Запорізький інститут економіки та
інформаційних технологій

Магістерська дипломна робота

Порівняльний аналіз протоколів віртуальних приватних мереж

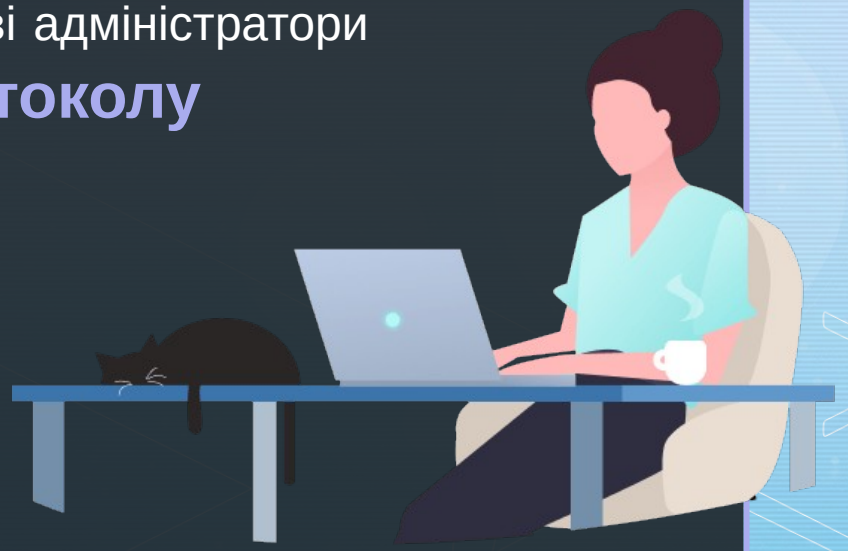
Виконав: студент групи КІ-111М, М.О. Капустін
Керівник: д.е.н., доц., Н.Р. Полуектова

Актуальність роботи

Щороку кількість віддалених працівників у всьому світі стрімко зростає. Згідно з дослідженням Flexjobs та Global Workplace Analytics за останні 12 років віддалена робоча сила зросла на **159%**

Більшість підприємств використовують VPN для забезпечення віддаленого доступу до своїх корпоративних мереж. Водночас мережеві адміністратори стикаються з проблемою **вибору протоколу**

Віддалені працівники у наш час можуть працювати з будь-якої точки світу, де є можливість підключення до мережі Інтернет. Це призводить до того, що віддалений доступ часто забезпечується в умовах **ненадійного мережевого з’єднання**



Об’єкт і предмет дослідження

VPN

Віртуальна приватна мережа (Virtual Private Network, VPN) – це спосіб розширення приватної мережі через загальнодоступну мережу, таку як Інтернет

ОБ’ЄКТ

Об’єктом дослідження є протоколи VPN. Протокол VPN – набір інструкцій, що визначає, як ваші дані будуть зашифровані та передані між вашим пристроєм і VPN-сервером

ПРЕДМЕТ

Предметом дослідження є продуктивність рішень VPN в умовах стабільного та ненадійного мережевого з’єднання

Мета і завдання роботи

МЕТА

Метою роботи є аналіз і порівняння продуктивності сучасних рішень віртуальних приватних мереж в умовах стабільного та ненадійного мережевого з’єднання, а також розробка рекомендацій для вибору найліпшого рішення

ЗАВДАННЯ

- дослідити проблему вибору протоколу віртуальної приватної мережі
- визначити перелік протоколів для порівняльного аналізу
- визначити метрики та інструменти для вимірювання продуктивності
- провести експериментальне дослідження продуктивності
- проаналізувати результати експерименту і порівняти продуктивність різних рішень, у різних середовищах та умовах застосування
- обґрунтувати рекомендації з вибору найліпшого протоколу

Обрані протоколи

OpenVPN

IPSec

WireGuard

Для порівняльного аналізу було обрано два провідні на сьогодні протоколи VPN, OpenVPN та IPSec, а також відносно новий протокол, що нарощує популярність – WireGuard

Метрики та інструменти

ЗАЛЕЖНА ЗМІННА

Пропускна здатність – це обсяг даних, що надсилається з однієї точки в іншу протягом певного періоду часу

НЕЗАЛЕЖНІ ЗМІННІ

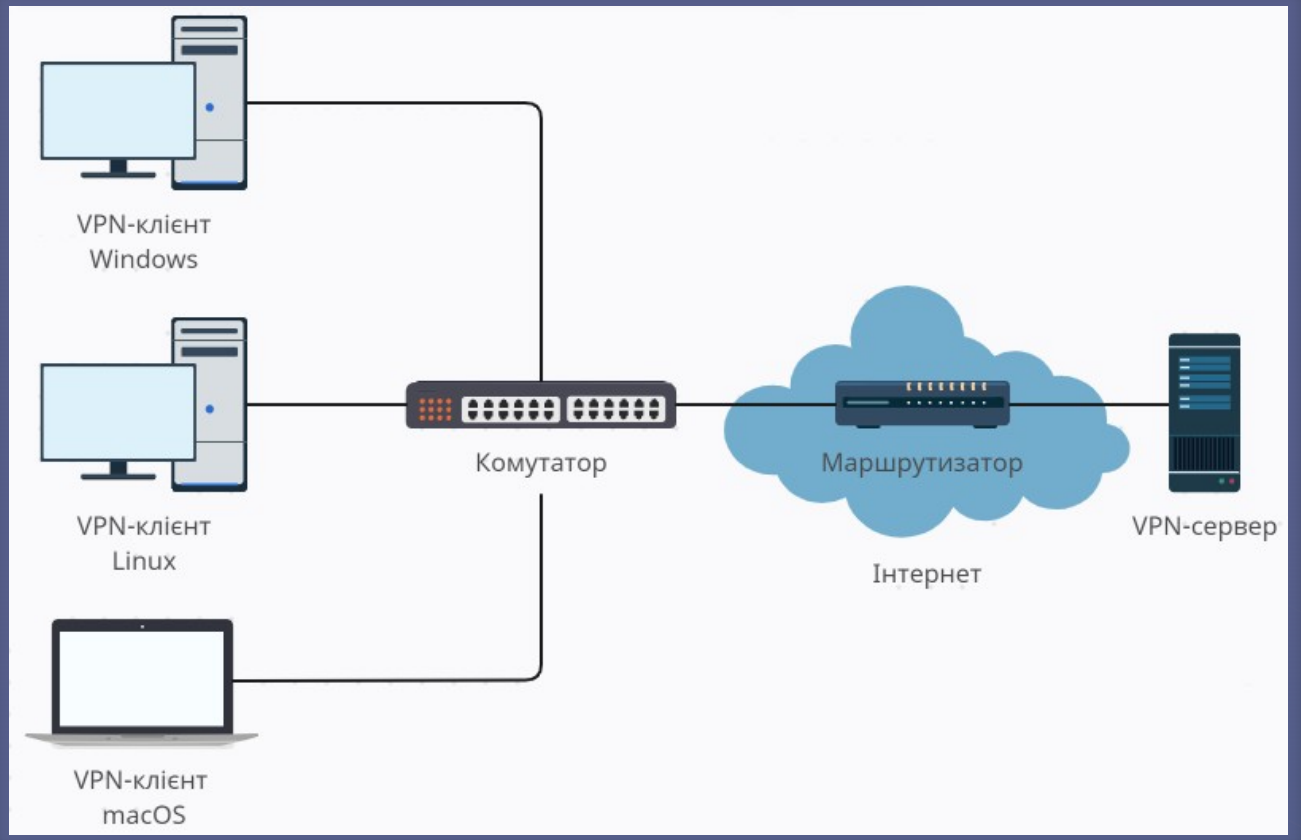
Затримка – час, необхідний для передачі пакета в одному напрямку, наприклад, від клієнта до сервера

Втрата пакетів – кількість пакетів, що не надійшли від джерела до місця призначення

ІНСТРУМЕНТ

iPerf – міжплатформний інструмент, який дозволяє виконувати стандартизовані вимірювання продуктивності для будь-якої мережі

Експериментальне дослідження



Топологія мережі в експерименті

3
рішення VPN

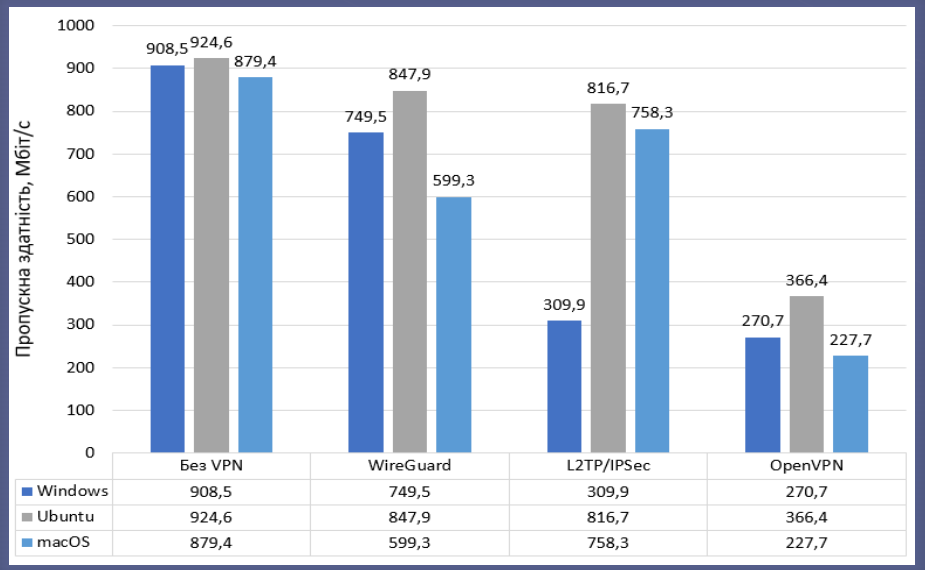
3
операційні системи

36
випадків тестування

50
тестів на випадок

Результати роботи

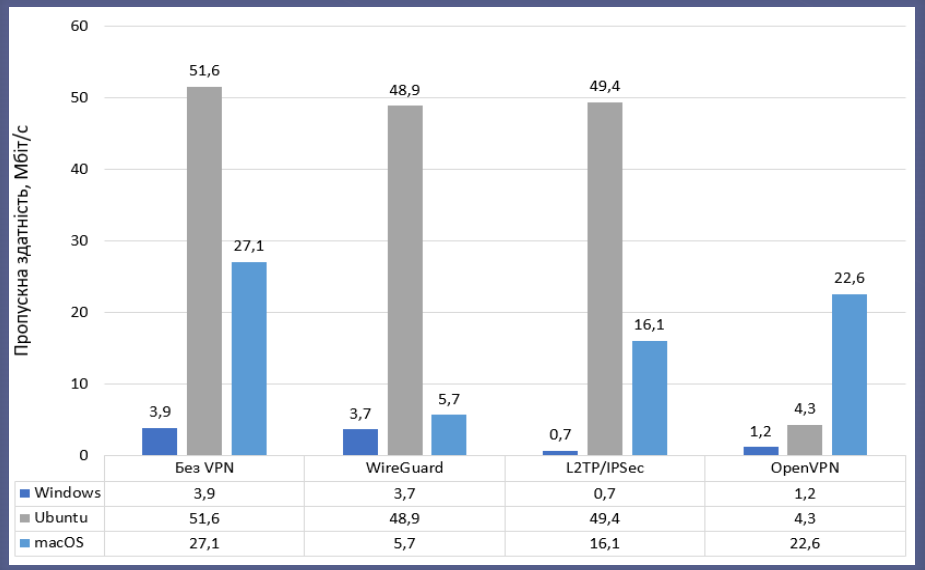
ТЕНДЕНЦІЇ В УМОВАХ СТАБІЛЬНОГО МЕРЕЖЕВОГО З’ЄДНАННЯ



- Найкращі результати в умовах стабільного мережевого з’єднання продемонстрували WireGuard та IPSec
- WireGuard став беззаперечним лідером у Windows, як в цьому тестуванні, так і в наступних
- OpenVPN виявився найменш продуктивним в усіх трьох операційних системах, подібні результати спостерігаються майже в усіх випадках тестування

Результати роботи

ТЕНДЕНЦІЇ В УМОВАХ НЕНАДІЙНОГО МЕРЕЖЕВОГО З’ЄДНАННЯ (ЗАТРИМКА)

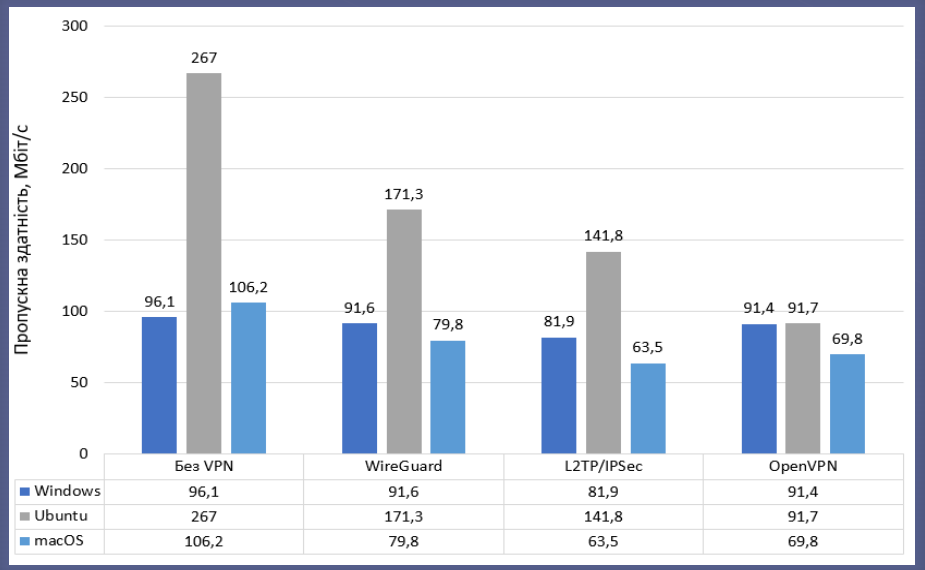


	Без VPN	WireGuard	L2TP/IPSec	OpenVPN
Windows	3,9	3,7	0,7	1,2
Ubuntu	51,6	48,9	49,4	4,3
macOS	27,1	5,7	16,1	22,6

- Додавання затримки спричинило істотне зниження продуктивності мережі в усіх трьох операційних системах, найчутливішою до затримки виявилася Windows
- В різних операційних системах перевага була за різними протоколами, тому в цьому тестуванні не було однозначного лідера
- OpenVPN мав першість у macOS, але це був єдиний випадок, коли цей протокол продемонстрував найкращі результати

Результати роботи

ТЕНДЕНЦІЇ В УМОВАХ НЕНАДІЙНОГО МЕРЕЖЕВОГО З’ЄДНАННЯ (ВТРАТА ПАКЕТІВ)

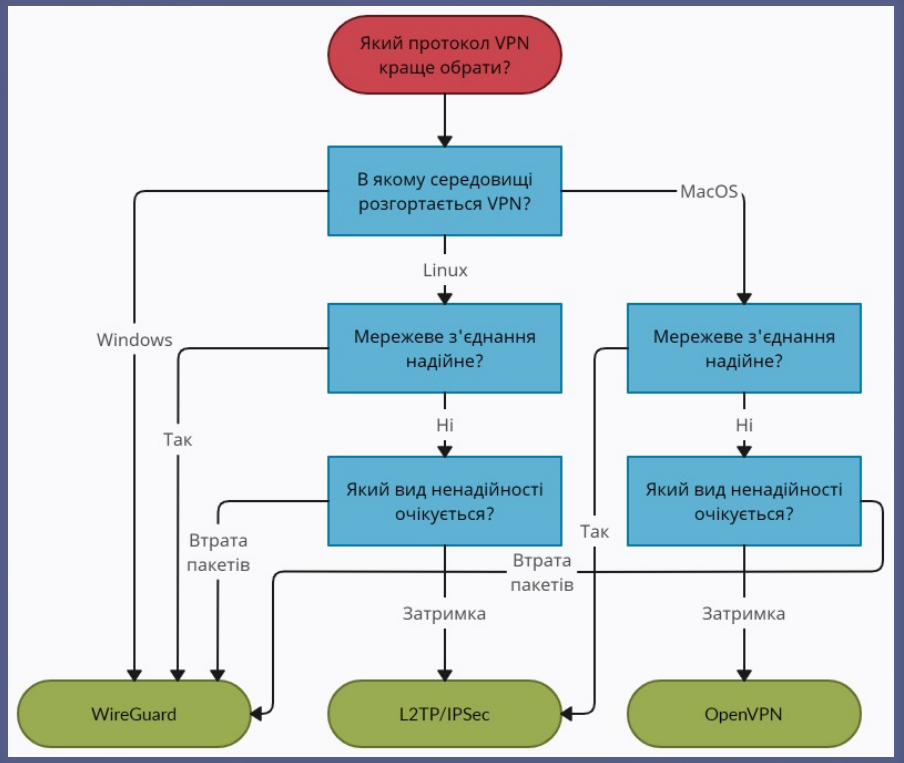


- Додавання втрати пакетів так само призвело до зниження продуктивності мережі, проте не такого значного, як у випадку із затримкою
- WireGuard найкраще впорався із втратою пакетів в усіх трьох операційних системах, як і в більшості випадків тестування
- IPSec виявився найменш продуктивним у Windows та macOS, і мав посередні результати в Ubuntu

Результати роботи

РЕКОМЕНДАЦІЇ ТА ДЕРЕВО РІШЕНЬ

Мережеве з'єднання	Windows	Ubuntu	macOS
Надійне	WireGuard	WireGuard	L2TP/IPSec
Можлива затримка	WireGuard	L2TP/IPSec	OpenVPN
Можлива втрата пакетів	WireGuard	WireGuard	WireGuard



Результати роботи

- З метою забезпечити високу якість результатів було розглянуто та оброблено декілька загроз валідності експерименту, а також декілька різновидів упереджень
- Було окреслено рекомендовані напрямки майбутніх досліджень, що можуть бути корисними для отримання докладніших і точніших результатів

ЗАГРОЗИ ВАЛІДНОСТІ ТА НАПРЯМКИ МАЙБУТНІХ ДОСЛІДЖЕНЬ

Наукова новизна

НАУКОВА НОВИЗНА

Вперше експериментальним шляхом було отримано метрики продуктивності сучасних рішень VPN в умовах ненадійності мережі, а відповідно вперше описано тенденції та обґрунтовано рекомендації на основі таких метрик

ПРАКТИЧНА ЦІННІСТЬ

Практична цінність полягає в можливості застосування отриманих результатів мережевими адміністраторами для оцінки варіантів рішень при розгортанні VPN і забезпеченні віддаленого доступу в умовах ненадійності мережі

Висновки

- Було досліджено проблему вибору протоколу VPN для забезпечення віддаленого доступу сучасними підприємствами
- Було розроблено методику аналізу продуктивності сучасних рішень VPN, що містить: обґрунтування метрик, вибір інструменту, налаштування експериментальної установки тощо
- Було виконано серію експериментів, що дозволили дослідити продуктивність трьох актуальних на сьогодні рішень VPN в різних середовищах та умовах застосування
- Аналіз результатів проведених експериментів дозволив розробити рекомендації з вибору найліпшого протоколу VPN для певної операційної системи і певної якості мережевого з’єднання

Дякую за увагу!