УДК 004.738.5:004.451 DOI https://doi.org/10.35546/kntu2078-4481.2024.3.37

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 Proxmox, 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 безперебійного 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

MULTI-LEVEL VPN-TUNNELING METHOD FOR ENSURING REMOTE ACCESS TO EXTRANET NETWORK NODES

This article proposes a new method of multilevel VPN tunneling. The method is aimed at ensuring secure and controlled remote access to corporate-level extranet network nodes. It allows the creation of a multilevel tunneling architecture, providing different levels of access for users depending on their roles and privileges within the corporate system. This approach significantly enhances the overall security of the network infrastructure, especially when handling confidential or critical data. The use of multiple consecutive VPN tunnels at various network levels adds additional layers of protection, ensuring reliable data transmission and defense against various cyberattacks targeting the compromise of specific nodes or communication channels. The article also provides a detailed examination of the technical aspects of the implementation and deployment of multilevel VPN tunneling. Detailed recommendations are presented for configuring VPN gateways on the Proxmox platform, choosing encryption protocols, and utilizing authentication tools at each level. Moreover, particular attention is given to optimizing the operation of VPN tunnels to minimize data transmission delays and improve the efficiency of network resource usage. This ensures more stable and faster connections for users while reducing the impact on network performance. Flexible user access control to different network segments significantly enhances security and reduces the risks of unauthorized access. Experimental research on the effectiveness of the proposed method was conducted by simulating an extranet network based on the local area network segment of the Department of Electronic Computers at Kharkiv National University of Radio Electronics. The results confirmed the method's effectiveness in providing uninterrupted and secure access to extranet resources, highlighting its suitability for use in modern corporate environments.

Key words: *method, VPN, extranet network, remote access.*

Постановка проблеми

Інформаційне суспільство XXI сторіччя усе більше залежить від інноваційних інформаційних технологій, що дозволяють організаціям забезпечувати роботу своїх працівників у будь-якому місці, де є доступ до глобальної мережі Інтернет [1-5]. Політика захисту корпоративних даних стала причиною появи таких сегментів глобальної мережі як корпоративні комп'ютерні мережі, які в свою чергу класифікуються як екстранет- та інтранет-мережі [6]. Однак, разом з цим виникає низка проблем технічного характеру, пов'язаних із забезпеченням безпечного та стабільного доступу до корпоративних ресурсів, особливо, через екстранет-мережі. Одним з ключових рішень для реалізації віддаленого доступу є використання VPN-технологій. Однак, традиційні VPN-рішення мають обмеження, а деякі протоколи вважаються такими як ненадійними [7]. Найуживаніші протоколи тунелювання мають нижчу продуктивність через складні процеси шифрування та розшифрування даних, високі вимоги до обчислювальних ресурсів тощо.

У контексті багаторівневого VPN-тунелювання проблема стає ще більш складною. Це пов'язано з тим, що потрібно забезпечити надійну автентифікацію користувачів на кількох рівнях тунелювання для додаткового захисту даних, при цьому необхідно підтримувати достатню швидкість передачі даних для ефективної роботи додатків користувачів для підключення до віддалених робочих станцій. Важливо також враховувати, що, наприклад, для малого бізнесу існує обмежений бюджет на придбання й утримання мережної інфраструктури, що робить необхідним пошук рішень, які не потребують значних витрат на обладнання або використання технологій віртуалізації у хмарах тощо.

Таким чином, однією з головних технічних проблем є організація безпечного віддаленого доступу до вузлів екстранет-мережі в умовах обмежених ресурсів, коли потрібно досягти максимального рівня захищеності без суттєвого збільшення навантаження на мережну інфраструктуру. Віддалені користувачі повинні мати можливість безпечно підключатися до корпоративних ресурсів через загальнодоступні (небезпечні) сегменти мережі Інтернет, при цьому мінімізуючи ризики витоку даних та збереження цілісності переданої інформації.

Аналіз останніх досліджень і публікацій

Точкові дослідження в галузі віртуальних комп'ютерних мереж зосереджені на вирішенні ряду проблем, зокрема, пов'язаних з ефективністю та надійністю VPN-технологій для забезпечення безпечного доступу до корпоративних мереж [8-15]. Однак швидкість роботи технічної системи та вимоги до ресурсів залишаються важливими проблемами, які потребують нових підходів. Відповідно, було виконано огляд останніх досліджень і публікацій, присвячених цим питанням, з метою аналізу існуючих підходів у вирішенні проблем VPN-тунелювання, зазначених при постановці проблематики досліджень.

Так, у роботі [8] авторами проаналізована проблематика продуктивності та оптимізації VPN-рішень. Автори зазначають, що використання стандартних VPN-протоколів, таких як IPsec та OpenVPN, забезпечує високий рівень захисту, але це часто відбувається за рахунок зниження швидкості передачі даних через складність процесів шифрування та розшифрування. Подібну проблему розглянуто у роботі [9], зокрема, авторами досліджено продуктивність VPN при одночасному підключенні великої кількості користувачів до корпоративної мережі. Вони рекомендують оптимізацію роботи тунелів через використання протоколу UDP

замість TCP, що забезпечує менші затримки, але вимагає додаткових налаштувань для підтримки стабільності з'єднання.

У роботі [10] автори підтверджують важливість вибору певних мережних протоколів для зменшення впливу на продуктивність системи. Наприклад, OpenVPN, один з найбільш популярних і надійних VPN-рішень, підтримує гнучкі методи автентифікації та захисту, але потребує достатньої кількості ресурсів для обслуговування великих потоків даних. Цей протокол демонструє задовільні результати при роботі з невеликими та середніми корпоративними мережами у відношенні до кількості віддалених користувачів та інтенсивності мережного трафіку, однак його використання в умовах великої кількості підключень вимагає оптимізації серверних налаштувань та відповідної конфігурації мережної інфраструктури.

В останні роки було проведено багато досліджень щодо удосконалення методів автентифікації користувачів та шифрування даних. Так у роботі [11] наведено результати дослідження деяких алгоритмів шифрування, які використовуються в VPN-рішеннях, включаючи AES та SSL/TLS. Автор відзначив, що оптимальним підходом є використання двосторонньої автентифікації сертифікатів, яка забезпечує високий рівень захисту від несанкціонованого доступу.

Також важливе місце в наукових дослідженнях посідає питання динамічної маршрутизації IP-адрес та контролю доступу користувачів [12]. Робота OpenVPN з використанням протоколу SSL/TLS дозволяє інтегрувати політики контролю доступу на рівні груп користувачів, що значно знижує ризик несанкціонованого доступу до ресурсів корпоративної мережі. В роботі [12] детально описано можливості комерційних VPN-сервісів для захисту корпоративних мереж, де основний акцент зроблено на простоту у використанні та надійність шифрування даних.

Останніми роками дослідники та практики почали активно застосовувати технології віртуалізації для підвищення ефективності використання VPN-рішень. Програмні платформи на основі контейнерів, такі як Proxmox, дозволяють розгортати VPN-сервери в ізольованих середовищах, що підвищує рівень безпеки та спрощує адміністрування мережі. Так, у роботі [13] описано переваги використання контейнерів для віртуалізації, оскільки це дозволяє уникати надмірного використання ресурсів фізичних серверів і спрощує процес налаштування VPN-тунелів.

Proxmox, зокрема, пропонує вбудовані інструменти для управління мережними ресурсами, включаючи кластеризацію серверів та оперативну міграцію віртуальних машин [13]. Це дозволяє масштабувати мережну інфраструктуру без необхідності інвестувати в нове обладнання, що є критичним для малого та середнього бізнесу. Крім того, Proxmox підтримує інтеграцію з OpenVPN, що робить можливим розгортання багаторівневих VPN-тунелів для безпечного доступу до ресурсів екстранет-мереж.

Поряд з традиційними рішеннями для VPN, популярність набирають хмарні VPN-сервіси, які надають можливість швидкого розгортання та масштабування мережевої інфраструктури. У роботі [14] описується, як хмарні рішення дозволяють бізнесу ефективно забезпечувати віддалений доступ до корпоративних ресурсів без необхідності підтримувати власну інфраструктуру. Проте, як зазначають автори, такі рішення часто стають менш контрольованими з точки зору безпеки, що може створювати додаткові ризики, особливо для великих компаній.

Пандемія COVID-19 та пов'язані з нею локдауни, повномасштабне вторгнення рф в Україну – різко збільшили попит на рішення для віддаленого доступу, що призвело до активного впровадження VPN у всіх сферах українського бізнесу. Так, у роботі [15] авторами зазначається, що український бізнес зіткнувся з необхідністю швидко адаптувати свою інфраструктуру для підтримки зростаючого навантаження віддалених підключень в умовах релокацій. Ця тенденція також призвела до підвищеного інтересу до віртуалізації та контейнерних рішень, таких як Proxmox, які забезпечують гнучкість та безпеку в умовах швидкої адаптації до нових викликів.

Таким чином, аналіз останніх досліджень і публікацій [8-15] показує, що ефективність VPN-рішень залежить від низки факторів, включаючи вибір протоколів шифрування, методів автентифікації та використання технологій віртуалізації. Технології на базі контейнерів, такі як Proxmox, у поєднанні з OpenVPN, демонструють великий потенціал для впровадження багаторівневих VPN-тунелів, що дозволяє забезпечити безпечний та ефективний віддалений доступ до вузлів екстранет-мережі, що, в свою чергу, забезпечує сталий розвиток бізнесу.

Формулювання мети дослідження

Метою дослідження є розробка та впровадження методу мультирівневого VPN-тунелювання для забезпечення безпечного віддаленого доступу до вузлів корпоративної екстранет-мережі, що дозволяє підвищити рівень захищеності даних, зменшити вразливість до несанкціонованого доступу та забезпечити надійне функціонування екстранет-мережі в умовах обмеженого ресурсного забезпечення.

Викладення основного матеріалу дослідження

Алгоритмічне забезпечення

Метод багаторівневого VPN-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі базується на інтеграції сучасних технологій шифрування, автентифікації та динамічного управління мережевими ресурсами. Новизна цього підходу полягає у тому, що має місце розвиток підходів багаторівневої архітектури

віртуальних мережних тунелів, що забезпечує диференційовані рівні доступу до різних ресурсів корпоративної мережі, підвищуючи як їх продуктивність, так і безпеку.

Метод багаторівневого VPN-тунелювання, який пропонується, включає в себе кілька послідовних кроків, які в свою чергу можуть мати різні сценарії виконання, в залежності від умов застосування даного методу. Отже:

Крок 1. Попередня аутентифікація та авторизація користувача. До встановлення VPN-з'єднання проводиться попередня перевірка користувача через інтерфейс аутентифікації за сертифікатами або іншими механізмами автентифікації (наприклад, двофакторна автентифікація). Цей крок є критично важливим для попередження доступу неавторизованих користувачів і дозволяє задати умови для наступних рівнів тунелювання. Якщо автентифікація не вдається, система автоматично відхиляє запит на з'єднання і крок може бути повтореним як користувачем, так і певною автоматизованою системою.

Крок 2. Створення першого рівня тунелювання. Перший тунель призначений для шифрування базового інтернет-трафіку користувача з мінімальними вимогами до ресурсів. Він забезпечує початковий рівень захисту та автентифікації на рівні VPN. Трафік може шифруватися за допомогою AES-256 або TLS/SSL, залежно від вибору протоколу. У разі успішної автентифікації на першому рівні користувач отримує доступ до внутрішніх ресурсів загального призначення, але доступ до критично важливих вузлів корпоративної мережі залишається обмеженим.

Крок 3. Налаштування внутрішньої маршрутизації та моніторингу трафіку. Після успішного з'єднання на першому рівні корпоративна мережа, яка функціонує з використанням даного методу, здійснює динамічний моніторинг трафіку. Вона аналізує типи запитів і класифікує їх відповідно до рівня доступу, який необхідний для виконання операцій. У разі виявлення підозрілого трафіку або незвичних патернів поведінки (наприклад, несанкціонованих запитів на доступ до критичних ресурсів) відповідні прикордонні вузли мережі можуть автоматично ініціювати обмеження або додаткову автентифікацію.

Крок 4. Створення другого рівня тунелювання. Другий рівень VPN-тунелювання забезпечує підвищену безпеку для користувачів, яким необхідний доступ до конфіденційних ресурсів внутрішньої мережі або екстранет-вузлів. Цей рівень включає додаткові процедури автентифікації, такі як одноразові паролі або цифрові підписи. Дані передаються через VPN-тунель із покращеними методами шифрування (наприклад, більш складні варіанти протоколів TLS із сертифікованими ключами). Якщо автентифікація не вдається, відповідний прикордонний вузол автоматично закриває другий рівень і обмежує доступ до основного рівня тунелювання.

Крок 5. Налаштування динамічного управління ресурсами. Корпоративна мережа використовує інтелектуальні алгоритми динамічного управління ресурсами на основі навантаження, активності користувачів і типу запитів. Наприклад, якщо обсяг трафіку або кількість підключених користувачів до другого рівня значно збільшується, прикордонні вузли можуть тимчасово призупинити прийняття нових підключень або перемикати запити на інші ресурси для забезпечення стабільності роботи корпоративної мережі.

Крок 6. Створення нового рівня тунелювання. Новий рівень VPN-тунелювання розрахований на спеціалізовані запити, що вимагають максимального рівня безпеки (наприклад, доступ до критично важливих серверів або баз даних). Для цього рівня використовується багаторівнева автентифікація з застосуванням апаратних токенів, а також посилені алгоритми шифрування даних (наприклад, алгоритми шифрування з довгими ключами або квантові механізми шифрування). Доступ на цьому рівні дозволяється лише після підтвердження додаткових прав доступу.

Крок 7. Закриття тунелів та завершення сесії. Після завершення роботи всі тунелі автоматично закриваються. Корпоративна мережа здійснює моніторинг залишкових даних і гарантує, що всі тимчасові ключі шифрування видаляються після завершення сесії. Це забезпечує відсутність можливості перехоплення або повторного використання ключів для несанкціонованого доступу в майбутньому.

Запропонований метод доцільно використовувати при наступних умовах:

– початковий рівень забезпечує загальне підключення користувачів та контроль за автентичністю. Основна умова – надання доступу лише авторизованим користувачам, що проходять першу автентифікацію. У разі збоїв або помилок з'єднання, тунель одразу закривається;

– другий рівень працює лише для користувачів, яким необхідний доступ до більш конфіденційних даних. Система застосовує механізми моніторингу активності для виявлення підозрілих дій. Якщо виявляються порушення, доступ блокується або переводиться в режим обмеженої доступності;

– більш глибинні рівні орієнтовані на спеціальні операції та ресурси. Умови доступу суворіші, а вимоги до автентифікації жорсткіші. Тунель працює лише при виконанні всіх умов перевірки.

Псевдокод, наведений нижче, дозволяє більш точно описати логіку виконання методу. У ньому зазначені конкретні умови, цикли, виклики функцій та обробку даних, що важливо для розуміння послідовності операцій у методі.

```
# 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()
```

Лістинг 1. Псевдокод запропонованого методу

Оцінка ефективності розробленого методу

Загальна ефективність методу багаторівневого VPN-тунелювання може бути визначена через зважену оптимізацію всіх факторів: швидкості передачі, рівня безпеки та ефективності використання ресурсів. Вона може бути виражена через наступну багатофакторну оптимізаційну задачу:

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

де α, β, γ – вагові коефіцієнти, які визначають пріоритети між швидкістю передачі даних, рівнем безпеки та ефективністю ресурсів;

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

Компоненти оптимізаційної задачі (1) представлені нижче:

1. Оцінка продуктивності передачі даних у тунелях з урахуванням криптографічної складності. Швидкість передачі даних (S) може бути зменшена 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:

$$S = \frac{B}{N \sum_{i=1}^{N} \left(C_{comp,i} + \frac{t_{enc,i}}{t_{trans.i}} \right)}, \quad (2)$$

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

N – кількість рівнів тунелювання, од.;

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

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

Обчислювальна складність залежить від використовуваного алгоритму шифрування (наприклад, AES-256), і співвідношення між часом шифрування та передачею даних на визначених рівнях.

2. Оцінка затримки передачі даних з урахуванням перемикання рівнів Затримка (L) повинна враховувати не тільки час шифрування і декодування, але й затримку через чергування (черги запитів) на кожному рівні тунелювання. Для цього можна застосувати модель чергування *M/M/1* [16] (середня затримка в системі з обслуговуванням):

$$L = \sum_{i=1}^{N} \left(\frac{1}{\mu_i - \lambda_i} + t_{enc,i} + t_{dec,i} + t_{trans,i} \right), \quad (3)$$

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

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

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

Дана формула (3) дозволяє моделювати вплив навантаження на систему та враховувати затримку через черги при підвищеному навантаженні на мережу.

3. Оцінка ефективності використання ресурсів із врахуванням заходів оптимізації. Ефективність використання ресурсів залежить від того, чи оптимально використовуються обчислювальні ресурси для шифрування та передачі даних. Це можна представити у такому вигляді:

$$R_{effect} = \frac{\sum_{j=1}^{M} D_j}{\sum_{i=1}^{N} \left(C_{enc,i} + C_{trans,i} \right) \times \max\left(\frac{t_{enc,i}}{t_{trans,i}}, 1 \right)}, \quad (4)$$

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 і-му рівні, од.;

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

M – кількість завдань на передачу даних.

4. Оцінка рівня безпеки через ймовірність складної атаки. Для оцінки рівня безпеки доцільно використати ймовірнісну модель, яка враховує не тільки ймовірність успішної атаки на кожен рівень, але й обчислювальну складність атаки на шифрування:

$$P_{total} = 1 - \prod_{i=1}^{N} \left(1 - \frac{P_{attack,i}}{C_{attack,i}} \right), \quad (5)$$

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

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

З (5) видно, що чим складніше алгоритм шифрування, тим менша ймовірність успішної атаки.

Даний підхід дозволяє комплексно оцінити ефективність методу багаторівневого VPN-тунелювання з врахуванням складності криптографічних алгоритмів, моделі чергування, ресурсоємності шифрування та передачі даних, а також ймовірності успішних атак. Ці моделі забезпечують більш точну кількісну оцінку взаємозв'язку між рівнем безпеки, швидкістю передачі та ефективністю використання ресурсів, що важливо для оптимізації системи VPN.

Постановка експерименту

На початковому етапі було виконано аналіз апаратних вимог. Він показав, що для продуктивної роботи OpenVPN можна використовувати процесор з щонайменше з 4 ядрами та максимальною частотою 2,9 ГГц. Об'єм ОЗУ залежить від кількості підключених пристроїв та потоку даних. З практичної точки зору 1 ГБ ОЗУ дозволяє ефективно обслуговувати до 150 пристроїв, які підключені до VPN-сервера, причому конфігурація серверної частини VPN-серверу вказує на можливість підключення до 100 клієнтів. За таким розрахунком, таке рішення можуть дозволити невеликі та середні компанії з урахуванням використання інших пристроїв, які входять до корпоративної мережі. Пропускна здатність каналу зв'язку складає 72 Мбіт/с, що цілком достатньо для обслуговування користувачів експериментальної корпоративної мережі. Жорсткий диск VPN-сервера повинен мати не менше 8 ГБ вільного місця.

В рамках експерименту реалізовано всі функції VPN-серверу та передбачені дії користувачів системи. Так, щоб підключитися до екстранет-мережі, віддалений користувач повинен спочатку встановити клієнтську програму, за допомогою якої здійснюється віддалене підключення до VPN-сервера корпоративної мережі.

Налаштування VPN-сервер виконується безпосередньо у контейнері Proxmox, тоді як надання клієнтських сформованих сертифікатів здійснюється за допомогою веб-інтерфейсу OpenVPN GUI. Розташування VPN-серверу у такий спосіб надає додатковий захист віддаленого підключення та уникає можливості виявлення адреси серверу при можливих атаках зловмисників. До непривілейованого контейнеру Proxmox також неможливо підключитися за SSH безпосередньо. Для можливості передавати будь-які дані з контейнеру необхідно додатково налаштовувати гостьову файлову систему. У такий спосіб виникає загроза витоку даних та несанкціонованого доступу до інформації локальної мережі, саме тому було обрано підключення веб-інтерфейсу OpenVPN GUI для керування групами користувачів, які будуть мати доступ до локальної мережі. На рисунку 1 представлено схему підключення користувачів до VPN-серверу.

Щоб підключитися до корпоративної мережі, віддалений користувач повинен спочатку встановити клієнтську програму VPN, яка використовується для підключення до VPN-сервера корпоративної мережі. Після успішного підключення користувач бачить сегмент корпоративної мережі.

На рисунку 2 можна побачити, що віддалений користувач підключається до VPN-серверу з мережі Інтернету через шлюз контейнеру Proxmox (шлюз від WAN до LAN). Тут він отримує ідентифікатор користувача з описаними правами доступу. Потім він може отримати доступ до екстранет-мережі та використовувати послуги, які ця мережа надає та дозволяє йому використовувати.

Захист системних даних здійснюється за AES-256 – протоколом шифрування даних. Використовується двосторонній сертифікат автентифікації, який вимагає від клієнта автентифікації сертифіката сервера, а від сервера – сертифіката клієнта, що забезпечує взаємну довіру.

Рис. 1. Схема підключення клієнтів до VPN-серверу

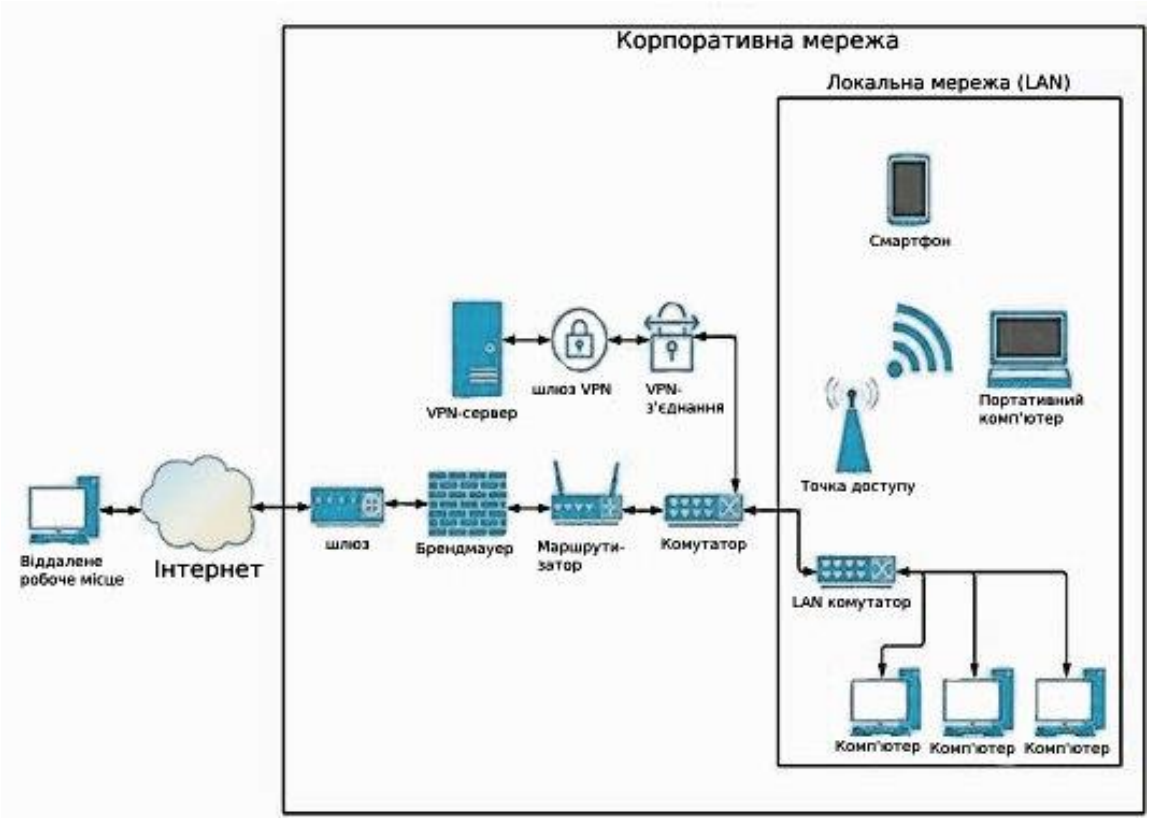

Рис. 2. Використання контейнеризації при реалізації методу

Використовуючи сервіси хмарних обчислень, розроблено та підготовлено модель тестування віртуальної системи. Комп'ютерна мережа та її функції були змодельовані за допомогою Linux Ubuntu Server версії 18.04, а клієнт – за допомогою Windows 10. Брандмауер налаштовується за допомогою нескладних правил, в які додаються правила прокидання портів та відкриття портів 943 –для з'єднання з OpenVPN GUI, 1194 – стандартним портом OpenVPN, а також портами, які обирає та встановлює адміністратор мережі для додаткового захисту мережі. При установці пакетів OpenVPN завантажуються сертифікати та конфігураційні файли, що забезпечують безпеку підключення. В OpenVPN GUI після виконання скрипту створюється інтерфейс користувача – адміністратора, який формує сертифікати користувачів, групи користувачів з відповідними правами доступу. Сформовані сертифікати користувачів надсилаються на хостову машину, де розгорнуто віртуальне середовище у контейнері Proxmox.

Спочатку тестова модель віртуальної системи використовувалася для перевірки роботоздатності VPN-тунелю. Для цього було виконано обмін різнорозмірними ICMP-пакетами.

При аналізі безпеки використовувалася програма Wireshark, яка відстежувала потоки даних, що проходять через тунель VPN. Після фільтрації тільки тих пакетів, що проходять через тунель VPN, можна побачити, що їх вміст зашифровано (рисунок 3).

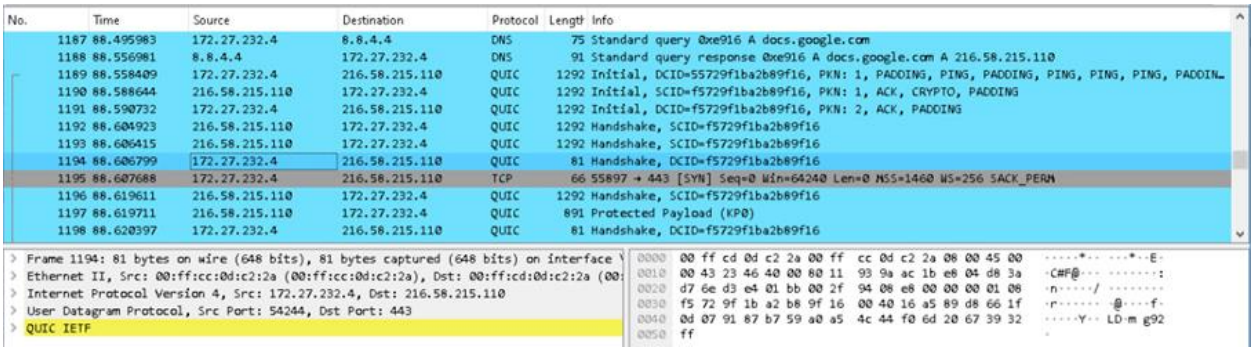

Рис. 3. Аналіз відфільтрованих пакетів

Таким чином, маємо, що із збільшенням кількості рівнів тунелювання спостерігається зменшення швидкості передачі даних через підвищення обчислювальної складності та часу шифрування (рисунок 4). При цьому загальна затримка залишається постійною, оскільки вона враховує сумарний вплив процесу шифрування та передачі для кожного рівня. Це показує вплив кожного додаткового рівня тунелювання на продуктивність. Експеримент показав, що збільшення кількості рівнів тунелювання також впливає на ефективність використання ресурсів.

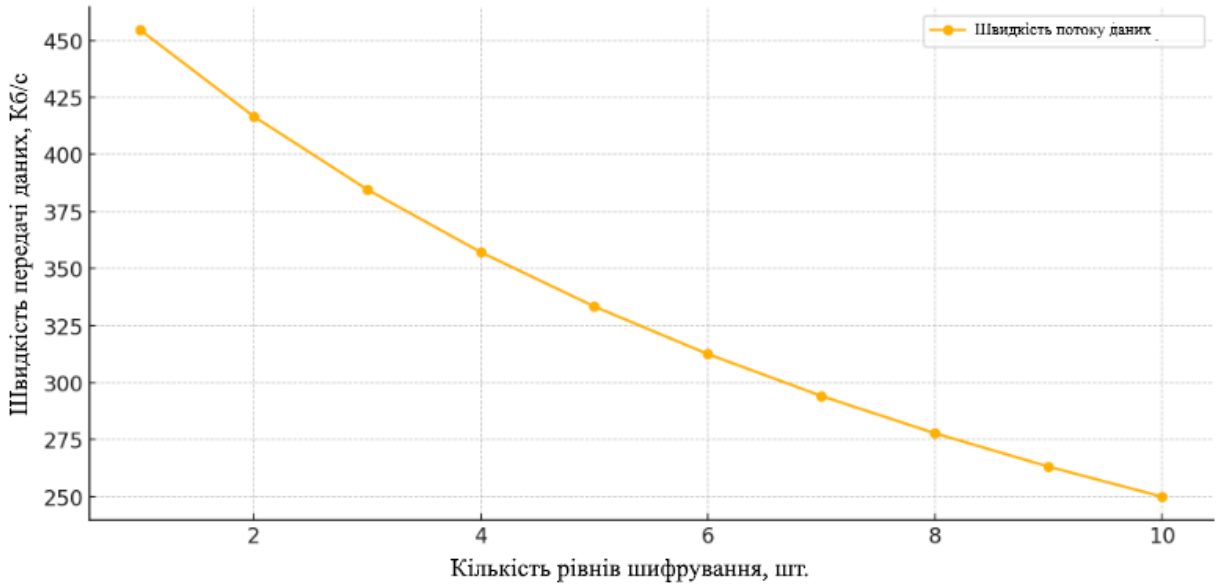

Рис. 4. Зміна значення швидкості передачі даних в залежності від кількості рівнів

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

Висновки

У цій статті було запропоновано та детально проаналізовано метод багаторівневого VPN-тунелювання для забезпечення безпечного віддаленого доступу до вузлів екстранет-мережі. Метод дозволяє створити кілька рівнів шифрування та автентифікації, що підвищує рівень безпеки і забезпечує захист конфіденційних даних під час передачі через загальнодоступні мережі. Наукова новизна полягає у подальшому розвитку багаторівневих архітектур, які дозволяють адаптивно підходити до балансування між продуктивністю, безпекою та ефективністю використання ресурсів.

Аналіз ефективності методу показав, що збільшення кількості рівнів тунелювання призводить до підвищення захисту від несанкціонованого доступу, зменшуючи ймовірність успішної атаки. Однак, швидкість передачі даних зменшується, а загальна ресурсозатратність системи зростає, особливо при використанні складних алгоритмів шифрування та автентифікації. Введення коефіцієнтів у (1) показує, що обчислювальні витрати і затримки можуть зростати значно швидше, ніж лінійно, при збільшенні кількості рівнів, що підтверджує необхідність оптимізації та балансування параметрів системи за пріоритетами задачі, яка вирішується при застосуванні даного методу.

При практичному застосуванні методу необхідно враховувати характер даних, які передаються, вимоги до захищеності, і ресурси, доступні для реалізації VPN-системи. Таким чином, запропонований метод може бути корисним для малого та середнього бізнесу, який прагне забезпечити надійний захист своїх екстранет-мереж при віддаленому доступі, особливо в умовах обмеженого ресурсного забезпечення.

Майбутні дослідження можуть бути спрямовані на подальшу оптимізацію методу, наприклад, шляхом адаптивного налаштування рівнів тунелювання в реальному часі або інтеграції новітніх криптографічних алгоритмів, щоб підвищити як продуктивність, так і безпеку системи.

Список використаної літератури

1. Федорова Ю. Інноваційні інформаційні технології в підготовці та управлінні персоналом. *Adaptive Management Theory and Practice Economics*. 2021. Т. 11, № 22. URL: https://doi.org/10.33296/2707-0654-11(22)-11.

2. Биців М. М. Значення інформаційних технологій як чинника інновацій у діяльності малого та середнього бізнесу // *Бізнес, інновації, менеджмент: проблеми та перспективи:* збірник тез доповідей ІІ Міжнародної наук.-практ. конференції, м. Київ, 22 квітня 2024 р. / Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2021. С. 206–207.

3. Дзямулич Микола, Шматковська Тетяна. Вплив сучасних інформаційних систем і технологій на формування цифрової економіки. *Економічний форум*. 2022. Т. 1, № 2. С. 3–8. URL: https://doi.org/10.36910/6775-2308-8559-2022-2-1.

4. Жиглей І. В., Лайчук С. М., Поліщук І. Р. Використання інформаційних технологій у бухгалтерському обліку. *Економіка, управління та адміністрування.* 2024. № 1(107). С. 95–102. URL: https://doi.org/10.26642/ema-2024-1(107)-95-102.

5. He W., Zhang Z., Li W. Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *International Journal of Information Management*. 2021. Vol. 57. P. 102287. URL: https://doi.org/10.1016/j.ijinfomgt.2020.102287.

6. 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.

7. Security Assessment and Evaluation of VPNs: A Comprehensive Survey / H. Abbas et al. *ACM Computing Surveys.* 2023. URL: https://doi.org/10.1145/3579162.

8. Security vs Bandwidth: Performance Analysis Between IPsec and OpenVPN in Smart Grid / K. Ghanem et al. 2022 *International Symposium on Networks, Computers and Communications (ISNCC)*, Shenzhen, China, 19–22 July 2022. 2022. URL: https://doi.org/10.1109/isncc55209.2022.9851717.

9. Chua C. H., Ng S. C. SSL VPN over TCP and UDP Tunnels. CCIOT 2022: *2022 7th International Conference on Cloud Computing and Internet of Things,* Okinawa Japan. New York, NY, USA, 2022. URL: https://doi.org/10.1145/3569507.3569511.

10. OpenVPN is Open to VPN Fingerprinting / D. Xue et al. *Communications of the ACM*. 2024. URL: https://doi.org/10.1145/3618117.

11. Amaldeep S., Sankaran S. Cross Protocol Attack on IPSec-based VPN. *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, Chattanooga, TN, USA, 11–12 May 2023. 2023. URL: https://doi.org/10.1109/isdfs58141.2023.10131787

12. Сучасні інформаційні технології та системи [Електронний ресурс]: монографія / Н. Г. Аксак, Л. Е. Гризун, О. В. Щербаков та ін.; за заг. ред. д-ра екон. наук, професора В. С. Пономаренка. Харків : ХНЕУ ім. С. Кузнеця, 2022. 271 с.

13. Чепурна І. С. Алгоритм організації віддаленого доступу до захищеного сегменту корпоративних комп'ютерних мереж. *Радіоелектроніка та молодь у XXI столітті: матеріали 28-го Міжнар. молодіж. форуму*, 16–18 квітня 2024 р. Харків : ХНУРЕ, 2024. Т. 5. С. 76–78. DOI: https://doi.org/10.30837/IYF.PCEIP.2024.076.

14. Santhanamahalingam S., Alagarsamy S., Subramanian K. A study of cloud-based VPN establishment using network function virtualization technique. *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 20–22 October 2022. 2022. URL: https://doi.org/10.1109/icosec54921.2022.9951894.

15. Новородовський В. Інформаційна безпека України в умовах російської агресії. *Society. Document. Communication.* 2020. № 9. С. 150–179. URL: https://doi.org/10.31470/2518-7600-2020-9-150-1179.

16. 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.

References

1. Fedorova, Y. (2021). Innovatsiini informatsiini tekhnolohii v pidhotovtsi ta upravlinni personalom [Innovative information technologies in training and personnel management]. Adaptive Management Theory and Practice Economics, 11(22). https://doi.org/10.33296/2707-0654-11(22)-11.

2. Bytsiv, M. M. (2021). Znachennia informatsiinykh tekhnolohii yak chynnyka innovatsii u diialnosti maloho ta serednioho biznesu [The importance of information technology as a factor of innovation in the activities of small and medium-sized businesses]. In Business, Innovations, Management: Problems and Prospects: Proceedings of the II International Scientific and Practical Conference (pp. 206–207). Kyiv, Ukraine: National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».

3. Dziamulich, M., & Shmatkovska, T. (2022). Vplyv suchasnykh informatsiinykh system i tekhnolohii na formuvannia tsyfrovoi ekonomiky [The impact of modern information systems and technologies on the formation of the digital economy]. Ekonomichnyi Forum, 1(2), 3–8. https://doi.org/10.36910/6775-2308-8559-2022-2-1.

4. Zhihlei, I. V., Laichuk, S. M., & Polishchuk, I. R. (2024). Vykorystannia informatsiinykh tekhnolohii u bukhhalterskomu obliku [The use of information technology in accounting]. Ekonomika, upravlinnia ta administruvannia, 1(107), 95–102. https://doi.org/10.26642/ema-2024-1(107)-95-102.

5. He, W., Zhang, Z., & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. International Journal of Information Management, 57, 102287. https://doi.org/10.1016/j.ijinfomgt.2020.102287.

6. Verkhovskyi, I., & Tkachov, V. (2023). Metody pobudovy virtualnykh tunneliv extranet-system [Methods of building virtual tunnels for extranet systems]. Scientific Review, 4(89), 22. https://doi.org/10.26886/2311-4517.4(89)2023.2.

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

8. Ghanem, K., et al. (2022). Security vs Bandwidth: Performance Analysis Between IPsec and OpenVPN in Smart Grid. In 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China. https://doi.org/10.1109/isncc55209.2022.9851717.

9. Chua, C. H., & Ng, S. C. (2022). SSL VPN over TCP and UDP Tunnels. In CCIOT 2022: 2022 7th International Conference on Cloud Computing and Internet of Things, Okinawa, Japan. https://doi.org/10.1145/3569507.3569511

10. Xue, D., et al. (2024). OpenVPN is Open to VPN Fingerprinting. Communications of the ACM. https://doi.org/10.1145/3618117.

11. Amaldeep, S., & Sankaran, S. (2023). Cross Protocol Attack on IPSec-based VPN. In 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA. https://doi.org/10.1109/isdfs58141.2023.10131787.

12. Aksak, N. H., Gryzun, L. E., & Shcherbakov, O. V. (2022). Suchasni informatsiini tekhnolohii ta systemy [Modern information technologies and systems] (Monograph). Kharkiv, Ukraine: KhNEU im. S. Kuznetsa.

13. 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.

14. Santhanamahalingam, S., Alagarsamy, S., & Subramanian, K. (2022). A study of cloud-based VPN establishment using network function virtualization technique. In 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India. https://doi.org/10.1109/icosec54921.2022.9951894.

15. Novorodovskyi, V. (2020). Informatsiina bezpeka Ukrainy v umovakh rosiiskoi ahresii [Information security of Ukraine in the conditions of Russian aggression]. Society. Document. Communication, (9), 150–179. https://doi.org/10.31470/2518-7600-2020-9-150-1179.

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