS. IPSec/IKEv2 дозволяє автоматизувати процес обміну ключів та забезпечує стійкість до відмов з'єднань. IPSec/L2TP використовується для додаткового захисту, забезпечуючи тунелювання без шифрування, проте IPSec сам накладає шифрування [45];

- SSL/TLS – це криптографічні протоколи, які використовуються для захищеного обміну даними в мережах. Вони забезпечують безпечне з’єднання з веб-ресурсами, а також активно застосовуються в VPN-

тунелюванні. Зокрема OpenVPN використовує SSL/TLS для шифрування трафіку [46];

- SSTP – протокол тунелювання, який розроблений компанією Microsoft. Він використовує SSL/TLS для шифрування VPN–трафіку. SSTP працює через порт 443, що дозволяє обходити більшість брандмауерів. Проте через недоступність для дослідницького тестування застосування цього протоколу є обмеженим через можливі вразливості;

- OpenSSH – це набір утиліт для безпечного віддаленого доступу до систем з використанням SSH–протоколу для тунелювання та захищеної передачі файлів. SSH виконує шифрування даних при передачі та дозволяє інкапсулювати будь-який протокол, працюючи на мережному рівні. Він широко застосовується для адміністрування серверів;

- WireGuard – це новий VPN-протокол, який дозволяє забезпечити високий рівень безпеки при мінімальних витратах на налаштування та підтримку. Завдяки своїй простоті він швидко набуває популярності в різних мережних середовищах. Для передачі даних в тунелі використовує протокол UDP;

- OpenVPN – це VPN-протокол з відкритим кодом, який використовує SSL/TLS для шифрування трафіку. Він підтримує широкий спектр налаштувань, дозволяючи користувачам обирати різні алгоритми шифрування та способи автентифікації. OpenVPN вважається одним з найгнучкіших та надійних протоколів для побудови VPN-тунелів та сумісний з більшістю існуючих операційних систем [47].

Таким чином, найбільш вживаними протоколами є IPSec, OpenVPN та WireGuard. Вони характеризуються високою універсальністю, що забезпечує їх сумісність з більшістю операційних систем, та ефективністю в різних середовищах, включаючи хмарні інфраструктури та оверлейні мережі.

В таблиці 2.1 наведено порівняльні характеристики основних протоколів VPN, які використовуються для побудови захищених мереж.

Таблиця 2.1 – Порівняння протоколів VPN

Протокол	**Швидкість**	**Шифрування**	**Потокова передача**	**Стабільність**	**P2P**
OpenVPN	швидкий	відмінно	добра	добра	добре
IpSec/IKEv2	швидкий	відмінно	добра	відмінно	добре
L2TP/IPSec	середній	середнє	бідна	добра	бідне
Wireguard	дуже швидкий	відмінно	добра	відмінно	добре
SSTP	середній	добре	середня	середня	добре

При організації VPN-тунелю формування маршруту включає кілька етапів. Спочатку визначаються кінцеві точки з'єднання – це можуть бути віддалені користувачі або мережні вузли, між якими необхідно організувати захищений канал зв’язку. Для цього адміністратор задає визначені статичні маршрути, що містять діапазон IP-адрес мережі або IP-адресу окремого вузла, які будуть доступні через VPN-тунель.

Наступним кроком є налаштування VPN-шлюзу, який забезпечує шифрування та інкапсуляцію переданого трафіку. На ньому встановлюються правила маршрутизації трафіку через VPN-тунель. На цьому кроці в таблицю маршрутизації шлюза додаються статичні маршрути, де VPN-шлюз вказується як шлюз за замовчуванням для визначених IP-адрес вузлів або підмереж.

Після налаштування маршрутизації виконується побудова тунелю та його підтримка. На цьому етапі протокол, що використовується для тунелювання, створює зашифрований канал зв'язку між кінцевими точками. Активність тунелю забезпечується обміном ключами шифрування та автентифікації кінцевих вузлів, що гарантує доступ лише авторизованих пристроїв до мережі. Окрім цього, на цьому етапі здійснюється моніторинг трафіку та забезпечення його цілісності. Використання механізмів перевірки

цілісності даних, таких як HMAC або цифрових підписів, дозволяє виявляти несанкціонований доступ до даних. Це дозволяє виявляти атаки, які можуть загрожувати конфіденційності та цілісності переданих даних. Завдяки цим механізмам VPN-тунелі забезпечують високий рівень захисту даних під час їх передачі через загальнодоступні або незахищені мережі [48].

Наступним етапом є налаштування VPN-сервера, де визначаються параметри шифрування та автентифікації, що забезпечує конфіденційність передачі даних. Опції налаштування включають вибір протоколу, параметрів ключів шифрування, механізмів автентифікації, зокрема ідентифікації за сертифікатами та логінами з паролями.

Після налаштування VPN-сервера створюються конфігураційні файли для клієнтських пристроїв. Для використання VPN-тунелів на клієнтських пристроях повинно бути встановлено додаткове програмне забезпечення, що відповідає обраному протоколу тунелювання, або виконано налаштування вбудованих VPN-клієнтів на операційних системах, як у випадку з SSTP. Автентифікація користувачів виконується за допомогою механізмів автентифікації та авторизації. Для цього використовуються надані клієнтам сертифікати для автентифікації, а також логіни та паролі для авторизації.

Наступним етапом є перевірка роботи VPN-тунелю, яка передбачає тестування з'єднання між вузлами. На цьому етапі перевірка може виконуватися за допомогою передачі пакетів ICMP або трасування маршрутів для оцінки стабільності та швидкості з'єднання. В разі виявлення збоїв виконується діагностика, яка включає перевірку таблиць маршрутизації, налаштувань брандмауера або виправлення помилок в конфігураційних файлах (рисунок 2.5).

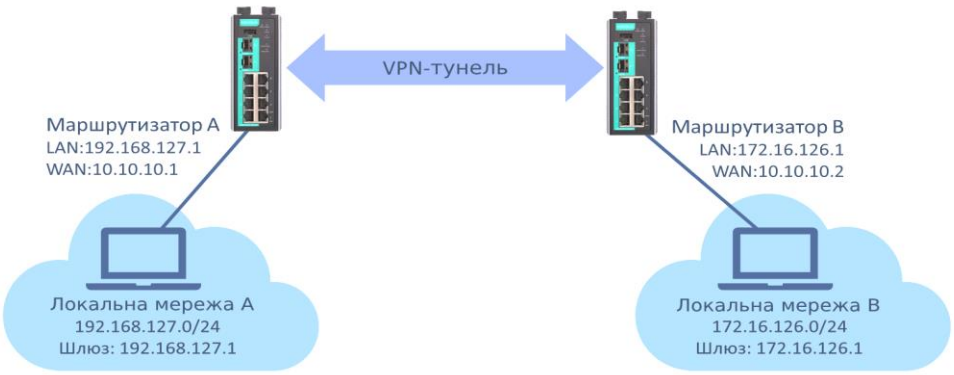


Рисунок 2.5 – Розподіл IP-адрес на LAN та WAN інтерфейсах маршрутизаторів при налаштуванні VPN-з’єднання

Після перевірки роботи віртуальний тунель використовується для передачі всього трафіку або визначених потоків трафіку через тунель. Для цього застосовуються правила фільтрації трафіку, які спрямовують потоки даних за визначеною IP-адресою VPN-сервера, яка додається до таблиць маршрутизації. Такі правила можуть містити перенаправлення трафіка за визначеною IP-адресою шлюза, а також включати додаткові параметри, зокрема вказання обраного інтерфейсу або порту передачі.. Це досягається за допомогою налаштування таблиці маршрутизації на рівні операційної системи або мережного обладнання, яке направляє весь передбачений трафік через VPN-інтерфейс. Всі дані, які передаються через цей інтерфейс, шифруються та інкапсулюються в мережні пакети VPN-протоколу, який застосовується для VPN-тунелю. Такий підхід унеможливлює доступ до переданих даних під час транзиту через загальнодоступні мережі.

Платформа віртуалізації Proxmox, яка забезпечує можливість розгортання контейнерів для побудови мережної інфраструктури, забезпечує розгортання VPN–серверів в ізольованих контейнерах, що суттєво підвищує рівень безпеки та спрощує адміністрування мережі [49]. В роботі [50] детально описано переваги використання контейнерів для віртуалізації, зокрема оптимізацію апаратних ресурсів, масштабування та захист фізичної

мережної інфраструктури. Proxmox надає вбудовані інструменти для управління мережними ресурсами, включаючи кластеризацію серверів та оперативну міграцію віртуальних машин [31]. Це дозволяє ефективно масштабувати мережну інфраструктуру без необхідності додаткових інвестицій в апаратне обладнання, що є важливим для малого та середнього бізнесу. Крім того, Proxmox підтримує інтеграцію з різними протоколами тунелювання, зокрема з OpenVPN, що забезпечує можливість розгортання багаторівневих VPN-тунелів, для безпечного доступу до ресурсів екстранет–мереж.

В разі використання контейнеризації формування статичних маршрутів включає кілька етапів. На першому етапі визначаються контейнери та мережні вузли, які взаємодіють між собою. Для визначених контейнерів обираються статичні маршрути в окремій мережі або в заданому сегменті мультисегментної корпоративної комп'ютерної мережі. Наступним кроком є налаштування мережних параметрів контейнерів віртуальної мережі, в рамках якої функціонують дані контейнери (рисунок 2.6).

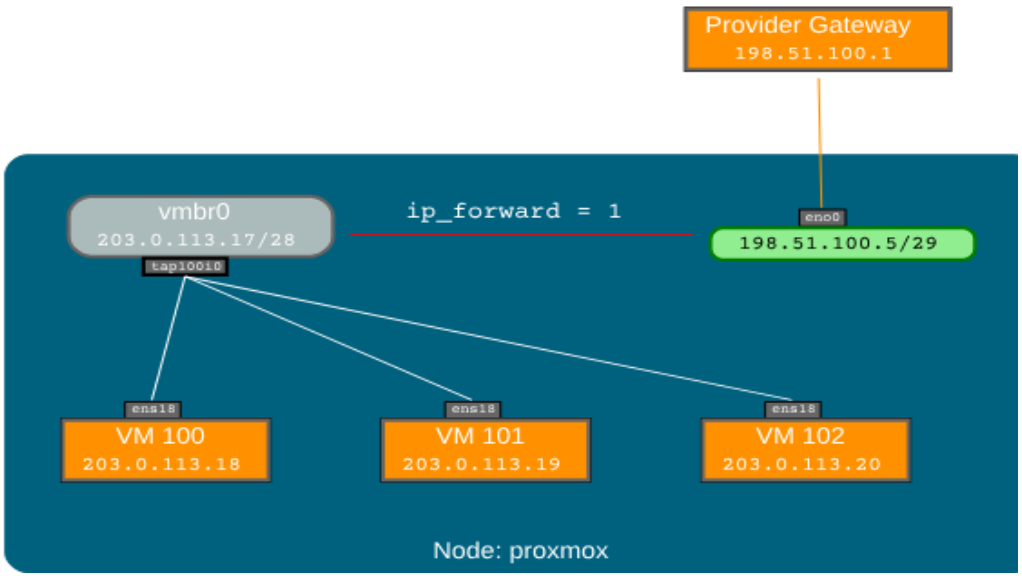


Рисунок 2.6 – Налаштування статичних маршрутів для контейнерів на платформі Proxmox

Після налаштування мережних параметрів виконується перевірка доступності IP-адрес та визначених маршрутів. Надалі здійснюється налаштування моніторингу та управління трафіком між контейнерами, що може включати використання систем моніторингу або налаштування журналів для відстеження продуктивності та стабільності мережних з'єднань.

Основна відмінність між оверлейними мережами та загальнодоступними мережами зі статичною маршрутизацією полягає в наданні додаткового рівня абстракції, що працює як надбудова поверх фізичної інфраструктури. Це забезпечує передачу даних між різними мережами, використовуючи узгоджені логічні маршрути, незалежно від фізичних з'єднань. Такий рівень абстракції сприяє оптимізації роботи мережі, особливо в умовах обмежених апаратних ресурсів, дозволяє масштабування мереж без значних витрат на фізичне обладнання. Підвищений рівень захисту та цілісності при передачі даних в оверлейних мережах, зокрема в VPN-тунелях, досягається через ізоляцію таких сегментів або тунелів від фізичної інфраструктури. Використання механізмів шифрування, авторизації та автентифікації при створенні VPN-тунелів зменшує ризик несанкціонованого доступу та витоку інформації.

2.2 Алгоритми динамічної маршрутизації

Динамічна або адаптивна маршрутизація в мережах дозволяє будувати маршрути передачі даних на основі поточного стану мережі, при цьому маршрутизатори постійно аналізують мережну топологію та доступність вузлів, а нові маршрути автоматично додаються до таблиць маршрутизації. Кожна зміна в мережі, зокрема відмова вузлів, вихід з ладу каналів зв'язку або поява нових вузлів, враховується в оновленні таблиць маршрутизації, які передаються сусіднім маршрутизаторам. Це дозволяє виконувати оновлення таблиць маршрутизації на всіх вузлах мережі без втручання адміністратора (рисунок 2.7).

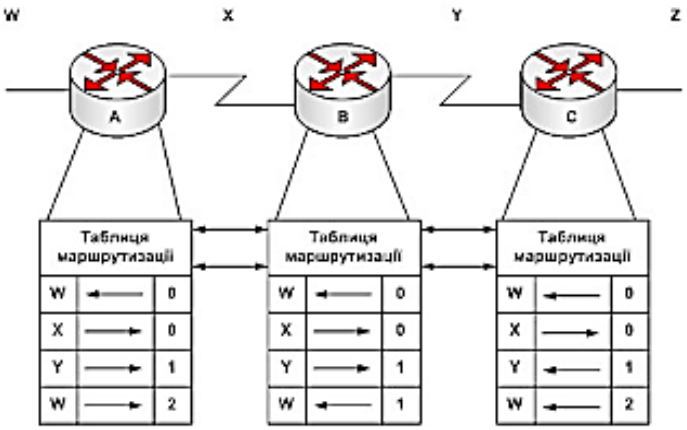


Рисунок 2.7 – Процес побудови структури мережі в дистанційно-векторному протоколі маршрутизації

В рамках динамічної маршрутизації загальнодоступні мережі розглядаються як сукупність автономних систем (AS), де між двома комп'ютерами однієї системи існує безліч можливих маршрутів. Всередині автономної системи маршрутизація забезпечує оптимізацію маршрутів для досягнення максимальної швидкості передачі за рахунок найкоротших маршрутів передачі даних. Вибір маршруту між автономними системами та в межах однієї системи здійснюється на основі порівняння параметрів передачі, які визначено для цієї мережі найактуальнішими або впливовими. Такими параметрами можуть бути швидкість передачі, пропускна здатність каналу зв’язку, відстань між вузлами або найменша кількість вузлів, через які проходить маршрут. Таким чином, в динамічній маршрутизації існує два типи протоколів:

- зовнішні протоколи, які використовуються для передачі даних між автономними системами;

- внутрішні протоколи, які використовуються для передачі даних в межах однієї автономної системи.

EGP та BGP відносяться до зовнішніх протоколів динамічної маршрутизації. EGP, який було розроблено компанією Cisco, наразі є застарілим протоколом, замість нього використовується BGP. За допомогою

EGP здійснюється оголошення про мережі, які доступні для AS за межами даної автономної системи – шлюз однієї AS передає шлюзу іншої AS інформацію про мережі, з яких складається його AS. Протокол BGP використовує політики маршрутизації, замість метрики відстані або стану зв'язків. За допомогою BGP вказуються характерні параметри (ваги) для маршрутів, що дозволяє обирати для передачі найкращий маршрут. Ці ваги призначаються адміністратором мережі, зокрема ними можуть виступати час доступу до ресурсів, кількість шлюзів, наступний вузол передачі тощо. Такі параметри формують політику маршрутизації, яка відповідає технічній політиці адміністрації даної AS при доступі до її інформаційних ресурсів з інших AS. Протокол BGP вважається складним протоколом через необхідність узгодження політик маршрутизації між різними автономними системами.

До внутрішніх протоколів динамічної маршрутизації відносять протоколи RIP, IS–IS, IGRP, EIGRP та OSPF (рисунок 2.8).

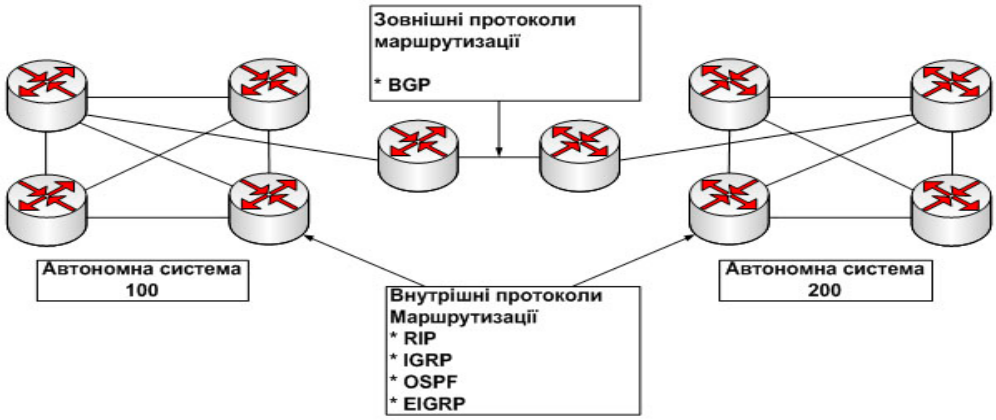


Рисунок 2.8 – Види протоколів динамічної маршрутизації

Динамічна маршрутизація може бути заснована на централізованих або розподілених алгоритмах. На відміну від централізованих алгоритмів, в розподілених передбачено рівноправну участь всіх вузлів маршрутизації в побудові таблиць маршрутизації, тобто кожен маршрутизатор створює власну

таблицю на основі інформації, отриманої від інших вузлів. За отриманою інформацією маршрутизатор приймає рішення про вибір наступного вузла передачі даних на основі його завантаженості або доступності. Це дозволяє забезпечити швидку реакцію на зміни в мережі в режимі реального часу, зокрема через втрату з'єднання або появи нових вузлів.

В свою чергу розподілені алгоритми динамічної маршрутизації поділяються на дистанційно-векторні (DVA) та алгоритми стану зв'язків (LSA). Дистанційно-векторні алгоритми використовують інформацію про відстань до різних вузлів мережі для побудови найкоротшого шляху передачі даних. Ці алгоритми також відомі за назвою алгоритмів Беллмана – Форда. Найбільш відомим прикладом дистанційно-векторного алгоритму є протокол RIP [51]. Він характеризується простотою адміністрування, проте має обмежене використання через низьку масштабованість, тому використовується в невеликих мережах.

Алгоритми стану зв'язків, зокрема OSPF, функціонують інакше. Принцип побудови маршруту цих алгоритмів полягає в побудові найкоротшого маршруту на базі інформації про доступні мережі та вузли, отриманої від сусідніх маршрутизаторів. Такий підхід дозволяє спочатку побудувати поточну топологію мережі у вигляді дерева, де відправною точкою слугує сам маршрутизатор, а гілки дерева – маршрути до інших вузлів. Надалі маршрутизатор обирає найкоротший шлях до визначеного вузлу, використовуючи інформацію про стан та доступність цього вузла. Завдяки такому механізму побудови найкоротшого шляху, протокол OSPF застосовується для великих IP-мереж. OSPF структурує мережу на області для зниження кількості службового трафіку, що полегшує керування маршрутизаторами у великих мережах. Він використовує метрику «вартість», яка може базуватися на таких параметрах, як пропускна здатність, затримка або завантаженість каналу, що дозволяє адаптувати маршрутизацію до реальних умов мережі [52]. На рисунку 2.9 представлено принцип роботи протоколу OSPF, де кожен маршрутизатор повідомляє своїм сусідам про стан своїх

зв’язків або каналів. AS може бути розділена на кілька зон, кожна з яких складається з групи підключених мереж або пристроїв. Граничні маршрутизатори зон мають кілька інтерфейсів та працюють на межах цих зон, що забезпечує обмін інформацією про стан мереж між ними. Маршрутизатор кожної зони використовує отриману інформацію для побудови топологічної бази даних, після чого застосовує алгоритм вибору найкоротшого шляху для визначення оптимальних маршрутів. Результати обчислень у вигляді нового маршруту додаються до таблиці маршрутизації. Для зменшення обсягу службових даних в кожній мережі обираються призначений (DR) та резервний (BDR) маршрутизатори, які керують обміном інформації про маршрутизацію між пристроями [53].

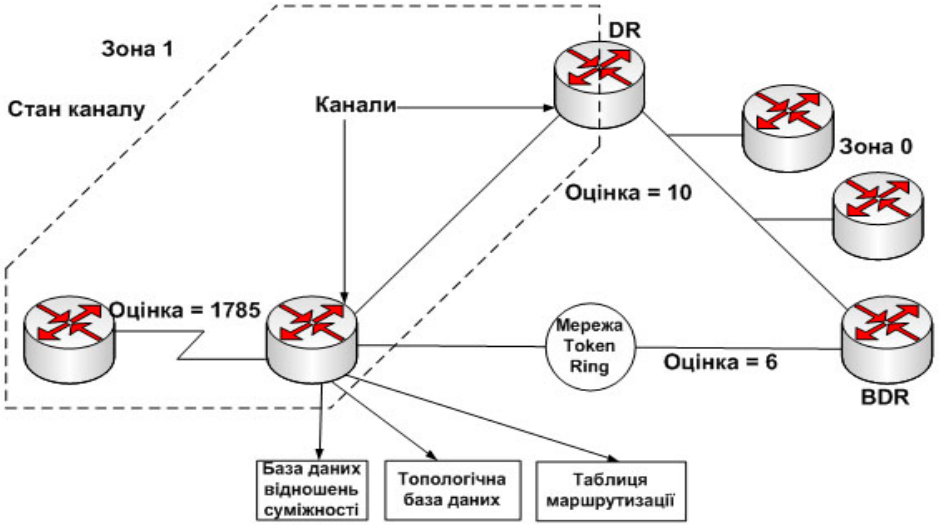


Рисунок 2.9 – Принцип роботи протоколу OSPF

Протоколи динамічної маршрутизації DSR та AODV застосовуються у Wi-Fi або мобільних ad-hoc мережах [54]. Вони функціонують за принципом пошуку маршрутів на вимогу, що дозволяє зменшити витрати на підтримку постійної таблиці маршрутизації. Маршрути зберігаються тимчасово та оновлюються в разі необхідності, що сприяє підвищенню безпеки користувачів. Водночас, часті зміни маршрутів в таких мережах викликають

перевантаження вузлів маршрутизації, що призводить до виникнення затримок та додаткового навантаження на вузли.

IS-IS широко застосовується в масштабованих мережах, зокрема в мережах провайдерів та дата-центрів. Цей протокол працює за аналогічним принципом вибору найкоротшого шляху, проте має іншу ієрархічну модель побудови графу та підхід до обчислення маршрутів. Це дозволяє використовувати протокол IS-IS в мережах з комплексною топологією. Він відзначається високою швидкістю конвергенції та масштабованістю, але є значно складнішим у налаштуваннях в порівнянні з іншими протоколами динамічної маршрутизації.

В таблиці 2.2 наведено порівняльний аналіз характеристик протоколів динамічної маршрутизації, який ілюструє особливості використання цих протоколів в сучасних корпоративних мережах.

Таблиця 2.2 – Порівняння характеристик протоколів динамічної маршрутизації

	дистанційно–векторні алгоритми (DVA)				**алгоритми стану зв'язків (LSA)**	
Критерій	**RIPv1**	**RIPv2**	**IEGP**	**EIGRP**	**OSPF**	**IS–IS**
Масштабованість (розмір мережі)	мала	мала	мала	велика	велика	велика
Підтримка VLSM	–	+	+	+	+	+
Ступінь використання ресурсів	низька	низька	низька	середня	висока	висока
Впровадження та підтримка	проста	проста	проста	складна	складна	складна

Після налаштування динамічної маршрутизації адміністратором за обраним протоколом, оновлення таблиць маршрутизації здійснюється

автоматично під час кожної зміни в топології. Налаштування динамічної маршрутизації реалізується безпосередньо на маршрутизаторах, в разі недоступності апаратних методів використовується спеціалізоване програмне забезпечення. Загалом, кожен комп'ютер виконує маршрутизацію власних вихідних пакетів, зокрема для розподілу трафіку. Таким чином здійснюється розподіл пакетів, які надходять до шлюзу та надалі передаються через загальнодоступні мережі, та пакетів, які призначені для використання в межах локальної мережі. Для маршрутизації зовнішніх IP–пакетів та формування таблиць маршрутизації застосовуються різні програмні рішення, зокрема:

- RRAS (Routing and Remote Access Service) у середовищі Windows Server;
- демони routed, gated, quagga в операційних системах на базі Unix, таких як Linux і FreeBSD [55, 56].

Однак, специфіка анонімних мереж, зокрема TOR, вимагає використання інших підходів до маршрутизації. На відміну від відкритих мереж, де швидкість передачі даних та надійність з'єднання є ключовими параметрами забезпечення ефективності, пріоритетом анонімних мереж є збереження анонімності користувачів та конфіденційності даних і маршрутів передачі. Мережа TOR працює «поверх» Інтернету та використовує динамічний підхід до маршрутизації. Принцип маршрутизації в TOR базується на багаторівневому перенаправленні зашифрованого трафіку через ланцюг проміжних вузлів, що забезпечує високу анонімність користувачів (рисунок 2.10).

Мережа TOR має децентралізовану архітектуру, яка надає особливості топології, водночас забезпечуючи високий рівень анонімності та складне адміністрування мережі. Концепція побудови мережі TOR заснована на добровільній участі в мережі, що дозволяє вузлам динамічно приєднуватися та покидати мережу, створюючи нестабільну топологію в реальному часі. Для підтримки актуальних даних про активні вузли використовуються

дирекційні сервери, що зберігають оновлені списки вузлів та їх мережні параметри. Цей механізм забезпечує адаптивну маршрутизацію в умовах постійних змін топології. Клієнтське програмне забезпечення TOR дозволяє обирати ланцюг проміжних вузлів для побудови маршруту на основі їх доступності та географічного розташування [57].

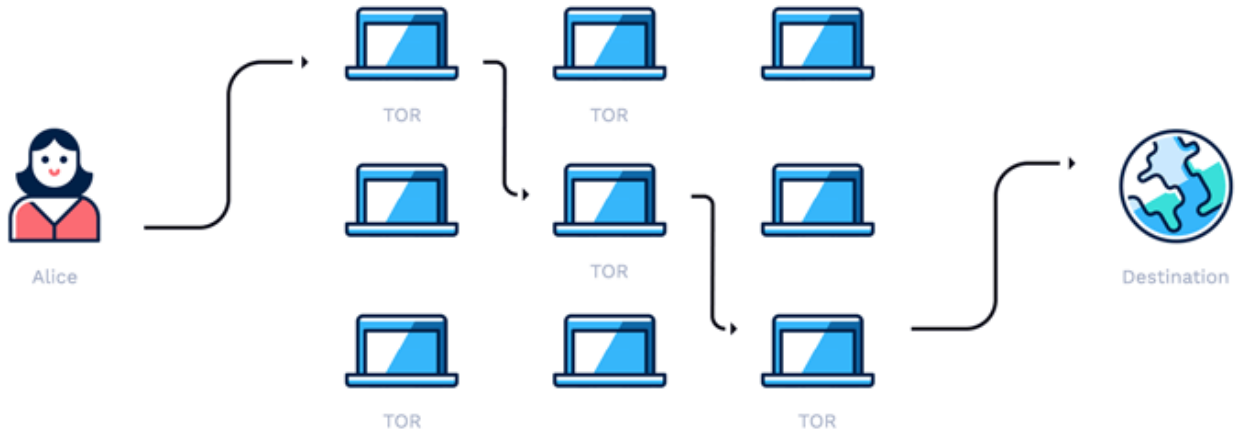


Рисунок 2.10 – Схема передачі запиту в мережі TOR за допомогою пошуку шляхів на вимогу

Після встановлення з’єднання запит спрямовується до вхідного вузла мережі TOR. На цьому етапі зв’язок між користувачем та вхідним вузлом вже захищено шифруванням. Далі запит проходить через ланцюг проміжних вузлів, які направляють його до вихідного вузла, забезпечуючи багаторівневе перенаправлення. Такий принцип передачі гарантує, що жоден з вузлів не володіє повною інформацією про відправника та одержувача запиту. Вихідний вузол мережі TOR перенаправляє запит до одержувача, володіючи даними лише про пункт призначення, що унеможливлює ідентифікацію відправника та значно ускладнює відстеження маршруту передачі. Такий принцип маршрутизації відповідає концепції динамічної маршрутизації на вимогу, що сприяє підвищенню конфіденційності користувачів.

Особливістю передачі даних в мережі TOR є багаторівневе шифрування трафіку відоме як «цибулева» маршрутизація. Всі вузли в мережі використовують протокол шифрування SSL/TLS для шифрування-розшифрування запиту. Це унеможливлює доступ до вмісту повідомлення, а також приховує адреси відправника та одержувача. Клієнт TOR використовує ефемерний ключ шифрування на кожному вузлі маршруту, що створює додаткові рівні захисту, а також гарантує, що ключі шифрування не зберігаються після завершення з'єднання, що ускладнює відстеження трафіку та ймовірності злому вузла з метою виявлення ключа [58].

Оригінальне повідомлення шифрується декількома шарами, де кожен шар шифрування розшифровується на наступному вузлі маршрута передачі даних. Перший шар розшифровується вихідним вузлом для отримання IP-адреси наступного вузла передачі, наступний шар – проміжним вузлом, а останній шар шифрування – вхідним вузлом. Таким чином, кожен вузол на маршруті обробляє лише свій шар шифрування та не має доступу до оригінального повідомлення, яке відкривається лише на вихідному вузлі перед передачею до одержувача. Такий підхід мінімізує потребу в довірі до проміжних вузлів, оскільки перехоплення та розшифрування оригінального повідомлення стає математично малоймовірним (рисунок 2.11) [59].

Таким чином, динамічна маршрутизація відкритих та анонімних мереж, зокрема мережі TOR, має суттєві відмінності, зумовлені вимогами до безпеки передачі даних та методами забезпечення цих вимог. У відкритих мережах алгоритми динамічної маршрутизації зосереджуються на оптимізації швидкості та надійності передачі даних, що забезпечують протоколи динамічної маршрутизації, зокрема BGP та OSPF. Водночас, у відкритих мережах затримки можуть виникати внаслідок відмов вузлів або збоїв обладнання, помилкових маршрутів та складного адміністрування, що також спричиняє затримки в передачі даних.

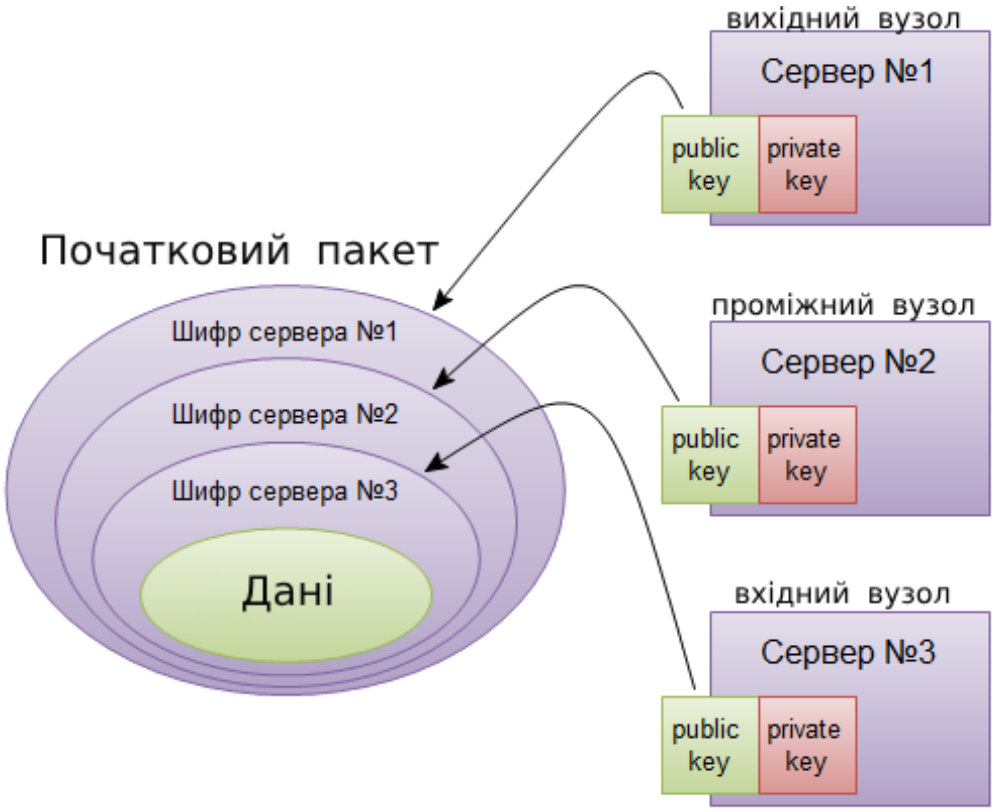


Рисунок 2.11 – Схема багатошарового «цибулевого» шифрування оригінального повідомлення в мережі Tor

В мережі TOR динамічна маршрутизація дозволяє вузлам самоорганізовуватися та адаптуватися до постійних змін в топології. Цей підхід включає використання механізмів пошуку шляхів за запитом, що дозволяє знизити навантаження на мережу. Водночас в таких мережах використовується багатошарове шифрування для забезпечення високого рівня анонімності та приховування маршрутів, яке вимагає додаткових обчислювальних ресурсів, що призводить до затримок в передачі даних.

2.3 Гібридні методи маршрутизації

Гібридні методи маршрутизації поєднують елементи статичних та динамічних підходів. Вони використовують фіксовані маршрути для основного сегменту передачі даних, водночас адаптують вторинні сегменти в

реальному часі на основі поточного стану мережі. Такий підхід дозволяє досягти підвищеного рівня безпеки та швидкості в порівнянні з виключно статичними або динамічними методами. Основний обсяг даних передається фіксованими маршрутами, а в разі виникнення збоїв або відмов вузлів, в мережі виконується динамічне коригування маршрутів [60]. Цей підхід також забезпечує балансування стабільності та гнучкості, що важливо для складних та масштабованих мереж [61].

Використання гібридних протоколів, зокрема EIGRP, BGP, та ZRP, дозволяє вузлам поєднувати стабільність за рахунок таблиць статичних маршрутів з можливістю динамічного реагування на зміни в мережі. Це сприяє ефективному управлінню трафіком, особливо в великих корпоративних та мобільних ad-hoc мережах.

Протокол EIGRP використовує метрики, зокрема затримку, пропускну здатність, надійність для динамічного розрахунку найкоротших шляхів. Оскільки протокол був розроблений компанією Cisco, його використання на даний час в мережах обмежено через його пропрієтарність. В гібридниих методах маршрутизації протокол BGP використовується для маршрутизації між автономними системами. Прикордонні вузли таких систем з використанням цього протоколу мають фіксовані IP-адреси, проте маршрути після встановлення з’єднання, використовуються динамічні. Також оновлення таблиць маршрутизації виконується автоматично з урахуванням поточного стану мереж (рисунок 2.12).

В мобільних мережах протокол ZRP використовує зональну маршрутизацію, поєднуючи проактивний підхід в межах визначеної зони та реактивну маршрутизацію для вузлів за її межами. Це дозволяє зменшувати службовий трафік та знижувати витрати на маршрутизацію, забезпечуючи при цьому гнучкість для швидкої адаптації до змін в топології мережі [62].

Протоколи резервування HSRP та VRRP доповнюють гібридну маршрутизацію, забезпечуючи неперервність обслуговування за рахунок резервних маршрутизаторів, які активуються в разі збою основного. Це

підвищує надійність мережі та забезпечує її стійкість в разі відмов основних вузлів [63].

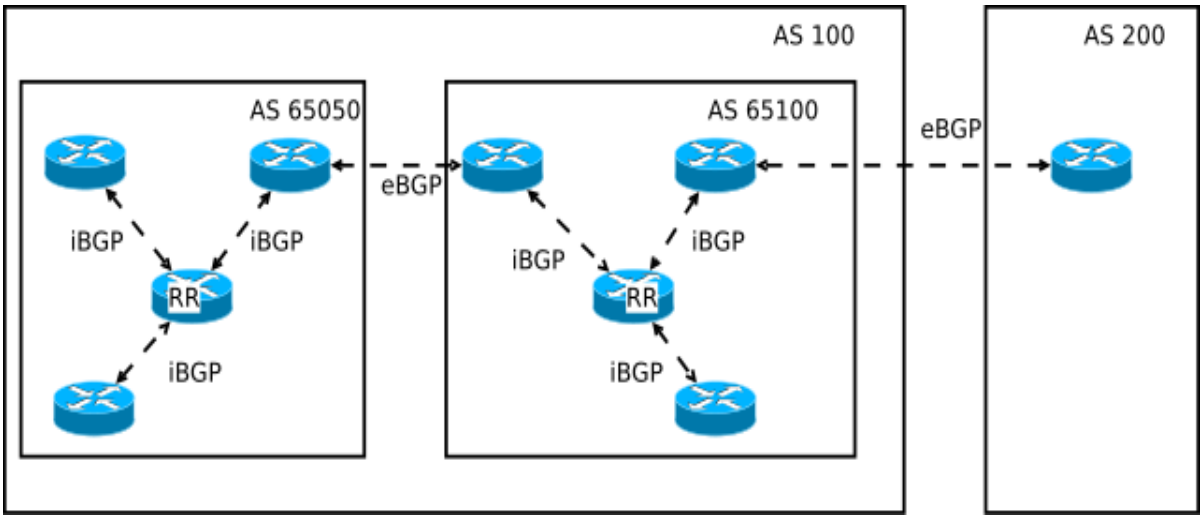


Рисунок 2.12 – Принцип роботи протокола BGP

Застосування гібридної маршрутизації в пірінгових мережах, де кожен вузол одночасно виконує функції клієнта та сервера, дозволяє забезпечити автономність кожного елемента мережі та швидку адаптацію до змін топології. В гібридній маршрутизації побудова маршрутів здійснюється з урахуванням навантаження вузлів та поточного стану мережі, що дозволяє забезпечити розподілене зберігання даних та підвищити стійкість до атак та збоїв, оскільки відмова одного вузла не впливає на функціонування всієї мережі.

P2P–мережі мають децентралізовану архітектуру, яка забезпечує розподіл завдань між вузлами, знижує навантаження на окремі сервери та забезпечує масштабованість мережі. До децентралізованих мереж відносяться Freenet, I2P, GNUnet, а також систему анонімної цифрової валюти Bitcoin [64].

Розподілені обчислення в P2P-мережах здійснюються шляхом розподілу завдань на частини, які виконуються на окремих вузлах. Такі мережі стали популярними для файлообміну, оскільки дозволяють обійти обмеження пропускної здатності та ефективно передавати великі обсяги даних. Прикладом

ранніх систем розподіленого обміну файлами є мережа Napster, яку потім замінила децентралізована мережа Gnutella. Пірингові мережі також використовуються для онлайн-ігор, спільного редагування документів, обміну повідомленнями та командної роботи (рисунок 2.13) [65].

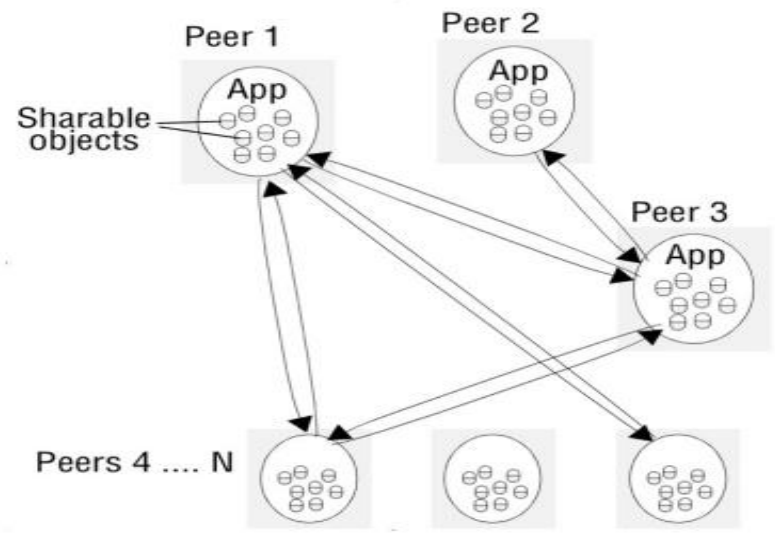


Рисунок 2.13 – Передача даних в піринговых мережах

Пірингові мережі за рівнем централізації поділяються на чисті та гібридні. В чистих системах всі вузли є рівноправними та виконують функції клієнтів і серверів без визначеного центрального сервера, проте така архітектура ускладнює пошук даних через розповсюдження запитів серед великої кількості вузлів. Прикладами таких мереж є Gnutella та Freenet. Гібридні P2P-мереж, в свою чергу, використовують центральний сервер для зберігання інформації про вузли, що полегшує пошук даних, але знижує рівень децентралізації [66].

Залежно від способу з’єднання вузлів в мережі, пірингові мережі поділяють на структуровані та неструктуровані. Неструктуровані мережі засновані на випадковій організації мережі, що дозволяє новим вузлам швидко підключатися до існуючих з’єднань. Такий підхід забезпечує швидке розгортання мережі, але має обмеження щодо пошуку рідкісних даних.

Структуровані мережі використовують розподілені хеш-таблиці (DHT), які дозволяють зв'язувати певний вузол з даними, що забезпечує ефективний пошук даних, навіть, якщо вони є рідкісними. Хешування дозволяє оптимізувати запити, оскільки кожен вузол має чітко визначене місце в топології мережі [67].

Саме на цьому принципі ґрунтуються протоколи обміну файлами в піринговых мережах, зокрема Gnutella, BitTorrent, eDonkey2000 та Direct Connect. Кожен з цих протоколів має свої методи пошуку та передачі даних.

Gnutella – це децентралізована файлообмінна мережа та водночас протокол для обміну файлами, який використовується в цій мережі [68]. Протокол Gnutella 0.4 включає кілька основних етапів, які відповідають за приєднання до мережі, пошукові запити та передачу даних. Передача даних в мережі Gnutella здійснюється в декілька етапів. Спочатку здійснюється підключення нового користувача до мережі Gnutella шляхом встановлення з’єднання з активним учасником цієї мережі та встановлення додаткового програмного забезпечення, наприклад GTK-Gnutella. Далі користувач-ініціатор надсилає Ping-запит із параметром TTL, що контролює кількість переходів запиту. Кожен вузол, який отримує Ping-запит, надсилає Pong–відповідь з власною IP-адресою, портом та інформацією про доступні файли. Pong–відповіді, які повертаються до ініціатора, формують список доступних вузлів та файлів для подальшого обміну.

Пошук файлів здійснюється шляхом розсилки запиту на всі вузли сформованого списку. Якщо файл знайдено, відповідний вузол надсилає інформацію про себе ініціатору, після чого вузол встановлює HTTP-з’єднання для завантаження файлу. Передача даних виконується за допомогою HTTP-запитів GET або PUSH, де GET використовується для прямого завантаження, а PUSH – для обходу мережних обмежень, зокрема NAT або брандмауерів, шляхом ініціювання зворотного з’єднання.

Всі етапи роботи протоколу – від підключення до передачі файлів – реалізовані на основі протоколу HTTP, що ускладнює відстеження та

блокування трафіку, оскільки HTTP є стандартним протоколом для більшості інтернет-з’єднань. Завдяки такому принципу роботи Gnutella забезпечує цілісність даних та знижує можливість відстеження ідентифікаційних даних відправника та одержувача. Використання механізму Ping/Pong для підтвердження активності вузлів і TTL для обмеження запитів забезпечує ефективну роботу у великих мережах, дозволяючи швидко будувати маршрути передачі даних на основі топології та поточного стану вузлів. Таким чином, протокол Gnutella залишається гнучким, масштабованим та адаптивним рішенням для забезпечення ефективного обміну файлами в умовах децентралізованих мереж [69].

Протокол BitTorrent використовує інший підхід, розбиваючи файли на дрібні фрагменти, які одночасно завантажуються на окремі вузли та передаються цими вузлами кінцевому одержувачу, що дозволяє підвищувати швидкість передачі даних та уникати перевантаження окремих вузлів. Для цього BitTorrent застосовує трекери та DHT для координації вузлів, що забезпечує додаткову стійкість мережі до збоїв та певний централізований підхід до управління поточним станом мережі.

Інші протоколи, зокрема eDonkey2000 та Direct Connect, використовують власні підходи. eDonkey2000 ґрунтується на спеціалізованих серверах для управління трафіком, тоді як Direct Connect використовує хаби – приватні або публічні точки доступу, де відбувається пошук та передача файлів.

Гібридні методи маршрутизації з використанням протоколів EIGRP, BGP та ZRP, які застосовуються у відкритих мережах, демонструють здатність комбінувати статичні та динамічні підходи для оптимізації та забезпечення стабільності маршрутів в умовах змінної топології, зберігаючи прозорість маршрутів. Протоколи EIGRP та BGP враховують топологію мережі та зміни навантаження при виборі оптимальних маршрутів передачі, що дозволяє забезпечувати гнучкість, масштабованість та підвищувати стійкість мережі до відмов та атак.

Гібридні методи маршрутизації в піринговых мережах орієнтовані на ефективний обмін файлами, зберігаючи високий рівень конфіденційності користувачів та знижуючи ймовірність відстеження маршрутів передачі даних. Для пошуку та передачі даних використовуються адаптивні алгоритми, які враховують поточний стан мережі та завантаженість вузлів. Такий підхід одночасно забезпечує конфіденційність та надійність роботи мережі. Гібридні методи маршрутизації в піринговых мережах, зокрема в Gnutella та BitTorrent, ефективно поєднують децентралізовану структуру з високою продуктивністю, надійністю, конфіденційністю та стійкістю до відмов та зовнішніх кіберзагроз.

Таким чином, в цьому розділі було проведено порівняльний аналіз статичних, динамічних та гібридних методів маршрутизації, які застосовуються у відкритих та анонімних мережах.

Отже, у відкритих мережах методи маршрутизації спрямовані на забезпечення стабільності та ефективності передачі даних при збереженні прозорості маршрутів, водночас анонімні оверлейні мережі орієнтовані на забезпечення високого рівня захисту та цілісності даних в умовах забезпечення відмовостійкості, стабільної та ефективної передачі даних. Розглянуті методи маршрутизації у відкритих та анонімних мережах мають свої особливості та переваги.

Застосування оверлейних мереж дозволяє створювати ізольовані мережні структури, які працюють поверх фізичної інфраструктури. Розгортання оверлейних мереж з використанням контейнерів дозволяє швидко масштабувати інфраструктуру, провести оптимізацію апаратних ресурсів та забезпечити додатковий рівень захисту фізичної мережної інфраструктури, завдяки ізоляції та створенню незалежної логічної інфраструктури.

Статичні методи маршрутизації, які використовуються в відкритих та анонімних мережах, забезпечують стабільність та простоту адміністрування, проте неефективні при зміні топології в реальному часі. VPN-тунелі, як

різновид оверлейних мереж, забезпечують високий рівень захисту та цілісності даних, знижують ризики витоку даних та несанкціонованого доступу, завдяки створенню віртуального захищеного тунелю та шифруванню даних під час передачі, проте обмежені використанням в масштабованих середовищах.

Динамічні методи маршрутизації в мережі TOR забезпечують максимальний рівень конфіденційності користувачів та приховування маршрутів, забезпечуючи при цьому адаптацію до змін в топології мережі. Проте динамічні методи маршрутизації мають суттєві обмеження щодо швидкості передачі даних, ефективності при високих навантаженнях, а також обмежено придатні для передачі даних в режимі реального часу, через значні затримки, які спричинені багаторівневим шифруванням.

Гібридні підходи, які застосовуються в піринговых мережах Gnutella та BitTorrent, комбінують переваги статичних та динамічних методів маршрутизації, забезпечуючи ефективність, автономність, стійкість до атак, завдяки децентралізованій архітектурі. Такі властивості децентралізованих мереж дозволяють забезпечити конфіденційність користувачів та підвищений рівень захисту даних. Проте наявність великої кількості активних вузлів може призвести до збільшення затримок при передачі даних під час пошуку актуальних маршрутів або їх оновлення.

3 ДОСЛІДЖЕННЯ АЛГОРИТМІВ МАРШРУТИЗАЦІЇ В АНОНІМНИХ МЕРЕЖАХ

3.1 Дослідження в умовах передачі еластичних даних

Потоки даних, які передаються комп'ютерними мережами поділяють на два види: еластичні та нееластичні. Кожен вид трафіку впливає на підходи до організації мережної інфраструктури, які мають наступні параметри та наведені в таблиці 3.1.

Таблиця 3.1 – Розподіл даних за типом та вимогами до параметрів передачі

Тип даних	**Вимоги до пропускної здатності**	**Чутливість до затримок**	**Чутливість до втрат пакетів**	**Приклади даних**
еластичні	низькі	нечутливі	нечутливі	електронна пошта, завантаження та обмін файлами, веб–серфінг, доступ до хмарного сховища
нееластичні	високі	високо чутливі	високо чутливі	IP–телефонія, відеоконференції, онлайн-ігри, моніторинг мережі в реальному часі (медичний, промисловий)

Еластичні дані здатні адаптуватися до змін пропускній здатності мережі без значного погіршення якості обслуговування (QoS) [70]. Вони здатні «переносити» коливання затримок та втрат пакетів без суттєвого впливу на кінцеву доставку пакетів. Проте, для нееластичних даних критично важливим є мінімізація затримок та втрат пакетів під час передачі, адже це

може призвести до погіршення якості відео або звуку, навіть, до переривання зв’язку [71].

Зі зростанням мультимедійного потокового контенту виникає перевантаження каналів передачі даних, що може призвести до затримок та накопичення пакетів в черзі на обробку [71]. Таке явище стає істотною проблемою для передачі нееластичного трафіку. Проте передача еластичного трафіку вимагає підтвердження доставки, що гарантує цілісність та закінчення процесу передачі даних. Моделювання та використання математичних моделей для розробки мережної інфраструктури з урахуванням вимог до пропускної здатності, типу трафіку та обсягів переданих даних дозволяє передбачити можливі вузькі місця або вразливості обраної мережної інфраструктури та алгоритмів маршрутизації.

Пропускна здатність каналу C визначає кількість переданих пакетів в одиницю часу та є основним параметром визначення ефективності мережі та відповідності вимогам щодо передачі певних видів трафіку. Пропускна здатність каналу обчислюється як

$$C = \frac{D}{T}\ , \tag{3.1}$$

де D – кількість переданих даних, біт;

T – час, за який передано дані, с.

Затримка визначається часом між відправленням та доставкою пакетів. Вона є критично важливим параметром для передачі даних в режимі реального часу. Комбінація втрат пакетів при доставці з затримкою викликає зниження ефективності передачі даних. Крім того, якщо виникають втрати пакетів, система намагається повторно надіслати втрачені дані, що спричиняє додаткове навантаження в мережі. Черги пакетів, які очікують на обробку, процеси шифрування та дешифрування на кожному вузлі під час передачі даних віртуальними тунелями, в також фізичні затримки в каналі, що

виникають через передачу сигналів, обробка пакетів на кожному вузлі маршруту передачі даних спричиняють додаткові затримки при передачі даних. Таким чином, загальна затримка L_{total} є сумою всіх затримок, що виникають під час передачі пакетів в мережі та може бути розрахована як:

$$L_{total} = L_t + L_p + L_q + L_{pr}, \tag{3.2}$$

де L_t – час передачі пакету, мс;

L_p – затримка на обробку пакету, мс;

L_q – затримка в черзі маршрутизаторів, мс;

L_{pr} – фізична затримка в каналі, мс.

Загальна затримка є важливим фактором, який впливає на швидкість та надійність передачі даних для всіх видів трафіку.

Втрати пакетів знижують реальну швидкість передачі даних, оскільки при передачі даних з використанням протоколу TCP гарантується доставка всіх пакетів, що буде вимагати повторної передачі втрачених пакетів. Це буде забезпечувати цілісність даних, що важливо для передачі еластичних даних. Втрати пакетів P_l є часткою від загальної кількості надісланих пакетів, які можуть бути розраховані як:

$$P_l = \left(\frac{P_s - P_r}{P_s} \right) \cdot 100\%, \tag{3.3}$$

P_r – кількість отриманих пакетів;

P_s – загальна кількість надісланих пакетів.

Реальна швидкість передачі є ключовим параметром ефективності роботи мережі, що враховує загальну затримку та втрати пакетів, які виникають в мережах під час передачі даних. Швидкість передачі даних R_{eff}

з урахуванням загальної затримки та втрат пакетів залежить від пропускної здатності каналу зв’язку та може бути розрахована як:

$$R_{eff} = \frac{C(1-P_l)}{1+L_{total}}. \quad (3.4)$$

де C – пропускна здатність каналу, біт/с;

P_l – частка втрачених пакетів;

L_{total} – загальна затримка в мережі, мс [72].

Таким чином, специфіка видів трафіку, який використовується в корпоративних мережах, буде значною мірою впливати на вибір методу маршрутизації, оскільки ключові параметри передачі, зокрема швидкість передачі даних, пропускна здатність каналу зв’язку та затримки визначають ефективність та надійність функціонування корпоративної комп’ютерної мережі.

3.1 Дослідження в умовах передачі еластичних даних

В анонімних оверлейних мережах передача еластичного та нееластичного трафіку обумовлена вимогою до підвищеного рівня захисту даних та конфіденційності користувачів із забезпеченням гарантованої доставки та цілісності даних.

Статична маршрутизація з фіксованими IP-адресами вузлів забезпечує стабільність та незмінність маршрутів. Застосування фіксованих маршрутів забезпечує стабільне навантаження та передбачувані затримки, а також знижує коливання в часі доставки даних. Такий підхід дозволяє передавати еластичні дані з високою швидкістю передачі з урахуванням вимог до підвищеного рівню безпеки. При передачі даних VPN-тунелями виконується шифрування та дешифрування трафіку за допомогою сучасного стандарту шифрування AES-256, який використовується багатьма протоколами

тунелювання, в тому числі протоколом OpenVPN. При цьому швидкість процесів шифрування-дешифрування за цим стандартом дозволяє ефективно передавати еластичні дані та не збільшує загальну затримку при передачі VPN-тунелями. Проте, при обмеженій пропускній здатності або в разі перевантаження основних вузлів передачі, можуть збільшуватися затримки та виникати втрати пакетів, що обмежує використання статичної маршрутизації в великомасштабних мережах [73].

Завдяки «цибулевій» маршрутизації в TOR маршрут передачі даних формується динамічно, при цьому на кожному вузлі виконуються процеси шифрування та дешифрування кожного пакету даних. З одного боку, такий підхід забезпечує високий рівень анонімності, з іншого – збільшує затримки через складність криптографічних алгоритмів SSl/TLS, які використовуються для шифруванн трафіку в TOR [74]. Через таке багатошарове шифрування здійснюється приховування вмісту пакету даних, проте збільшує затримки через обчислювальну складність шифрування даних та створює додаткове навантаження на вузли маршруту.

За умови змінної доступності вузлів побудова маршрутів в мережі TOR здійснюється за тим же принципом вибору оптимального шляху, як в протоколі OSPF [75]. Під час передачі даних мережею TOR користувачі можуть самостійно обирати вихідні вузли та ланцюги проміжних вузлів з урахуванням їх доступності та географічного розташування, що також дозволяє зменшити затримки та підтримувати стабільність з’єднання під час кожної сесії в мережі TOR. В такому разі ланцюг проміжних вузлів маршруту зберігається на весь час користувацької сесії. Наступна сесія буде використовувати інший ланцюг, який буде сформовано автоматично, без участі користувача на основі поточного стану мережі. Таким чином, зважаючи на динамічно змінну топологію, мережа TOR забезпечує достатній рівень пропускної здатності та швидкості передачі еластичних даних. Основним протоколом для передачі даних в мережі TOR є TCP, який забезпечує гарантовану доставку пакетів [76].

Таким чином, динамічні методи маршрутизації в мережі TOR дозволяють підтримувати задовільну пропускну здатність та швидкість передачі даних, проте багатошарове шифрування на кожному вузлі спричиняє збільшення затримки. Оскільки еластичні дані нечутливі до затримок та низької пропускної здатності, це дозволяє забезпечувати надійну передачу еластичних даних в мережі TOR з високим рівнем анонімності.

Пірингові мережі Gnutella та BitTorrent також мають децентралізовану архітектуру. Так само як в мережі TOR, в цих мережах топологія є динамічно змінюваною. Це дозволяє оптимізувати передачу даних з урахуванням поточного стану мережі, її навантаження та доступності ресурсів та вузлів.

Проте в Gnutella та BitTorrent використовуються гібридні методи маршрутизації на відміну від мережі TOR. Ці мережі використовуються для обміну файлами, що відповідає передачі еластичних даних. Основний протокол, який використовується для передачі даних в Gnutella є TCP, що гарантує цілісність переданих даних.

В Gnutella кожен вузол використовує локальні таблиці маршрутизації для пошуку ресурсів, що забезпечує швидке визначення можливих маршрутів. В разі зміни доступності вузлів маршрути автоматично коригуються, що дозволяє підтримувати високу ефективність передачі за умови виникнення часткових збоїв у мережі. Крім цього, на централізованих вузлах зберігаються розподілені хеш-таблиці (DHT) з унікальними хеш-ідентифікаторами вузлів, що сприяє зменшенню часу пошуку вузлів та підвищенню швидкості передачі даних [77]. Слід зазначити, що для службового трафіку, зокрема для пошуку доступних вузлів та встановлення з’єднання, в Gnutella використовується протокол UDP, який пришвидшує швидкість передачі даних з урахуванням динамічної топології мережі.

Також гібридний підхід включає використання трекерів для координації взаємодії вузлів. Зокрема в BitTorrent трекери виконують роль централізованих координаторів, які допомагають знаходити визначені вузли, що прискорює обмін файлами. Однією з особливостей використання

BitTorrent є розділ файлів на фрагменти, які зберігаються на різних вузлах мережі. Завдяки фрагментації кожен вузол завантажує лише окрему частину файлу на противагу повному обсягу файла, що знижує загальне навантаження на мережу та забезпечує адаптивність маршрутів залежно від доступності та завантаженості вузлів. Це сприяє рівномірному розподілу трафіку, зменшуючи ризик перевантаження окремих учасників мережі. Таким чином, фрагментація та використання трекерів прискорює обмін еластичними даними в мережі [78].

Проте, підвищена складність алгоритмів побудови маршрутів вимагає додаткових обчислювальних ресурсів для оперативної обробки змін у мережі. Також постійна варіативність підключень в динамічному середовищі може призводити до проблем з синхронізацією даних між вузлами, навіть за умови використання централізованих вузлів, що знижує швидкість завантаження еластичних даних, особливо при пошуку рідкісних файлів або значному навантаженні на окремі вузли. Це спричиняє зниження продуктивності мережі в умовах високого попиту на певні ресурси та забезпечення стабільності передачі даних в динамічно змінюваному середовищі.

Водночас, використання протоколу BitTorrent дозволяє регулювати завантаження та вивантаження даних, балансуючи пропускну здатність між активними вузлами. Це забезпечує мінімізацію перевантаження за умов високої кількості одночасних підключень в мережі [79]. В Gnutella, децентралізована архітектура та використання протоколів обміну даними сприяє рівномірному розподілу трафіку. Це дозволяє зменшити затримки та забезпечити ефективну маршрутизацію у великих та нерівномірно навантажених мережах [80].

3.2 Дослідження в умовах передачі нееластичних даних

Нееластичні дані вимогливі до стабільної пропускної здатності, затримки та надійності передачі даних. IP-телефонія та відеоконференції є прикладом передачі нееластичних даних.

Завдяки фіксованим маршрутам та визначеним IP-адресам вузлів, статична маршрутизація забезпечує передбачуваність затримок та стабільність передачі даних, що є критично важливим для нееластичних даних. Завдяки цьому при передачі даних в режимі реального часу мінімізуються затримки, а також це дозволяє уникнути спотворень та роз’єднань під час передачі нееластичних даних.

Проте, варіативність пропускної здатності або перевантаження в мережі, які спричинені збільшенням обсягу пакетів, що надходять до прикордонних вузлів може спричиняти збільшення черги пакетів на обробку вузлами. Через це збільшується загальна затримка та виникають паузи під час відтворення потокового відео чи голосового зв'язку.

Шифрування даних, яке використовується при передачі даних у віртуальних тунелях додає обчислювального навантаження на мережні вузли, причому зі збільшенням складності криптографічних алгоритмів, збільшується навантаження, що призводить до зниження швидкості передачі даних та максимізації затримок. Це, в свою чергу, буде негативно впливати на нееластичний трафік та може знижувати ефективність анонімної оверлейної мережі.

Використання криптографічного стандарту AES-256 дозволяє підтримувати високий рівень захисту даних та забезпечити низьку затримку через процеси шифрування-розшифрування на кінцевих вузлах VPN-тунелів, які використовують статичні алгоритми маршрутизації. Використання протокола UDP при передачі даних в тунелях також сприяє стабільній передачі нееластичних даних, що дозволяє використовувати VPN-тунелювання для забезпечення високого рівня захисту та цілісності даних в умовах передачі потокового відео та голосового зв’язку за умови достатньої пропускної здатності каналу [81].

Передача даних в децентралізованих мережах здійснюється за динамічно змінюваною топологієї мережі. Так, в мережі TOR виконується динамічне перенаправлення трафіку через випадково обрані вузли, які на час

кожної сесії формують ланцюг проміжних вузлів маршруту передачі даних. Проте, динамічна маршрутизація через постійну зміну доступності вузлів-посередників спричиняє додаткові затримки на оновлення та побудову маршрутів. Це позначається на якості обслуговування під час передачі нееластичних даних, що, в свою чергу, знижує продуктивність анонімних оверлейних мереж на кшталт TOR.

Складність оптимізації маршрутів в мережі TOR ускладнює налаштування передачі нееластичних даних під користувацькі вимоги. Часті зміни маршрутів роблять складним прогнозування поведінки мережі та оптимізацію для досягнення мінімальних затримок і максимальної пропускної здатності. Крім того, труднощі з діагностикою проблем в мережі TOR ускладнюють виявлення та усунення неполадок, пов'язаних із передачею даних.

Багатошарове шифрування, яке відбувається на кожному вузлі мережі TOR у «цибулевій» маршрутизації виконується з використанням SSl/TLS, яке використовує шифрування RSA, що використовує ключи з довжиною 2048, 3072 або 4096 біт. Складніший алгоритм шифрування RSA, в порівнянні з AES-256, збільшує затримку шифрування під час обробки пакету на вузлі. Зважаючи, що в мережі TOR, процеси шифрування-розшифрування даних відбуваються на кожному вузлі маршруту, то загальна затримка значно зростає, ось чому в мережі TOR при перегляді потокового відео виникають численні затримки під час передачі пакетів.

Крім цього передача даних в мережі TOR підтримується протоколом TCP, що гарантує доставку переданих пакетів. Проте такий підхід погіршує передачу нееластичних даних, через те, що в динамічній топології TOR можуть виникати втрати пакетів через оновлення та перебудову маршрутів. Оскільки для передачі нееластичного трафіку використовується протокол UDP, що дозволяє зберігати високу швидкість потоку даних у відкритих мережах, то для мережі TOR визначені пакети доводиться інкапсулювати в

TCP-пакети. Така інкапсуляція призводить до значного підвищення затримки та зниження швидкості передачі даних.

Таким чином, високі затримки, багатошарове шифрування, нестабільна пропускна здатність та складність оптимізації мережі значно обмежують використання TOR для передачі нееластичного трафіку, незважаючи на високий рівень анонімності, який надає ця мережа.

Пірингова мережа Gnutella теж має децентралізовану архітектуру, проте в ній застосовуються гібридні методи маршрутизації. Комбінація фіксованих IP-адрес вузлів, що мають свої хеш-ідентифікатори та зберігаються на централізованих вузлах, та топології, що змінюється в реальному часі, дозволяє адаптувати маршрутизацію в мережі до динамічних змін та змінюваної пропускної здатності. Це дозволяє ефективно передавати еластичний трафік в таких мережах, а також виявляє значний потенціал для передачі нееластичного трафіку.

Агрегація ресурсів багатьох вузлів-пірів дозволяє досягати значно більшої пропускної здатності в порівнянні з клієнт-серверною архітектурою. Автоматична перебудова мережі в разі значних навантажень або відмови одного чи декількох вузлів дозволяє забезпечити стабільну роботу мережі за умови високого навантаження. Це забезпечує високу пропускну здатність та швидкість передачі даних. Кожен вузол мережі використовує свої власні ресурси, що дозволяє ефективно розподіляти навантаження серед учасників мережі, знижуючи ризик перевантаження окремих вузлів і забезпечуючи більшу стійкість до проблем з пропускною здатністю [82].

Також розподілена архітектура дозволяє покращити відмовостійкість мереж та захист від DDoS-атак, оскільки динамічна побудова маршруту враховує можливі збої в мережі або вихід окремих вузлів з мережі. Це, в свою чергу, дозволяє підвищити рівень захисту даних, що передаються мережею та забезпечити приховування ідентифікаційних даних відправника та одержувача.

Основним протоколом, який використовується в пірингових мережах для передачі даних є протокол TCP, що дозволяє гарантувати доставку пакетів, зберігаючи цілісність даних. Протокол UDP забезпечує передачу службового трафіку, тобто використовується для пошуку вузлів та встановлення з'єднання при передачі даних. Оскільки протокол UDP забезпечує передачу нееластичних даних у відкритих мережах та використовується для встановлення з'єднань в пірингових мережах, то такий підхід дозволяє використовувати пірингові мережі для передачі нееластичних даних, що реалізовано в месенджері Element, який базується на протоколі Matrix. Окрім передачі медіаконтенту, що є еластичним трафіком, протокол Matrix та децентралізована архітектура серверів-пірів, яку використовує цей месенджер, дозволяє передавати нееластичні дані в реальному часі [83]. Matrix поєднує централізовані та дистрибутивні елементи, що забезпечує стійкість до атак та адаптивність до змін у мережі. Пірингова архітектура знижує залежність від центральних серверів, підвищуючи безпеку даних, та використовує ресурси кожного учасника мережі для підтримки високої пропускної здатності.

Таким чином, пірингові мережі, які базуються на гібридних підходах до маршрутизації, мають високий потенціал для використання в якості ефективного середовища для передачі нееластичних даних. Висока адаптивність до змін топології, оптимальне використання ресурсів та відмовостійкість дозволяє використовувати пірингові мережі для передачі великих обсягів даних із збереженням високої швидкості та забезпеченням високого рівня конфіденційності. Проте, на даний час пірингові мережі найбільше використовуються для передачі еластичного трафіку, що забезпечено використанням протоколу TCP як основного транспортного протоколу в цих мережах. Зважаючи, що в пірингових мережах також використовується протокол UDP для пошуку вузлів та встановлення сеансів зв'язку, використання пірингових мереж є перспективним напрямком для передачі нееластичного трафіку.

Отже, при дослідженні методів передачі еластичних та нееластичних даних в анонімних оверлейних мережах встановлено, що на вибір алгоритму маршрутизації впливає вид даних, які можуть передаватися в таких мережах. Для еластичних даних, які менш чутливі до затримок та обмежень пропускної здатності можливо використовувати будь-який з описаних методів маршрутизації. Причому використання протоколу TCP в якості основного протоколу передачі даних в оверлейних мережах з підвищеним рівнем захисту даних дозволяє гарантувати цілісність даних, що забезпечує даний протокол.

В разі передачі нееластичних даних, які вимагають стабільної пропускної здатності та низьких затримок придатними є оверлейні мережі, які можуть забезпечити стабільність передачі даних. VPN-тунелі, які використовуються на прикордонних вузлах мережі та забезпечують віддалений доступ до екстранет-мереж дозволяють забезпечити задовільну пропускну здатність каналу зв’язку та захищений зв’язок, що досягається використанням алгоритмів шифрування. Таким чином статичні методи маршрутизації, які реалізовані з використанням VPN-тунелювання, дозволяють забезпечити передачу нееластичних даних в умовах підвищеного рівня безпеки та цілісності даних. Перспективним напрямком для передачі нееластичних даних є пірингові мережі, які забезпечують стійкість до відмов мережі, надійність передачі даних та підвищений рівень безпеки та конфіденційності користувачів, проте наразі мають збільшені затримки при передачі даних, в порівнянні зі статичними методами, через недосконалі алгоритми побудови динамічних маршрутів. Застосування анонімних мереж на кшталт TOR, які забезпечують максимальний рівень захисту маршрутів передачі та конфіденційності користувачів, для передачі нееластичних даних, наразі є недоцільним через значні затримки, що обумовлені процесами шифрування-розшифрування даних на кожному вузлі, динамічною побудовою маршруту, та неможливістю оптимізації маршрутизації через варіативність побудови та прогнозування маршруту.

4 РОЗРОБКА МЕТОДУ МУЛЬТИРІВНЕВОГО ВІРТУАЛЬНОГО ТУНЕЛЮВАННЯ В АНОНІМНИХ МЕРЕЖАХ ПРИ ОРГАНІЗАЦІЇ ДОСТУПУ ДО ЕКСТРАНЕТ-СЕГМЕНТУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

З розвитком мережної інфраструктури все більше уваги приділяється налаштуванню політики безпечного доступу до корпоративних мереж. Це спричинило розподіл мереж на екстранет та інтранет-мережі, де екстранет-мережі надають доступ для зовнішніх користувачів з урахуванням політики безпеки, а інтранет-мережі використовуються лише співробітниками внутрішньої корпоративної мережі [84]. Одним з ключових підходів для реалізації безпечного доступу до інтранет-мереж є використання технологій VPN. Проте ряд існуючих рішень з використанням VPN-технологій мають низку недоліків, зокрема зниження продуктивності через складність процесів шифрування та розшифрування, високі вимоги до апаратного забезпечення та збільшення затримок при передачі даних через віртуальні тунелі [85].

В умовах сучасної розвиненої мережної інфраструктури найбільше застосовуються багаторівневі архітектури мереж, що вимагає забезпечення надійної автентифікації на різних рівнях доступу до конфіденційних даних, а також ускладнюється збереженням достатньої швидкості передачі даних для підтримки ефективної роботи та підключення віддалених робочих місць. Крім цього впровадження дороговартісних рішень унеможливлює застосування таких підходів в бізнес-процесах малого та середнього бізнесу. Це зумовлює пошук економічно обґрунтованих методів, які використовуються в умовах обмеження апаратних ресурсів та забезпечують надійний віддалений захищений доступ до корпоративних ресурсів в умовах забезпечення високого рівня безпеки та цілісності даних.

Метод багаторівневого VPN-тунелювання для забезпечення віддаленого доступу до вузлів екстранет–мережі ґрунтується на застосуванні

сучасних підходів до криптологічного захисту та динамічного управління мережними ресурсами. Віддалений доступ до вузлів екстранет-мережі забезпечується різними рівнями доступу користувачів, залежно від їх ролей та наданих привілеїв в корпоративній комп'ютерній мережі. Наукова новизна методу полягає в розробці багаторівневої архітектури VPN-тунелів, які забезпечують додатковий захист від різноманітних можливих кібератак, спрямованих на компрометацію вузлів або каналів зв'язку в корпоративній мережі, забезпечуючи надійність передачі даних.

Для даного методу розроблено послідовний алгоритм в залежності від сценаріїв використання методу, виконання якого включає наступні етапи:

1) Попередня автентифікація та авторизація користувача, яка виконується перед встановленням VPN-з'єднання та початком сесії. На цьому етапі проводиться перевірка користувача за сертифікатами, логіном та паролем, або іншими механізмами автентифікації. В разі невідповідних даних користувача, система автоматично відхиляє запит на з'єднання, надаючи можливість повторної спроби для автентифікації.

2) Створення першого рівня VPN-тунелювання. Цей базовий VPN-тунель призначений для шифрування основного інтернет-трафіку користувачів з мінімальними вимогами до обчислювальних ресурсів. Для шифрування можуть бути використані алгоритми AES-256 або протоколи TLS/SSL, залежно від вибору протоколу тунелювання. В разі успішної автентифікації попереднього етапу, користувач отримує доступ до внутрішніх ресурсів мережі, які доступні всім користувачам. Водночас доступ до критично важливих вузлів буде залишатися обмеженим для загальної кількості користувачів.

3) Налаштування внутрішньої маршрутизації та моніторингу трафіку. Після успішного з'єднання на першому рівні система реалізує динамічний моніторинг мережного трафіку. Вона аналізує тип запитів та класифікує їх залежно від необхідного рівня доступу. В разі виявлення аномалій, таких як підозрілий трафік або несанкціонований запити на доступ до критичних

ресурсів, система ініціює обмеження доступу або додаткові етапи автентифікації.

4) Реалізація другого рівня тунелювання. Другий рівень VPN-тунелювання призначено для забезпечення доступу до конфіденційних ресурсів внутрішньої мережі або вузлів екстранету. На цьому етапі виконуються додаткові процедури автентифікації, а саме може бути налаштовано використання одноразових паролей (OTP) або використання цифрового підпису. На цьому рівні застосовується тунелювання з покращеними методами шифрування, наприклад застосування сучасних версій протоколу TLS із сертифікованими ключами. В разі невдалої автентифікації другий рівень тунелювання автоматично закривається відповідним прикордонним вузлом, а доступ для користувача обмежується лише базовим рівнем тунелювання.

5) Налаштування динамічного управління мережними ресурсами, яке виконується за допомогою використання інтелектуальних алгоритмів управління на основі навантаження, активності користувачів та типів запитів, які надходять до цієї корпоративної мережі. Наприклад, в разі значного збільшення вхідного трафіку або кількості користувацьких підключень до другого рівня, система може на деякий час припинити приймання запитів на нові підключення та виконати перенаправлення запитів на інші ресурси.

6) Створення нового рівня тунелювання. Спеціалізовані запити, що надходять в мережу для доступу до конфіденційних ресурсів, вимагають нового рівня тунелювання, який забезпечується багаторівневою автентифікацією. Таку автентифікацію можливо виконати через використання апаратних токенів або посилених алгоритмів шифрування даних. Доступ до цих ресурсів здійснюється після підтвердження додаткових прав доступу.

7) Завершення сесії та закриття тунелів. Після завершення роботи всі активні тунелі автоматично закриваються. Корпоративна комп’ютерна мережа здійснює перевірку залишкових даних, забезпечуючи видалення всіх тимчасових ключів шифрування. Це унеможливлює перехоплення або

повторне використання ключів шифрування для несанкціонованого доступу в майбутньому.

Обґрунтованість використання методу підтверджується його адаптивністю до різних сценаріїв, зокрема:

- на початковому рівні здійснюється лише загальне підключення користувачів з моніторингом їх автентифікації. В разі збою автентифікації або помилкового з'єднання тунель автоматично відразу закривається;

- другий рівень виконує обслуговування користувачів з доступом до конфіденційних даних, причому система виконує моніторинг активності підозрілих дій, в разі виявлення яких доступ до ресурсів з підвищеною конфіденційністю блокується, а користувач отримує доступ лише до ресурсів базового рівня;

- інші, глибинні рівні тунелювання, орієнтовані на виконання спеціалізованих операцій. Доступ до ресурсів цього рівня виконується за умови виконання всіх умов перевірки та відповідності обраним методам автентифікації.

В додатку Б наведено псевдокод, який надає логічну структуру виконання запропонованого методу. В ньому представлено умови, цикли, виклики функцій та обробки даних, що надає розуміння послідовності виконання операцій та налаштувань даного методу.

Зважена оптимізація всіх факторів, а саме швидкості передачі, рівня безпеки та ефективності використання ресурсів складає загальну ефективність методу багаторівневого VPN-тунелювання, яка може бути виражена через вагові коефіцієнти та ключові параметри в наступній багатофакторній оптимізаційній задачі:

$$E_{total} = \max(\alpha \cdot S + \beta \cdot (1 - P_{total} \cdot \log(C_{attack})) + \gamma \cdot \mathrm{R}_{eff} \ \textit{при}\ C_{attack} = \min(C_{attack,i}), \quad (4.1)$$

де α, β, γ – вагові коефіцієнти, які визначають пріоритети ключових параметрів задачі;

C_{attack} – мінімальна обчислювальна складність атаки на рівні шифрування.

Компонентами оптимізаційної задачі є:

1. Оцінка продуктивності передачі даних в тунелях з урахуванням криптографічної складності. Швидкість передачі даних (S) знижується через обчислювальну складність алгоритмів шифрування на кожному рівні тунелювання. Нехай $C_{comp,i}$ – обчислювальна складність шифрування на i-му рівні, тоді ефективна швидкість передачі даних може бути представлена як:

$$S = \frac{B}{N\sum_{i=1}^{N}\left(C_{comp,i} + \frac{t_{enc,i}}{t_{trans.i}}\right)}, \tag{4.2}$$

де B – базова швидкість мережі без шифрування, Б/с;

N – кількість рівнів тунелювання, од.;

$t_{enc,i}$ – час, необхідний для шифрування на i-му рівні, с;

$t_{trans.i}$ – час передачі даних через мережу на i-му рівні, с.

Обчислювальна складність залежить від використовуваного алгоритму шифрування та від співвідношення між часом шифрування та передачею даних на визначених рівнях.

2. Оцінка затримки передачі даних враховує перемикання рівнів. Затримка (L) враховує не лише час шифрування та декодування, але й затримку через чергування запитів на кожному рівні тунелювання. Для цього можна застосувати модель чергування M/M/1 [86] (середня затримка в системі з обслуговуванням):

$$L = \sum_{i=1}^{N}\left(\frac{1}{\mu_i - \lambda_i} + t_{enc,i} + t_{dec,i} + t_{trans,i}\right), \tag{4.3}$$

де μ_i – середня швидкість обробки запитів на i-му рівні;

λ_i – інтенсивність вхідних запитів, середня кількість запитів на одиницю часу;

$t_{dec,i}$ – час, необхідний для декодування даних на i-му рівні, с.

Дана формула (3) моделює вплив навантаження на систему та враховує затримку черги запитів при підвищеному навантаженні на мережу.

3. Оцінка ефективності використання ресурсів залежить від оптимального використання обчислювальних ресурсів для шифрування та передачі даних, що можна представити в наступному вигляді:

$$R_{effect} = \frac{\sum_{j=1}^{M} D_j}{\sum_{i=1}^{N} \left(C_{enc,i} + C_{trans,i} \right) \times \max\left(\frac{t_{enc,i}}{t_{trans,i}}, 1 \right)}, \quad (4.4)$$

де D_j – обсяг даних, переданий на j-му рівні, Б (відноситься до завдань передачі даних);

$C_{enc,i}$ – обчислювальні ресурси, витрачені на шифрування на i-му рівні, од.;

$C_{trans,i}$ – обчислювальні ресурси, витрачені на передачу на i-му рівні, од.;

M – кількість завдань на передачу даних.

4. Оцінка рівня безпеки через ймовірність складної атаки. Імовірнісну модель, яку доцільно використовувати для оцінки рівня безпеки, враховує ймовірність успішної атаки на кожен рівень та обчислювальну складність такої атаки на шифрування:

$$P_{total} = 1 - \prod_{i=1}^{N} \left(1 - \frac{P_{attack,i}}{C_{attack,i}} \right), \quad (4.5)$$

де $P_{attack,i}$ – ймовірність успішної атаки на і-му рівні;

$C_{attack,i}$ – обчислювальна складність успішної атаки на шифрування на і-му рівні.

Таким чином, складність алгоритму шифрування зменшує ймовірність успішної атаки.

Математичне моделювання запропонованого методу дозволяє комплексно оцінити ефективність методу багаторівневого VPN-тунелювання з урахуванням складності алгоритмів шифрування, моделі чергування, ресурсоємності шифрування та передачі даних, а також ймовірності успішних атак. Використана математична модель забезпечує кількісну оцінку оптимізації системи VPN.

Аналіз апаратних вимог на початковому етапі показав, що для стабільного функціонування OpenVPN-сервера потрібно застосовувати процесор з принаймні чотирма ядрами та максимальною частотою 2,9 ГГц. Обсяг ОЗУ залежить від кількості підключених пристроїв та потоку переданих даних. З точки зору практичного використання відомо, що 1 ГБ ОЗУ дозволяє обслуговувати до 150 підключених пристроїв, які можуть одночасно використовувати це VPN–з’єднання. Така конфігурація VPN-серверу буде цілком достатньою для обслуговування невеликих та середніх підприємств за умови, що в мережі можуть використовуватися додаткові пристрої, крім безпосередньо робочих станцій. Пропускна здатність каналу зв’язку становить 72 Мбіт/с, що забезпечує обслуговування користувачів експериментальної корпоративної мережі. Обсяг дискового простору VPN-сервера повинен мати не менше 8 ГБ вільного місця.

Для з’єднання з VPN–сервером екстранет-мережі віддаленому користувачу потрібно встановити додаткове програмне забезпечення клієнта, а саме OpenVPN client, яке може бути встановлено на різні операційні системи, зокрема Windows, MacOS або на Linux.

Налаштування VPN-сервера здійснюється в ізольованому контейнері Proxmox, при цьому формування клієнтських сертифікатів відбувається через

веб-інтерфейс OpenVPN GUI. Розташування VPN-сервера в ізольованому контейнері забезпечує додатковий рівень захисту, що унеможливлює виявлення IP-адреси сервера при несанкціонованому доступі. Непривілейований контейнер Proxmox має ще одну перевагу в контексті забезпечення додаткового рівня безпеки – до нього неможливо підключитися за прямим SSH-підключенням. В разі необхідності додатково можливо налаштувати файлову гостьову систему. На рисунку 4.1 представлено схему підключення користувачів до OpenVPN-серверу.

Рисунок 4.1 – Схема підключення клієнтів до OpenVPN-серверу

Після встановлення програмного клієнтського забезпечення та успішного з'єднання користувач отримує доступ до ресурсів базового рівня згідно з політикою доступу щодо ролей та привілеїв користувачів визначеної корпоративної мережі.

На рисунку 4.2, віддалений користувач спочатку проходить автентифікацію – в клієнтському застосунку потрібно ввести пароль та логін користувача, а також завантажити наданий користувачу сертифікат, який було сформовано через веб-інтерфейс OpenVPN GUI. Надалі він підключається до VPN-серверу з загальнодоступної мережі через шлюз

ізольованого контейнера Proxmox, який забезпечує маршрутизацію між сегментами корпоративної мережі та екстранет-мережею. Таким чином, користувач отримує унікальний ідентифікатор з визначеними доступом до сервісів, які йому дозволено використовувати. Захист даних здійснюється за AES-256 – криптографічним протоколом, а також використовується двосторонній сертифікат, відповідно для клієнта та сервера, що забезпечує взаємну довіру та відповідність сервера та клієнта при з'єднанні.

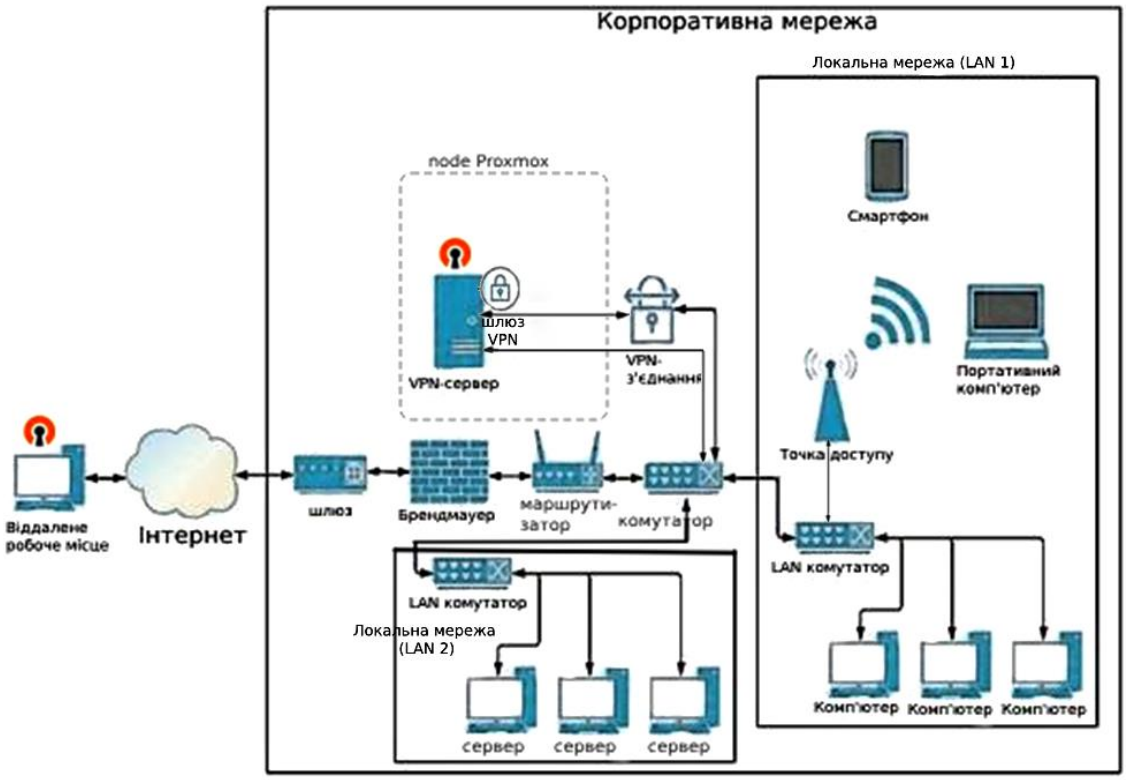


Рисунок 4.2 – Використання контейнеризації при реалізації методу

Для реалізації моделі було використано сервіси хмарних обчислень та підготовлено тестову модель віртуальної системи. Сервер було налаштовано на операційній системі Linux Ubuntu Server версії 18.04, на клієнті було встановлено ОС Windows 10. Також для фільтрації трафіку було додано правила для брандмауера та налаштовано правила NAT. Для додаткового захисту доступу до веб-інтерфейсу OpenVPN GUI та безпосередньо

OpenVPN-серверу було налаштовано перенаправлення портів, а саме 943 – для з'єднання з OpenVPN GUI, 1194 – стандартного порта OpenVPN при використанні протоколу UDP в якості основного протоколу передачі в віртуальному тунелі. За необхідності адміністратор мережі може налаштувати інші обрані порти для цих правил.

Після виконання скрипта в ізольованому контейнері Proxmox надається доступ до OpenVPN GUI, де надалі виконуються налаштування сервера, крім базових, а також формуються сертифікати користувачів та налаштовуються політики доступу та привілеї користувачів.

Перш за все, тестову модель було перевірено на працездатність, тобто виконано обмін різнорозмірними ICMP-пакетами. Після успішної перевірки працездатності віртуального тунелю було здійснено аналіз потоків пакетів за допомогою аналізатора трафіку Wireshark, які проходять через віртуальний тунель, а також основних параметрів передачі даних, зокрема швидкості передачі, пропускної здатності каналу, затримки тощо при передачі еластичних та нееластичних даних. Після фільтрації пакетів, які проходять через VPN-тунель, було підтверджено, що вміст пакетів залишається зашифрованим. Це свідчить про ефективність застосування алгоритмів шифрування (рисунок 4.3). Результати проведеної апробації даного методу наведено в таблиці 4.1.

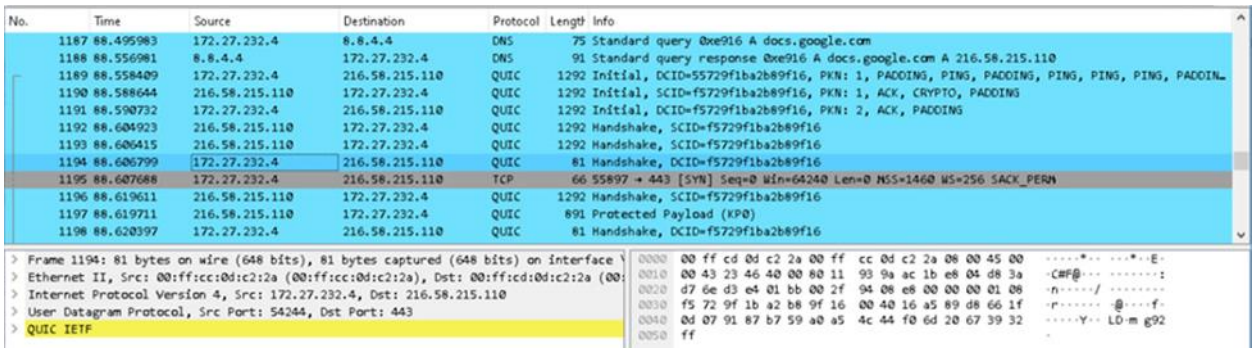


Рисунок 4.3 – Аналіз відфільтрованих пакетів

Таблиця 4.1 – Результати апробації методу мультирівневого VPN-тунелювання

параметр	**Метод мультирівневого VPN-тунелювання**	
	TCP	**UDP**
Пропускна здатність, Гбіт/с	0,0800	
Загальний обсяг даних, Мб	123,55	
Швидкість передачі, Гбіт/с	0,0850	0,0201
Затримка, мс	0,0114	0,0018
Частка у трафіку, %	57,55	42,45
Еластичні дані	+	
Нееластичні дані	+	

Отже, зі збільшенням кількості рівнів VPN-тунелювання, спостерігається зменшення швидкості, що зумовлене обчислювальною складністю та часом шифрування (рисунок 4.4). При цьому значення загальної затримки залишається постійним, оскільки вона є сумарним впливом процесів шифрування та передачі на кожному рівні. Це свідчить про те, що кожний додатковий рівень тунелювання впливає на загальну продуктивність методу. Апробація запропонованого методу показує, що при збільшенні рівнів тунелювання ефективність використання ресурсів зменшується.

Постановка експерименту була виконана на базі лабораторії обчислювальних систем та мережних технологій кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки.

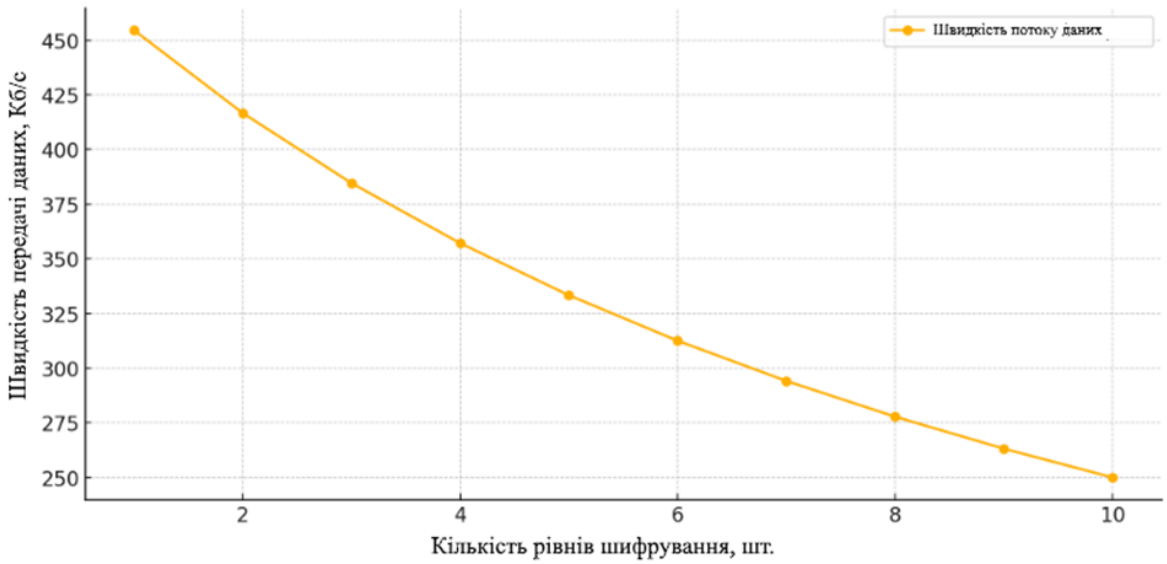


Рисунок 4.4 – Зміна значення швидкості передачі даних в залежності від кількості рівнів шифрування

На основі даного методу була підготовлена стаття «Метод мультирівневого VPN-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі». Стаття містить детальний аналіз методу багаторівневого VPN-тунелювання, який використовується для забезпечення адаптивного підходу до балансування між ефективністю, безпекою та використанням мережних ресурсів.

Майбутні дослідження в цьому напрямі зорієнтовані на подальшій оптимізації запропонованого методу. Наприклад, інтеграція більш сучасних криптографічних алгоритмів дозволяє підвищити продуктивність та безпеки системи.

5 АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ АЛГОРИТМІВ МАРШРУТИЗАЦІЇ У АНОНІМНИХ МЕРЕЖАХ

В даному розділі наведено експериментальні дослідження алгоритмів маршрутизації, що застосовуються в анонімних мережах, які спрямовані на аналіз параметрів передачі даних статичних, динамічних та гібридних методів маршрутизації.

5.1 Моделювання статичного алгоритму маршрутизації

В рамках моделювання статичної маршрутизації проведено дослідження роботи VPN-сервера, який використовує фіксований маршрут для доступу до ресурсів локальної мережі для віддалених користувачів. Для розгортання VPN-сервера використано віртуальну платформу Proxmox, в якій був створений ізольований контейнер з подальшим налаштуванням конфігурації сервера для забезпечення стабільної роботи сервісу (рисунок 5.1).

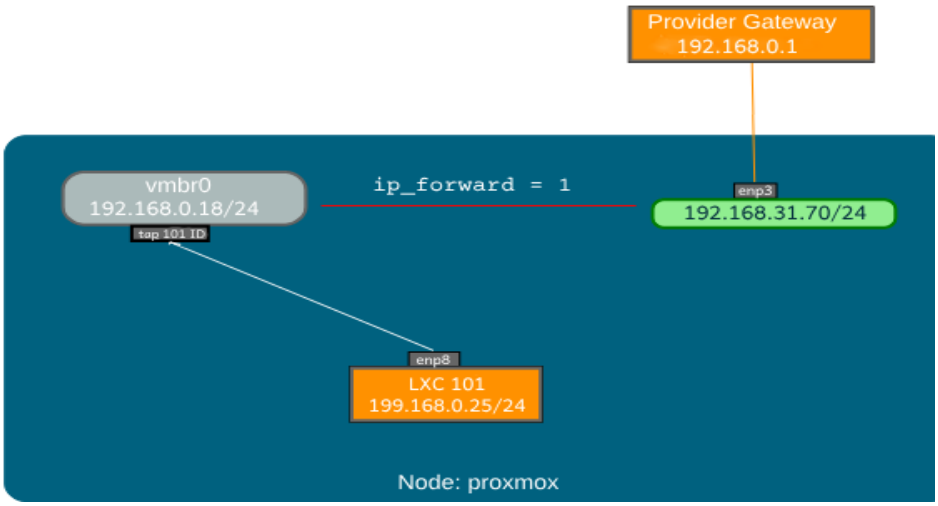


Рисунок 5.1 – Схема налаштування VPN-серверу на платформі Proxmox з використанням контейнера 101

Для створення ізольованого контейнера використано наступний покроковий алгоритм:

Крок 1. Створення ізольованого контейнеру на хості Proxmox з операційною системою Ubuntu 20.04 (Focal Fossa)

Лістинг 5.1 – Створення ізольованого контейнеру 101

```
#pveam download local ubuntu-20.04-standard_20.04-1_amd64.tar.gz
#  pct create 101 local:vztmpl/ubuntu-20.04-standard_20.04-
1_amd64.tar.gz --unprivileged 1 -features nesting=1 --net0
name=eth0,bridge=vmbr0,firewall=1,ip=dhcp,type=veth --storage
local-lvm
```

Крок 2. Додавання прав на використання ізольованого контейнеру

Лістинг 5.2 – Створення ізольованого контейнеру 101

```
 # chown 100000:100000 /dev/net/tun
 # ls -l /dev/net/tun
```

Крок 3. Перехід до контейнеру та розгортання скрипту для доступу до веб-інтерфейса VPN-сервера

Лістинг 5.3 – Перехід до ізольованого контейнера із запуском скрипта доступу до веб-інтерфейса VPN–сервера

```
# pct start 123
# pct enter 123
# apt update && apt -y install openvpn-as
```

Крок 4. Доступ до веб-інтерфейсу OpenVPN GUI адміністратора. Після виконання скрипта надається логін та пароль для адміністратора VPN–сервера за відповідним посиланням https://openvpnas:943/admin, де вказується порт підключення 943, який може бути змінений на обраний порт за потреби адміністратора при подальшому налаштуванні VPN-сервера.

Сервер було налаштовано з IP-адресою 192.168.0.25/24. За виконаними налаштуваннями конфігурації сервера, який обслуговує мережу

172.27.224.0/24, клієнту, що працює під операційною системою Windows, надається динамічна IP-адреса 172.27.224.3/24. Для реалізації з’єднання обрано протокол TCP, з перенаправленням на порт 5055 та використанням алгоритму шифрування AES-128-CBC. Такі налаштування забезпечують ізоляцію трафіка від основної фізичної мережі та знижують ризик несанкціонованого доступу до веб-інтерфейсу адміністратора та VPN-сервера. Конфігураційний файл містить основні параметри налаштування:

Лістинг 5.4 – Зміст конфігураційного файлу клієнта VPN-сервера

```
OVPN_ACCESS_SERVER_USERNAME=user
# OVPN_ACCESS_SERVER_PROFILE=user@192.168.0.25
# Default Cipher
cipher AES-256-CBC
client
server-poll-timeout 4
nobind
remote 192.168.0.25 1194 udp
remote 192.168.0.25 443 tcp
dev tun
dev-type tun
remote-cert-tls server
tls-version-min 1.2
tun-mtu 1420
auth-user-pass
verb 3
<ca>
# 2048 bit OpenVPN static key (Server Agent)
</tls-crypt>
## DIGEST:sha256
```

В процесі налаштування статичної маршрутизації було додано правила для міжмережного екрану для дозволу передачі TCP-трафіку через обраний порт, а також додані правила для NAT.

Після налаштування VPN-з'єднання було здійснено детальний аналіз роботи даної мережної моделі за допомогою програмного засобу Wireshark. Основну увагу в моделюванні приділено аналізу ключових параметрів. Загальний час спостереження склав 13,66 хв. На рисунку 5.2 наведено вміст потоку TCP-пакетів, який показує спотворення вмісту пакетів через шифрування, що підтверджує передачу даних через налаштоване VPN-з'єднання.

Рисунок 5.2 – Візуалізація шифрованого потоку TCP-пакетів VPN-тунелю в Wireshark

За результатами досліджень було отримано наступні дані ключових параметрів аналізу, які наведено в таблиці 5.1.

Таблиця 5.1 – Результати досліджень моделі статичної маршрутизації

Параметр	**Значення**
Пропускна здатність, Гбіт/с	0,0903
Швидкість передачі UDP, Гбіт/с	0,0025
Швидкість передачі TCP, Гбіт/с	0,0878
Затримка UDP, мс	0,0200
Затримка TCP, мс	0,0135
Загальний обсяг даних, Мб	120,506
Частка UDP у трафіку, %	43,29
Частка TCP у трафіку, %	56,71

Таким чином, при моделюванні статичної маршрутизації було виконано передачу еластичних даних у вигляді медіаконтенту та передачу нееластичних даних, зокрема відеоконтенту в режимі реального часу. Отримані результати підтверджують задовільну пропускну здатність при передачі трафіку різної пропускної здатності, забезпечення надійної та стабільної передачі даних обраним методом маршрутизації. В порівнянні зі швидкістю передачі даних у відкритій мережі зниження швидкості передачі обумовлено процесами шифрування та дешифрування даних, які спричиняють підвищення затримок. Висока частка UDP-пакетів потоку переданих пакетів підтверджує передачу нееластичних даних статичним методом маршрутизації.

5.2 Моделювання динамічного методу маршрутизації

Для моделювання динамічної маршрутизації проведено дослідження процесу передачі даних у мережі TOR. Для цього на віртуальній машині з операційною системою Windows 10 та IP-адресою 192.168.0.33/24 було встановлено TOR Browser, який забезпечує доступ до мережі TOR. Клієнтом для цього з’єднання виступає віртуальна машина з операційною системою Windows 10. Після підключення сервером було отримано вихідну IP-адресу 162.247.72.192 в мережі TOR (рисунок 5.3).

Після налаштування TOR-з'єднання було здійснено аналіз роботи даного методу маршрутизації за допомогою Wireshark. Загальний час спостереження склав 19,63 хв.

На рисунку 5.4 наведено вміст потоку TCP–пакетів, які було передано на клієнта через мережу TOR, який підтверджує шифрування TCP-пакетів під час передачі даних цим методом маршрутизації.

За результатами досліджень було отримано наступні дані ключових параметрів динамічної маршрутизації, які наведено в таблиці 5.2.

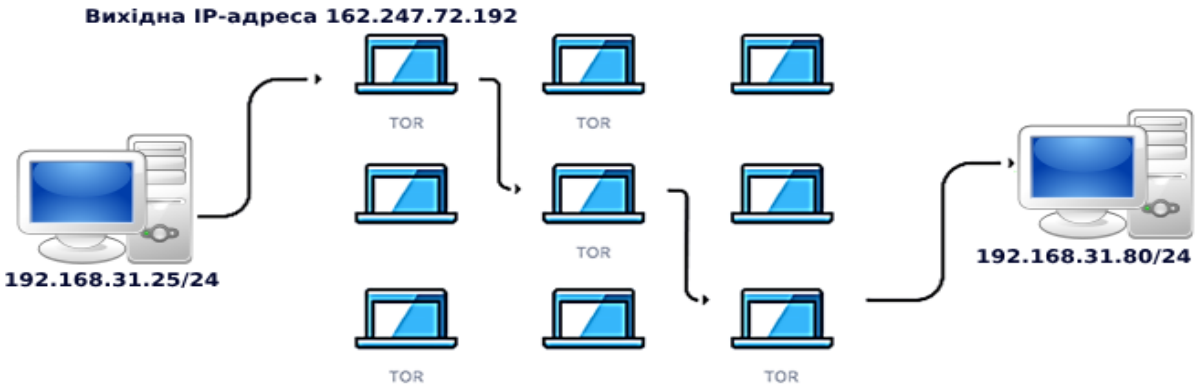


Рисунок 5.3 – Схема налаштування динамічної маршрутизації через мережу TOR

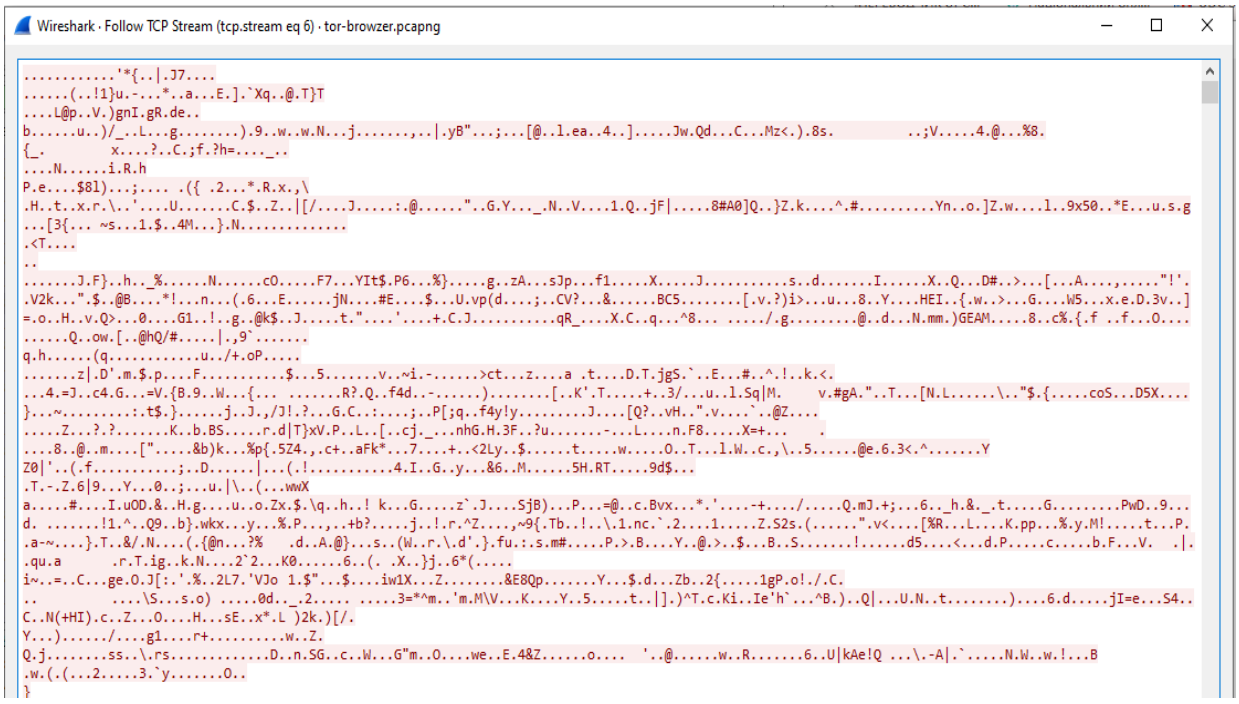


Рисунок 5.4 – Візуалізація шифрованого потоку TCP-пакетів через мережу TOR в Wireshark

За результатами аналізу параметрів трафіку методом динамічної маршрутизації в мережі TOR підтверджено, що затримка для TCP-пакетів значно збільшується через багаторівневе шифрування на кожному вузлі передачі мережею TOR. Загальний обсяг переданих даних становить 120,361 Мб, причому переданий трафік складався з даних різної пропускної здатності.

Таблиця 5.2 – Результати досліджень моделі динамічної маршрутизації

Параметр	Значення
Пропускна здатність, Гбіт/с	0,0808
Швидкість передачі UDP, Гбіт/с	0,0031
Швидкість передачі TCP, Гбіт/с	0,0778
Затримка UDP, мс	1,21
Затримка TCP, мс	3,61
Загальний обсяг даних, Мб	120,361
Частка UDP у трафіку, %	3,82
Частка TCP у трафіку, %	96,18

Отримані результати підтверджують, що основний протокол передачі, який застосовується в мережі TOR є TCP, а незначна частка UDP-пакетів вказує на використання UDP протоколу для встановлення з’єднання між вузлами анонімної мережі. Зважаючи, що для моделювання цього методу маршрутизації також був використаний поток нееластичних даних, структура та шифрування вмісту потоку переданих пакетів підтверджує інкапсуляцію даних в TCP-пакети, які використовуються для передачі в мережі TOR, що спричиняє додаткові затримки при передачі даних в режимі реального часу, та знижує ефективність анонімних мереж з високим рівнем анонімності. Маршрут, який був запропонований для виконання моделювання динамічної маршрутизації та може бути обраний користувачем за допомогою запропонованого ланцюгу проміжних вузлів, підтверджує випадковість вибору проміжних вузлів, що унеможливлює прогнозування та відстеження маршруту сторонніми спостерігачами.

5.3 Моделювання гібридного методу маршрутизації

В рамках моделювання гібридної маршрутизації виконано налаштування передачі еластичних даних в піринговій мережі Gnutella з застосуванням протоколу BitTorrent. Для цієї моделі на віртуальну машину, яка використана в якості сервера, встановлено операційну систему Ubuntu 20.04. Надалі на сервері було налаштовано VPN-сервер з основним протоколом TCP, який забезпечує передачу даних в одноранговій мережі. Конфігурацію сервера було виконано з використанням скрипта, який містить основні налаштування серверної частини, автоматичне створення сертифікатів клієнта та сервера, сесійних ключів та правил маршрутизації трафіку (рисунок 5.5).

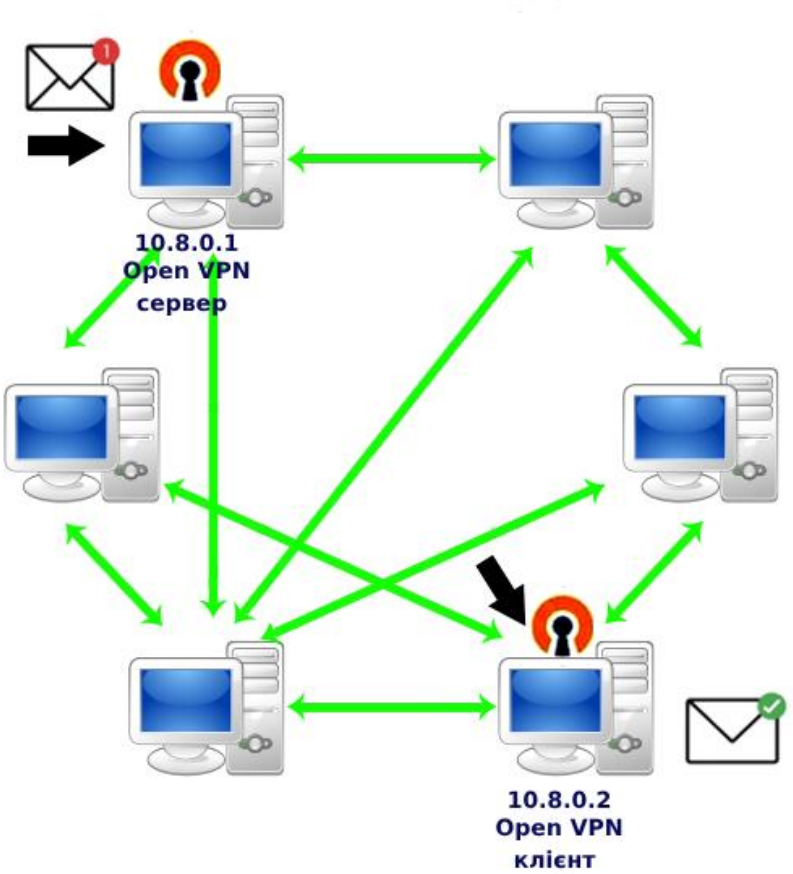


Рисунок 5.5 – Схема налаштування гібридної маршрутихації з використанням OpenVPN та Gnutella

Для підключення до мережі Gnutella було інстальовано програмне забезпечення FrostWire, яке забезпечує обмін файлами в межах цієї мережі. Надалі було виконано передачу еластичних даних через встановлене VPN-з'єднання та мережу Gnutella. Додатково було налаштовано маршрутизацію для фільтрації трафіку та роботи програмного забезпечення FrostWire, додано правила NAT (рисунок 5.6).

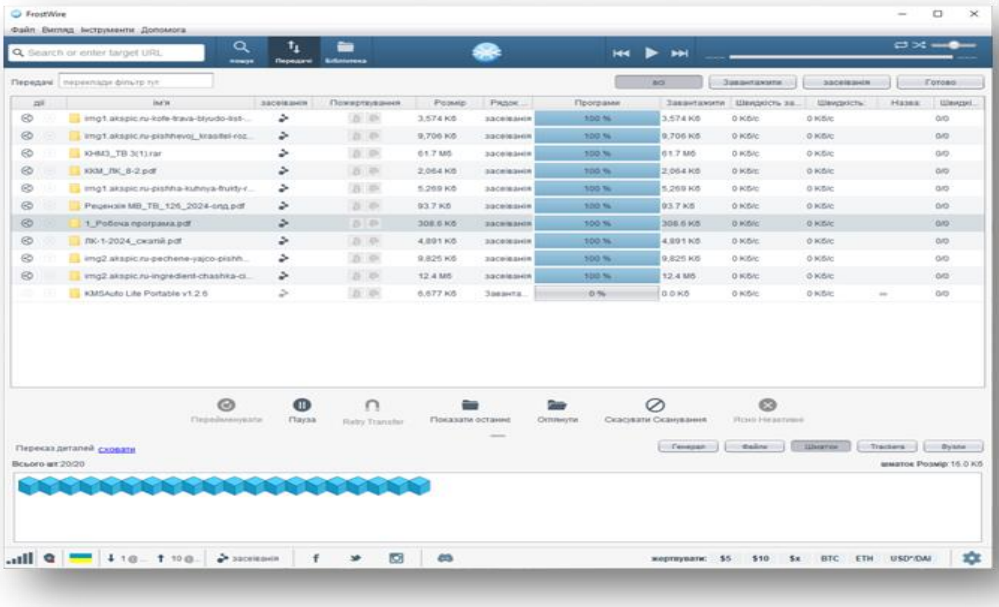


Рисунок 5.6 – Інтерфейс програмного забезпечення FrostWire для передачі файлів в Gnutella

Під час здійснення передачі даних мережею Gnutella було виконане аналіз вмісту TCP-пакетів даних та переданого трафіку за допомогою Wireshark. Загальний час спостереження склав 23,31 хв.

На рисунку 5.7 наведено вміст потоку TCP–пакетів, які було передано на клієнта через мережу Gnutella, який підтверджує передачу еластичних даних за допомогою протоколу Bittorrent.

За результатами досліджень було отримано наступні значення параметрів для клієнта та сервера при передачі даних через Gnutella, які наведено в таблиці 5.3.

Таблиця 5.3 – Результати досліджень моделі гібридної маршрутизації

Параметр	Значення	
	10.8.0.1	10.8.0.2
Пропускна здатність, Гбіт/с	0,000738	0,000738
Швидкість передачі UDP, Гбіт/с	0,000003	0,000032
Швидкість передачі TCP, Гбіт/с	0,000354	0,000242
Затримка UDP, мс	0,0001	0,0049
Затримка TCP, мс	0,0477	0,0647
Загальний обсяг даних, Мб	123	123
Частка UDP у трафіку, %	0,17	6,97
Частка TCP у трафіку, %	99,83	92,92

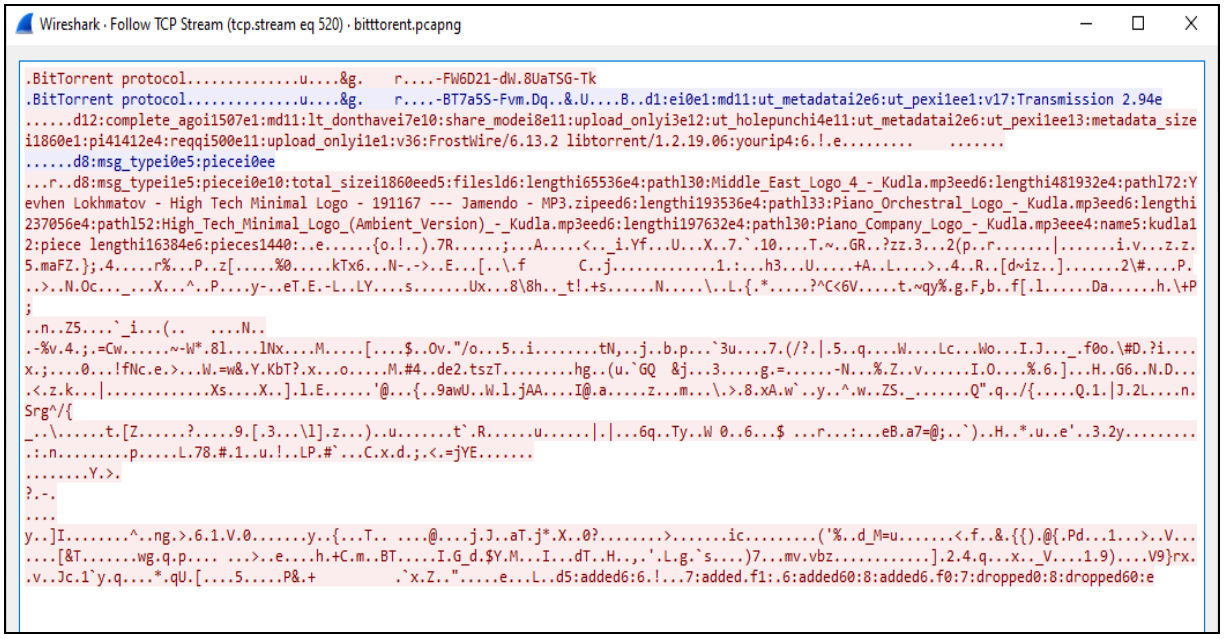


Рисунок 5.7 – Візуалізація шифрованого потоку TCP–пакетів через мережу Gnutella в Wireshark

За отриманими результатами моделювання гібридного методу маршрутизації вміст TCP-пакетів показує використання протоколу BitTorrent, що підтверджує передачі даних через мережу Gnutella, а також розбиття даних на фрагменти при передачі в цій мережі. Незначна частка UDP-пакетів, в порівнянні з часткою TCP-пакетів, вказує на використання даного протоколу для пошуку вузлів мережі Gnutella, які містять запитувані файли. Тобто протокол UDP використовується для передачі службового трафіку та пошук пірів через DHT. Основна частка TCP-пакетів забезпечує ефективну передачу файлів з гарантованою доставкою, причому збільшена затримка на клієнті виникає через пошук та побудову маршруту запитуваних файлів, який відбувається на початку сеансу передачі даних. Також процеси шифрування–дешифрування додають свій внесок в збільшення затримки на стороні клієнта.

ВИСНОВКИ

В кваліфікаційній роботі здійснено аналіз сучасних методів маршрутизації в анонімних оверлейних мережах, зокрема статичних, динамічних та гібридних методів. Основна увага приділена таким оверлейним мережам, як Tor та Gnutella, а також використанню технології VPN.

Проведено дослідження параметрів передачі даних в рамках кожного методу маршрутизації при передачі даних різної пропускної здатності в умовах підвищеного рівня безпеки та цілісності даних.

Вибір алгоритму маршрутизації в умовах забезпечення високого рівня безпеки передачі та цілісності даних базується на забезпеченні задовільного рівня продуктивності, масштабованості та відмовостійкості корпоративної комп'ютерної мережі з урахуванням збільшення обсягів даних, пропускної здатності та характеристик трафіку, який передається корпоративною комп'ютерною мережею.

В кваліфікаційній роботі було розроблено метод багаторівневого VPN-тунелювання для забезпечення безпечного віддаленого доступу до вузлів екстранет–мережі, який дозволяє створити багаторівневу структуру для забезпечення захисту корпоративної комп'ютерної мережі. Метод дозволяє адаптивно підходити до балансування між продуктивністю, ефективністю використання мережних ресурсів та кількістю рівнів тунелювання для забезпечення захисту від несанкціонованого доступу.

Аналіз ефективності методу показав, що існує лінійна залежність швидкості передачі даних від кількості рівнів тунелювання, що підтверджує необхідність оптимізації та балансування параметрів системи з урахуванням вимог до захисту та наявних ресурсів, які доступні для реалізації VPN-тунелювання. Таким чином, запропонований метод може бути застосований в корпоративних комп'ютерних мережах малого та середнього бізнесу для забезпечення надійного захисту при віддаленому доступі до робочих місць в в умовах обмеженого ресурсного забезпечення та організації безперервних бізнес-процесів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Волинець В. В. Юридичні аспекти захисту конфіденційності та безпеки даних в електронній комерції // Академічні візії.– 2024. – вип. 29. DOI: https://doi.org/10.5281/zenodo.11189625

2. Лагодієнко О. Анонімність – що ми знаємо про неї?. Next generation whistleblowing platform. URL: https://ethicontrol.com/uk/blog/ anonymity–uk (дата звернення: 02.10.2024).

3. Базові аспекти цифровізації та їх правове забезпечення : монографія. Харків : НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. 180 с. URL: https://ndipzir.org.ua/wp–content/uploads/2021/ Tsyfrovizatsiya21/ Tsyfrovizatsiya21.pdf (дата звернення: 02.10.2024).

4. «Что такое «луковая маршрутизация»? – Ценные бумаги.io.» Securities.io, 18 January 2023, https://www.securities.io/ru/what–is–onion–routing/. Accessed 25 July 2024.

5. Пат. UA123445 (C2) Україна, МПК H04L47/43. Secure Dynamic Communication Network And Protocol / Williams Richard K, Verzun Ievgen, Oleksandr Golub – № a 2018 07936 ; заявл. 10.01.2019 ; опубл. 07.04.2021, Бюл. № 14. – 315 с.

6. Vitalii, Tkachov, et al. «Method of building dynamic multi–hop VPN chains for ensuring security of terminal access systems.» 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). IEEE, 2020.

7. Бурячок В. Л. Технології забезпечення безпеки мережної інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

8. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д–р права,

проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с.

9. Риндич, Є. Дослідження технологій тунелювання в сучасних комп’ютерних мережах / Є. Риндич, А. Боровик, О. Боровик О. // Технічні науки та технології. – 2021. – № 4 (26). – С. 67–74.

10. Gentile, A.F.; Macrì, D.; Greco, E.; Fazio, P. Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment. Future Internet 2024, 16, 283. https://doi.org/10.3390/fi16080283

11. Гавриш, Б. М., et al. «Технології анонімних мереж.» (2022).

12. Yevhen, Zhyvylo ІСНУЮЧІ ВРАЗЛИВОСТІ TOR–МЕРЕЖ / Yevhen, Zhyvylo, Simonkin, Andrii // Theoretical and Applied Cybersecurity. Матеріали другої всеукраїнської науково–практичної конференції (TACS–2024). – Київ: Інжиніринг. –2024. – стр. 62–66.

13. Кренцін М. Д., Куперштейн Л. М. Аналіз тенденцій розвитку пірингових мереж. Вісник Хмельницького національного університету. Технічні науки. 2021. Т. 4, № 299. С. 25–29

14. Куперштейн Л. М. Аналіз протоколів пірингових мереж / Л. М. Куперштейн, М. Д. Кренцін // Матеріали LI Науково–технічної конференції підрозділів ВНТУ, Вінниця, 30–31 травня 2022 р. – https://conferences.vntu.edu.ua/index.php/all–fitki/all–fitki–2022/paper/view/16141/13544

15. Куперштейн, Л., М. Кренцін, А. Дудатьєв, і В. Каплун. «Аналіз проблем безпеки пірингових мереж». Інформаційні технології та комп’ютерна інженерія, вип. 54, вип. 2, Червень 2022, с. 5–14, doi:10.31649/1999–9941–2022–54–2–5–14.

16. Гунько, М. А. «Метод організації туманних обчислень у динамічній обчислювальній оверлейній мережі на базі полінгових мереж.» (2024).

17. Simon, M., & Huraj, L. (2023, April). VirtualBox and Proxmox VE in Network Management: A User-Centered Comparison for University

Environments. In Computer Science On-line Conference (pp. 486-495). Cham: Springer International Publishing.

18. Kaur, K., Mangat, V., & Kumar, K. (2022). A review on Virtualized Infrastructure Managers with management and orchestration features in NFV architecture. Computer Networks, 217, 109281.

19. Чалий Д. В. Дослідження інструментів безпеки мережної інфраструктури / Д. В. Чалий ; наук. керівник ст. вик., к.т.н. М. М. Калюжний // Радіоелектроніка та молодь у XXI столітті : матеріали 28–го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. – Харків : ХНУРЕ, 2024. – Т. 4. – С. 172–173. – DOI: https://doi.org/10.30837/IYF.PDICIMT.2024.172.

20. Ruonan Wang and Yuefeng Zhao. 2022. A Survey on Anonymous Communication Systems Traffic Identification and Classification. In Proceedings of the 3rd International Conference on Advanced Information Science and System (AISS '21). Association for Computing Machinery, New York, NY, USA, Article 36, 1–5. https://doi.org/10.1145/3503047.3503087

21. V. Tkachov, Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems / V. Tkachov, B. Anna, H. Kateryna and D. Hrebeniuk // 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine.– 2020.– pp. 613–618. doi: 10.1109/PICST51311.2020.9467953.

22. Oldenburg, L., Juarez, M., Rúa, E. A., & Diaz, C. (2024). MixMatch: Flow Matching for Mixnet Traffic. Proceedings on Privacy Enhancing Technologies.

23. J. Saleem, R. Islam and M. A. Kabir, «The Anonymity of the Dark Web: A Survey,» in IEEE Access, vol. 10, pp. 33628–33660, 2022, doi: 10.1109/ACCESS.2022.3161547.

24. Sampaio, S.; Sousa, P.R.; Martins, C.; Ferreira, A.; Antunes, L.; Cruz–Correia, R. Collecting, Processing and Secondary Using Personal and (Pseudo)Anonymized Data in Smart Cities. Appl. Sci. 2023, 13, 3830. https://doi.org/10.3390/app13063830

25. Мережева модель OSI для чайників. [Електронний ресурс] / | KR. Laboratories. KR. Laboratories. – 2024. – Режим доступу до ресурсу: https://kr–labs.com.ua/blog/model–osi/ (дата звернення: 05.10.2024).

26. Кулаков Ю. О. Комп’ютерні мережі. – 2022.

27. Коваль Ю. В. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. – Київ, 2021. – 84 с.

28. Muhammad, T. (2021). Overlay Network Technologies in SDN: Evaluating Performance and Scalability of VXLAN and GENEVE. International Journal Of Computer Science And Technology, 5(1), 39-75.

29. K. Zhongmiao, D. Jinwan, Z. Yufan, C. Feipeng, W. Zhenzhong and C. Cheng, «Study on Key Technologies of Distribution Communication Network Virtualization Based on Overlay Network,» 2021 Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS), Shenyang, China, 2021, pp. 290-294, doi: 10.1109/ACCTCS52002.2021.00064.

30. Oktian, Y. E., Witanto, E. N., & Lee, S.-G. (2021). A Conceptual Architecture in Decentralizing Computing, Storage, and Networking Aspect of IoT Infrastructure. IoT, 2(2), 205-221. https://doi.org/10.3390/iot2020011

31. Tkachov, V., Kovalenko, A., Kharchenko, V., Hvozdetska, K., Hunko, M. (2022). An Overlay Network Based on Cellular Technologies for the Secure Control of Intelligent Mobile Objects. In: Ignatenko, O., et al. ICTERI 2021 Workshops. ICTERI 2021. Communications in Computer and Information Science, vol 1635. Springer, Cham. https://doi.org/10.1007/978-3-031-14841-5_32

32. Kathiravelu, P., Zaiman, Z., Gichoya, J., Veiga, L., & Banerjee, I. (2022). Towards an internet-scale overlay network for latency-aware decentralized workflows at the edge. Computer networks, 203, 108654.

33. Lei, J., Munikar, M., Suo, K., Lu, H., & Rao, J. (2021). Parallelizing packet processing in container overlay networks. EuroSys 2021.

34. D. Tipper, A. Babay, B. Palanisamy and P. Krishnamurthy, «Network Connectivity Resilience in Next Generation Backhaul Networks: Challenges and Future Opportunities,» in IEEE Transactions on Network and Service

Management, vol. 21, no. 5, pp. 5321-5334, Oct. 2024, doi: 10.1109/TNSM.2024.3392857.

35. Achary, R. (2021). Service Resiliency in Cloud and Network Function Virtualization. In Cloud Reliability Engineering (pp. 117-158). CRC Press.

36. Shahrokhkhani, V. (2021). An Analysis on Network Virtualization Protocols and Technologies.

37. Munawar, Sofia. 2024. «Peer to Peer Overlay Network in IoT: An Overview.»

38. Kaur, Karamjeet, Veenu Mangat, and Krishan Kumar. «A review on Virtualized Infrastructure Managers with management and orchestration features in NFV architecture.» Computer Networks 217 (2022): 109281.

39. Patel, Nimeshkumar. «SECURE ACCESS SERVICE EDGE (SASE):–EVALUATING THE IMPACT OF CONVEREGED NETWORK SECURITY ARCHITECTURES IN CLOUD COMPUTING.» Journal of Emerging Technologies and Innovative Research. https://www. jetir. org/papers/JETIR2403481. pdf (2024).

40. Haruna, Yusuf & Ahmad, Abdulmalik & Yarima, Muhammad & Ahmad, Mustapha & Sani, & Ahmad, Mustapha & Abdulkadir, Sani & Yarima, Kamaluddeen Ibrahim. (2022). Analysis of Docker Networking and Optimizing the Overhead of Docker Overlay Networks Using OS Kernel Support. Advances in Networks. Volume 10. 15-30. 10.11648/j.net.20221002.11.

41. Програмні технології в інфокомунікаційних системах. Навчальний посібник для студентів спеціальності 172 «Телекомунікації та радіотехніка» : електронний навчальний посібник комбінованого (локального та мережного) використання [Електронний ресурс] / Васильківський М. В., Бортник Г. Г., Кичак В. М. – Вінниця : ВНТУ, 2023. – 141 с

42. GeeksforGeeks. Difference between Static and Dynamic Routing. [Електронний ресурс] / GeeksforGeeks. GeeksforGeeks. – 2024. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/difference–between–static–and–dynamic–routing/ (Дата звернення 05.10.2024).

43. What is Routing table – Cybersecurity Terms and Definitions. [Електронний ресурс] / VPN Unlimited – Fast & Secure VPN service. – 2024. – Режим доступу до ресурсу: https://www.vpnunlimited.com/help/cybersecurity/routing–table?_gl=1*1hs4uhw*_up*MQ..*_ga*MTU4NDI3NjA3NS4xNzI4MTUwMTc2*_ga_DE85JZ9NSX*MTcyODE1MDE3NS4xLjAuMTcyODE1MDE3NS4wLjAuMA.. (Дата звернення 05.10.2024).

44. Bentaleb, O., Belloum, A. S., Sebaa, A., & El-Maouhab, A. (2022). Containerization technologies: Taxonomies, applications and challenges. The Journal of Supercomputing, 78(1), 1144-1181.

45. Принцип роботи VPN-протоколу IKEv2: Детальний огляд - Блог - HostZealot. HostZealot. URL: https://www.hostzealot.com.ua/blog/about-solutions/princip-roboti-vpn-protokolu-ikev2-detalnii-oglyad (дата звернення: 18.11.2024).

46. Что такое сертификат SSL? – Описание сертификатов SSL/TLS – AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/ru/what-is/ssl-certificate/ (дата звернення: 18.11.2024).

47. Найкращі протоколи VPN та відмінності між типами VPN. NordVPN. URL: https://nordvpn.com/uk/blog/protokoly/ (дата звернення: 18.11.2024).

48. Uriawan, W., Ramadita, R., Putra, R. D., Siregar, R. I., & Addiva, R. (2024). Authenticate and Verification Source Files using SHA256 and HMAC Algorithms.

49. Сизов А. Гіпервізор Proxmox VE і його можливості?. SERVER SOLUTIONS. URL: https://serversolutions.com.ua/blogs/news/гіпервізор-proxmox-ve-і-його-можливості?srsltid=AfmBOorTviVQAWbXMa9cImEwmKS4NCjS6JRc1c0DkYkKU2cLwwuTZyEB (дата звернення: 18.01.2025).

50. Šimon, M., Huraj, L., & Búčik, N. (2023). A Comparative Analysis of High Availability for Linux Container Infrastructures. Future Internet, 15(8), 253.

51. RIP Version 2. [Електронний ресурс] / IETF | Internet Engineering Task Force. Version 15. – 2024. – Режим доступу до ресурсу: https://www.ietf.org/rfc/rfc2453.txt (Дата звернення 06.11.2024).

52. Computer simulation model of a computer network with fractal traffic for testing routing algorithms / H. Drieieva, Y. Meleshko, O. Drieiev, V. Mikhav // Сучасні інформаційні системи = Advanced Information Systems. – 2022. – Т. 6, № 4. – С. 11–18.

53. Азаров О.Д. Комп'ютерні мережі: підручник / Азаров О.Д., Захарченко С.М., Кадук О.В., Орлова М.М., Тарасенко В.П. – Вінниця: ВНТУ. – 2020. – 378 с.

54. Al Ajrawi, S., & Tran, B. (2024). Mobile wireless ad–hoc network routing protocols comparison for real–time military application. Spatial Information Research, 32(1), 119–129.

55. Ahmed Abdallah Abaker, Mustafa ElGili Mustafa. The Impact of Network Topologies on OSPF Networks and Router's CPU Utilization. [Електронний ресурс] / International Journal of Computer Networks (IJCN). 2024. Vol. 11, Issue 1. P. 1–10. Режим доступу до ресурсу: https://www.cscjournals.org/manuscript/Journals/IJCN/Volume11/Issue1/IJCN–342.pdf.

56. AIX 7.2. [Електронний ресурс] / IBM – United States. – 2024. – Режим доступу до ресурсу: https://www.ibm.com/docs/ru/aix/7.2?topic=routing–static–dynamic (Дата звернення 08.11.2024).

57. ПРО TOR BROWSER. Tor Browser. Tor Browser User Manual. [Електронний ресурс] / | Tor Project | Tor Browser Manual. – 2024. – Режим доступу до ресурсу: https://tb–manual.torproject.org/uk/about/ (Дата звернення 08.11.2024).

58. Tell me about all the keys Tor uses | Tor Project | Support. How can we help? | Tor Project | Support. URL: https://support.torproject.org/about/key–management/ (date of access: 30.10.2024).

59. Havrysh, B.M. et al. (2022) ‘Technology of Anonymous Networks’, Scientific Papers (Ukrainian Academy of Printing), 2(65), pp. 42–56. doi:10.32403/1998–6912–2022–2–65–42–56.

60. V. Marbukh, «On Potential Risks of “Natural” Hybrid Load Balancing in Large–Scale Clouds: Work in Progress,» 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2023, pp. 979–980, doi: 10.1109/CCNC51644.2023.10060156.

61. Sha, Z., Huo, R., Sun, C., Wang, S., & Huang, T. (2023). A task–oriented hybrid routing approach based on deep deterministic policy gradient. Computer Communications, 210, 183–193.

62. Khan, H., Kushwah, K. K., Thakur, J. S., Soni, G. G., & Tripathi, A. (2024). Improving Mobile Ad hoc Networks through an investigation of AODV, DSR, and MP–OLSR Routing Protocols. EAI Endorsed Transactions on Scalable Information Systems.

63. Kambhampati, R. T. (2024). Routing And Switching: Foundations Of Modern Network Design And Implementation. International Journal Of Computer Engineering And Technology (IJCET), 15(4), 610–621.

64. Що таке однорангова мережа (P2P), і як вона пов'язана з блокчейном та криптовалютами? [Електронний ресурс] / BROKKER.NEWS. – 2024. – Режим доступу до ресурсу: https://brokker.news/p2p–114 (дата звернення: 08.11.2024).

65. C. Vaidya, K. Takalkar, A. Ghosekar, S. Nimgade і V. Ghode, «Decentralized File Sharing», 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) , Bhopal, India, 2023, pp 1–6, doi: 10.1109/SCEECS57921.2023.10062977.

66. Arti Bandhana, Tomá Kroupa, and Sebastián García. 2024. Trust in Shapley: A Cooperative Quest for Global Trust in P2P Network. In Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS '24). International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 132–140.

67. Mikhav, Volodymyr & Meleshko, Yelyzaveta. (2023). Метод роботи рекомендаційної системи у комп’ютерній мережі типу peer to peer. Системи управління, навігації та зв’язку. Збірник наукових праць. 1. 112–117. 10.26906/SUNZ.2023.1.112.

68. Regarding gnutella – GNU Project – Free Software Foundation [Електронний ресурс] / [A GNU head] – 2024. – Режим доступу до ресурсу: https://www.gnu.org/philosophy/gnutella.html.en (Дата звернення 08.11.2024).

69. Peer–to–peer computing and Networking. [Електронний ресурс] / Claudia Müller-Birn, Barry Linnert. – 2023. – Режим доступу до ресурсу: https://www.inf.fu–berlin.de/inst/ag–se/teaching/V–NSEQ–2023/20_Peer2Peer.pdf (Дата звернення 08.11.2024)

70. X. Zhang and T. Wang, «Elastic and Reliable Bandwidth Reservation Based on Distributed Traffic Monitoring and Control,» in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 12, pp. 4563–4580, 1 Dec. 2022, doi: 10.1109/TPDS.2022.3196840.

71. M. A. Makarem, A. Q. Algaolahi, A. A. Alhajri and M. A. Razaz, «Enhancing load balancing & Fault Tolerance in Real–Time Applications Using SD–WAN,» 2024 4th International Conference on Emerging Smart Technologies and Applications (eSmarTA), Sana'a, Yemen, 2024, pp. 1–6, doi: 10.1109/eSmarTA62850.2024.10638874.

72. Andrew S. Tanenbaum, David J. Wetherall, Computer Networks (6th Edition), Prentice Hall, ISBN 978–0132126953

73. Ni, Z.; You, J.; Li, Y. An ICN–Based On–Path Computing Resource Scheduling Architecture with User Preference Awareness for Computing Network. Electronics 2024, 13, 933. https://doi.org/10.3390/electronics13050933

74. SCHOOL T. A complete overview of SSL/TLS and its cryptographic system. DEV Community. URL: https://dev.to/techschoolguru/a-complete-overview-of-ssl-tls-and-its-cryptographic-system-36pd (date of access: 18.11.2024).

75. Barstad, H. (2021). Deanonymizing communications on the Onion Router (TOR) network with Deep Learning (Master's thesis, The University of Bergen).

76. . R. Jansen and A. Johnson, ‘On the accuracy of tor bandwidth estimation,’ in International Conference on Passive and Active Network Measurement, Springer, 2021, pp. 481–498.

77. The Gnutella Protocol Specification v0.4. [Електронний ресурс] / courses.cs.washington.edu. – 2024. Режим доступу до ресурсу: https://courses.cs.washington.edu/courses/cse522/05au/gnutella_protocol_0.4.pdf (Дата звернення 18.11.2024).

78. BitTorrent.org. [Електронний ресурс] / BitTorrent.org. – 2024. – Режим доступу до ресурсу: https://www.bittorrent.org/index.html (Дата звернення 18.11.2024).

79. Anandaraj, M., et al. «A novel fuzzy programming approach for piece selection problem in P2P content distribution network.» PeerJ Computer Science 10 (2024): e1645.

80. Karras, A., Karras, C., Schizas, N., Sioutas, S., & Zaroliagis, C. (2023, September). Algorithmic Aspects of Distributed Hash Tables on Cloud, Fog, and Edge Computing Applications: A Survey. In International Symposium on Algorithmic Aspects of Cloud Computing (pp. 133–171). Cham: Springer Nature Switzerland.

81. Что такое шифрование AES-256 и как оно работает?. Website Rating. URL: https://www.websiterating.com/ru/blog/cloud-storage/what-is-aes-256-encryption/ (дата звернення: 18.11.2024).

82. Jayaram, K. R., Muthusamy, V., Thomas, G., Verma, A., & Purcell, M. (2022, December). Adaptive aggregation for federated learning. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 180-185). IEEE.

83. Element – an app for productivity. [Електронний ресурс] / Element | Secure collaboration and messaging. – 2024. – Режим доступу до ресурсу: https://element.io/app–for–productivity (Дата звернення 18.11.2024)

84. Верховський І., Ткачов В. Методи побудови віртуальних тунелів extranet–систем. Scientific review. 2023. Т. 4, № 89. С. 22. URL: https://doi.org/10.26886/2311–4517.4(89)2023.2.

85. Abbas, H., et al. (2023). Security Assessment and Evaluation of VPNs: A Comprehensive Survey. ACM Computing Surveys. https://doi.org/10.1145/3579162.

86. Moltafet M., Leinonen M., Codreanu M. Average Age of Information for a Multi-Source M/M/1 Queueing Model With Packet Management. 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 21–26 June 2020. 2020. URL: https://doi.org/10.1109/isit44484.2020.9174099.

87. Chepurna, I. S. (2024). Alhorytm orhanizatsii viddalenoho dostupu do zakhyshchenoho segmentu korporatyvnykh komputerovykh merezh [Algorithm for organizing remote access to the protected segment of corporate computer networks]. In Radioelektronika ta molod u XXI stolitti: Materialy 28-ho Mizhnarodnogo molodizhnoho forumu (Vol. 5, pp. 76–78). Kharkiv, Ukraine: KhNURE. https://doi.org/10.30837/IYF.PCEIP.2024.076.

88. Чепурна, І. С., and І. С. Заброда. "Аналіз алгоритмів маршрутизації в анонимних оверлейних мережах." (2024)

89. Tkachov V. The promising method of secure transmission of inelastic data in peer-to-peer networks / V. Tkachov, I. Chepurna, D. Frolov // Computer and information systems and technologies : Proceedings of Seventh International Scientific and Technical Conference, September 26-27, 2024. – Kharkiv : NURE, 2024. − P. 15−16.

90. ТКАЧОВ, ВМ, ІС ЧЕПУРНА, and ТГ ФЕСЕНКО. «МЕТОД МУЛЬТИРІВНЕВОГО VPN-ТУНЕЛЮВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІДДАЛЕНОГО ДОСТУПУ ДО ВУЗЛІВ ЕКСТРАНЕТ-МЕРЕЖІ» *Вісник Херсонського національного технічного університету* 3 (90) (2024): 299-308.