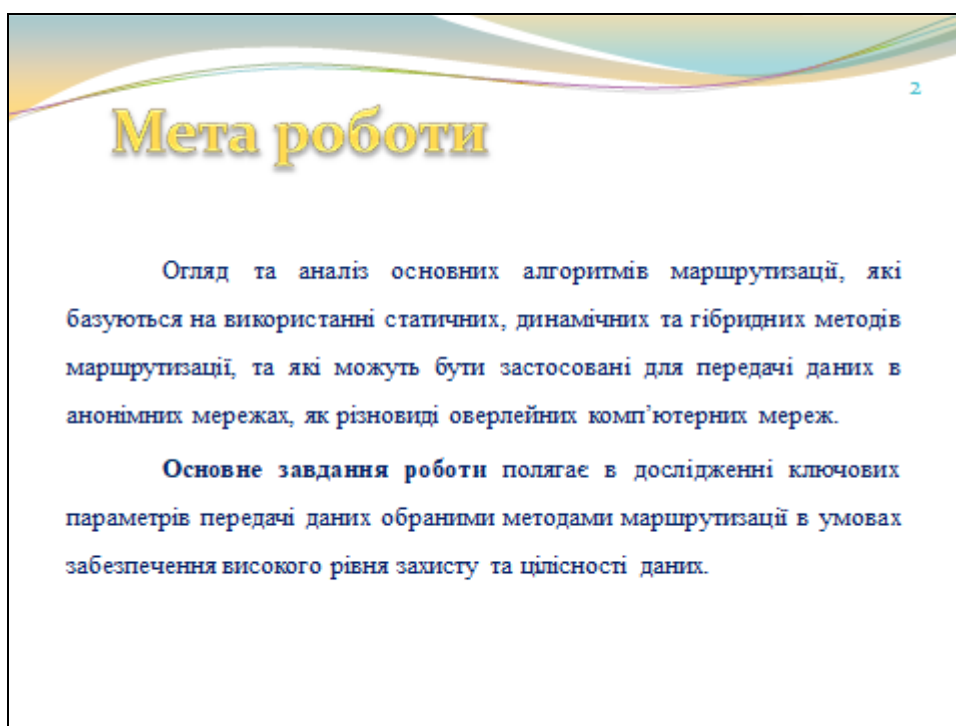
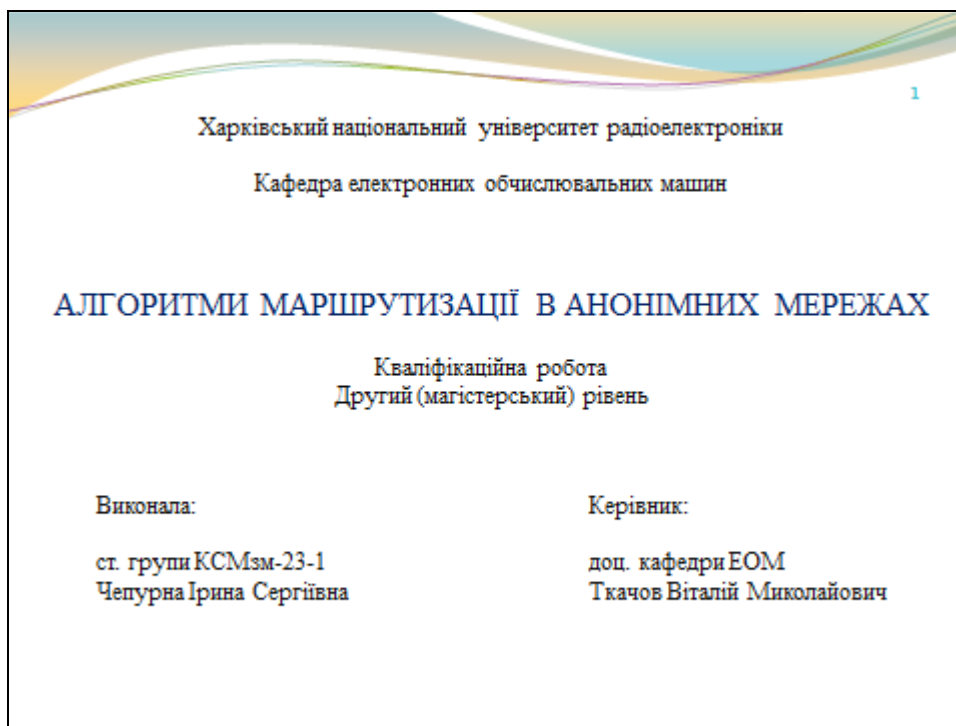


ДОДАТОК А

Графічний матеріал кваліфікаційної роботи



Оверлейні мережі - це мережні структури, які функціонують як логічна надбудова над фізичними мережами, пристрої в яких взаємодіють за допомогою віртуальних або логічних з'єднань. 3

Анонімні мережі - це різновид оверлейних мереж, орієнтований на досягнення високого рівня конфіденційності.

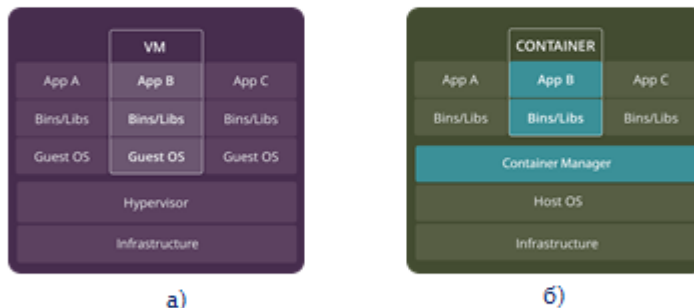


Схема архітектур віртуальної машини та контейнера:
а) віртуальна машина; б) контейнер

Підходи до забезпечення анонімності:

- 1 Шифрування трафіку
- 2 Багатоступенева маршрутизація
- 3 Підміна IP-адреси
- 4 Механізм «змішування» трафіку
- 5 Використання оверлейних мереж
- 6 Використання децентралізованих мереж
- 7 Анонімні профілі та псевдонімізація
- 8 Часове обмеження сесій

Статична маршрутизація

Протокол	Швидкість	Шифрування	Потокова передача	Стабільність	P2P
OpenVPN	швидкої	підмітно	добра	добра	добре
Ipsec/IKEv2	швидкої	підмітно	добра	підмітно	добре
Wireguard	дуже швидкої	підмітно	добра	підмітно	добре
SSTP	середній	добре	середня	середня	добре

Динамічна маршрутизація

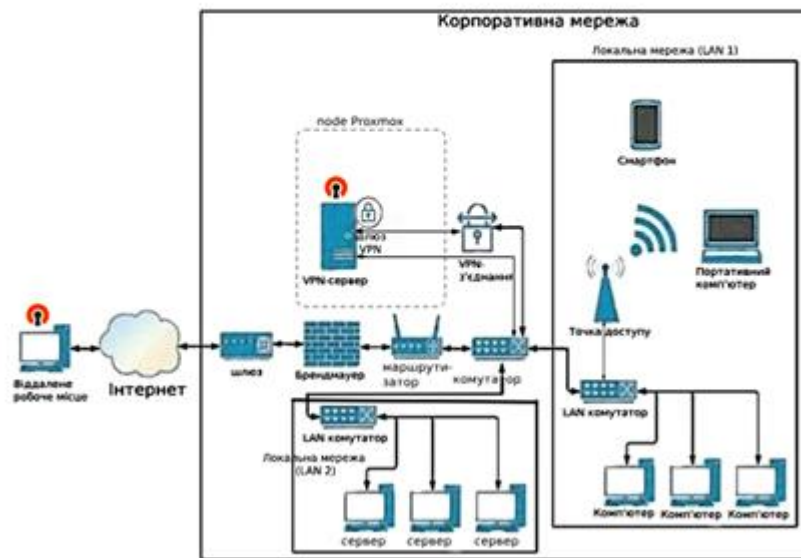
Гібридна маршрутизація

7



Метод мультирівневого VPN-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі

8



Висновки

15

В кваліфікаційній роботі здійснено детальний аналіз сучасних методів маршрутизації, зокрема статичних, динамічних та гібридних алгоритмів, у контексті анонімних мереж. Основна увага приділена поверхневим мережам, зокрема VPN, мережам Tor та Gnutella.

Проведено моделювання методів маршрутизації в анонімних мережах та аналіз ключових параметрів кожного з методів маршрутизації, а також їх вплив на ефективність передачі еластичних та нееластичних даних.

Порівняльна таблиця результатів апробації методів маршрутизації

параметр	статична маршрутизація		динамічна маршрутизація		гібридна маршрутизація		Метод мультірівневого VPN-тунелювання	
	TCP	UDP	TCP	UDP	TCP	UDP	TCP	UDP
Пропускна здатність, Гбіт/с	0,0903		0,0808		0,000738		0,0800	
Загальний обсяг даних, Мб	120,506		120,361		123,0		123,55	
Швидкість передачі, Гбіт/с	0,0878	0,025	0,0778	0,0031	0,000298	0,000018	0,0850	0,0201
Затримка, мс	0,0135	0,0200	3,61	1,21	0,0562	0,0025	0,0114	0,0018
Частка у трафіку, %	56,71	43,29	96,18	3,82	95,38	3,57	57,55	42,45
Еластичні дані	+		+		+		+	
Нееластичні дані	+/-		-		+/-		+	

ДОДАТОК Б

Лістинг запропонованого методу

```
# 1. Ініціація підключення клієнта
client_initiates_connection()
# 2. Створення першого тунелю
vpn_tunnel_1 = establish_vpn_tunnel(server_address_1,
encryption="AES-256")
if not authenticate_user(vpn_tunnel_1, user_certificate):
    terminate_connection()
    exit()
# 3. Створення другого тунелю для доступу до внутрішніх вузлів
vpn_tunnel_2 = establish_vpn_tunnel(server_address_2,
encryption="AES-256")
if not authenticate_user(vpn_tunnel_2, user_certificate):
    terminate_connection()
    exit()
# 4. Опціональний третій тунель для спеціалізованих ресурсів
if needs_specialized_access():
    vpn_tunnel_3 = establish_vpn_tunnel(server_address_3,
encryption="AES-256")
    if not authenticate_user(vpn_tunnel_3, user_certificate):
        terminate_connection()
        exit()
# 5. Виконання запитів користувача через відповідний тунель
access_resources(vpn_tunnel_2 or vpn_tunnel_3)
# 6. Завершення сесії
terminate_vpn_tunnels([vpn_tunnel_1, vpn_tunnel_2,
vpn_tunnel_3])
terminate_connection()
```

ДОДАТОК В

Апробація результатів кваліфікаційної роботи

ISSN 2078-4481

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**ВІСНИК**ХЕРСОНСЬКОГО НАЦІОНАЛЬНОГО
ТЕХНІЧНОГО УНІВЕРСИТЕТУ

3(90)

Рекомендовано до друку Вченою радою
Херсонського національного технічного університету
(протокол № 3 від 29.10.2024 року)

Журнал включено до Переліку наукових фахових видань України
категорії «Б» за економічними науками, спец. – 051, 071, 072, 073, 075, 076, 242
(Наказ МОН України від 17.03.2020 № 409),
281 (Наказ МОН України від 29.06.2021 № 735);
та за технічними науками, спец. – 121, 122, 123, 125, 126, 131, 132, 133, 151, 274, 275
(Наказ МОН України від 02.07.2020 № 886)
та спец. 141, 161, 182 (Наказ МОН України від 24.09.2020 № 1188)

Журнал включено до наукометричних баз, електронних бібліотек та репозитаріїв:
GoogleScholar, Crossref, National Library of Ukraine (Vernadsky)Видавничий дім
«Гельветика»
2024

В. М. ТКАЧОВ

кандидат технічних наук, доцент,
доцент кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-6524-9937

І. С. ЧЕПУРНА

асистент кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0009-0008-2442-6221

Т. Г. ФЕСЕНКО

доктор технічних наук, професор,
професор кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0000-0001-9636-9598

МЕТОД МУЛЬТИРІВНЕВОГО VPN-ТУНЕЛЮВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІДДАЛЕНОГО ДОСТУПУ ДО ВУЗЛІВ ЕКСТРАНЕТ-МЕРЕЖІ

У статті запропоновано новий метод мультирівневого VPN-тунелювання. Метод спрямований на забезпечення безпечного та контрольованого віддаленого доступу до вузлів екстранет-мережі корпоративного рівня. Метод дозволяє створити багаторівневу архітектуру тунелювання, що забезпечує різні рівні доступу для користувачів, залежно від їхньої ролі та привілеїв у корпоративній системі. Це дозволяє значно підвищити загальний рівень безпеки мережної інфраструктури, зокрема у випадках роботи з конфіденційними або критично важливими даними. Використання кількох послідовних VPN-тунелів на різних рівнях мережі створює додаткові шари захисту, що забезпечують надійність передачі даних і захист від різноманітних кібератак, спрямованих на компрометацію окремих вузлів або каналів зв'язку. У статті також детально розглядаються технічні аспекти впровадження та реалізації багаторівневого VPN-тунелювання. Представлено детальні рекомендації щодо налаштування VPN-шлюзів на платформі Proxmoх, вибору протоколів шифрування та використання засобів автентифікації для кожного рівня. Крім того, особливу увагу приділено питанням оптимізації роботи VPN-тунелів з метою мінімізації затримок у передачі даних і підвищення ефективності використання мережевих ресурсів. Це дозволяє забезпечити більш стабільне та швидке з'єднання для користувачів, зменшивши вплив на продуктивність мережі. Гнучке розмежування прав доступу користувачів до різних сегментів мережі значно підвищує безпеку та зменшує ризики несанкціонованого доступу. Експериментальне дослідження ефективності роботи реалізації запропонованого методу проводилося за допомогою імітування екстранет-мережі на базі сегменту локальної комп'ютерної мережі кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки та підтвердило його ефективність у забезпеченні безперервного та захищеного доступу до екстранет-ресурсів, що підкреслює доцільність його використання в сучасних корпоративних середовищах.

Ключові слова: метод, VPN, екстранет-мережа, віддалений доступ.

V. M. TKACHOV

Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-6524-9937

I. S. CHEPURNA

Assistant at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0009-0008-2442-6221

T. G. FESENKO

Doctor of Technical Sciences, Professor,
Professor at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0000-0001-9636-9598