ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «СИСТЕМА ВІДДАЛЕНОГО ДОСТУПУ ДО ПРИВАТНОЇ ІНФРАСТРУКТУРИ НА БАЗІ WIREGUARD»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми «Комп'ютерна інженерія»
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Сергій БЕРЕЖНИЙ*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Сергій БЕРЕЖНИЙ
Ім'я, ПРІЗВИЩЕ

Керівник: Ярослав ТОРОШАНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
«_____» _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бережний Сергій Володимирович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Система віддаленого доступу до приватної інфраструктури на базі WireGuard»
керівник кваліфікаційної роботи: Ярослав ТОРОШАНКО, кандидат технічних наук, доцент, старший науковий співробітник ,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» лютого 2026р. №51
2. Строк подання кваліфікаційної роботи«14» травня 2026р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, протоколи захищеного з'єднання (WireGuard, IPSec, OpenVPN), принципи тунелювання і криптографічного захисту трафіку, архітектура систем віддаленого доступу, особливості OpenWRT, базові методи конфігурації через Web UI та CLI, механізми маршрутизації та контролю доступу, підходи до тестування, моніторингу та оцінки продуктивності VPN-систем, принципи edge-архітектур.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
    1. Теоретичні основи організації віддаленого доступу до приватних мереж
    2. Проєктування та реалізація системи віддаленого доступу на базі граничного маршрутизатора
    3. Системний аналіз ефективності та техніко-економічне обґрунтування VPN-шлюзу
5. Перелік ілюстративного матеріалу: *презентація*
    1. Мета, об'єкт, предмет дослідження
    2. Актуальність роботи
    3. Обраний підхід (Edge VPN)
    4. Архітектура системи
    5. Апаратна платформа системи
    6. Програмна платформа системи
    7. Практична реалізація (налаштування)
    8. Алгоритми встановлення з'єднання та маршрутизації

9. Практичні результати
10. Виявлені проблеми та оптимізація
11. Особливості обраної апаратної платформи
12. Вартість володіння (ТСО)
13. Масштабування системи
14. Висновки
15. Публікації та апробація роботи

6. Дата видачі завдання «20» лютого 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	22.02-20.03.2026	Виконано
2	Обробка матеріалу	20.03-30.03.2026	Виконано
3	Розробка теоретичної частини	31.03-10.04.2026	Виконано
4	Проєктування та реалізація системи віддаленого доступу на базі граничного маршрутизатора	11.04-20.04.2026	Виконано
5	Висновки за результатами аналізу	21.04-26.04.2026	Виконано
6	Оформлення пояснювальної записки	26.04-28.04.2026	Виконано
7	Розробка презентації	29.04-01.05.2026	Виконано
8	Передзахист	08.05-11.05.2026	Виконано
9	Здача в деканат	08.05-14.05.2026	Виконано

Здобувач(ка) вищої освіти _____ Сергій БЕРЕЖНИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ярослав ТОРОШАНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 92 стор., 37 рис., 6 табл., 36 джерел.

Мета роботи – оптимізація та спрощення підключення користувачів до внутрішніх ресурсів приватної інфраструктури за рахунок використання сучасних криптографічних методів VPN-з'єднання та edge-архітектури.

Об'єкт дослідження – процеси організації захищеного віддаленого доступу до приватних мережевих ресурсів.

Предмет дослідження – засоби та технології побудови, конфігурації та оптимізації VPN-систем на базі WireGuard і вбудованих мережевих платформ.

Короткий зміст роботи: У роботі розглянуто теоретичні основи організації віддаленого доступу, принципи функціонування VPN-технологій, криптографічні механізми захисту трафіку та архітектурні підходи до побудови систем захищеного доступу. Проаналізовано сучасні протоколи, зокрема WireGuard, IPSec та OpenVPN, а також особливості їх реалізації, моделі маршрутизації, механізми автентифікації та контролю доступу, що дозволило обґрунтувати вибір оптимального рішення для побудови ефективної системи.

Окрему увагу приділено практичній реалізації системи автоматизованого підключення користувачів на базі маршрутизатора GL.iNet GL-XE3000 (Puli AX) з використанням OpenWRT та WireGuard. Реалізовано механізми генерації конфігурацій, передачі через QR-код, створення тимчасових сесій, а також алгоритми маршрутизації та управління доступом, проведено тестування продуктивності, моніторинг трафіку та оцінку ефективності, що підтвердило доцільність використання edge-підходу.

КЛЮЧОВІ СЛОВА: ВІДДАЛЕНИЙ ДОСТУП, VPN, WIREGUARD, OPENWRT, EDGE-АРХІТЕКТУРА, КРИПТОГРАФІЯ, МАРШРУТИЗАЦІЯ, GL-INET, АВТОМАТИЗАЦІЯ, МОНІТОРИНГ, ПРОДУКТИВНІСТЬ.

ЗМІСТ

ВСТУП 8
1. ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ ДО ПРИВАТНИХ МЕРЕЖ 9
1.1 Основні принципи організації віддаленого доступу до мережевих ресурсів 9
1.2 Протоколи та технології захищеного мережевого з'єднання 16
1.3 Архітектура сучасних систем захищеного доступу 25
1.4 Методи забезпечення безпеки мережевого доступу 29
1.5 Аналіз сучасних інструментів реалізації систем віддаленого доступу. 37
2. ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ НА БАЗІ ГРАНИЧНОГО МАРШРУТИЗАТОРА 43
2.1 Архітектура мережі та концепція апаратного вузла доступу 43
2.2 Розгортання та конфігурація системи (Web UI та OpenWRT CLI) 50
2.3 Алгоритми функціонування та управління з'єднаннями 60
2.4 Апаратна реалізація, тестування та моніторинг навантаження 70
3. СИСТЕМНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ТА ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ VPN-ШЛЮЗУ 77
3.1 Технічний аудит та методи оптимізації конфігурації 77
3.2 Порівняльний аналіз архітектурних рішень віддаленого доступу 84
3.3 Економічна доцільність та масштабованість проєкту 91
ВИСНОВКИ 99
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 100
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 103

ВСТУП

Сучасні мережеві інфраструктури активно трансформуються під впливом потреби у надійному віддаленому доступі до приватних ресурсів. Це обумовлює необхідність створення безпечних і масштабованих механізмів взаємодії, що базуються на поєднанні мережевих моделей, принципів маршрутизації та засобів суворого контролю. Такий підхід забезпечує стабільність роботи та повну ізоляцію систем навіть за умов динамічного середовища та нестабільних параметрів підключення.

Розвиток технологій захищеного з'єднання призвів до впровадження ефективних VPN-рішень, що реалізують тунелювання трафіку з використанням сучасних криптографічних алгоритмів. Особлива увага приділяється мінімізації накладних витрат та спрощенню процесів конфігурації. Аналіз протоколів демонструє еволюцію від складних багаторівневих систем до продуктивних підходів, які гарантують швидке встановлення з'єднання та стійкість до мережевих змін.

Архітектура систем віддаленого доступу визначається взаємодією між клієнтами та шлюзами, де критично важливими є методи автентифікації та захист від несанкціонованих дій. Використання криптографічних ключів, сегментації мережі та мережевих екранів дозволяє сформувати контрольоване середовище. Порівняльний аналіз підтверджує доцільність використання рішень із відкритим кодом, зокрема протоколу WireGuard, як найбільш ефективної основи для побудови таких систем.

У практичній частині реалізується система на базі маршрутизатора з OpenWRT, де розгортається VPN-шлюз із використанням WireGuard. Передбачено конфігурацію через веб-інтерфейс та консольні інструменти, а також впровадження механізмів генерації ключів для постійних і тимчасових сесій. Фінальне тестування продуктивності та аналіз трафіку в реальних умовах дозволять підтвердити придатність обраного підходу до подальшого масштабування.

1. ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ ДО ПРИВАТНИХ МЕРЕЖ

1.1 Основні принципи організації віддаленого доступу до мережевих ресурсів

У світі розвитку комп’ютерних мереж та інформаційних технологій особливої актуальності набуває забезпечення стабільного, безпечного та безперервного доступу до мережевих ресурсів, оскільки глобальні процеси цифровізації та широке впровадження дистанційної роботи привели до суттєвого зростання потреби у віддаленій взаємодії з інформаційними системами, що, у свою чергу, сформувало нові вимоги до організації доступу до приватної інфраструктури через публічні мережі, зокрема через мережу Інтернет або інші канали зв’язку. У результаті цього віддалений доступ став невід’ємною складовою мережевої інфраструктури, оскільки дозволяє користувачам здійснювати підключення до необхідних ресурсів незалежно від їх фізичного місцезнаходження, забезпечуючи при цьому можливість виконання професійних завдань у будь-який час та з будь-якої точки доступу.

Поняття віддаленого доступу та його роль у мережевій інфраструктурі. Під віддаленим доступом у контексті комп’ютерних мереж розуміється сукупність технологій та методів, що забезпечують можливість взаємодії користувачів із ресурсами мережі за межами її фізичної локалізації, причому такі ресурси можуть включати:

- сервери;
- бази даних;
- файлові сховища;
- веб-додатки;
- корпоративні сервіси.

Всі ті ресурси, які функціонують у межах приватної мережі. В умовах інформаційних систем, що характеризуються розподіленою структурою та високим рівнем інтеграції різних сервісів, потреба у віддаленому доступі значно зросла, особливо з урахуванням розвитку хмарних технологій, гібридних робочих моделей та мобільності користувачів, що призвело до необхідності забезпечення доступу до внутрішніх ресурсів організацій поза межами локальної мережі (див. рис. 1.1) [1].



Рисунок 1.1 – Модель взаємодії «клієнт–сервер» у віддаленому доступі

Зростання популярності дистанційної роботи, а також активне використання розподілених інформаційних систем спричинили підвищення вимог до технологій організації віддаленого доступу, оскільки забезпечення доступу до приватних мереж більше не є допоміжною функцією, а виступає ключовим елементом функціонування як великих корпорацій, так і малих організацій або приватних мереж. У таких умовах виникає необхідність створення механізмів, які дозволяють безпечно, стабільно та контрольовано здійснювати доступ до ресурсів внутрішньої мережі через публічні канали зв’язку, що, у свою чергу, вимагає використання спеціалізованих технологій захисту інформації.

Однією з ключових характеристик віддаленого доступу є необхідність забезпечення захисту переданих даних від несанкціонованого доступу, перехоплення або модифікації, оскільки передача інформації через відкриті мережі

супроводжується підвищеними ризиками безпеки, що потребує застосування криптографічних методів захисту, механізмів автентифікації користувачів та контролю доступу до ресурсів. У цьому контексті особливе значення мають технології, що дозволяють створювати захищені канали зв’язку між віддаленими пристроями та внутрішньою мережею [1].

Серед таких технологій важливе місце займають віртуальні приватні мережі (VPN), які забезпечують формування захищеного тунелю для передачі даних між клієнтськими пристроями та серверною інфраструктурою, використовуючи механізми шифрування та автентифікації. Використання VPN дозволяє реалізувати логічне розширення приватної мережі через публічні канали зв’язку, що створює ефект прямого підключення користувача до внутрішньої мережі незалежно від його фізичного розташування [1].

Організація систем віддаленого доступу передбачає використання комплексного підходу, який включає застосування:

— мережевих протоколів;
— криптографічних алгоритмів;
— програмного забезпечення;
— апаратних ресурсів.

Все це разом формує єдину інфраструктуру доступу. Така інфраструктура повинна забезпечувати інтеграцію різних компонентів мережі на різних рівнях моделі взаємодії, що дозволяє досягти високого рівня ефективності та надійності функціонування системи.

Основні моделі доступу до приватних мереж. Для організації віддаленого доступу до мережевих ресурсів застосовуються різноманітні архітектурні моделі, що визначають способи взаємодії між користувачами та елементами мережевої інфраструктури, причому така взаємодія зазвичай реалізується у двосторонньому режимі, забезпечуючи як передачу даних від клієнта до мережі, так і зворотний обмін інформацією, що є необхідною умовою повноцінної роботи з ресурсами приватної інфраструктури. Вибір конкретної моделі залежить від структури мережі, кількості користувачів, рівня розподіленості інфраструктури та вимог до

безпеки, оскільки різні сценарії використання передбачають різні підходи до організації доступу.

Однією з найбільш поширених моделей є client-server модель, яка передбачає підключення окремого клієнтського пристрою до центрального вузла, що виконує роль точки доступу до приватної мережі, причому таким вузлом зазвичай виступає сервер, який безпосередньо інтегрований у внутрішню інфраструктуру організації. У межах цієї моделі клієнтський пристрій повинен використовувати спеціалізоване програмне забезпечення або мережевий клієнт, який забезпечує встановлення захищеного з'єднання із сервером, виступаючи своєрідним інтерфейсом взаємодії між користувачем та внутрішніми ресурсами мережі. Після встановлення такого з'єднання відкривається можливість доступу до сервісів приватної мережі, включаючи файлові ресурси, бази даних, прикладні сервіси та інші елементи інфраструктури, при цьому вся взаємодія відбувається через захищений канал зв'язку, що дозволяє забезпечити необхідний рівень конфіденційності та цілісності даних [2].

Іншою важливою моделлю є модель з'єднання типу site-to-site, яка використовується переважно у випадках, коли необхідно об'єднати декілька окремих мереж у єдину логічну інфраструктуру, що особливо актуально для великих організацій, які мають декілька офісів, філій або дата-центрів, розташованих у різних географічних точках. У такій ситуації побудова єдиної фізичної мережі часто є неможливою або економічно недоцільною, що зумовлює необхідність використання захищених каналів зв'язку для об'єднання окремих сегментів інфраструктури. Реалізація цієї моделі передбачає створення VPN-тунелів між мережевими вузлами, які забезпечують передачу даних між різними сегментами мережі через публічні канали зв'язку без ризику їх перехоплення або несанкціонованого доступу (див. рис. 1.2) [2].

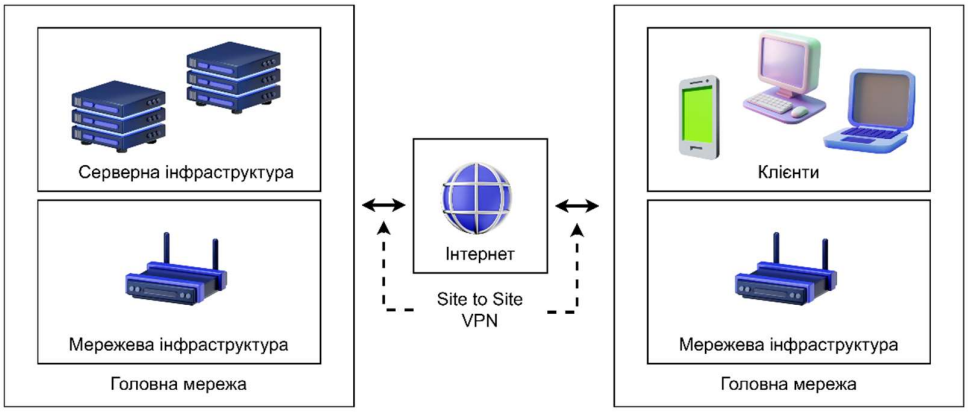


Рисунок 1.2 – Модель взаємодії «site-to-site» у віддаленому доступі

У випадку розподіленої мережевої інфраструктури, де різні підрозділи організації використовують власні локальні мережі, що з'єднані між собою через маршрутизатори, комутатори або мережеві шлюзи, виникає необхідність забезпечення взаємодії між цими сегментами, оскільки ресурси можуть бути розташовані у різних частинах мережі, що ускладнює доступ до них без використання спеціалізованих механізмів. Об'єднання таких сегментів у єдину логічну структуру дозволяє забезпечити централізований доступ до ресурсів та спростити управління мережею, що є важливим фактором для великих організацій із складною інфраструктурою [1-2].

Важливою особливістю обох моделей є використання механізмів шифрування та автентифікації, оскільки передача даних через відкриті мережі потребує забезпечення їх захисту від несанкціонованого доступу, перехоплення або модифікації, що досягається шляхом застосування криптографічних алгоритмів та перевірки достовірності учасників з'єднання. Наявність таких механізмів дозволяє гарантувати конфіденційність інформації та забезпечити контроль доступу до ресурсів приватної мережі, що є критично важливим у сучасних умовах, коли кіберзагрози стають все більш поширеними.

Типові сценарії використання віддаленого доступу у корпоративних та приватних мережах. Віддалений доступ у сучасних комп'ютерних мережах набув широкого застосування у різних сферах діяльності, оскільки забезпечує можливість зручної та безпечної взаємодії користувачів із ресурсами, що розміщені у межах

приватної інфраструктури, при цьому незалежність від фізичного місцезнаходження дозволяє організаціям оптимізувати робочі процеси та підвищити ефективність використання інформаційних систем. Найбільш поширеним сценарієм використання віддаленого доступу є організація дистанційної або гібридної роботи співробітників, що особливо актуально в умовах розвитку цифрових технологій, коли значна частина компаній переходить на моделі роботи, які не потребують постійної присутності працівників у межах офісної інфраструктури, а доступ до внутрішніх ресурсів здійснюється через мережу Інтернет із використанням захищених каналів зв'язку [3].

У таких умовах виникає необхідність забезпечення доступу до корпоративних сервісів, серед яких можуть бути системи управління базами даних, внутрішні веб-додатки, файлові сервери та інші елементи інфраструктури, що функціонують у межах приватної мережі організації, причому доступ до них повинен здійснюватися із дотриманням вимог безпеки та контролю, оскільки передача даних відбувається через публічні мережі. Водночас важливим аспектом є адміністрування серверної інфраструктури, оскільки системні адміністратори використовують віддалений доступ для управління серверами, мережевим обладнанням та іншими компонентами інформаційної системи, що дозволяє виконувати налаштування, моніторинг та обслуговування інфраструктури без фізичної присутності у місці її розташування [3].

Застосування віддаленого доступу також охоплює сценарії взаємодії між різними підрозділами організації, коли необхідно забезпечити обмін даними між окремими сегментами мережі або доступ до ресурсів, що розташовані у різних частинах інфраструктури, причому такі сценарії часто поєднують доступ користувачів із можливістю роботи із внутрішніми сервісами, що формує єдину екосистему взаємодії між працівниками та ресурсами організації. Таким чином, доступ користувачів і доступ до ресурсів є взаємопов'язаними складовими, які не можуть розглядатися окремо, оскільки ефективність роботи системи залежить від їх узгодженого функціонування.

Вимоги до безпеки, стабільності та масштабованості систем віддаленого доступу. У процесі організації системи віддаленого доступу особлива увага приділяється вимогам до безпеки, оскільки передача даних через відкриті канали зв'язку супроводжується ризиками перехоплення, несанкціонованого доступу або модифікації інформації, що потребує впровадження відповідних механізмів захисту. Однією з основних вимог є забезпечення конфіденційності переданих даних, що досягається шляхом використання криптографічних методів шифрування, які дозволяють захистити інформацію від стороннього доступу навіть у випадку перехоплення мережевого трафіку.

Поряд із забезпеченням конфіденційності важливим елементом є автентифікація користувачів, яка передбачає перевірку достовірності осіб, що здійснюють підключення до системи, використовуючи різні методи, серед яких:

— паролі;
— криптографічні ключі;
— цифрові сертифікати;
— багатофакторні механізми автентифікації.

Все це значно підвищує рівень захисту системи. Наявність таких механізмів дозволяє запобігти несанкціонованому доступу до приватної мережі та забезпечити контроль над використанням її ресурсів, що є критично важливим для організацій, які працюють із конфіденційною інформацією [4].

Не менш важливою вимогою є стабільність функціонування системи віддаленого доступу, оскільки безперервність роботи мережевих сервісів має забезпечуватися навіть у випадках нестабільного з'єднання або підвищеного навантаження на мережу, що вимагає використання технологій, здатних підтримувати надійність з'єднання та мінімізувати затримки у передачі даних. У багатьох випадках також виникає потреба у забезпеченні високої продуктивності системи, що дозволяє ефективно обробляти великий обсяг трафіку та підтримувати одночасну роботу значної кількості користувачів.

Додатковою вимогою є масштабованість системи, яка передбачає можливість її розширення відповідно до зростання кількості користувачів або

мережевих ресурсів, причому таке розширення повинно здійснюватися без суттєвого зниження продуктивності або ускладнення процесу адміністрування. У великих корпоративних мережах, де кількість підключень може постійно збільшуватися, ця характеристика є особливо важливою, оскільки дозволяє адаптувати систему до змін у структурі організації та обсягах її діяльності [4].

Важливим елементом функціонування системи є також забезпечення ефективного управління доступом, моніторингу мережевих з’єднань та ведення журналів подій, що дозволяє відслідковувати активність користувачів, аналізувати роботу системи та своєчасно виявляти потенційні загрози безпеці, при цьому наявність журналів підключень забезпечує можливість проведення аудиту та підвищує рівень контролю над використанням мережевих ресурсів. Сукупність цих вимог формує основу для побудови надійної, безпечної та ефективної системи віддаленого доступу, здатної відповідати сучасним викликам у сфері комп’ютерних мереж.

1.2 Протоколи та технології захищеного мережевого з'єднання

Зі розвитком комп’ютерних мереж та інформаційних систем значна частина мережевої інфраструктури функціонує у середовищі, де поєднуються як відкриті, так і приватні мережі, причому потреба у захисті переданих даних стає особливо актуальною через зростання обсягів інформації, що передається між користувачами та сервісами. Передача даних через публічні канали зв’язку, зокрема через мережу Інтернет, супроводжується ризиками перехоплення, несанкціонованого доступу або модифікації інформації, що створює необхідність використання спеціалізованих технологій для забезпечення конфіденційності та цілісності даних, оскільки у відкритому середовищі відсутні гарантії безпеки без застосування додаткових механізмів захисту.

Принципи роботи VPN-технологій у комп'ютерних мережах. У цьому контексті одним із найбільш ефективних підходів до організації захищеного обміну інформацією є використання технологій віртуальних приватних мереж, які дозволяють створювати захищене середовище передачі даних поверх існуючої мережевої інфраструктури, незалежно від того, чи використовується вона у корпоративних цілях, чи для приватного доступу до ресурсів. Використання таких технологій забезпечує можливість формування захищених каналів зв'язку, які функціонують поверх публічних мереж, створюючи ілюзію прямого підключення до внутрішньої мережі.

VPN-технології базуються на принципі створення захищеного каналу передачі даних між віддаленими вузлами мережі, який реалізується шляхом формування так званого тунелю, що використовується для передачі мережевого трафіку між клієнтом і сервером або між окремими мережами, причому цей тунель забезпечує захист інформації за рахунок використання криптографічних механізмів. У процесі передачі даних інформація перед відправкою у мережу піддається шифруванню, що унеможливлює її прочитання сторонніми особами навіть у випадку перехоплення трафіку, оскільки без відповідного ключа дешифрування отримані дані залишаються недоступними для аналізу [5].

Функціонування VPN-технологій ґрунтується на декількох базових принципах, які визначають їх ефективність та рівень безпеки, серед яких важливе місце займає автентифікація, що дозволяє перевіряти достовірність користувачів або пристроїв перед встановленням з'єднання, забезпечуючи доступ лише для авторизованих учасників системи. Поряд із цим застосовується шифрування даних, яке виконується за допомогою сучасних криптографічних алгоритмів і забезпечує захист інформації від несанкціонованого доступу під час її передачі через мережу [5].

Ще одним важливим принципом є забезпечення цілісності даних, що передбачає використання механізмів контролю, які дозволяють визначити, чи була інформація змінена під час передачі, що є критично важливим для підтримки достовірності переданих даних. Разом із цим використовується тунелювання, яке

передбачає інкапсуляцію мережевих пакетів у спеціальні формати для їх передачі через захищений канал, що дозволяє приховати внутрішню структуру мережевого трафіку та забезпечити його безпечну доставку до кінцевого вузла [5].

У результаті застосування таких принципів формується логічно ізольоване середовище, у межах якого пристрої можуть взаємодіяти між собою так, ніби вони знаходяться в одній локальній мережі, незважаючи на їх фізичну віддаленість, що дозволяє організувати доступ до внутрішніх ресурсів організації незалежно від географічного розташування користувачів. Такий підхід значно розширює можливості використання мережевих сервісів та забезпечує гнучкість у побудові інформаційних систем.

Системи VPN є складними комплексами, що поєднують у собі мережеві протоколи, криптографічні алгоритми та програмне забезпечення, яке забезпечує управління з'єднаннями та обробку мережевого трафіку, причому ефективність їх функціонування залежить від правильності налаштування та інтеграції усіх компонентів. Завдяки своїм характеристикам такі технології широко застосовуються у корпоративних мережах, хмарних інфраструктурах та системах віддаленої роботи, забезпечуючи необхідний рівень безпеки та надійності передачі даних в умовах розвитку інформаційних технологій.

Огляд протоколів IPSec, OpenVPN, SSL VPN. Для реалізації захищеного з'єднання у межах VPN-технологій застосовуються спеціалізовані мережеві протоколи, кожен з яких має власні особливості, переваги, обмеження та специфіку використання, що визначає доцільність їх застосування у конкретних умовах побудови мережевої інфраструктури. Серед найбільш поширених рішень виділяються:

— IPSec;

— OpenVPN;

— SSL VPN.

Всі вони отримали широке застосування у корпоративних і приватних мережах завдяки здатності забезпечувати надійний захист переданих даних (див. табл. 1.1) [6-8].

Таблиця 1.1 – Порівняльна характеристика VPN-протоколів

Параметр	IPSec	OpenVPN	WireGuard
Рівень роботи	Мережевий (L3)	Транспортний (L4)	Мережевий (L3)
Тип шифрування	AES, SHA	SSL/TLS (AES, RSA)	ChaCha20, Poly1305
Продуктивність	Висока	Середня	Дуже висока
Затримки	Низькі	Середні	Мінімальні
Складність конфігурації	Висока	Середня	Низька
Гнучкість	Обмежена	Висока	Середня
Накладні витрати	Значні	Середні	Мінімальні
Рівень безпеки	Високий	Високий	Високий
Підтримка NAT	Обмежена	Добра	Вбудована
Основне застосування	Site-to-site	Remote access	Універсальне

IPSec розглядається як набір протоколів, призначених для забезпечення захищеної передачі інформації на мережевому рівні, що дозволяє реалізувати захист безпосередньо на рівні IP-пакетів незалежно від прикладних сервісів, які використовуються у мережі, завдяки чому досягається універсальність та висока ефективність у різних сценаріях застосування. Архітектура IPSec передбачає використання двох основних компонентів, серед яких протокол автентифікації заголовка забезпечує перевірку цілісності та автентичності даних, а також протокол інкапсуляції захищеного навантаження, який відповідає за шифрування переданої інформації, що дозволяє гарантувати її конфіденційність. Додатково використовується механізм обміну ключами, який забезпечує узгодження криптографічних параметрів між сторонами з’єднання та дозволяє організувати безпечний процес встановлення захищеного каналу. Завдяки своїй архітектурі IPSec широко застосовується для побудови з’єднань типу site-to-site, що дозволяє об’єднувати окремі сегменти мережевої інфраструктури у єдину логічну мережу [6].

OpenVPN представляє собою програмну реалізацію VPN-технології, що використовує протоколи SSL та TLS для створення захищених каналів зв’язку, при цьому функціонування відбувається на транспортному рівні, що забезпечує

гнучкість у налаштуванні та адаптації до різних умов мережевого середовища. Використання стандартних криптографічних бібліотек дозволяє застосовувати широкий спектр алгоритмів шифрування, що підвищує рівень безпеки системи та забезпечує можливість налаштування відповідно до вимог конкретної інфраструктури. Особливістю OpenVPN є можливість роботи як через UDP, так і через TCP, що дозволяє обходити обмеження мережевих екранів та адаптуватися до різних сценаріїв використання, включаючи мережі з жорсткими політиками фільтрації трафіку. Завдяки підтримці різних механізмів автентифікації, систем управління сертифікатами та високій гнучкості конфігурації OpenVPN широко використовується як у корпоративних, так і у приватних системах віддаленого доступу [7].

SSL VPN базується на використанні протоколів SSL або TLS для забезпечення захищеного доступу до мережевих ресурсів, причому однією з його особливостей є можливість встановлення з'єднання без використання спеціалізованого програмного забезпечення на стороні клієнта, оскільки доступ може здійснюватися через стандартний веб-браузер, що значно спрощує процес підключення. Такий підхід дозволяє організувати доступ до внутрішніх веб-додатків та сервісів організації без необхідності встановлення додаткових клієнтських програм, що робить SSL VPN зручним рішенням для користувачів з різними типами пристроїв. Використання стандартних протоколів, зокрема HTTPS, забезпечує високу сумісність із сучасними мережевими інфраструктурами та дозволяє інтегрувати це рішення у вже існуючі системи без значних змін у їх архітектурі [8].

Принципи тунелювання та шифрування мережевого трафіку. Одним із фундаментальних елементів функціонування VPN є механізм тунелювання, який забезпечує передачу мережевих пакетів через іншу мережу у вигляді інкапсульованих даних, що дозволяє створити логічний канал зв'язку між вузлами, незалежно від фізичної структури мережі. У процесі тунелювання вихідний пакет інкапсулюється у новий пакет, який містить додаткову службову інформацію, необхідну для передачі через публічну мережу, після чого передається до кінцевого

вузла, де здійснюється його декапсуляція та відновлення початкових даних для подальшої обробки у внутрішній мережі. Такий підхід дозволяє приховати внутрішню структуру мережевого трафіку та забезпечити його захищену передачу через відкриті канали зв'язку (див. рис. 1.3) [9].



Рисунок 1.3 – Схема тунелювання мережевого трафіку

Поряд із тунелюванням важливе значення має шифрування мережевого трафіку, яке передбачає перетворення відкритих даних у зашифровану форму за допомогою криптографічних алгоритмів, що дозволяє захистити інформацію від несанкціонованого доступу навіть у випадку її перехоплення під час передачі. Використання криптографічних ключів забезпечує можливість як шифрування, так і подальшого розшифрування даних, причому доступ до інформації можуть

отримати лише ті учасники з’єднання, які володіють відповідними ключами (див. рис. 1.4) [9].

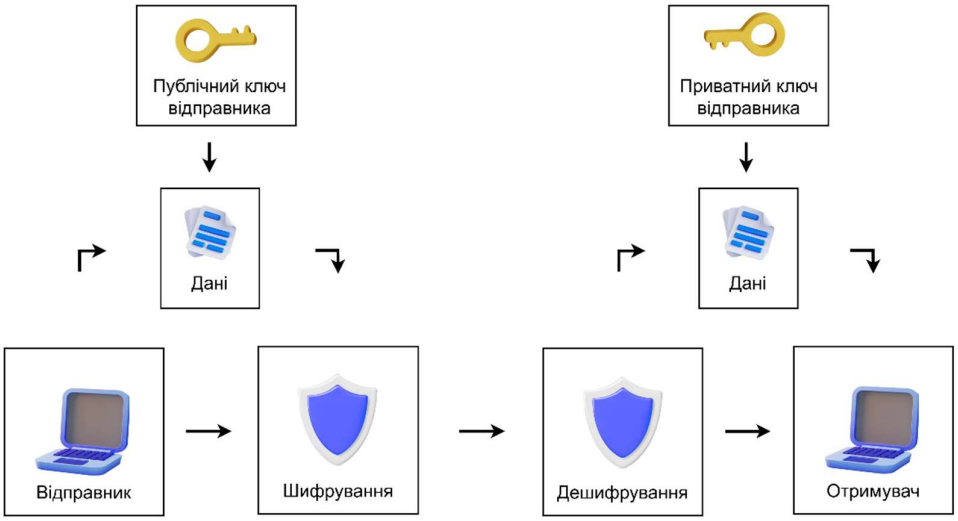


Рисунок 1.4 – Процес шифрування та дешифрування даних

Додатково застосовуються механізми перевірки цілісності даних, які дозволяють виявити будь-які зміни інформації під час передачі, використовуючи криптографічні хеш-функції та спеціальні коди автентичності, що забезпечує контроль над достовірністю переданих даних та підвищує рівень загальної безпеки системи. Сукупність зазначених механізмів формує основу функціонування сучасних VPN-рішень, забезпечуючи захищену, надійну та ефективну передачу інформації у комп’ютерних мережах різного масштабу [9].

Використання сучасних криптографічних алгоритмів у VPN. Криптографічні алгоритми становлять фундаментальну основу забезпечення безпеки у VPN, оскільки саме завдяки їх використанню реалізується захист даних під час передачі через публічні мережі, де існує високий ризик перехоплення, несанкціонованого доступу або модифікації інформації. У межах VPN-з’єднань криптографічні механізми застосовуються для виконання декількох ключових функцій, серед яких:

— шифрування даних;

— обмін ключами;

— автентифікація учасників з’єднання;

— контроль цілісності переданої інформації.

Все це у сукупності дозволяє сформувати надійне та захищене середовище передачі даних [10].

Сучасні VPN-системи використовують різні типи криптографічних алгоритмів, які можна класифікувати на:

— симетричні;

— асиметричні;

— хеш-функції.

Причому кожен із цих типів виконує окрему функцію у процесі забезпечення безпеки з’єднання. Симетричні алгоритми передбачають використання одного і того самого ключа для шифрування та розшифрування даних, що забезпечує високу швидкість обробки інформації та ефективність при передачі великих обсягів трафіку. Одним із найбільш поширених алгоритмів цього типу є стандарт шифрування AES, який широко застосовується у різних системах захисту інформації завдяки своїй надійності та продуктивності, що робить його оптимальним вибором для використання у VPN-з’єднаннях [10].

Асиметричні алгоритми базуються на використанні пари ключів, відкритого та закритого, що дозволяє реалізувати безпечний обмін криптографічними ключами між учасниками з’єднання, а також забезпечити автентифікацію сторін, які встановлюють з’єднання. У межах VPN-технологій такі алгоритми застосовуються переважно на етапі встановлення з’єднання, коли необхідно узгодити параметри шифрування та сформувати спільний секретний ключ для подальшого використання у симетричних алгоритмах. Серед найбільш відомих алгоритмів цього типу виділяються RSA та алгоритми на основі еліптичних кривих, які забезпечують високий рівень безпеки при відносно невеликій довжині ключів, що позитивно впливає на продуктивність системи [10].

Для забезпечення цілісності даних використовуються криптографічні хеш-функції, які перетворюють вхідні дані у фіксований за довжиною унікальний хеш-код, що змінюється навіть при незначній зміні вихідної інформації, що дозволяє

виявити будь-які спроби модифікації даних під час їх передачі. У VPN-системах часто застосовуються алгоритми сімейства SHA-2 або SHA-3, які забезпечують високий рівень надійності та стійкість до сучасних криптографічних атак [10].

Окрему роль у забезпеченні безпеки VPN-з'єднань відіграють алгоритми обміну ключами, серед яких широко використовується алгоритм Діффі-Хеллмана та його модифікації, зокрема варіанти на основі еліптичних кривих, які дозволяють сторонам з'єднання сформувати спільний секретний ключ навіть у разі передачі даних через відкриту мережу. Такий підхід забезпечує можливість безпечного узгодження параметрів шифрування без необхідності попереднього обміну секретною інформацією, що значно підвищує рівень захисту системи [10].

Поєднання симетричних, асиметричних алгоритмів та хеш-функцій дозволяє створити комплексну систему криптографічного захисту, яка забезпечує конфіденційність, цілісність та автентичність даних у процесі їх передачі, що є необхідною умовою функціонування сучасних VPN-технологій (див. рис. 1.5).

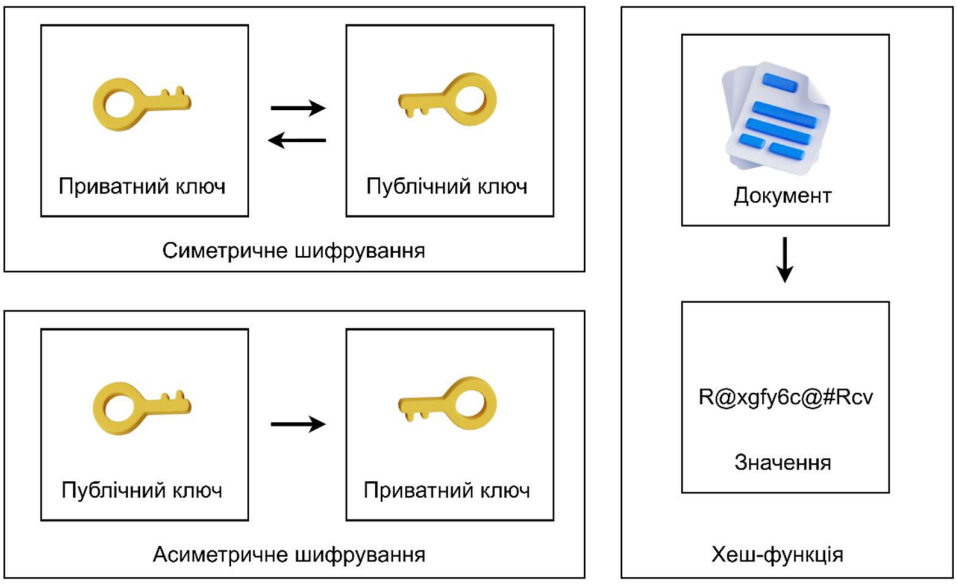


Рисунок 1.5 – Використання криптографічних алгоритмів у VPN

Наявність таких механізмів дозволяє ефективно протидіяти відомим мережевим атакам, забезпечуючи високий рівень безпеки навіть у складних умовах

функціонування інформаційних систем, де передача даних здійснюється через публічні канали зв’язку.

1.3 Архітектура сучасних систем захищеного доступу

Сучасні системи захищеного доступу формуються в умовах складної та багаторівневої мережевої інфраструктури, яка включає сервери, мережеві пристрої, бази даних, прикладні сервіси та інші компоненти інформаційного середовища, що функціонують у межах приватних мереж організацій або окремих користувачів, причому така інфраструктура часто є розподіленою та може охоплювати різні фізичні локації, що ускладнює організацію доступу до ресурсів. У таких умовах виникає необхідність забезпечення безпечної взаємодії користувачів із внутрішніми сервісами незалежно від їх місцезнаходження, що досягається шляхом впровадження систем віддаленого доступу, архітектура яких передбачає інтеграцію програмних і апаратних компонентів, що взаємодіють між собою для створення єдиного захищеного середовища.

Організація доступу до приватної мережі передбачає врахування того, що значна частина користувачів може знаходитися поза межами цієї мережі, при цьому необхідність отримання доступу до внутрішніх ресурсів зберігається, що створює потребу у використанні спеціалізованих механізмів, здатних забезпечити захищене підключення через публічні канали зв’язку. Такий підхід дозволяє розширити межі приватної інфраструктури, створюючи логічне середовище, у якому віддалені користувачі можуть взаємодіяти з ресурсами так, ніби вони фізично знаходяться у межах локальної мережі.

Структура систем віддаленого доступу у приватних мережах. Типова структура системи віддаленого доступу включає декілька взаємопов’язаних компонентів, серед яких виділяються:

— сервер доступу;

— клієнтські пристрої;

— мережеві шлюзи;

— системи автентифікації;

— внутрішні ресурси.

Причому кожен із цих елементів виконує визначену функцію та забезпечує узгоджену роботу всієї системи. Центральним елементом виступає сервер доступу або VPN-шлюз, який є основною точкою входу до мережі та приймає запити на підключення від клієнтських пристроїв, виконуючи перевірку облікових даних користувачів і забезпечуючи встановлення захищеного з'єднання у разі успішної автентифікації [11].

Клієнтські пристрої, які можуть бути представлені як:

— персональними комп'ютерами;

— ноутбуками;

— мобільними пристроями;

— іншими мережевими вузлами.

Всі вони виступають кінцевими точками доступу до системи та використовують спеціалізоване програмне забезпечення або вбудовані засоби операційних систем для встановлення захищеного з'єднання із сервером доступу. Використання таких засобів дозволяє забезпечити взаємодію між клієнтом і сервером через захищений канал, що створює умови для безпечного обміну даними.

У межах системи також використовуються мережеві шлюзи та інші інфраструктурні компоненти, які забезпечують маршрутизацію трафіку та взаємодію між різними сегментами мережі, що є особливо важливим у випадках, коли інфраструктура має складну структуру та складається з декількох підмереж. Системи автентифікації виконують функцію перевірки користувачів, забезпечуючи контроль доступу до ресурсів та запобігаючи несанкціонованому підключенню [11].

Внутрішні ресурси, до яких здійснюється доступ, можуть включати:

— файлові сервери;

— бази даних;

— веб-сервіси;

— інші прикладні компоненти.

Причому доступ до них повинен бути організований таким чином, щоб забезпечити як зручність використання, так і високий рівень безпеки. У результаті взаємодії всіх зазначених компонентів формується єдина система, яка дозволяє користувачам отримувати доступ до ресурсів приватної мережі через захищене з'єднання.

Роль серверів автентифікації, шлюзів та мережевих вузлів. Сервери автентифікації у системах захищеного доступу формують один із базових елементів, що забезпечує перевірку облікових даних користувачів та контроль їхнього доступу до ресурсів приватної мережі, при цьому саме через механізми автентифікації здійснюється ідентифікація кожного суб'єкта перед наданням можливості підключення до внутрішньої інфраструктури, що дозволяє обмежити доступ лише для авторизованих користувачів та знизити ризики несанкціонованого проникнення. Використання таких серверів передбачає застосування різноманітних методів перевірки, серед яких можуть використовуватися:

— паролі;

— криптографічні ключі;

— багатофакторна автентифікація;

— цифрові сертифікати.

Все це забезпечує гнучкість у виборі рівня захисту відповідно до вимог конкретної системи, а також дозволяє адаптувати політики доступу до різних категорій користувачів [12].

У корпоративних середовищах часто застосовуються централізовані служби автентифікації, які реалізують єдину точку управління обліковими записами та дозволяють ефективно адмініструвати доступ до ресурсів, що значно спрощує підтримку великої кількості користувачів та забезпечує узгодженість політик безпеки у межах всієї інфраструктури. Такий підхід дозволяє інтегрувати різні компоненти системи у єдине середовище керування ідентифікацією, що підвищує рівень контролю над доступом та спрощує процес адміністрування.

Мережеві шлюзи у цій архітектурі виконують функцію посередника між зовнішніми мережами та внутрішньою інфраструктурою, забезпечуючи прийом запитів на підключення, їхню обробку та подальшу передачу до відповідних компонентів системи, при цьому саме через шлюз здійснюється організація взаємодії між клієнтськими пристроями та ресурсами приватної мережі. У випадку використання VPN-технологій шлюзи також виконують функції шифрування та дешифрування мережевого трафіку, що дозволяє забезпечити захист даних під час їх передачі через публічні канали зв’язку, причому весь трафік, який проходить між клієнтом і внутрішньою мережею, обробляється через цей компонент, що дозволяє централізувати контроль над передачею інформації [12].

Передача даних через шлюз супроводжується перетворенням інформації у зашифровану форму перед відправленням у публічну мережу та зворотним процесом при отриманні, що забезпечує конфіденційність та цілісність даних, а також унеможливлює їх використання сторонніми особами навіть у випадку перехоплення трафіку. Такий механізм дозволяє створити захищений канал зв’язку між віддаленими користувачами та внутрішньою інфраструктурою без необхідності прямого відкритого доступу до ресурсів.

Мережеві вузли, до яких належать маршрутизатори, комутатори та сервери, забезпечують функціонування всієї системи шляхом організації передачі даних між різними сегментами мережі, виконуючи задачі маршрутизації, комутації та обробки інформації, що дозволяє забезпечити ефективну взаємодію між клієнтами та ресурсами. Вони формують основу мережевої інфраструктури, через яку проходить трафік, і забезпечують його коректне спрямування відповідно до визначених правил (див. рис. 1.6).

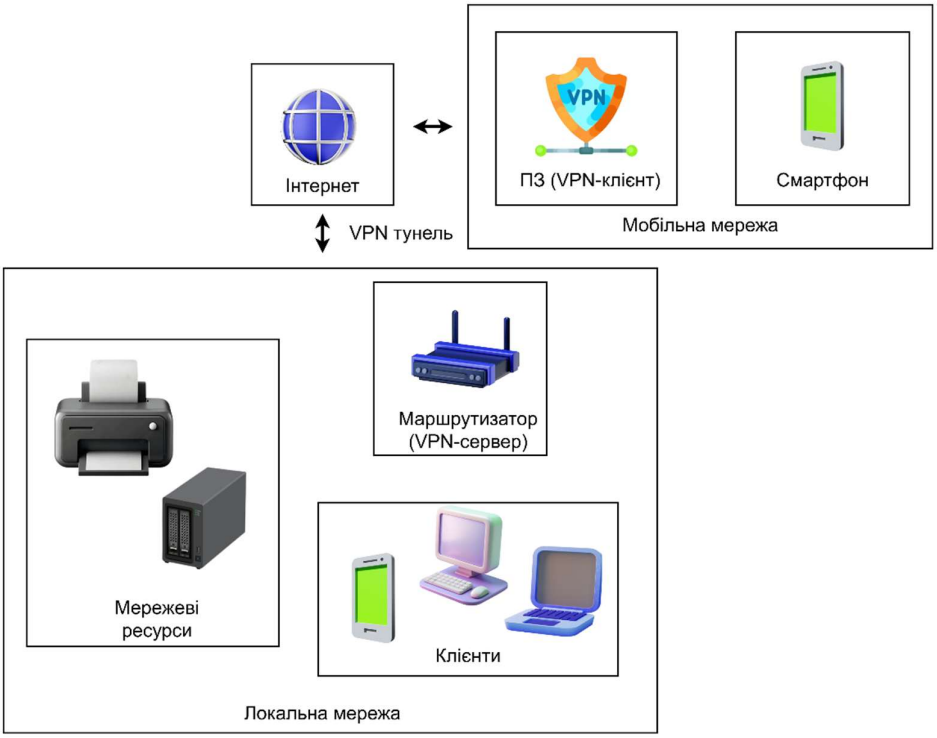


Рисунок 1.6 – Взаємодія мережевих вузлів у VPN-системі

Узгоджена взаємодія серверів автентифікації, мережевих шлюзів та інших мережевих вузлів дозволяє сформувати комплексну систему захищеного доступу, у якій забезпечується контроль доступу, захист даних та стабільність функціонування, що є необхідною умовою для ефективної роботи сучасних інформаційних систем, орієнтованих на використання віддаленого доступу до приватної інфраструктури.

1.4 Методи забезпечення безпеки мережевого доступу

Організація віддаленого доступу до приватної мережевої інфраструктури супроводжується необхідністю забезпечення високого рівня безпеки, оскільки передача даних відбувається через публічні канали зв’язку, що створює потенційні ризики перехоплення, несанкціонованого доступу та модифікації інформації, у

зв’язку з чим будь-яка система такого типу повинна базуватися на комплексному підході до захисту, який включає використання механізмів автентифікації, авторизації, криптографічних засобів, а також мережевих технологій захисту. Забезпечення безпеки передбачає не лише захист даних під час передачі, але й контроль доступу до ресурсів, моніторинг активності користувачів та впровадження засобів протидії сучасним загрозам, що формує багаторівневу систему захисту приватної інфраструктури.

Механізми автентифікації та авторизації користувачів. У структурі такої системи одним із базових елементів виступають механізми автентифікації та авторизації, які дозволяють визначити особу користувача або пристрою, що намагається отримати доступ до ресурсів, а також встановити рівень дозволених дій у межах системи. Автентифікація розглядається як процес підтвердження ідентичності, під час якого перевіряється відповідність наданих облікових даних тим, що зберігаються у системі, що дозволяє визначити, чи є користувач тим, за кого себе видає, перед наданням доступу до мережевих ресурсів.

У традиційних системах найбільш поширеним методом автентифікації тривалий час залишалося використання паролів, які представляють собою унікальні комбінації символів, що зберігаються у зашифрованому вигляді та використовуються для перевірки доступу, проте сучасні умови експлуатації інформаційних систем показали обмеженість такого підходу через його вразливість до різних типів атак, зокрема підбору паролів або їх компрометації. З урахуванням цих обмежень сучасні системи переходять до більш надійних методів, серед яких широкого застосування набуває багатофакторна автентифікація, яка передбачає використання декількох незалежних факторів підтвердження особи, що значно підвищує рівень захисту [13].

У межах багатофакторної автентифікації можуть використовуватися різні типи факторів, зокрема знання користувача у вигляді пароля, наявність фізичного пристрою, наприклад апаратного токена або мобільного телефону для отримання одноразових кодів, а також біометричні характеристики, що дозволяє забезпечити більш надійний контроль доступу та знизити ризик несанкціонованого входу до

системи. Такий підхід дозволяє компенсувати слабкі сторони окремих методів за рахунок їх комбінування [13].

Після успішного проходження етапу автентифікації система переходить до процесу авторизації, який визначає, які саме дії дозволені користувачу у межах мережевої інфраструктури, причому різні користувачі можуть мати різні рівні доступу залежно від їх ролі, функцій або політик безпеки, що застосовуються у конкретній організації. Наприклад, один користувач може мати доступ лише до файлових ресурсів, інший — до баз даних або адміністративних сервісів, що дозволяє реалізувати принцип розмежування доступу та мінімізації привілеїв (див. рис. 1.7) [13].



Рисунок 1.7 – Механізм автентифікації та авторизації користувача

У корпоративних системах авторизація часто реалізується за допомогою централізованих систем управління доступом, які дозволяють визначати ролі користувачів, встановлювати політики доступу та контролювати взаємодію з ресурсами мережі, що значно спрощує адміністрування та забезпечує узгодженість правил безпеки. Використання таких систем дозволяє централізовано керувати доступом до різних сегментів мережі та оперативно змінювати політики у разі необхідності.

Використання криптографічних ключів та сертифікатів. Поряд із механізмами автентифікації та авторизації, що визначають ідентичність користувачів та їх права доступу, важливим елементом забезпечення безпеки мережевого доступу виступають криптографічні механізми, які дозволяють захистити дані під час передачі через публічні канали зв’язку, серед яких особливе

місце займають криптографічні ключі та цифрові сертифікати, що забезпечують високий рівень конфіденційності та довіри між учасниками з'єднання. Використання таких засобів дозволяє створити захищене середовище передачі інформації, у якому навіть у випадку перехоплення трафіку сторонні особи не можуть отримати доступ до змісту переданих даних.

Криптографічні ключі являють собою спеціалізовані набори даних, які застосовуються для шифрування та розшифрування інформації, причому їх використання дозволяє створювати захищені канали зв'язку між клієнтами та серверами або між окремими вузлами мережі, що забезпечує конфіденційність переданих даних. У сучасних системах використовуються як симетричні, так і асиметричні ключі, кожен з яких виконує визначену функцію у процесі захисту інформації [14].

Симетричні ключі передбачають використання одного і того самого ключа для шифрування та розшифрування даних, що забезпечує високу швидкість обробки інформації та ефективність при передачі великих обсягів трафіку, що робить їх доцільними для використання у процесі безпосередньої передачі даних у межах VPN-з'єднання. Асиметричні ключі, у свою чергу, базуються на використанні пари ключів, відкритого та закритого, де відкритий ключ може бути доступний іншим учасникам, а закритий зберігається у таємниці, що дозволяє реалізувати безпечний обмін інформацією навіть через відкриті мережі без ризику компрометації даних [14].

Цифрові сертифікати використовуються для підтвердження автентичності криптографічних ключів та ідентифікації учасників з'єднання, при цьому вони видаються спеціалізованими центрами сертифікації та містять інформацію про власника ключа, що дозволяє перевірити його достовірність. Використання сертифікатів дозволяє сформувати інфраструктуру довіри, у межах якої кожен учасник з'єднання може переконатися у справжності іншої сторони, що особливо важливо при встановленні з'єднань через публічні мережі, де існує ризик підміни вузлів або перехоплення даних [14].

Захист від атак типу MITM, brute-force та несанкціонованого доступу. Системи віддаленого доступу, що функціонують через публічні мережі, піддаються різноманітним кіберзагрозам, серед яких значну небезпеку становлять:

— атаки типу «людина посередині»;

— атаки підбору облікових даних;

— спроби несанкціонованого доступу.

Атака типу MITM передбачає перехоплення мережевого трафіку між двома сторонами з'єднання, при якому зловмисник розміщується між клієнтом і сервером, отримуючи можливість перехоплювати, змінювати або підміняти передані дані, що може призвести до витоку конфіденційної інформації та порушення цілісності системи (див. рис. 1.8) [10].



Рисунок 1.8 – Приклад атаки типу MITM

Для протидії таким атакам застосовуються механізми шифрування та перевірки автентичності, які дозволяють гарантувати, що встановлюється з'єднання саме з легітимним сервером, а не з підробленим вузлом, при цьому використання цифрових сертифікатів дозволяє перевірити достовірність сервера перед початком обміну даними, що значно знижує ризик реалізації подібних атак.

Атаки типу brute-force базуються на багаторазових спробах підбору паролів або ключів доступу шляхом перебору можливих комбінацій, причому для цього часто використовуються автоматизовані інструменти, що дозволяють здійснювати велику кількість спроб за короткий проміжок часу. Для захисту від таких атак застосовуються різні методи, серед яких:

1. обмеження кількості спроб входу;
2. використання складних паролів;
3. впровадження багатофакторної автентифікації;
4. впровадження систем моніторингу активності.

Все це дозволяє виявляти підозрілу поведінку та своєчасно реагувати на потенційні загрози [10].

Захист від несанкціонованого доступу до ресурсів мережі забезпечується за допомогою механізмів контролю доступу, які визначають, які саме дії може виконувати користувач у межах системи, при цьому доступ надається лише у межах визначених політик, а будь-які спроби порушення цих правил блокуються системою. Такий підхід дозволяє забезпечити контроль над використанням ресурсів та запобігти несанкціонованим діям, що є необхідною умовою функціонування захищених систем віддаленого доступу у сучасних мережевих середовищах.

Роль мережевих екранів, NAT та сегментації мережі. Забезпечення безпеки мережевого доступу не обмежується використанням криптографічних механізмів, а також систем автентифікації та авторизації, оскільки важливим аспектом виступає контроль на рівні мережевих протоколів і інфраструктурних технологій, де застосовуються такі засоби, як:

— мережеві екрани;
— трансляція мережевих адрес;
— сегментація мережі.

Все це дозволяє сформувати додатковий рівень захисту та зменшити ризики несанкціонованого доступу до внутрішніх ресурсів.

Мережеві екрани, більш відомі як firewall, представляють собою спеціалізовані програмні або апаратні рішення, які здійснюють контроль мережевого трафіку між різними сегментами інфраструктури, аналізуючи пакети даних та приймаючи рішення щодо їх пропуску або блокування відповідно до визначених правил безпеки, що дозволяє обмежити доступ до внутрішніх ресурсів лише для авторизованих користувачів і запобігти проникненню сторонніх осіб у мережу. Функціонування таких систем базується на фільтрації трафіку за різними параметрами, зокрема IP-адресами, портами, протоколами та іншими характеристиками, що дозволяє реалізувати гнучку політику безпеки відповідно до вимог конкретної інфраструктури [15].

Застосування мережевих екранів дозволяє не лише контролювати доступ до ресурсів, але й виявляти підозрілу активність, блокуючи потенційно небезпечні запити ще на етапі їх надходження, що значно знижує ймовірність реалізації атак та підвищує загальний рівень захищеності системи. Такий підхід забезпечує додатковий рівень контролю, який доповнює інші механізми безпеки та дозволяє ефективно реагувати на загрози.

Технологія трансляції мережевих адрес використовується для перетворення внутрішніх IP-адрес у зовнішні під час передачі даних через публічні мережі, що дозволяє приховати реальну структуру приватної мережі від зовнішніх користувачів, унаслідок чого зменшується ймовірність прямого доступу до внутрішніх вузлів. Такий підхід дозволяє ізолювати внутрішню інфраструктуру від зовнішнього середовища, забезпечуючи додатковий рівень захисту та ускладнюючи процес ідентифікації окремих вузлів з боку потенційних зловмисників [15].

При використанні NAT зовнішній світ взаємодіє лише з обмеженою кількістю публічних адрес, що виступають у ролі посередників між внутрішньою мережею та інтернетом, що дозволяє централізувати контроль над мережевими з’єднаннями та обмежити доступ до внутрішніх ресурсів. Така архітектура забезпечує підвищення рівня безпеки без необхідності відкритого доступу до кожного окремого вузла мережі (див. рис. 1.9) [15].

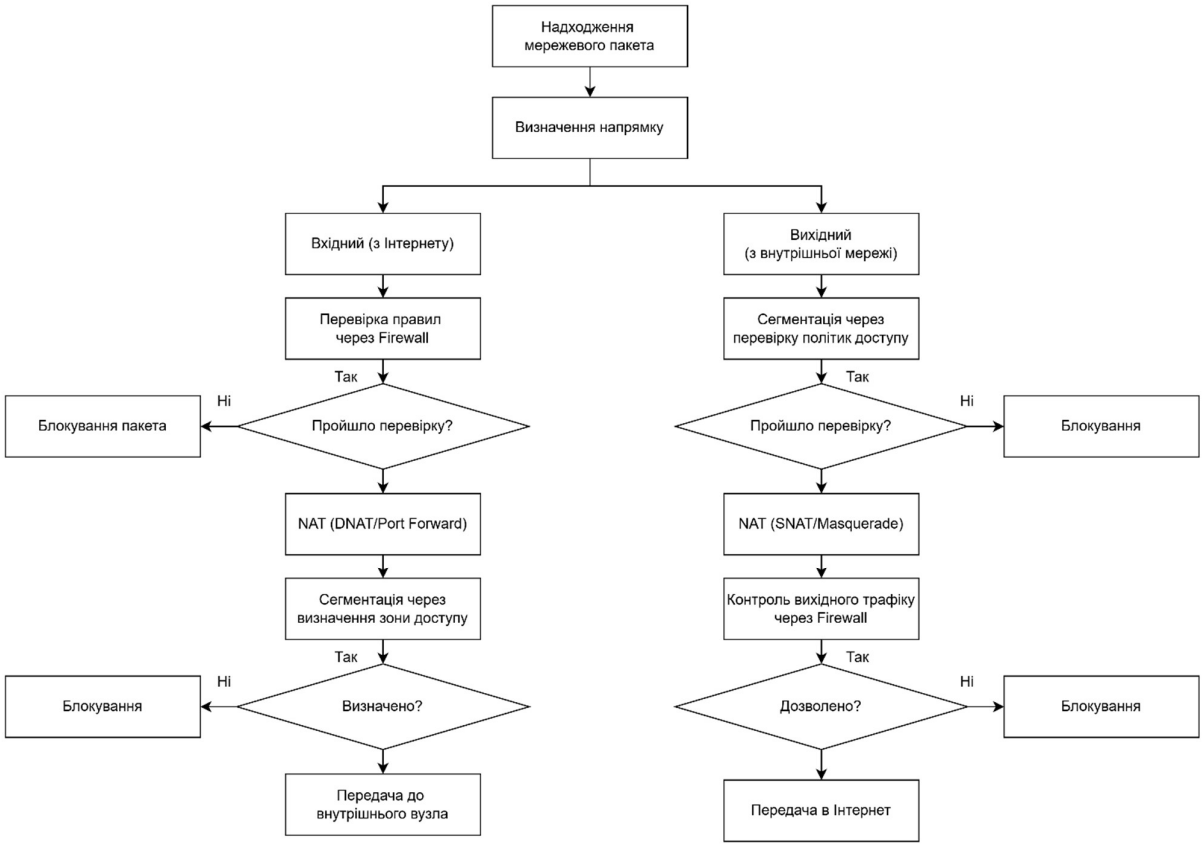


Рисунок 1.9 – Робота мережевого екрану та NAT

Сегментація мережі передбачає поділ єдиної інфраструктури на окремі ізольовані сегменти, які можуть бути реалізовані, зокрема, за допомогою віртуальних локальних мереж, що дозволяє розмежувати доступ до ресурсів та встановити окремі політики безпеки для кожного сегмента. У такій структурі кожна група користувачів або сервісів функціонує у власному ізольованому середовищі, що дозволяє обмежити доступ до критичних ресурсів та зменшити площу потенційного впливу у разі виникнення інциденту безпеки [15].

Поділ мережі на сегменти дозволяє локалізувати можливі загрози, оскільки навіть у випадку компрометації одного сегмента доступ до інших частин інфраструктури залишається обмеженим, що значно знижує ризик масштабного поширення атаки. Такий підхід широко використовується у корпоративних мережах, де необхідно забезпечити різні рівні доступу для різних категорій

користувачів та сервісів, а також підвищити загальний рівень захисту інформаційної системи.

1.5 Аналіз сучасних інструментів реалізації систем віддаленого доступу

Організація віддаленого доступу до приватних мереж у сучасних умовах розвитку інформаційних технологій тісно пов’язана з використанням спеціалізованих програмних інструментів, які дозволяють створювати захищені канали зв’язку між користувачами та внутрішніми ресурсами мережевої інфраструктури, при цьому доступ здійснюється через публічні мережі, зокрема інтернет, що потребує впровадження додаткових механізмів безпеки, контролю та управління з’єднаннями, оскільки передача даних у відкритому середовищі завжди супроводжується ризиками перехоплення, модифікації або несанкціонованого доступу.

У цьому контексті сучасні програмні рішення для реалізації систем віддаленого доступу базуються на використанні технологій віртуальних приватних мереж, які дозволяють формувати логічно ізольовані канали передачі даних, що функціонують поверх існуючої мережевої інфраструктури, забезпечуючи при цьому конфіденційність, цілісність та автентичність переданої інформації, а також контроль доступу до внутрішніх ресурсів приватної мережі.

Огляд популярних програмних рішень для реалізації VPN-систем. Серед найбільш поширених програмних рішень можна виділити OpenVPN, який є універсальним інструментом з відкритим вихідним кодом і використовує протоколи SSL та TLS для організації захищеного з’єднання, при цьому підтримується широкий спектр операційних систем, що робить його гнучким рішенням для різних середовищ, а також IPSec, який реалізується як набір протоколів і часто інтегрується безпосередньо у мережеве обладнання, забезпечуючи захист на мережевому рівні та дозволяючи організовувати тунелі між

різними сегментами мережі, що особливо актуально для корпоративних інфраструктур [16].

Окрім класичних рішень, активно розвиваються сучасні технології, орієнтовані на спрощення налаштування та підвищення продуктивності, серед яких варто відзначити WireGuard, що характеризується компактною реалізацією, високою швидкодією та використанням сучасних криптографічних алгоритмів, а також такі інструменти як ZeroTier і Tailscale, які базуються на концепції програмно-визначених мереж і дозволяють об’єднувати пристрої незалежно від їх фізичного розташування або мережевих обмежень, створюючи єдину віртуальну інфраструктуру [16].

Порівняння open-source та комерційних систем віддаленого доступу. Порівняння open-source та комерційних систем віддаленого доступу дозволяє виявити суттєві відмінності у підходах до їх використання, оскільки рішення з відкритим вихідним кодом забезпечують високу гнучкість, можливість модифікації та відсутність ліцензійних обмежень, що робить їх привабливими для невеликих організацій, навчальних середовищ або індивідуального використання, при цьому такі рішення потребують глибоких технічних знань для налаштування та подальшого адміністрування, що може ускладнювати їх впровадження.

Комерційні системи, навпаки, орієнтовані на забезпечення максимальної зручності використання, інтеграції з корпоративними сервісами та централізованого управління, що досягається за рахунок використання спеціалізованих інтерфейсів, автоматизованих механізмів конфігурації та наявності технічної підтримки, однак використання таких рішень пов’язане з фінансовими витратами, які можуть зростати залежно від масштабів інфраструктури та кількості користувачів [17].

У процесі вибору конкретного інструменту для реалізації системи віддаленого доступу необхідно враховувати не лише вартість та складність впровадження, але й рівень безпеки, продуктивність, масштабованість та сумісність з існуючими компонентами мережевої інфраструктури, оскільки кожне

рішення має власні особливості реалізації тунелювання, механізмів шифрування та управління доступом.

Окремої уваги заслуговують можливості використання сучасних протоколів тунелювання, які забезпечують ефективну передачу даних через публічні мережі шляхом інкапсуляції мережевих пакетів у захищений контейнер, що дозволяє створювати логічні канали зв'язку між вузлами незалежно від їх фізичного розташування, при цьому сучасні протоколи орієнтовані на мінімізацію накладних витрат, підвищення швидкості передачі та спрощення конфігурації, що є важливим фактором для динамічних мережевих середовищ [17].

Використання WireGuard як основи системи віддаленого доступу обґрунтовується його архітектурними особливостями, які передбачають мінімалістичний підхід до реалізації функціональності, завдяки чому досягається висока продуктивність та зниження ймовірності виникнення вразливостей, оскільки менший обсяг програмного коду спрощує аудит безпеки та зменшує поверхню атаки [17].

Можливості використання сучасних протоколів тунелювання. У сучасних комп'ютерних мережах організація захищеного віддаленого доступу безпосередньо пов'язана з використанням протоколів тунелювання, які забезпечують передачу даних через публічні мережі у захищеному вигляді, при цьому сама передача інформації відбувається таким чином, що зовнішня мережа фактично не має доступу до внутрішнього вмісту пакетів, оскільки вони інкапсулюються та шифруються перед відправкою, що дозволяє формувати логічно ізольовані канали зв'язку між різними вузлами незалежно від їх фізичного розташування.

У процесі функціонування таких протоколів ключовим механізмом виступає інкапсуляція мережевих пакетів, при якій вихідні дані, сформовані на рівні прикладних або транспортних протоколів, поміщаються всередину нового пакету, що містить службову інформацію для передачі через публічну мережу, при цьому зовнішній пакет може використовувати іншу схему адресації, що дозволяє забезпечити сумісність між різними мережами навіть у випадку використання

приватних IP-адрес або наявності мережевих екранів і механізмів трансляції адрес [18].

Такий підхід дозволяє реалізувати універсальний механізм взаємодії між віддаленими сегментами мережі, коли різні вузли можуть обмінюватися даними так, ніби вони знаходяться в межах єдиної локальної інфраструктури, що є особливо важливим для корпоративних систем, де ресурси можуть бути розподілені між декількома географічно віддаленими локаціями.

Різні протоколи тунелювання реалізують цей механізм на різних рівнях моделі взаємодії мережевих систем, що визначає їх функціональні можливості та сферу застосування, наприклад рішення, побудовані на основі IPSec, працюють на мережевому рівні та забезпечують захист IP-пакетів незалежно від прикладних протоколів, у той час як OpenVPN функціонує на транспортному рівні, використовуючи можливості протоколів SSL та TLS для створення захищених каналів передачі даних [18].

Подальший розвиток технологій тунелювання призвів до появи більш оптимізованих рішень, орієнтованих на підвищення продуктивності та спрощення конфігурації, серед яких особливе місце займає WireGuard, що використовує сучасні криптографічні алгоритми та мінімалістичну архітектуру, завдяки чому досягається значне зменшення затримок і підвищення швидкості передачі даних у порівнянні з традиційними VPN-рішеннями.

Важливою характеристикою сучасних протоколів тунелювання є їх здатність ефективно працювати в умовах обмежених ресурсів, що дозволяє використовувати їх не лише на серверних системах, але й на мобільних пристроях, вбудованих системах та мережевому обладнанні, при цьому оптимізація обробки пакетів і використання ефективних алгоритмів шифрування дозволяють зменшити навантаження на процесор та пам’ять [18].

Ще однією важливою особливістю є можливість гнучкого налаштування маршрутів передачі даних через тунель, що дозволяє реалізувати як повне тунелювання, при якому весь трафік користувача проходить через захищений канал, так і роздільне тунелювання, коли через VPN передається лише частина

трафіку, наприклад доступ до внутрішніх ресурсів, у той час як інші запити обробляються через звичайне інтернет-з’єднання [18].

Застосування сучасних протоколів тунелювання також дозволяє вирішувати проблему обходу мережевих обмежень, пов’язаних з використанням NAT або міжмережевих екранів, оскільки інкапсульований трафік може передаватися через стандартні порти та протоколи, що значно спрощує встановлення з’єднання навіть у складних мережевих умовах.

Обґрунтування вибору технології WireGuard як основи системи. У контексті вибору технології для реалізації системи віддаленого доступу важливим є врахування таких параметрів як рівень безпеки, продуктивність, складність налаштування та сумісність з існуючою інфраструктурою, при цьому сучасні вимоги до мережевих систем передбачають необхідність забезпечення високої швидкодії при одночасному збереженні високого рівня захисту переданих даних.

З огляду на ці вимоги технологія WireGuard розглядається як одна з найбільш перспективних для побудови систем віддаленого доступу, оскільки вона поєднує у собі простоту реалізації, високу ефективність та сучасні підходи до забезпечення безпеки, при цьому її архітектура передбачає використання обмеженого набору криптографічних примітивів, що дозволяє уникнути складності конфігурації та зменшити ймовірність помилок під час налаштування [19].

Додатковою перевагою є компактність програмного коду, що значно спрощує аудит безпеки та зменшує поверхню потенційних атак, оскільки менша кількість рядків коду означає меншу ймовірність наявності вразливостей, що особливо важливо для систем, які працюють у середовищі підвищених ризиків.

Використання сучасних криптографічних алгоритмів, зокрема ChaCha20 для шифрування та Poly1305 для перевірки цілісності даних, забезпечує високий рівень захисту інформації навіть при роботі на пристроях з обмеженими ресурсами, що дозволяє застосовувати дану технологію у широкому спектрі сценаріїв від мобільних клієнтів до серверних інфраструктур [19].

Важливим аспектом є також швидкість встановлення з’єднання, оскільки WireGuard використовує спрощений механізм обміну ключами та мінімізує

кількість необхідних етапів ініціалізації тунелю, що дозволяє значно скоротити час підключення та підвищити стабільність роботи у випадках нестабільного мережевого середовища [19].

Простота конфігурації також є значною перевагою, оскільки налаштування з’єднання зводиться до визначення базових параметрів, таких як криптографічні ключі, адреси вузлів та правила маршрутизації, що значно спрощує процес розгортання системи навіть у великих мережах з великою кількістю користувачів.

Підтримка різних операційних систем та платформ забезпечує універсальність використання даної технології, що дозволяє інтегрувати її у різноманітні мережеві середовища без необхідності суттєвих змін існуючої інфраструктури, при цьому можливість роботи як у режимі клієнт-сервер, так і у форматі з’єднань між мережами розширює сферу застосування.

З урахуванням усіх зазначених характеристик вибір WireGuard як основи системи віддаленого доступу обґрунтовується його здатністю забезпечувати високий рівень безпеки, продуктивності та зручності використання одночасно, що відповідає сучасним вимогам до побудови ефективних і надійних мережевих рішень, особливо в умовах зростання кількості віддалених підключень та необхідності забезпечення стабільного доступу до приватних ресурсів у глобальному середовищі.

2. ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ НА БАЗІ ГРАНИЧНОГО МАРШРУТИЗАТОРА

2.1 Архітектура мережі та концепція апаратного вузла доступу

Побудова системи віддаленого доступу до приватної інфраструктури неможлива без чіткого формулювання архітектури, яка охоплює не лише логічну організацію мережі, але й фізичні аспекти розгортання обладнання, включаючи його розміщення, канали зв’язку та обчислювальні можливості, що безпосередньо впливають на стабільність і безпеку функціонування всієї системи, при цьому сучасні підходи дедалі більше орієнтуються на інтеграцію функцій захисту безпосередньо у мережеві вузли, що дозволяє перенести механізми контролю доступу, фільтрації трафіку та шифрування на периферію мережі, формуючи концепцію "edge computing", у рамках якої обробка даних та прийняття рішень здійснюється максимально близько до джерела трафіку, що зменшує затримки та підвищує ефективність використання мережевих ресурсів, у результаті така модель дозволяє поєднати в одному пристрої функції маршрутизації, криптографічного захисту та централізованого управління доступом, що відповідає сучасним тенденціям розвитку розподілених інформаційних систем і забезпечує більш високий рівень контролю над потоками даних.

У рамках даної архітектури ключовим елементом виступає граничний маршрутизатор, який виконує роль VPN-шлюзу та є точкою входу до приватної мережі, оскільки саме через нього проходить увесь зашифрований трафік від віддалених клієнтів, при цьому така централізація дозволяє реалізувати єдину політику безпеки, забезпечити контроль підключень і виконувати аудит мережевої активності, а також мінімізувати необхідність налаштування окремих серверів чи додаткових вузлів у внутрішній інфраструктурі, що значно спрощує загальну структуру системи та підвищує її надійність.

Архітектура VPN-шлюзу та вибір апаратної платформи. Вибір апаратної платформи визначає практичну реалізованість усієї системи, оскільки саме від характеристик пристрою залежить:

— рівень продуктивності;

— стабільності;

— можливість масштабування рішення.

У даному випадку використовується маршрутизатор GL.iNet GL-XE3000 (Puli AX), який поєднує функції мережевого шлюзу та повноцінної програмно-керованої платформи на базі вбудованої операційної системи Linux, що дозволяє реалізувати складні мережеві сценарії без необхідності використання окремих серверів, при цьому архітектура VPN-шлюзу базується на інтеграції механізмів тунелювання безпосередньо у мережевий стек операційної системи, завдяки чому обробка зашифрованого трафіку виконується на рівні ядра, що суттєво зменшує затримки та знижує накладні витрати на обробку пакетів (див. рис. 2.1).



Рисунок 2.1 – Зовнішній вигляд маршрутизатора GL.iNet GL-XE3000

Особливістю обраного пристрою виступає так звана двошарова модель управління, яка поєднує пропрієтарний веб-інтерфейс виробника для швидкого налаштування базових параметрів мережі та відкриту операційну систему OpenWRT із доступом через командний рядок, що надає можливість глибокої кастомізації конфігурації, така комбінація дозволяє одночасно забезпечити

зручність для початкового розгортання та гнучкість для досвідчених користувачів, які потребують детального контролю над параметрами маршрутизації, фільтрації трафіку та криптографічних механізмів, у результаті формується універсальне середовище, придатне як для швидкого впровадження, так і для дослідницьких або навчальних цілей (див. рис. 2.2) [20].

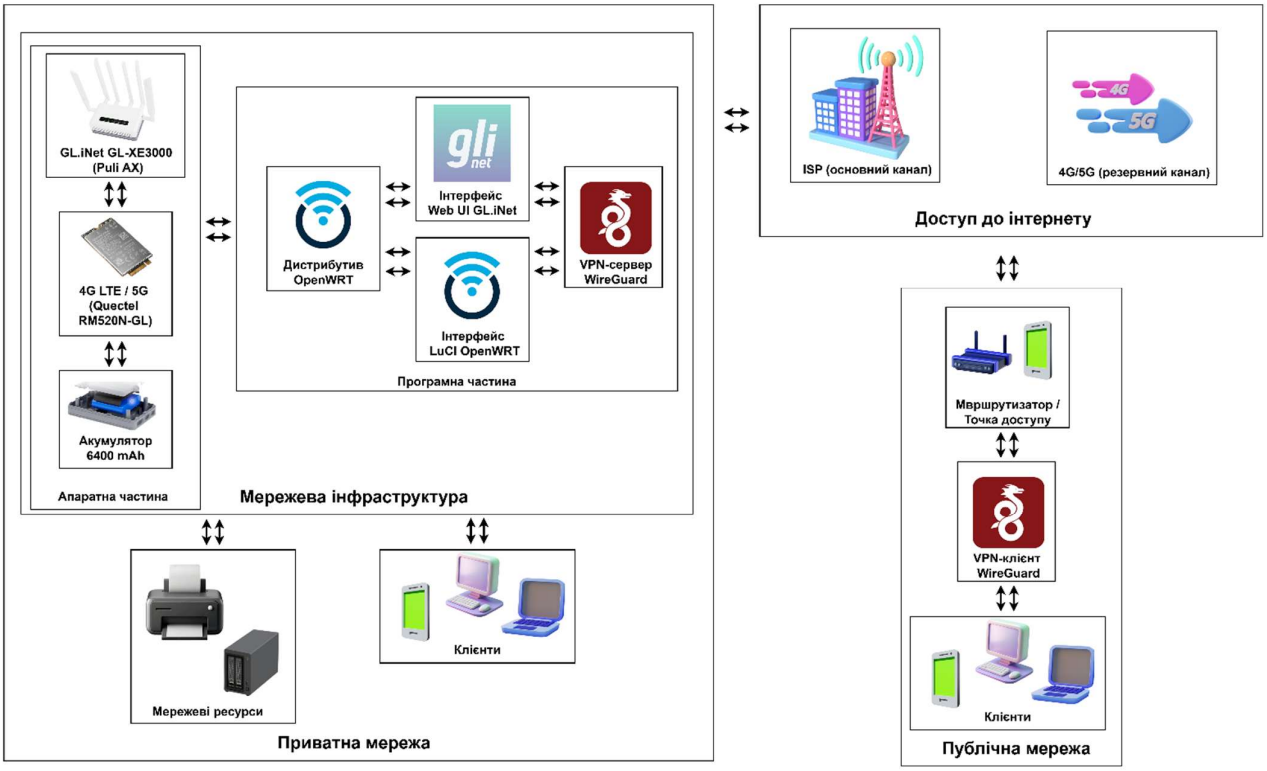


Рисунок 2.2 – Загальна архітектура системи VPN-шлюзу

Апаратна основа пристрою побудована на процесорі архітектури ARM, що забезпечує достатній рівень продуктивності для обробки зашифрованого трафіку навіть у мобільних або обмежених умовах, при цьому сучасні ARM-процесори демонструють високу енергоефективність і здатність виконувати криптографічні операції з мінімальними затримками, що робить їх оптимальним вибором для побудови вбудованих VPN-рішень, у результаті використання такого підходу дозволяє досягти балансу між продуктивністю, енергоспоживанням і компактністю пристрою.

Додатковою перевагою виступає можливість розширення функціональності за рахунок встановлення додаткових пакетів у середовищі OpenWRT, що дозволяє інтегрувати інструменти моніторингу, аналізу трафіку або додаткові мережеві сервіси без зміни апаратної платформи, у результаті маршрутизатор перетворюється на універсальний вузол мережевої інфраструктури, здатний виконувати широкий спектр завдань, включаючи роль VPN-шлюзу, міжмережевого екрана, проксі-сервера або навіть системи збору та аналізу даних (див. табл. 2.1) [20].

Таблиця 2.1 – Технічні характеристики апаратної платформи VPN-шлюзу

Параметр	Значення
Модель	GL.iNet GL-XE3000 (Puli AX)
Процесор	ARM (quad-core)
Оперативна пам’ять	2 GB RAM
Накопичувач	8 GB eMMC
ОС	OpenWRT (Linux-based)
Підтримка VPN	WireGuard, OpenVPN
Мобільний зв’язок	4G LTE / 5G (Quectel RM520N-GL)
Wi-Fi	Wi-Fi 6 (802.11ax)
Ethernet	2× Gigabit LAN/WAN
Акумулятор	Вбудований (автономна робота)
USB	USB 3.0
Додатково	SIM-карта, failover, load balancing

Мобільність та автономність як ключові переваги. Однією з визначальних особливостей використання граничного маршрутизатора в архітектурі віддаленого доступу є його здатність функціонувати у змінних та часто нестабільних умовах експлуатації, включаючи сценарії з обмеженим доступом до електроживлення або відсутністю стаціонарної мережевої інфраструктури, що формує необхідність орієнтації на мобільні та автономні рішення, у цьому контексті особливу увагу привертає GL.iNet GL-XE3000 (Puli AX) як пристрій, який поєднує у собі характеристики повноцінного VPN-шлюзу та портативного мережевого вузла, здатного забезпечувати стабільний доступ до приватної інфраструктури незалежно від зовнішніх умов [21].

Наявність вбудованого акумулятора забезпечує можливість безперервної роботи пристрою протягом тривалого часу без підключення до електромережі, що дозволяє підтримувати активні VPN-з'єднання навіть у випадках перебоїв живлення або під час переміщення вузла, при цьому автономність на рівні декількох годин створює достатній запас часу для збереження доступу до критичних ресурсів, включаючи системи керування, сервери або інші елементи приватної інфраструктури, що особливо актуально у середовищах із підвищеними вимогами до безперервності доступу, одночасно із цим обчислювальні ресурси пристрою дозволяють обслуговувати значну кількість клієнтських підключень без суттєвої деградації продуктивності, що робить його придатним для використання не лише у персональних, але й у невеликих корпоративних сценаріях [21].

Інтеграція мобільного модема з підтримкою сучасних стандартів зв'язку дозволяє використовувати стільникові мережі як повноцінний канал передачі даних, що усуває залежність від провідного інтернету та відкриває можливості для розгортання систем віддаленого доступу у польових умовах, на віддалених об'єктах або тимчасових локаціях, де відсутня традиційна мережева інфраструктура, у таких випадках маршрутизатор виконує роль автономного вузла, який одночасно забезпечує підключення до глобальної мережі та реалізує функції захищеного VPN-доступу, що значно розширює сферу застосування системи [21].

Практичні сценарії використання включають розгортання у мобільних середовищах, таких як транспортні засоби або пересувні робочі станції, де необхідно забезпечити стабільний доступ до корпоративних ресурсів під час переміщення, при цьому пристрій може функціонувати як центральна точка доступу для декількох клієнтів, забезпечуючи їх підключення через захищений тунель незалежно від типу використовуваного каналу зв'язку, у результаті формується універсальне рішення, придатне для широкого спектру задач, включаючи моніторинг, адміністрування або доступ до внутрішніх сервісів.

Додатковою перевагою виступає можливість автоматичного перемикання між доступними каналами зв'язку, що забезпечує безперервність роботи системи у випадках відмови основного підключення, такий підхід дозволяє мінімізувати

простої та зберігати стабільність VPN-з’єднання навіть у складних умовах експлуатації, одночасно із цим мобільність пристрою дозволяє використовувати його як резервний вузол, який може бути швидко розгорнутий у разі аварій або відмов основної мережевої інфраструктури, що підвищує загальну надійність системи та її стійкість до зовнішніх впливів [21].

Узагальнення наведених характеристик дозволяє сформувати уявлення про мобільний VPN-шлюз як про універсальний інструмент побудови віддаленого доступу, який поєднує у собі функціональність, автономність та адаптивність до змінних умов експлуатації, що забезпечує можливість створення стійких до відмов систем, здатних підтримувати безпечний доступ до приватної інфраструктури незалежно від зовнішніх факторів.

Топологічні схеми використання. У процесі проєктування системи віддаленого доступу важливим етапом виступає визначення топологічних схем її функціонування, які описують:

1. способи взаємодії між вузлами мережі;
2. напрямки передачі трафіку;
3. принципи організації доступу до внутрішніх ресурсів.

При цьому вибір конкретної топології безпосередньо впливає на рівень безпеки, масштабованість і зручність адміністрування всієї системи, у даному випадку розглядається використання маршрутизатора GL.iNet GL-XE3000 (Puli AX) як центрального або допоміжного вузла у різних сценаріях побудови VPN-інфраструктури, що дозволяє адаптувати рішення до конкретних умов експлуатації та вимог користувачів.

Перший базовий сценарій передбачає використання маршрутизатора у ролі центрального VPN-шлюзу для доступу до внутрішньої приватної інфраструктури, у межах якого клієнтські пристрої, такі як ноутбуки, смартфони або інші мобільні термінали, підключаються до захищеного тунелю та отримують можливість взаємодії з ресурсами локальної мережі, включаючи сервери, робочі станції або мережеве обладнання, при цьому вся взаємодія проходить через один граничний вузол, що дозволяє централізувати контроль доступу, спростити управління

політиками безпеки та забезпечити уніфіковану точку входу до мережі, одночасно із цим кожному клієнту призначаються індивідуальні параметри доступу, включаючи криптографічні ключі та дозволені мережеві адреси, що підвищує рівень ізоляції між користувачами та зменшує ризик несанкціонованого доступу [22].

Другий сценарій передбачає використання маршрутизатора у ролі клієнта у топології типу "site-to-site", у якій він встановлює захищене з’єднання з центральною інфраструктурою організації, у результаті чого віддалена мережа інтегрується у єдиний адресний простір підприємства та функціонує як його логічне продовження, такий підхід дозволяє забезпечити доступ до корпоративних ресурсів без необхідності індивідуального налаштування кожного клієнтського пристрою, оскільки взаємодія відбувається на рівні мережевих сегментів, що значно спрощує адміністрування та знижує кількість конфігураційних операцій, особливо у випадках, коли необхідно об’єднати декілька віддалених офісів, виробничих об’єктів або тимчасових локацій у єдину інформаційну систему [22].

Можливість комбінування наведених підходів дозволяє формувати гібридні топології, у межах яких один і той самий маршрутизатор може одночасно виконувати функції VPN-сервера для мобільних клієнтів та VPN-клієнта для підключення до іншої мережі, у результаті формується багаторівнева система доступу, де граничний вузол виступає як точка агрегації трафіку та засіб інтеграції різних сегментів мережі, що значно розширює функціональні можливості всієї інфраструктури та дозволяє реалізовувати складні сценарії взаємодії між вузлами без суттєвого ускладнення конфігурації (див. рис. 2.3) [22].

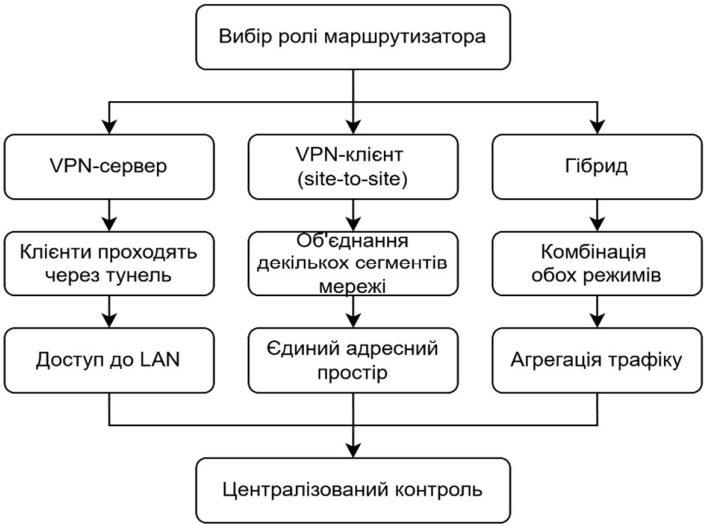


Рисунок 2.3 – Концепція edge-підходу у VPN

Гнучкість такої архітектури забезпечує можливість її використання у широкому спектрі задач, починаючи від простих домашніх або навчальних середовищ і завершуючи складними корпоративними мережами, де необхідно забезпечити надійний, безпечний та масштабований доступ до розподілених ресурсів, при цьому використання єдиного програмного середовища на базі OpenWRT дозволяє зберігати уніфікований підхід до конфігурації незалежно від обраної топології, що спрощує процес впровадження, супроводу та подальшого розвитку системи віддаленого доступу.

2.2 Розгортання та конфігурація системи (Web UI та OpenWRT CLI)

У процесі практичної реалізації системи віддаленого доступу до приватної інфраструктури формується як комплексний підхід, що базується на використанні маршрутизатора GL.iNet Puli AX GL-XE3000 та передбачає застосування двох принципово різних, але взаємодоповнюючих методів конфігурації, які характерні для сучасних мережевих рішень, де поєднується зручність графічного управління із гнучкістю низькорівневої взаємодії через консоль, при цьому веб-інтерфейс,

реалізований виробником, виступає надбудовою над OpenWRT, тоді як доступ через CLI забезпечує прямий контроль над системою на рівні операційної системи, що дозволяє не лише розгортати базову функціональність, але й виконувати детальну оптимізацію та експериментальне налаштування, у результаті чого формується універсальна модель керування, яка охоплює як початковий рівень адміністрування, так і глибоку інженерну конфігурацію, забезпечуючи адаптивність системи до різних сценаріїв використання та рівнів підготовки адміністратора (див. рис. 2.4).

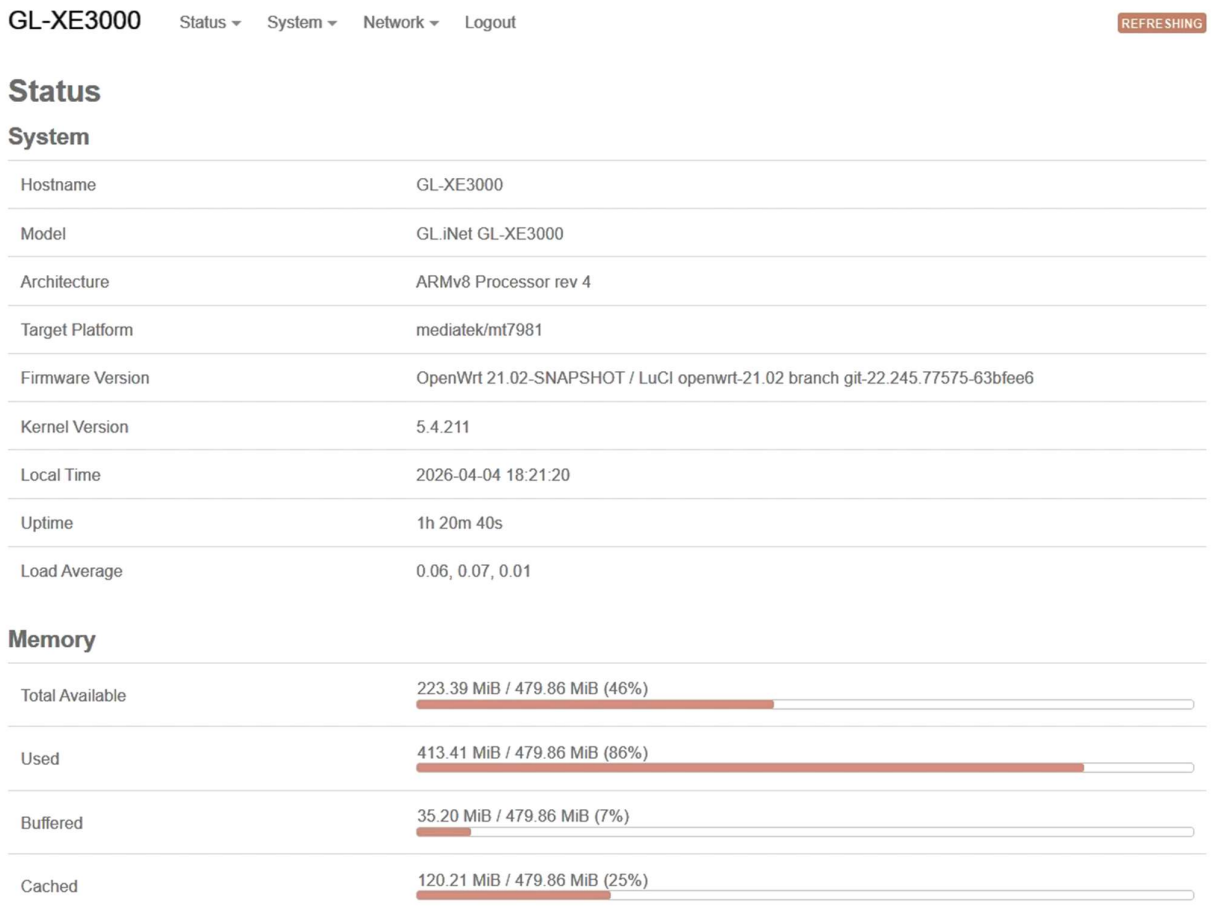


Рисунок 2.4 – Інтерфейс LuCI OpenWRT

Базова ініціалізація через Web-інтерфейс. Початковий етап розгортання передбачає використання графічного веб-інтерфейсу, який значно спрощує взаємодію з пристроєм та дозволяє швидко виконати основні налаштування без необхідності глибокого занурення у внутрішню структуру системи, при цьому

доступ до панелі керування здійснюється через стандартну локальну IP-адресу маршрутизатора, що відкриває можливість централізованого управління всіма параметрами мережі, включаючи (див. рис. 2.5):

— активацію VPN-сервера;

— генерацію криптографічних ключів;

— створення базової конфігурації тунелю.

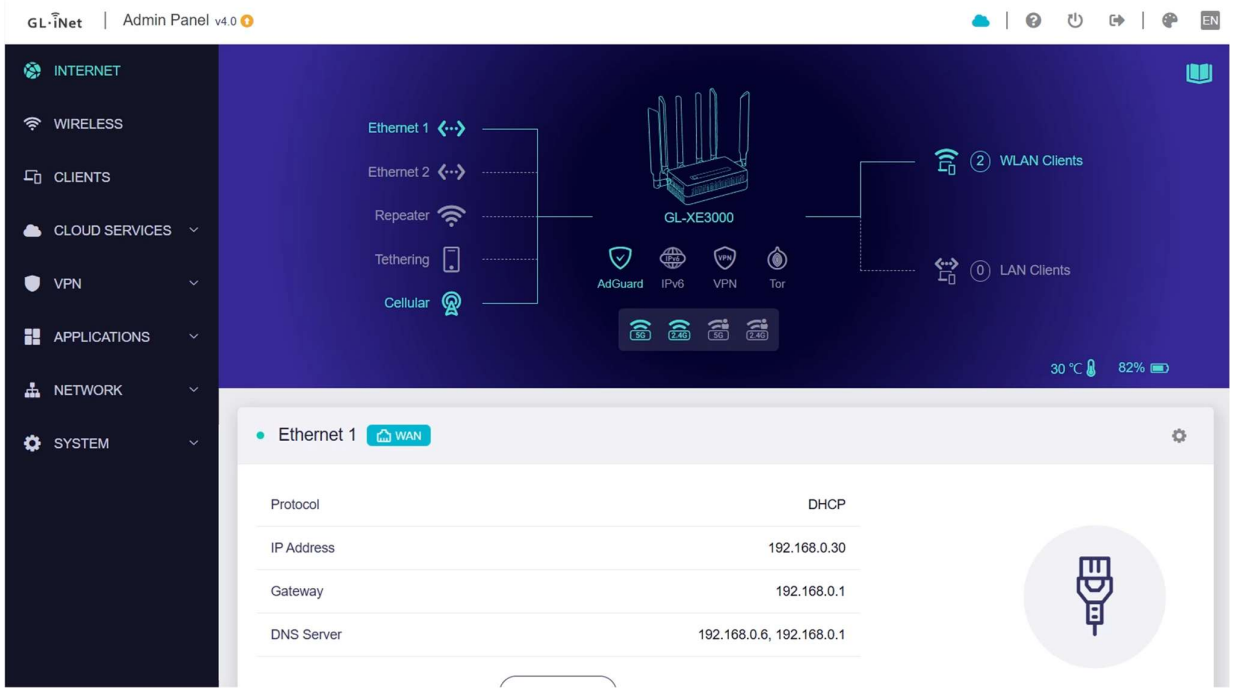


Рисунок 2.5 – Інтерфейс Web UI GL.iNet

Тут важливим аспектом виступає забезпечення зовнішньої доступності вузла, оскільки у випадках використання мобільного інтернету або підключення за NAT необхідно реалізувати механізми, що дозволяють клієнтам встановлювати з’єднання із сервером, тому виконується налаштування пробросу портів для UDP-з’єднань, зазвичай на порту 51820, що є стандартним для WireGuard, а також інтеграція з сервісом динамічного DNS дозволяє прив’язати змінну зовнішню IP-адресу до постійного доменного імені, що особливо актуально для мобільних або нестабільних мережевих середовищ (див. рис. 2.6).

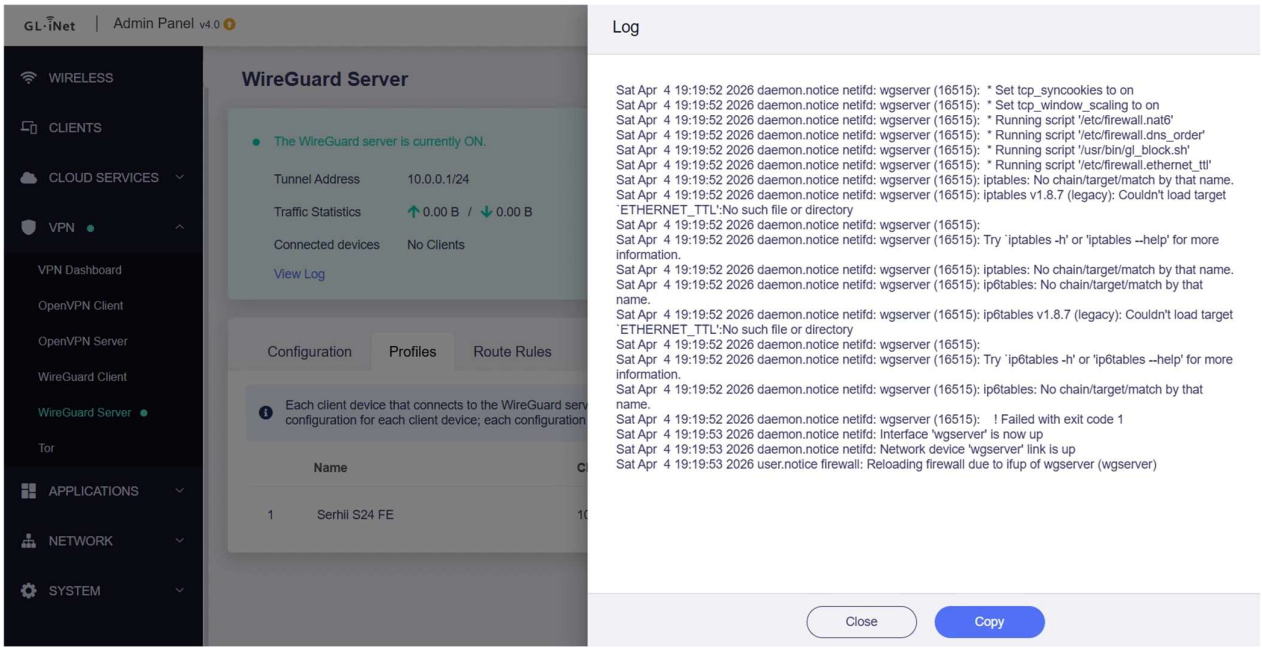


Рисунок 2.6 – Налаштування WireGuard через Web-інтерфейс

Додатково у процесі конфігурації визначаються політики доступу до локальної мережі, які регламентують, які саме ресурси будуть доступні клієнтам після встановлення VPN-з'єднання, оскільки без відповідного налаштування маршрутизації та правил доступу тунель може функціонувати лише як канал передачі даних без реального доступу до внутрішньої інфраструктури, що фактично нівелює його практичну цінність, тому реалізується відкриття доступу до необхідних підмереж або окремих пристроїв, одночасно забезпечуючи ізоляцію клієнтів між собою шляхом обмеження їх взаємодії, що відповідає принципу мінімальних привілеїв та підвищує загальний рівень безпеки системи, у результаті чого використання веб-інтерфейсу дозволяє швидко створити працездатну конфігурацію, придатну для подальшого тестування та розширення.

Консольна генерація ключів та конфігурацій (SSH). У процесі побудови більш гнучкої та контрольованої системи налаштування використовується доступ до маршрутизатора через протокол SSH по порту 22, що дозволяє працювати безпосередньо з операційною системою OpenWRT як із повноцінним середовищем на базі ядра Linux, яке адаптоване для мережевих пристроїв і фактично виступає спеціалізованим дистрибутивом для маршрутизаторів, підключення до такого

середовища потребує знання IP-адреси пристрою, логіна та пароля адміністратора, де типовим користувачем є "root", а пароль відповідає тому, який було встановлено під час первинної ініціалізації маршрутизатора, після встановлення з’єднання через термінал відкривається можливість повноцінного керування системою, включаючи доступ до файлової системи, мережевих інтерфейсів та внутрішніх механізмів маршрутизації, що створює умови для більш глибокої конфігурації порівняно з можливостями веб-інтерфейсу (див. рис. 2.7).

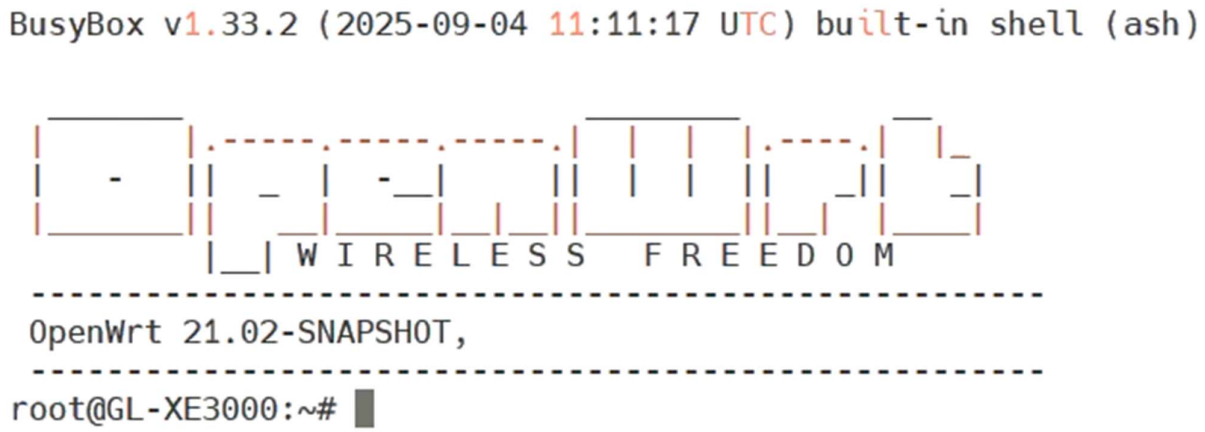


Рисунок 2.7 – Підключення через SSH до маршрутизатора

Такий підхід дозволяє виконувати ручну генерацію криптографічних ключів та формування конфігурацій клієнтів без використання графічних засобів, де за допомогою утиліт WireGuard здійснюється створення приватного та публічного ключів, після чого формується конфігураційний файл клієнта, який містить параметри інтерфейсу та підключення до серверного вузла, включаючи адресу, DNS, публічний ключ сервера та список дозволених мереж, подальшим кроком виконується додавання нового піра до серверного інтерфейсу за допомогою команди "wg set", що дозволяє динамічно змінювати конфігурацію без перезапуску сервісу, у результаті чого формується активне підключення, яке може бути перевірене через команду "wg show", де відображається інформація про інтерфейс, список підключених клієнтів, їх IP-адреси, обсяг переданого трафіку та час останнього криптографічного обміну (див. рис. 2.8) [23].

```
root@GL-XE3000:~# mkdir wireguard && cd wireguard
root@GL-XE3000:~/wireguard# wg genkey | tee client_private.key | wg pubkey > client_public.key
root@GL-XE3000:~/wireguard# ll
drwxr-xr-x    2 root     root          3488 Apr  7 11:57 ./
drwxr-xr-x    1 root     root          3488 Apr  7 11:57 ../
-rw-r--r--    1 root     root            45 Apr  7 11:57 client_private.key
-rw-r--r--    1 root     root            45 Apr  7 11:57 client_public.key
```

Рисунок 2.8 – Генерація ключів у терміналі

Практична реалізація даного підходу може бути виконана через послідовність команд, яка включає генерацію ключів, створення конфігураційного файлу та додавання клієнта до серверної частини, що дозволяє повністю автоматизувати процес у межах одного сценарію виконання, при цьому використання конструкцій оболонки дає можливість інтегрувати ці дії у shell-скрипти для подальшого масштабування або повторного використання, а також забезпечує незалежність від обмежень графічного інтерфейсу, що є особливо важливим у випадках масового розгортання або тестування різних конфігурацій (див. рис. 2.9).

```
root@GL-XE3000:~/wireguard# cat client.conf
[Interface]
PrivateKey = [redacted]
Address = 10.0.0.2/32
DNS = 1.1.1.1

[Peer]
PublicKey = [redacted]
Endpoint = [redacted]:51820
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 25
```

Рисунок 2.9 – Приклад конфігураційного файлу клієнта

Особливістю такого способу конфігурації є те, що клієнти, додані через командний рядок, не відображаються у списку профілів веб-інтерфейсу, хоча фактично функціонують і можуть передавати трафік, у самому інтерфейсі вони позначаються як невідомі, що пояснюється внесенням конфігурації безпосередньо

у ядро системи, минаючи механізми управління профілями, реалізовані у графічній оболонці, що демонструє розділення логіки між рівнем управління та рівнем виконання (див. табл. 2.2).

Таблиця 2.2 – Параметри конфігурації WireGuard-з’єднання

Параметр	Опис
PrivateKey	Приватний ключ клієнта
PublicKey	Публічний ключ сервера
AllowedIPs	Дозволені IP-мережі для маршрутизації
Endpoint	IP-адреса та порт сервера
ListenPort	Порт прослуховування
Address	Внутрішня IP-адреса клієнта
DNS	DNS-сервер
PersistentKeepalive	Інтервал підтримки з’єднання
Interface	Віртуальний мережевий інтерфейс
Peer	Конфігурація віддаленого вузла

Безпечна передача конфігурації через термінальний QR-код. У процесі практичної реалізації системи віддаленого доступу застосовується підхід, який дозволяє значно спростити передачу конфігурацій клієнтським пристроям та одночасно підвищити рівень безпеки, де замість традиційного копіювання конфігураційного файлу або його передачі через сторонні канали зв’язку, що часто супроводжується ризиками перехоплення або помилками під час імпорту, використовується механізм генерації QR-коду безпосередньо у термінальному середовищі маршрутизатора, який працює на базі OpenWRT, такий підхід реалізується за допомогою спеціалізованої утиліти qrencode, яка після встановлення у систему дозволяє перетворити текстовий конфігураційний файл клієнта у візуальне представлення у вигляді QR-коду, що відображається прямо у консолі [24].

Процес генерації виконується через команду "qrencode -t ansiutf8 < client.conf", у результаті чого у терміналі формується символьне зображення QR-коду, яке може бути зчитане камерою смартфона, на якому встановлено клієнт WireGuard (див. рис. 2.10).



Рисунок 2.10 – Генерація QR-коду в терміналі

Після сканування відбувається автоматичний імпорт усіх параметрів підключення, включаючи:

— приватний ключ;

— адресу тунелю;

— DNS-сервери;

— параметри серверного піра.

Все це дозволяє миттєво підключити клієнта без необхідності ручного введення або передачі файлів (див. рис. 2.11) [24].

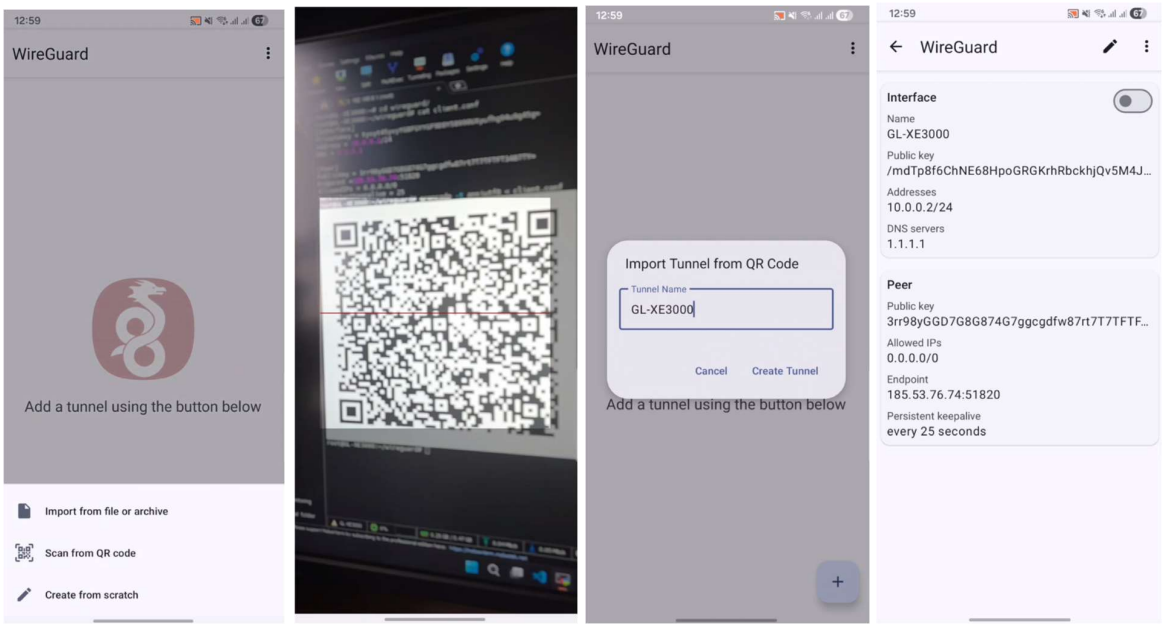


Рисунок 2.11 – Сканування QR-коду у клієнтському додатку WireGuard

Такий спосіб передачі конфігурації забезпечує відсутність необхідності використання мережевих каналів для обміну чутливими даними, що знижує ймовірність витоку інформації та виключає залежність від сторонніх сервісів, одночасно з цим підвищується швидкість розгортання клієнтів, оскільки весь процес зводиться до одного сканування, що є особливо зручним у мобільних або польових умовах, де доступ до додаткових інструментів може бути обмеженим.

Додатковою перевагою виступає зниження кількості помилок, пов’язаних із ручним введенням конфігураційних параметрів, оскільки всі дані передаються у готовому вигляді без необхідності редагування, що підвищує надійність підключення та спрощує процес адміністрування, при цьому адміністратор може оперативно створювати нові конфігурації та одразу передавати їх користувачам без проміжних етапів.

Концепція тимчасових сесій (Volatile Configuration). Процес розгортання системи віддаленого доступу на базі маршрутизатора передбачає не лише класичне налаштування постійних VPN-профілів, але й використання більш гнучких підходів, серед яких окреме місце займає концепція тимчасових сесій, що реалізується через консольні інструменти управління, зокрема через механізми

прямої взаємодії з інтерфейсом WireGuard на рівні ядра операційної системи, де клієнт додається безпосередньо за допомогою команди "wg set", що фактично означає «ін’єкцію» конфігурації у поточний стан мережевого інтерфейсу без її збереження у постійних конфігураційних файлах системи.

Такий підхід формує окремий клас підключень, які функціонують лише в рамках поточної сесії роботи пристрою, оскільки після перезавантаження маршрутизатора всі подібні записи автоматично видаляються, що з технічної точки зору пояснюється відсутністю синхронізації між runtime-конфігурацією WireGuard та файловою системою OpenWRT, де зазвичай зберігаються постійні налаштування, і таким чином формується чітке розділення між тимчасовими та персистентними конфігураціями [25].

У середовищі графічного інтерфейсу GL.iNet такі підключення не відображаються як повноцінні профілі, оскільки вони не проходять через механізм управління конфігураціями, натомість у розділі активних клієнтів вони можуть відображатися як підключені вузли зі статусом "Unknown", що фактично вказує на відсутність прив’язки до збереженого профілю, але при цьому не впливає на їхню функціональність, оскільки сам тунель залишається повністю працездатним, а передача даних здійснюється відповідно до заданих параметрів [25].

Така поведінка системи не є помилкою або обмеженням, а навпаки формує окрему функціональну можливість, яка може бути використана у практичних сценаріях адміністрування, де необхідно забезпечити швидкий, контрольований та тимчасовий доступ без внесення змін у основну конфігурацію пристрою, зокрема це актуально для випадків надання доступу технічному персоналу, проведення діагностики або тестування мережевих сервісів, де важливо уникнути накопичення зайвих записів у конфігурації та зберегти її структурну чистоту.

У подібних сценаріях адміністратор отримує можливість створювати клієнтські підключення «на льоту», використовуючи лише консольні команди, що значно скорочує час реагування та усуває необхідність роботи з веб-інтерфейсом, при цьому вся логіка взаємодії зводиться до генерації ключів, додавання піра до інтерфейсу WireGuard та, за необхідності, формування конфігураційного файлу для

клієнта, який може бути переданий у будь-який зручний спосіб, включаючи QR-код.

Одночасно з цим зберігається можливість повного контролю над такими сесіями, оскільки вони відображаються у виводі команди "wg show", де можна відстежити:

— їхню активність;

— обсяг переданих даних;

— час останнього криптографічного обміну.

Все це дозволяє здійснювати моніторинг навіть для тимчасових підключень без необхідності інтеграції їх у постійну систему обліку.

У ширшому контексті така модель підкреслює переваги двошарової архітектури маршрутизатора, де поєднання зручного графічного інтерфейсу та повноцінного доступу до операційної системи створює середовище, придатне як для базового адміністрування, так і для реалізації складних інженерних сценаріїв, і дозволяє адаптувати поведінку системи відповідно до конкретних вимог експлуатації.

Розмежування між постійними конфігураціями, які зберігаються через веб-інтерфейс або системні файли, та тимчасовими, що існують лише у пам’яті ядра, створює додатковий рівень гнучкості, завдяки якому система може одночасно підтримувати стабільну роботу основної інфраструктури та забезпечувати динамічне підключення нових користувачів без ризику порушення існуючих налаштувань.

2.3 Алгоритми функціонування та управління з’єднаннями

У процесі побудови системи віддаленого доступу на базі WireGuard, розгорнутої безпосередньо на граничному маршрутизаторі з операційною системою OpenWRT, виникає необхідність не лише у практичній реалізації

конфігурацій, але й у глибокому розумінні логіки функціонування всієї системи, оскільки саме внутрішні алгоритми визначають поведінку тунелю, обробку мережевого трафіку та механізми контролю доступу до ресурсів приватної інфраструктури, при цьому опис таких процесів у вигляді послідовних алгоритмів дозволяє формалізувати роботу системи, зробити її передбачуваною та придатною для аналізу, оптимізації і подальшого масштабування.

У загальному вигляді функціонування системи базується на трьох взаємопов'язаних процесах, які включають:

— встановлення захищеного з'єднання;

— маршрутизацію зашифрованого трафіку;

— динамічне управління підключеннями.

Кожен із цих процесів реалізується за допомогою чітко визначених механізмів, що інтегровані безпосередньо у мережевий стек операційної системи, що дозволяє досягти високої ефективності навіть на вбудованих пристроях із обмеженими ресурсами.

Алгоритм ініціалізації та криптографічного обміну (Handshake). Алгоритм ініціалізації та криптографічного обміну, який лежить в основі встановлення VPN-з'єднання, реалізується за принципом мінімалістичного, але криптографічно надійного Handshake-механізму, де відсутні традиційні для інших VPN-рішень багатокрокові процедури узгодження параметрів, що значно спрощує логіку та зменшує затримки, початковим етапом виступає формування попередньої конфігурації, у межах якої кожен учасник з'єднання, як клієнт, так і сервер, генерує власну пару ключів, що складається з приватного та публічного компонентів, при цьому публічні ключі обмінюються заздалегідь через конфігураційні файли або альтернативні механізми передачі, такі як QR-коди, що дозволяє уникнути необхідності централізованих систем автентифікації.

Після цього ініціалізація з'єднання виконується клієнтською стороною, яка формує початковий пакет, що містить криптографічні параметри та ідентифікатор, пов'язаний із його публічним ключем, і передає його на сервер, де відбувається перевірка відповідності цього ключа списку дозволених пірів, у випадку

відсутності такого запису пакет ігнорується без формування відповіді, що реалізує принцип так званого "silent drop", який підвищує безпеку шляхом мінімізації інформації для потенційного зловмисника.

У разі успішної перевірки сервер формує відповідний пакет-відповідь, використовуючи власний приватний ключ, у результаті чого обидві сторони незалежно обчислюють спільний сесійний ключ, який надалі використовується для симетричного шифрування трафіку, завершення Handshake відбувається після отримання клієнтом відповіді, після чого з’єднання переходить у фазу активної передачі даних, де всі пакети шифруються та автентифікуються відповідно до встановлених параметрів (див. рис. 2.12).

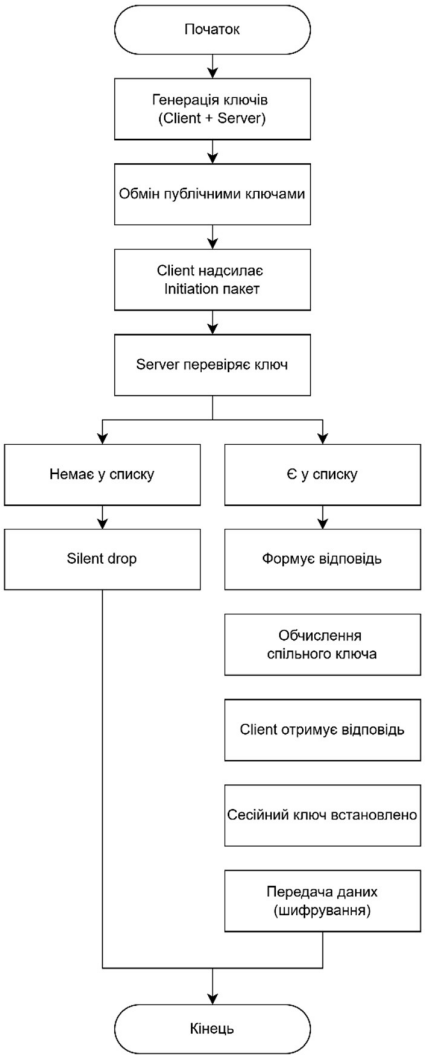


Рисунок 2.12 – Алгоритм встановлення з’єднання (Handshake)

Особливістю такого підходу є відсутність класичних механізмів автентифікації у вигляді логінів і паролів, оскільки ідентифікація здійснюється виключно на основі криптографічних ключів, що значно спрощує архітектуру та одночасно підвищує її стійкість до атак, додатково мінімальна кількість обмінів під час встановлення з'єднання, яка обмежується фактично двома повідомленнями, забезпечує швидке встановлення тунелю, що у практичних умовах проявляється як майже миттєве підключення навіть при зміні мережевого середовища, наприклад при переході між Wi-Fi та мобільною мережею.

Така логіка роботи безпосередньо впливає і на ефективність використання апаратних ресурсів маршрутизатора, оскільки зменшення кількості операцій узгодження та перенесення криптографічних обчислень у простір ядра дозволяє знизити навантаження на процесор, що є особливо важливим для ARM-пристроїв, які використовуються у вбудованих мережевих рішеннях, у результаті чого система зберігає стабільну продуктивність навіть при одночасному обслуговуванні декількох клієнтів.

У ширшому контексті описаний алгоритм демонструє, що WireGuard орієнтований на мінімалізм та ефективність, де кожен елемент протоколу має чітке функціональне призначення без надлишкових механізмів, що дозволяє не лише спростити реалізацію, але й забезпечити передбачувану поведінку системи у різних умовах експлуатації, включаючи мобільні сценарії та середовища з нестабільним мережевим підключенням, що у підсумку формує основу для побудови надійної, швидкої та гнучкої системи віддаленого доступу до приватної інфраструктури [26].

Алгоритм маршрутизації Cryptokey Routing (AllowedIPs). У межах функціонування системи віддаленого доступу на базі WireGuard окрему увагу привертає алгоритм маршрутизації, реалізований через механізм Cryptokey Routing, який поєднує у собі логіку класичної IP-маршрутизації та контроль доступу до мережевих ресурсів, що формує принципово інший підхід до обробки трафіку у порівнянні з традиційними VPN-рішеннями, де ці функції зазвичай розділені між таблицями маршрутизації, списками контролю доступу та міжмережевими екранами, у даному випадку вся ця логіка зосереджена в одному

параметрі — AllowedIPs, який одночасно визначає, які адреси дозволено використовувати певному клієнту, і куди саме має бути направлений трафік [27].

У загальному вигляді алгоритм починається з моменту надходження мережевого пакета на інтерфейс WireGuard, наприклад "wg0" або "wgserver", після чого першочергово виконується криптографічна перевірка та розшифрування, якщо пакет не проходить перевірку автентичності або не відповідає очікуваним криптографічним параметрам, він відкидається ще до етапу маршрутизації, що дозволяє мінімізувати ризики несанкціонованого доступу, після успішного розшифрування система переходить до визначення джерела пакета, яке здійснюється не за класичними IP-ознаками, а через прив’язку до конкретного піра на основі його публічного ключа, що вже саме по собі формує додатковий рівень ідентифікації.

Наступним етапом виконується перевірка відповідності IP-адреси джерела списку AllowedIPs для конкретного піра, тобто система аналізує, чи має право даний клієнт використовувати зазначену адресу, і якщо вхідний пакет містить IP, що не входить до дозволеного діапазону, він негайно відкидається, що реалізує модель "default deny", де будь-яка невідома або несанкціонована активність блокується за замовчуванням без додаткових правил фільтрації.

Після проходження перевірки вхідного трафіку система переходить до обробки вихідного трафіку, де логіка роботи полягає у визначенні відповідного піра для передачі пакета, у цьому випадку WireGuard аналізує IP-адресу призначення і шукає серед усіх налаштованих пірів той, у якого в AllowedIPs присутній відповідний діапазон, якщо такий пір знайдено, пакет маршрутизується через нього, у протилежному випадку використовується стандартна таблиця маршрутизації операційної системи, що дозволяє інтегрувати VPN-тунель у загальну мережеву архітектуру без конфліктів.

Завершальним етапом є шифрування пакета та його передача через відповідний тунель, при цьому всі операції виконуються у просторі ядра, що забезпечує високу швидкість обробки навіть на пристроях із обмеженими апаратними ресурсами, і саме така інтеграція дозволяє уникнути зайвих накладних

витрат, характерних для рішень, які працюють у користувацькому просторі (див. рис. 2.13).

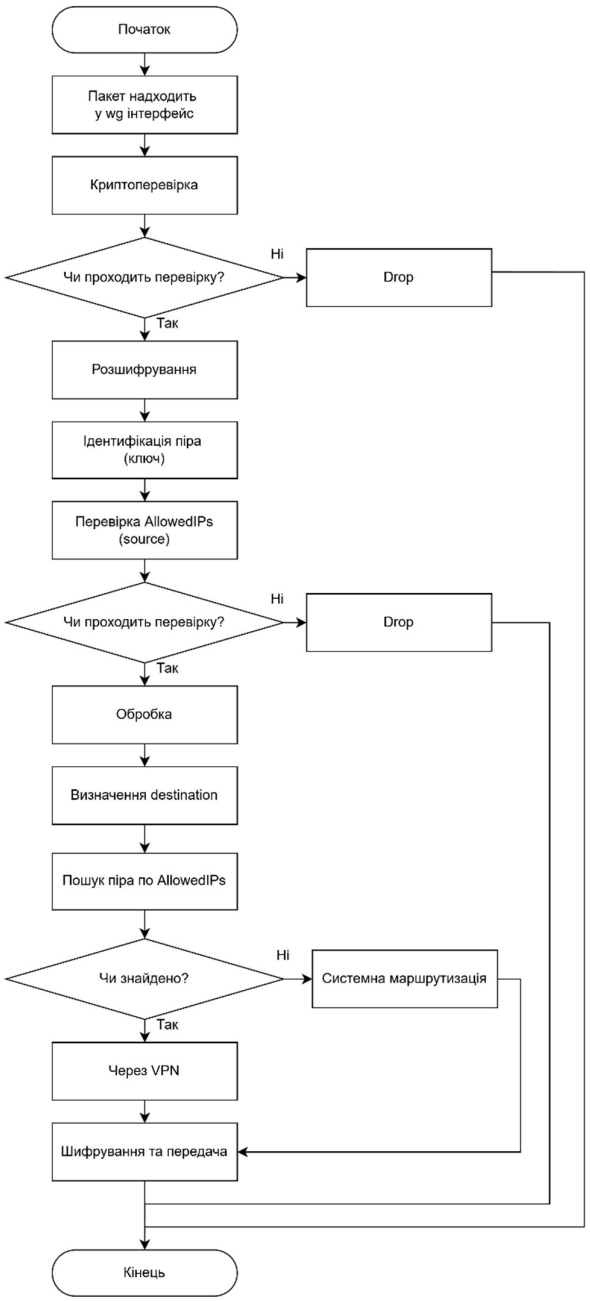


Рисунок 2.13 – Алгоритм маршрутизації Cryptokey Routing (AllowedIPs)

Практичне застосування цього механізму можна розглянути на прикладі конфігурації, де для клієнта задано "AllowedIPs = 10.0.0.2/32", "192.168.8.0/24", у такому випадку адреса "10.0.0.2" однозначно закріплюється за конкретним

клієнтом як його ідентифікатор у VPN-мережі, тоді як діапазон "192.168.8.0/24" визначає перелік внутрішніх ресурсів, до яких клієнт отримує доступ через тунель, відповідно сервер буде направляти весь трафік до цих адрес саме через даний пір, що одночасно означає і надання доступу, і визначення маршруту.

У ширшому контексті такий підхід дозволяє відмовитися від складних схем маршрутизації та великої кількості правил міжмережевого екрану, оскільки вся логіка доступу інкапсулюється у конфігурації самого WireGuard, що значно спрощує адміністрування та зменшує ймовірність помилок при налаштуванні, додатково підвищується рівень безпеки завдяки тому, що кожен клієнт має чітко визначений набір дозволених адрес і не може виходити за його межі.

Ефективність такого механізму особливо помітна на вбудованих пристроях, де обмежені ресурси вимагають максимально оптимізованих рішень, і поєднання маршрутизації з контролем доступу в одному параметрі дозволяє зменшити кількість обчислювальних операцій та спростити обробку пакетів, у результаті формується компактна, зрозуміла та водночас високоефективна модель керування трафіком, яка добре масштабується та легко адаптується під різні сценарії використання, починаючи від простих домашніх мереж і завершуючи складними корпоративними інфраструктурами.

Алгоритм створення тимчасового доступу (CLI Flow). У межах реалізації системи віддаленого доступу на базі WireGuard окремий інтерес становить алгоритм створення тимчасового доступу, який базується на використанні консольного інтерфейсу та безпосередній взаємодії з ядром операційної системи Linux, де конфігурація формується не через стандартні механізми збереження, а шляхом динамічного внесення параметрів у поточний стан мережевого інтерфейсу, що дозволяє організовувати підключення без фіксації змін у постійній конфігурації пристрою, і таким чином формується підхід, який суттєво відрізняється від класичної моделі через графічний веб-інтерфейс, де кожен клієнт додається як окремий профіль із збереженням у файловій системі.

У цьому випадку логіка роботи будується як послідовність дій адміністратора, яка починається з встановлення захищеного з’єднання з

маршрутизатором через протокол SSH, що забезпечує доступ до командного рядка операційної системи OpenWRT, де використовується стандартний порт 22 та облікові дані користувача з адміністративними привілеями, після чого відкривається можливість виконання команд безпосередньо у середовищі Linux, що дозволяє здійснювати повний контроль над мережею та службами [28].

Наступним етапом формується криптографічна основа майбутнього підключення, де за допомогою утиліт WireGuard виконується генерація пари ключів клієнта, при цьому приватний ключ зберігається локально у файлі, а публічний використовується для ідентифікації клієнта на сервері, що реалізується через послідовність команд, яка об’єднує процес створення ключів в один конвеєр, і таким чином забезпечується швидке отримання готових даних для подальшої конфігурації.

Після генерації ключів виконується формування конфігураційного файлу клієнта, який містить базові параметри інтерфейсу, зокрема приватний ключ, внутрішню IP-адресу у межах VPN-підмережі, налаштування DNS та параметри підключення до сервера, включаючи його публічний ключ, зовнішню адресу та список AllowedIPs, що визначає маршрутизацію трафіку через тунель, і таким чином створюється повноцінний опис клієнтського вузла, готовий до використання.

Далі відбувається ключовий етап, який відрізняє даний підхід від класичних методів конфігурації, а саме додавання піра безпосередньо до інтерфейсу WireGuard за допомогою команди "wg set", у результаті чого новий клієнт миттєво реєструється у системі без внесення змін до конфігураційних файлів, при цьому вказується його публічний ключ та дозволений діапазон IP-адрес, що фактично визначає як його ідентифікацію, так і межі доступу до мережі.

Паралельно з цим може бути реалізовано механізм зручної передачі конфігурації клієнту, де використовується генерація QR-коду безпосередньо у терміналі за допомогою утиліти qrencode, у результаті чого текстовий файл конфігурації перетворюється у візуальне представлення, придатне для сканування мобільним пристроєм, що дозволяє уникнути передачі файлів через мережу та

спрощує процес підключення, особливо у польових умовах або при обмеженому доступі до додаткових інструментів.

Після отримання конфігурації користувач активує тунель у клієнтському застосунку, що ініціює процес встановлення з’єднання, і на цьому етапі адміністратор може виконати перевірку через команду "wg show", яка відображає стан інтерфейсу, список підключених пірів, час останнього криптографічного обміну та обсяг переданого трафіку, що дозволяє оперативно оцінити коректність роботи системи та підтвердити успішність підключення.

Особливістю такого підключення є його статус у графічному інтерфейсі маршрутизатора, де відсутність запису у постійній конфігурації призводить до відображення клієнта як "Unknown", що підкреслює його тимчасовий характер, при цьому вся інформація про нього зберігається лише у runtime-стані ядра і повністю втрачається після перезавантаження пристрою, що вимагає повторного виконання процедури додавання у разі необхідності відновлення доступу.

Така модель роботи формує окремий клас сценаріїв використання, де тимчасовий доступ може бути наданий без ризику зміни основної конфігурації системи, що є особливо корисним для проведення тестування, підключення технічного персоналу або організації короткострокового доступу для зовнішніх користувачів, при цьому відсутність збереження конфігурації забезпечує автоматичне очищення системи після завершення роботи або перезавантаження (див. рис. 2.14).

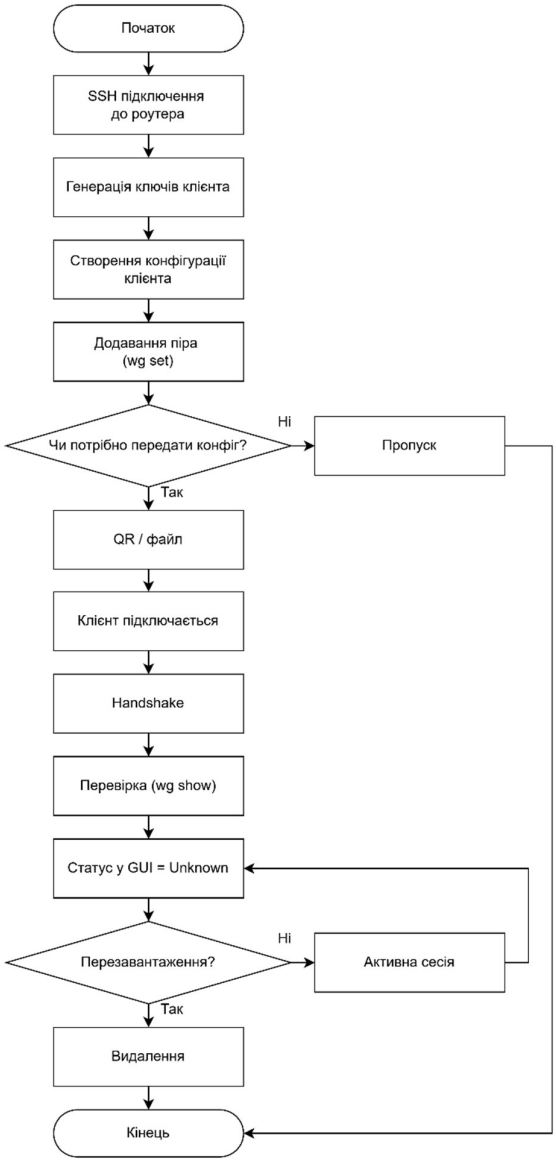


Рисунок 2.14 – Алгоритм створення тимчасового доступу (CLI Flow)

У підсумку описаний алгоритм демонструє високий рівень гнучкості, де поєднання можливостей командного рядка та механізмів WireGuard дозволяє створювати динамічні підключення з мінімальними витратами часу, зберігаючи при цьому повний контроль над параметрами доступу, а також відкриває можливості для подальшої автоматизації через використання shell-скриптів, що дозволяє масштабувати даний підхід у більш складних інфраструктурних сценаріях без необхідності ручного налаштування кожного клієнта окремо.

2.4 Апаратна реалізація, тестування та моніторинг навантаження

Апаратна реалізація, тестування та моніторинг навантаження в межах побудованої системи віддаленого доступу до приватної інфраструктури розглядаються як завершальний етап практичної перевірки працездатності всієї архітектури, що була сформована на базі граничного маршрутизатора GL.iNet GL-XE3000 (Puli AX), де основна увага зосереджується на підтвердженні коректності встановлення VPN-з’єднання, аналізі поведінки трафіку, вимірюванні пропускної здатності та оцінці ефективності використання апаратних ресурсів пристрою як edge-вузла, при цьому всі експерименти виконуються у середовищі OpenWRT із застосуванням як графічного Web UI від виробника, так і консольних інструментів, що дозволяє отримати повну картину функціонування системи на різних рівнях абстракції та керування.

Верифікація мережевих параметрів. Першочерговим етапом тестування виступає верифікація мережевих параметрів, яка передбачає підтвердження факту встановлення стабільного VPN-з’єднання між клієнтським пристроєм, зокрема смартфоном, та маршрутизатором, що виконує функції VPN-шлюзу, причому перевірка здійснюється як на стороні клієнта, так і на стороні сервера, де використовується команда "wg show" для отримання детальної інформації про стан інтерфейсу "wgserver", у виводі якої аналізуються такі параметри, як "latest handshake", що відображає час останнього успішного криптографічного обміну, transfer, який демонструє обсяг переданих та отриманих даних, endpoint, що містить зовнішню IP-адресу клієнта, а також "Allowed IPs", які визначають призначену внутрішню адресу в межах VPN-мережі, і наявність актуального значення часу останнього "handshake", наприклад у межах кількох секунд або хвилин, свідчить про активний стан тунелю та коректну взаємодію між вузлами (див. рис. 2.15).

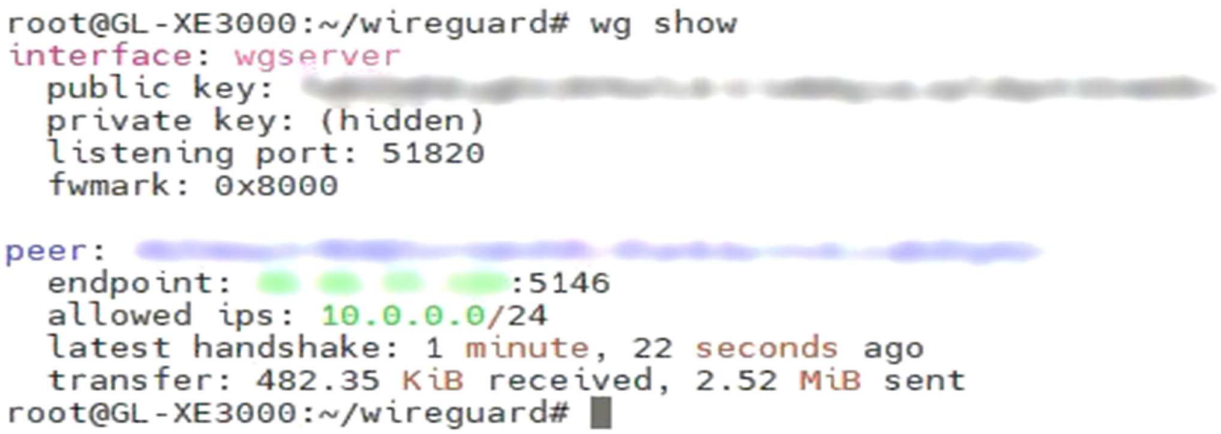


Рисунок 2.15 – Вивід команди wg show

Подальша перевірка передбачає аналіз внутрішньої адресації, де після встановлення з’єднання клієнт отримує віртуальну IP-адресу з попередньо визначеної підмережі, у даному випадку "10.0.0.2", яка використовується для доступу до ресурсів приватної інфраструктури, причому відповідність цієї адреси перевіряється як у клієнтському застосунку WireGuard, так і на стороні маршрутизатора через той самий "wg show", що дозволяє переконатися у правильності налаштування адресного простору та відсутності конфліктів у мережі.

Окремим аспектом виступає перевірка підміни зовнішньої IP-адреси, яка дозволяє підтвердити факт маршрутизації всього клієнтського трафіку через VPN-тунель, де до встановлення з’єднання клієнт використовує IP-адресу свого провайдера, наприклад мобільного оператора, а після активації тунелю зовнішня IP-адреса змінюється на адресу VPN-шлюзу, у цьому випадку "185.53.76.74", що підтверджується за допомогою спеціалізованих веб-сервісів перевірки IP, і така поведінка свідчить про реалізацію режиму повного тунелювання, при якому весь трафік, включаючи запити до інтернет-ресурсів, проходить через захищений канал, що одночасно забезпечує як конфіденційність, так і централізований контроль доступу (див. рис. 2.16).

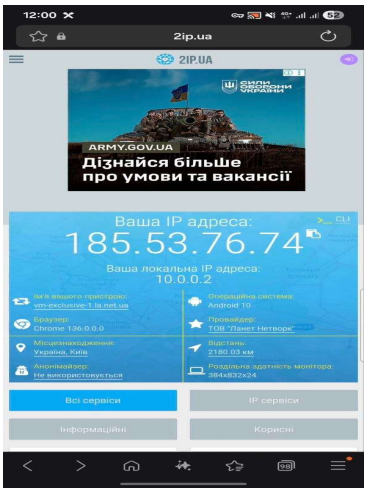


Рисунок 2.16 – Перевірка IP-адресації клієнта

Моніторинг трафіку в реальному часі. Моніторинг трафіку в реальному часі у межах побудованої системи віддаленого доступу розглядається як необхідний етап підтвердження її працездатності та оцінки фактичного навантаження на мережеву інфраструктуру, де особлива увага приділяється аналізу поведінки трафіку на інтерфейсі VPN-тунелю, зокрема на "wgserver", через який проходить увесь зашифрований обмін даними між клієнтами та сервером, при цьому контроль здійснюється із використанням консольних інструментів, що надають змогу отримувати інформацію у режимі реального часу безпосередньо з мережевого стеку операційної системи OpenWRT, що працює на маршрутизаторі.

У процесі моніторингу фіксуються ключові параметри, серед яких визначаються IP-адреси джерела та призначення, зокрема внутрішня адреса клієнта у VPN-мережі, наприклад "10.0.0.2", а також його зовнішня адреса, напрямок передавання трафіку, який поділяється на вхідний та вихідний потоки, і поточна швидкість передачі даних, що відображається у кілобайтах або мегабайтах за секунду, що дозволяє сформувати цілісне уявлення про інтенсивність використання каналу та характер мережевої активності, і завдяки цьому стає можливим визначення того, який саме обсяг даних проходить через VPN-тунель, наскільки активно клієнт використовує мережеві ресурси та чи відповідає фактичне навантаження очікуваним параметрам системи.

Для реалізації такого підходу використовується утиліта "iftop", яка запускається через SSH-доступ до маршрутизатора та відображає інформацію у вигляді динамічної таблиці з переліком активних з’єднань, де кожен рядок відповідає окремому мережевому потоку, а зміна значень у реальному часі дозволяє спостерігати за поведінкою трафіку під час виконання різних операцій, включаючи завантаження файлів або потокове відтворення відео, і така візуалізація забезпечує швидке виявлення пікових навантажень або нестандартної активності без необхідності застосування складних систем аналізу (див. рис. 2.17) [29].

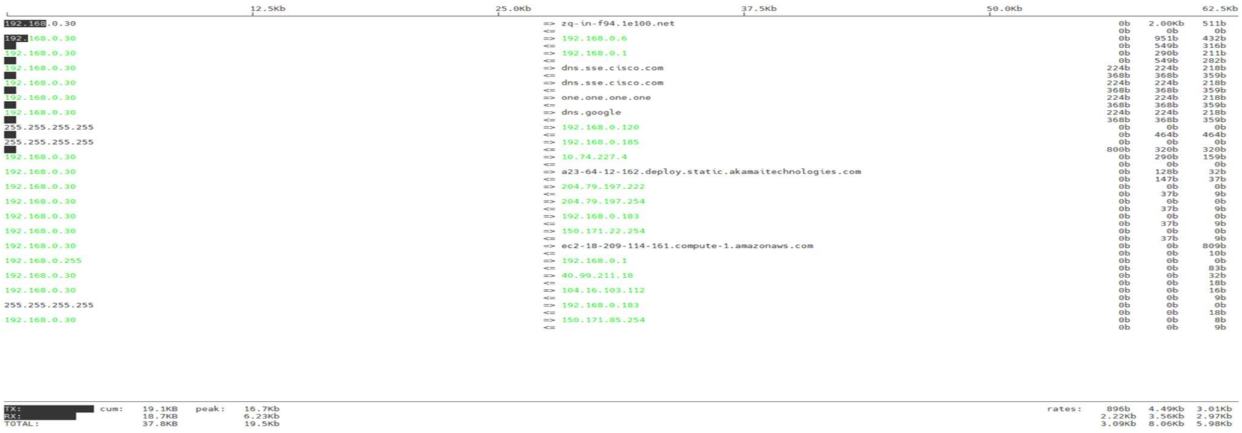


Рисунок 2.17 – Моніторинг трафіку через iftop

Поряд із цим можуть використовуватися альтернативні інструменти, які розширюють можливості моніторингу, зокрема "vnstat" для накопичення довгострокової статистики використання мережі, що дозволяє аналізувати обсяги трафіку за певні періоди часу, "nload" для наочного графічного відображення швидкості передачі даних у реальному часі, а також вбудовані засоби OpenWRT, доступні через веб-інтерфейс LuCI, де представлена базова інформація про стан інтерфейсів, завантаження каналу та загальні показники мережевої активності, що забезпечує додатковий рівень зручності при адмініструванні системи без необхідності використання командного рядка [29].

Аналіз отриманих даних у процесі моніторингу дозволяє виявляти аномальну активність, яка може свідчити про некоректну роботу клієнтів або потенційні загрози безпеці, оцінювати фактичне навантаження на канал зв’язку та визначати

вузькі місця у системі, які можуть обмежувати її продуктивність, наприклад перевантаження процесора або недостатню пропускну здатність мережевого інтерфейсу, а також контролювати використання ресурсів окремими клієнтами, що є важливим у сценаріях з великою кількістю підключень або обмеженими ресурсами каналу.

Навантажувальне тестування пропускної здатності. Навантажувальне тестування пропускної здатності в межах побудованої системи віддаленого доступу розглядається як обов'язковий етап оцінки її продуктивності, оскільки саме в умовах підвищеного навантаження стає можливим визначення реальних меж функціонування VPN-тунелю та ефективності використання апаратних ресурсів маршрутизатора, при цьому застосовуються як синтетичні, так і практичні сценарії тестування, що дозволяє отримати комплексне уявлення про поведінку системи в різних умовах експлуатації.

Синтетичний тест передбачає контрольоване навантаження на канал шляхом завантаження еталонного файлу фіксованого розміру, наприклад 100 МБ, через VPN-тунель, де послідовність виконання включає:

1. підключення клієнта до захищеної мережі;
2. ініціацію завантаження з віддаленого сервера;
3. подальшу фіксацію середньої швидкості передачі даних протягом усього процесу.

Такий підхід дозволяє ізолювати вплив сторонніх факторів та оцінити максимально можливу пропускну здатність тунелю, що формується на базі протоколу WireGuard, а результати вимірювань демонструють стабільну швидкість передачі без різких коливань, що свідчить про ефективну роботу механізмів шифрування та маршрутизації навіть при тривалому навантаженні.

Практичний сценарій тестування орієнтований на реальні умови використання системи та включає відтворення мультимедійного контенту високої якості, зокрема відео у форматі 4K з популярних відеохостингів, таких як YouTube, де оцінюються параметри, пов'язані із користувацьким досвідом, серед яких відсутність буферизації, стабільність якості відео, швидкість адаптації потоку при

зміні бітрейту та затримка під час перемикання між сегментами відео, і отримані результати свідчать про те, що VPN-з'єднання здатне забезпечувати безперервне відтворення контенту без деградації якості, що є важливим показником для систем, які використовуються не лише для передачі службових даних, але й для роботи з мультимедійними ресурсами (див. рис. 2.18).

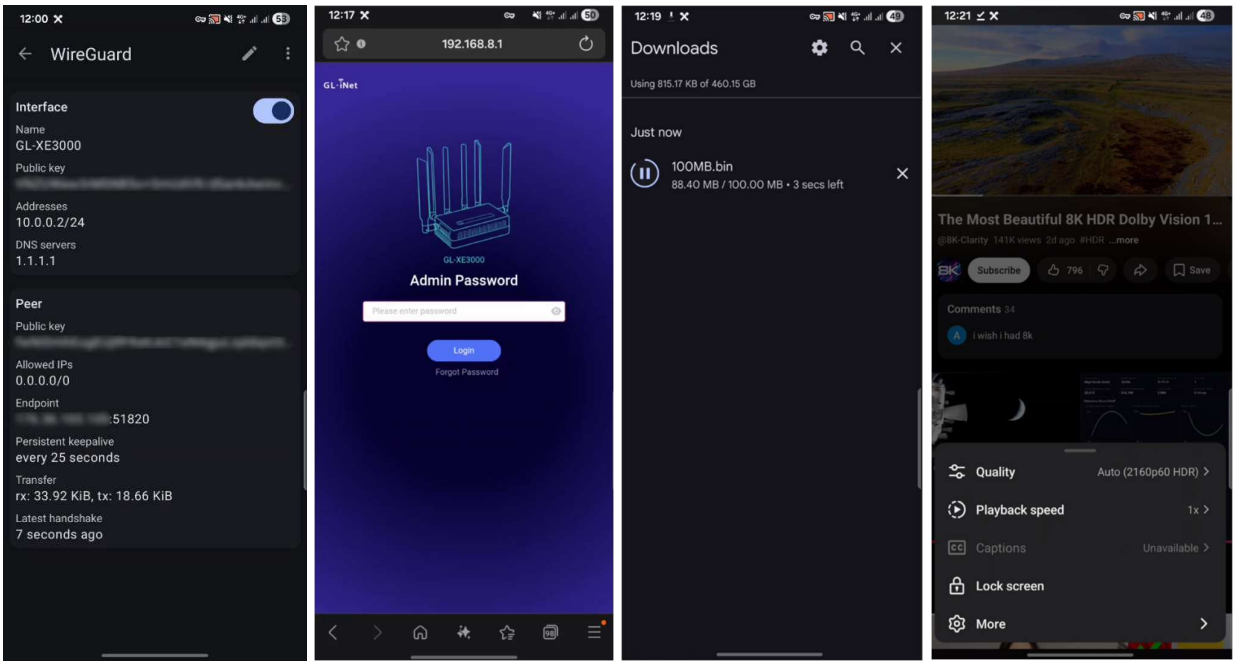


Рисунок 2.18 – Отримання доступу та спрямування трафіку через VPN до приватної інфраструктури

У процесі аналізу результатів тестування фіксується, що середня швидкість передачі даних у тунелі досягає приблизно 50 Мбіт/с і може перевищувати це значення залежно від умов мережі та навантаження на пристрій, при цьому спостерігається стабільність з'єднання без суттєвих втрат пакетів або значних затримок, що підтверджує ефективність використання протоколу WireGuard на вбудованих апаратних платформах, і така продуктивність дозволяє використовувати систему для широкого спектра задач, включаючи віддалене адміністрування, передачу великих обсягів даних, доступ до файлових сховищ або баз даних, а також роботу з мультимедійним контентом у реальному часі (див. рис. 2.19).

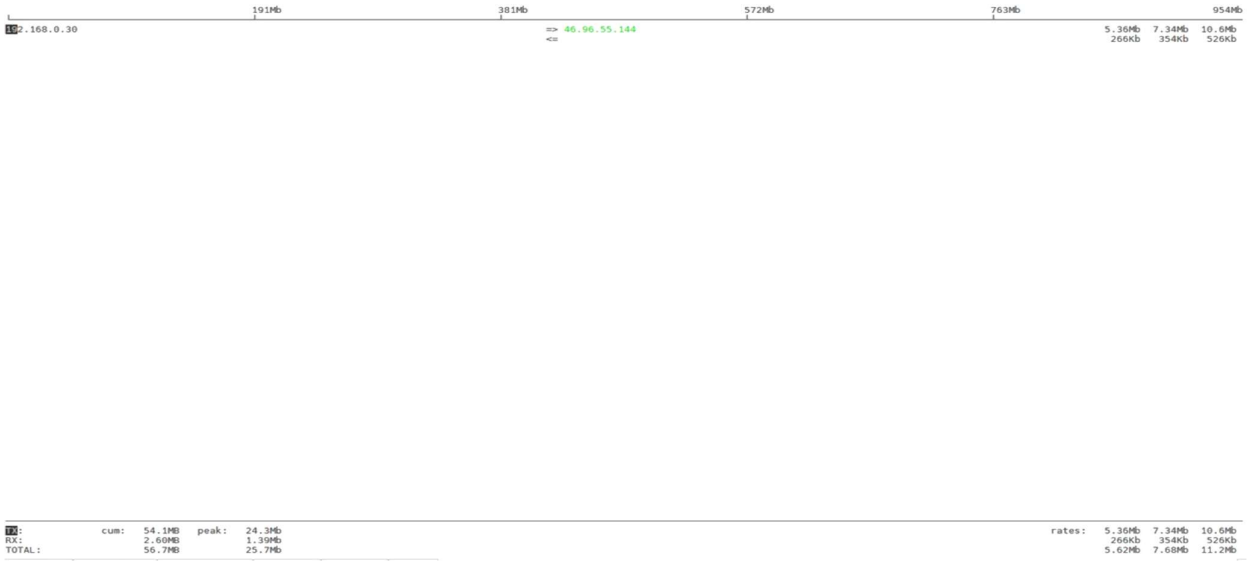


Рисунок 2.19 – Навантаження мережі під час завантаження файла фіксованого об’єму 100 МБ

Отримані результати навантажувальних тестів демонструють, що навіть за умов використання енергоефективного маршрутизатора система здатна забезпечувати рівень продуктивності, достатній для сучасних мережевих сценаріїв, де поєднуються вимоги до швидкості, стабільності та безпеки, а також підтверджують доцільність застосування такого підходу для розгортання VPN-шлюзів у мобільних або віддалених умовах, де використання повноцінних серверних рішень може бути обмеженим або економічно недоцільним (див. табл. 2.3).

Таблиця 2.3 – Результати навантажувального тестування пропускної здатності

Сценарій	Швидкість (Мбіт/с)	Затримка (мс)	Втрати пакетів (%)	Стабільність
Завантаження файлу (100 МБ)	50–60	20–30	<1%	Висока
Стрімінг 4K	45–55	25–35	<1%	Висока
Web-серфінг	30–40	15–25	<0.5%	Висока
Пікове навантаження	до 70	30–50	1–2%	Середня
Idle (очікування)	–	<10	0%	Стабільна

3. СИСТЕМНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ТА ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ VPN-ШЛЮЗУ

3.1 Технічний аудит та методи оптимізації конфігурації

У процесі практичної реалізації системи віддаленого доступу, розгорнутої на базі маршрутизатора класу edge з використанням OpenWRT, зокрема GL.iNet GL-XE3000 (Puli AX), формуються як логічне продовження етапів розгортання, тестування з’єднання та аналізу навантаження, де вже на практиці проявляються інженерні особливості, які не завжди очевидні на рівні теоретичного проєктування, оскільки реальне середовище експлуатації виявляє залежності між конфігураційними параметрами, поведінкою мережевого стеку, обмеженнями апаратної платформи та специфікою роботи криптографічних механізмів, і внаслідок цього аудит перетворюється не лише на процес виявлення та усунення помилок, а й на інструмент глибокої оптимізації системи, що дозволяє досягти стабільної, передбачуваної та безпечної роботи VPN-шлюзу з урахуванням реальних умов використання.

Верифікація криптографічних пар. У межах такого підходу особлива увага приділяється верифікації криптографічних пар, оскільки саме механізм обміну ключами лежить в основі функціонування WireGuard, де на відміну від класичних VPN-рішень із логіном і паролем довіра між вузлами повністю базується на коректності відповідності публічних і приватних ключів, і кожен вузол, незалежно від того чи виступає він сервером чи клієнтом, має власну унікальну пару ключів, при цьому приватний ключ зберігається локально та не передається жодній іншій стороні, тоді як публічний ключ використовується для ідентифікації та додається до конфігурації протилежного вузла.

У процесі практичного налаштування, особливо при використанні консольного підходу через SSH, генерація ключів здійснюється вручну через "wg

genkey" та "wg pubkey", що забезпечує повний контроль над криптографічними параметрами, проте одночасно підвищує ризик виникнення помилок, серед яких найпоширенішими виступають плутанина між приватним і публічним ключами, некоректне копіювання значень із додаванням зайвих символів або переносів рядків, а також використання ключів, що належать іншому вузлу, і такі неточності призводять до ситуації, коли VPN-тунель формально налаштований, порт прослуховується, але з'єднання фактично не встановлюється, що проявляється у відсутності параметра "latest handshake" у виводі діагностичних команд (див. рис. 3.1).

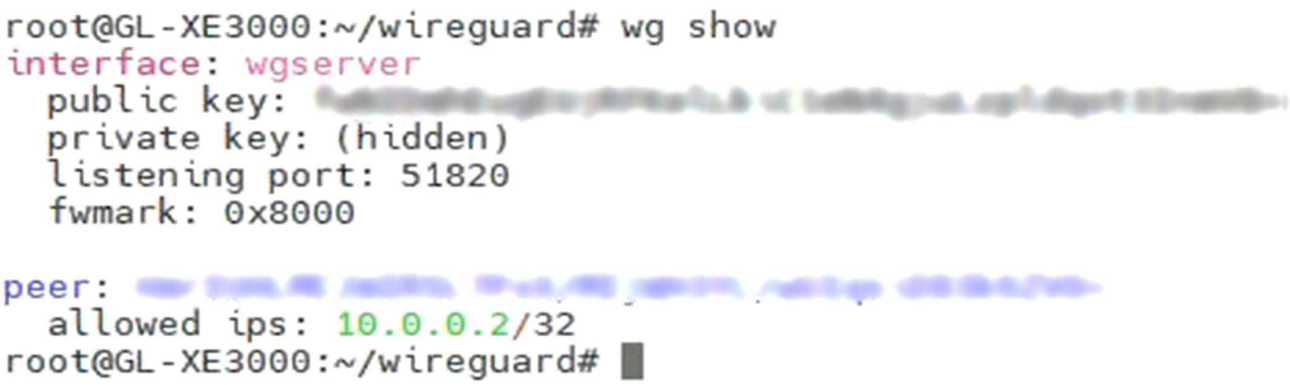


Рисунок 3.1 – Помилка конфігурації ключів

Для виявлення подібних проблем застосовується команда "wg show", яка дозволяє отримати повну інформацію про стан інтерфейсу, включаючи наявність або відсутність криптографічного обміну, обсяг переданого трафіку та перелік підключених peer-вузлів, і у випадку, коли "handshake" не відбувається, першочерговою дією виступає перевірка відповідності ключів, що може бути виконана шляхом повторного обчислення публічного ключа з приватного за допомогою команди "wg pubkey" та подальшого порівняння отриманого значення з тим, що вказане у конфігурації протилежної сторони, і такий підхід дозволяє швидко локалізувати помилку без необхідності аналізу всіх інших параметрів системи (див. рис. 3.2).

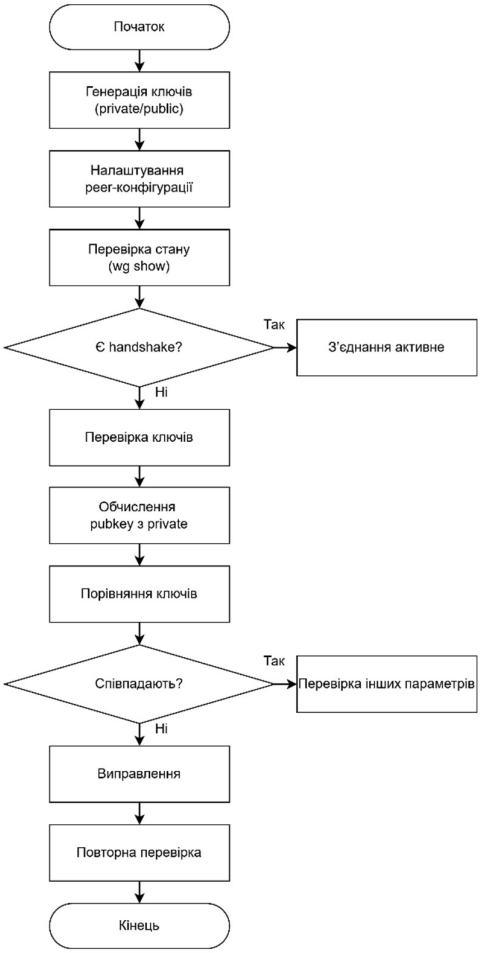


Рисунок 3.2 – Верифікація криптографічних пар

Узагальнюючи, верифікація криптографічних пар розглядається як базовий етап технічного аудиту, що дозволяє забезпечити коректність фундаментального механізму автентифікації у WireGuard, а також виступає відправною точкою для подальшої оптимізації конфігурації, оскільки будь-які інші налаштування втрачають сенс у разі порушення цілісності криптографічної взаємодії між вузлами, і врахування типових помилок на цьому рівні дозволяє підвищити надійність системи та уникнути повторення подібних ситуацій у подальшій експлуатації.

Валідація мережевої адресації. Валідація мережевої адресації у процесі побудови системи віддаленого доступу виступає одним із критичних аспектів, що безпосередньо впливає на коректність функціонування VPN-з'єднання, оскільки неправильне налаштування IP-адрес або масок мережі може призводити до

помилок маршрутизації, відмови у встановленні з’єднання або некоректної обробки трафіку, і в умовах практичної реалізації, де кожен клієнт отримує окрему внутрішню адресу в межах віртуальної підмережі, наприклад "10.0.0.2", особливо важливо забезпечити відповідність між цією адресою та параметрами, що задаються у конфігурації WireGuard.

Під час конфігурації часто використовується параметр "AllowedIPs", який визначає як дозволені адреси для конкретного клієнта, так і правила маршрутизації, і у випадку некоректного зазначення маски, наприклад у вигляді "10.0.0.2/24", система може повертати помилку типу "RTNETLINK answers: invalid argument (nonzero host part) ", що виникає через невідповідність між адресою вузла та маскою мережі, оскільки маска "/24" означає цілу підмережу "10.0.0.0/24", тоді як вказується конкретний хост, що суперечить базовим принципам адресації та маршрутизації в Linux-системах.

У процесі оптимізації конфігурації правильним рішенням виступає використання маски "/32" для кожного окремого клієнта, наприклад "10.0.0.2/32", що означає визначення єдиного вузла без розширення на всю підмережу, і такий підхід повністю відповідає логіці роботи WireGuard, зокрема механізму Cryptokey Routing, де кожен peer асоціюється з конкретним набором IP-адрес, які він має право використовувати, і завдяки цьому досягається чітка ізоляція клієнтів один від одного та виключається можливість несанкціонованого доступу до інших адрес у межах тієї ж підмережі (див. рис. 3.3).

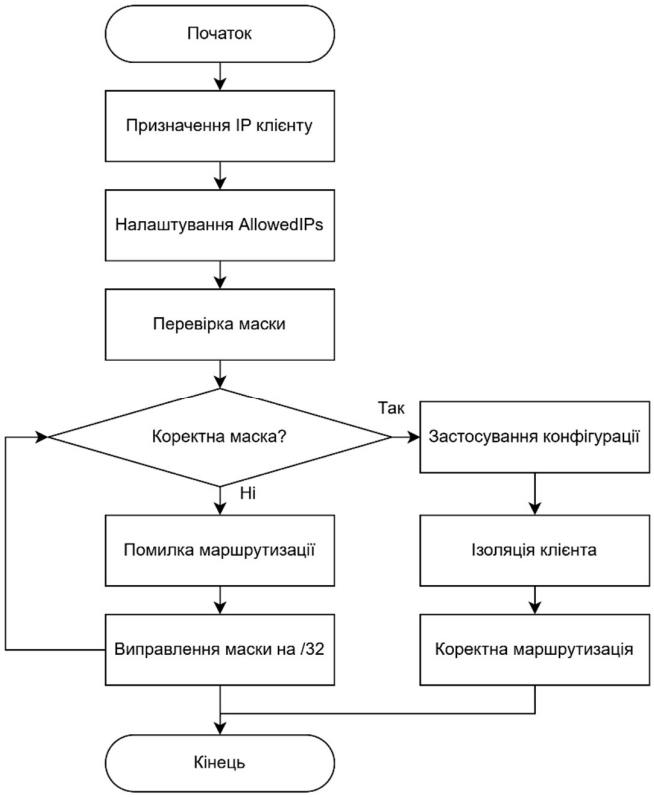


Рисунок 3.3 – Валідація мережевої адресації

Застосування коректної адресації має низку важливих наслідків, серед яких підвищення рівня безпеки за рахунок обмеження доступу кожного клієнта лише до визначених ресурсів, спрощення контролю доступу, оскільки кожен вузол ідентифікується однозначно, а також усунення потенційних конфліктів маршрутизації, які можуть виникати при перекритті адресних просторів або неправильному визначенні мережевих діапазонів, і таким чином правильна побудова адресного простору перестає бути лише технічною вимогою, переходячи у площину архітектурних рішень, що впливають на загальну надійність та безпеку всієї системи віддаленого доступу.

Синхронізація CLI-налаштувань з системними службами. У процесі практичної реалізації системи віддаленого доступу на базі маршрутизатора класу Embedded із використанням середовища OpenWRT, зокрема на прикладі GL.iNet GL-XE3000, формується необхідність глибшого розуміння взаємодії між динамічними налаштуваннями, що виконуються через консоль, та постійними

конфігураціями, які зберігаються у системних службах. Особливу увагу привертає використання команди "wg set", яка дозволяє додавати нових клієнтів безпосередньо у простір ядра Linux, фактично виконуючи «ін’єкцію» параметрів у runtime-середовище без зміни конфігураційних файлів. Такий підхід відкриває широкі можливості для оперативного адміністрування, проте водночас формує специфічну поведінку системи, пов’язану з тим, що всі внесені зміни існують лише до моменту перезавантаження пристрою.

При застосуванні цієї моделі конфігурації доданий клієнт стає активним одразу після виконання команди, отримує доступ до VPN-тунелю та може передавати трафік відповідно до заданих параметрів, однак після рестарту маршрутизатора всі такі налаштування повністю зникають, оскільки вони не були записані у постійні конфігураційні файли OpenWRT. Подібна поведінка пояснюється тим, що "wg set" працює виключно на рівні оперативного стану інтерфейсу WireGuard, минаючи механізми ініціалізації системних служб, які відповідають за відновлення конфігурації під час запуску системи. У результаті після перезавантаження необхідно повторно виконувати команду додавання піра, наприклад "wg set wgserver peer <public_key> allowed-ips 10.0.0.2/32", що створює додаткове навантаження на адміністратора у випадку, якщо така поведінка не була врахована заздалегідь.

У цьому контексті виникає потреба у синхронізації між тимчасовими CLI-налаштуваннями та постійними механізмами конфігурації системи, що може бути реалізовано декількома підходами, кожен із яких має власні особливості застосування залежно від сценарію використання. Перший підхід полягає у перенесенні сформованих параметрів у конфігураційні файли OpenWRT, зокрема через редагування системних файлів у директорії "/etc/config/", де описується мережева логіка, інтерфейси та параметри WireGuard, що дозволяє забезпечити автоматичне відновлення всіх налаштувань після перезапуску. Альтернативним варіантом виступає використання веб-інтерфейсу GL.iNet, який інтегрує ці налаштування у власну систему керування профілями, забезпечуючи їх збереження

та синхронізацію з внутрішніми службами без необхідності ручного редагування конфігураційних файлів.

Додатково може застосовуватись підхід автоматизації через скрипти ініціалізації, коли необхідні команди додаються до файлу "/etc/rc.local" або оформлюються у вигляді окремих init-скриптів, що виконуються під час старту системи, таким чином відновлюючи runtime-конфігурацію автоматично без участі адміністратора. Такий варіант є особливо доцільним у випадках, коли потрібно зберегти гнучкість динамічного налаштування, але водночас уникнути ручного повторення команд після кожного перезавантаження (див. рис. 3.4).

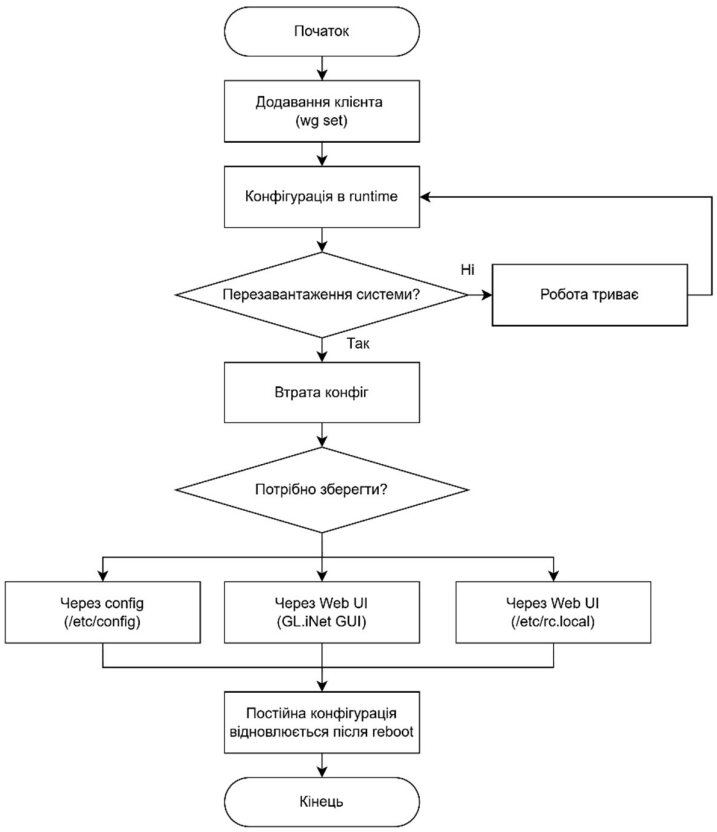


Рисунок 3.4 – Синхронізація CLI-налаштувань з системними службами

Подібна модель подвійної конфігурації, де одночасно існують як тимчасові, так і постійні налаштування, формує гнучку архітектуру управління доступом, у якій можна свідомо обирати між стабільністю та динамічністю залежно від поставлених задач. Тимчасові конфігурації дозволяють швидко організовувати

доступ без зміни основної структури системи, що є зручним для тестування, налагодження або надання короткострокового доступу технічному персоналу чи зовнішнім користувачам, тоді як постійні налаштування забезпечують довготривалу стабільність і передбачуваність роботи VPN-шлюзу в умовах постійної експлуатації.

У результаті така поведінка системи не сприймається як недолік, а розглядається як функціональна особливість, що значно розширює можливості адміністрування, дозволяючи адаптувати систему під різні сценарії використання, поєднуючи оперативність змін із надійністю збережених конфігурацій і формуючи збалансований підхід до управління мережею в умовах змінного навантаження та різнорідних вимог до доступу.

3.2 Порівняльний аналіз архітектурних рішень віддаленого доступу

У процесі побудови системи віддаленого доступу до приватної інфраструктури виникає необхідність проведення порівняльного аналізу двох фундаментально різних архітектурних підходів, що застосовуються для реалізації VPN — класичної серверної моделі та сучасної моделі, заснованої на концепції Edge Computing, у якій функції шифрування, автентифікації та маршрутизації інтегруються безпосередньо у граничний мережевий вузол, що у даному випадку представлений маршрутизатором класу GL.iNet GL-XE3000, який працює під керуванням OpenWRT та виконує роль повноцінного VPN-шлюзу, що дозволяє оцінити доцільність такого підходу з точки зору ефективності, стабільності та економічної обґрунтованості на основі практичних результатів тестування, аналізу затримок, пропускної здатності та особливостей обробки мережевого трафіку.

Ефективність Edge Computing vs Centralized Server. Архітектурні відмінності між цими підходами стають очевидними вже на рівні побудови логічної схеми взаємодії компонентів, оскільки у класичній серверній моделі клієнтський

пристрій встановлює VPN-з’єднання з окремим сервером, який розміщений у внутрішній мережі за маршрутизатором, у результаті чого трафік проходить послідовність вузлів, що включає:

— клієнта;
— зовнішню мережу Інтернет;
— граничний маршрутизатор;
— внутрішній VPN-сервер.

Лише після цього досягає цільових ресурсів локальної мережі, тоді як у моделі Edge Computing VPN-функціональність інтегрована безпосередньо у маршрутизатор, що дозволяє скоротити цей ланцюг до послідовності клієнт — Інтернет — VPN-шлюз — локальна мережа, усуваючи проміжний рівень у вигляді окремого сервера та відповідно змінюючи характер обробки трафіку.

Подібна трансформація архітектури безпосередньо впливає на ефективність функціонування системи, оскільки відсутність додаткового мережевого переходу, який у класичних схемах часто позначається як "extra hop", призводить до зменшення затримок передачі даних, скорочення кількості операцій обробки пакетів та зниження навантаження як на мережеву інфраструктуру, так і на обчислювальні ресурси окремих вузлів, при цьому розшифрування трафіку відбувається безпосередньо на вході до мережі, після чого пакет одразу маршрутизується до кінцевого ресурсу, наприклад до внутрішніх серверів або служб із адресами типу "192.168.8.1", без необхідності повторної передачі через додаткові внутрішні вузли, що особливо важливо у сценаріях, де критичними є мінімальні затримки, таких як доступ до баз даних у режимі реального часу або передача відеопотоків високої якості [30].

Поряд із цим спрощується загальна логіка побудови мережі, оскільки у класичному підході необхідно виконувати додаткові налаштування, пов’язані з організацією доступу до внутрішнього VPN-сервера, включаючи налаштування NAT, відкриття портів, конфігурацію правил міжмережевого екрану та забезпечення коректної маршрутизації між сегментами мережі, що підвищує складність адміністрування та створює додаткові точки потенційних помилок, тоді

як у моделі з інтегрованим VPN-шлюзом уся логіка контролю доступу концентрується в одному пристрої, що виступає єдиною точкою входу до інфраструктури та забезпечує централізоване управління політиками доступу, маршрутизацією та шифруванням (див. табл. 3.1).

Таблиця 3.1 – Порівняння Edge VPN-шлюзу та централізованого серверного рішення

Критерій	Edge VPN-шлюз	Централізований сервер
Кількість мережевих переходів	Мінімальна	Більша
Затримка	Низька	Вища
Архітектура	Спрощена	Складна
Відмовостійкість	Висока (локалізація)	Залежить від сервера
Масштабованість	Гнучка	Обмежена
Адміністрування	Централізоване	Розподілене
Вартість розгортання	Низька	Висока
Продуктивність	Висока	Середня

Практичні результати експлуатації підтверджують переваги такого підходу, оскільки встановлення з’єднання відбувається швидко, доступ до внутрішніх ресурсів здійснюється без відчутних затримок, а відсутність додаткових етапів обробки трафіку дозволяє досягти більш стабільної роботи навіть за умов змінної якості зовнішнього каналу зв’язку, що особливо актуально при використанні мобільного інтернету або резервних каналів передачі даних.

Апаратна стійкість в умовах критичної інфраструктури. Аналізуючи питання стійкості мережевих рішень в умовах нестабільної інфраструктури, стає очевидним, що традиційні серверні підходи до організації VPN, навіть за наявності високопродуктивного обладнання, мають низку системних обмежень, пов’язаних передусім із залежністю від зовнішніх факторів, серед яких визначальними залишаються безперебійність електроживлення, стабільність роботи провайдера та фізична прив’язаність до конкретної локації розміщення серверного вузла, унаслідок чого будь-яке порушення у цих компонентах безпосередньо впливає на доступність сервісу та призводить до розриву VPN-з’єднань, втрати доступу до внутрішніх ресурсів і порушення безперервності бізнес-процесів.

Класична модель передбачає використання окремого серверного обладнання, яке потребує постійного живлення, а отже вимагає додаткового впровадження систем безперебійного живлення, що збільшує як вартість розгортання, так і складність обслуговування, при цьому у випадку тривалого відключення електроенергії навіть наявність ДБЖ має обмежений ефект, оскільки його ресурс є кінцевим, а також не вирішує проблему втрати зв’язку у разі аварій на стороні провайдера, коли сервер фізично залишається увімкненим, але недоступним ззовні через відсутність каналу передачі даних.

На цьому фоні апаратний VPN-шлюз, реалізований на базі маршрутизатора класу GL.iNet GL-XE3000, демонструє принципово інший підхід до забезпечення відмовостійкості, який базується на інтеграції мережевих, обчислювальних і енергетичних компонентів у межах одного компактного пристрою, що дозволяє мінімізувати залежність від зовнішньої інфраструктури та забезпечити стабільну роботу навіть у складних умовах експлуатації. Наявність вбудованого акумулятора ємністю близько 6400 мА·год забезпечує автономне функціонування пристрою протягом кількох годин, що на практиці може досягати 8–10 годин безперервної роботи, унаслідок чого VPN-з’єднання зберігається навіть при повному зникненні електроживлення у мережі, а доступ до критичних ресурсів не переривається (див. рис. 3.5).

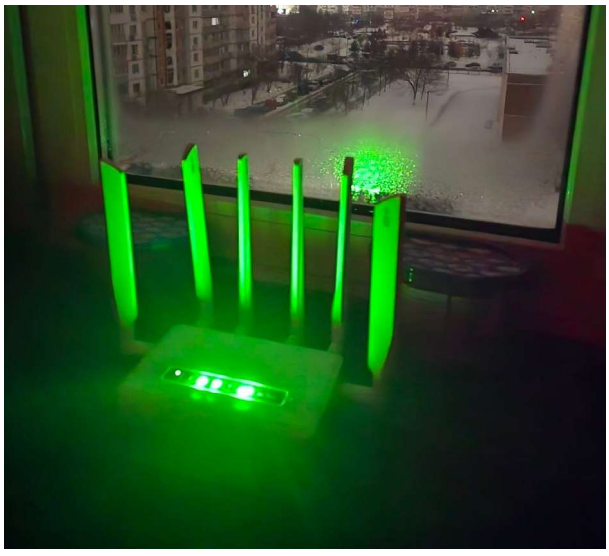


Рисунок 3.5 – Робота VPN при зникнені електроенергії

Додатковий рівень стійкості формується за рахунок інтегрованого модема з підтримкою мобільних мереж стандартів 4G та 5G, використовуючи потужний модуль Quectel RM520N-GL, що дозволяє використовувати пристрій як автономний вузол доступу без прив’язки до провідного інтернету, причому реалізується механізм резервування каналу зв’язку з автоматичним перемиканням за принципом "failover", коли у разі втрати основного з’єднання система самостійно переходить на альтернативний канал передачі даних, зберігаючи активність VPN-тунелю та прозорість роботи для кінцевих користувачів (див. рис. 3.6).

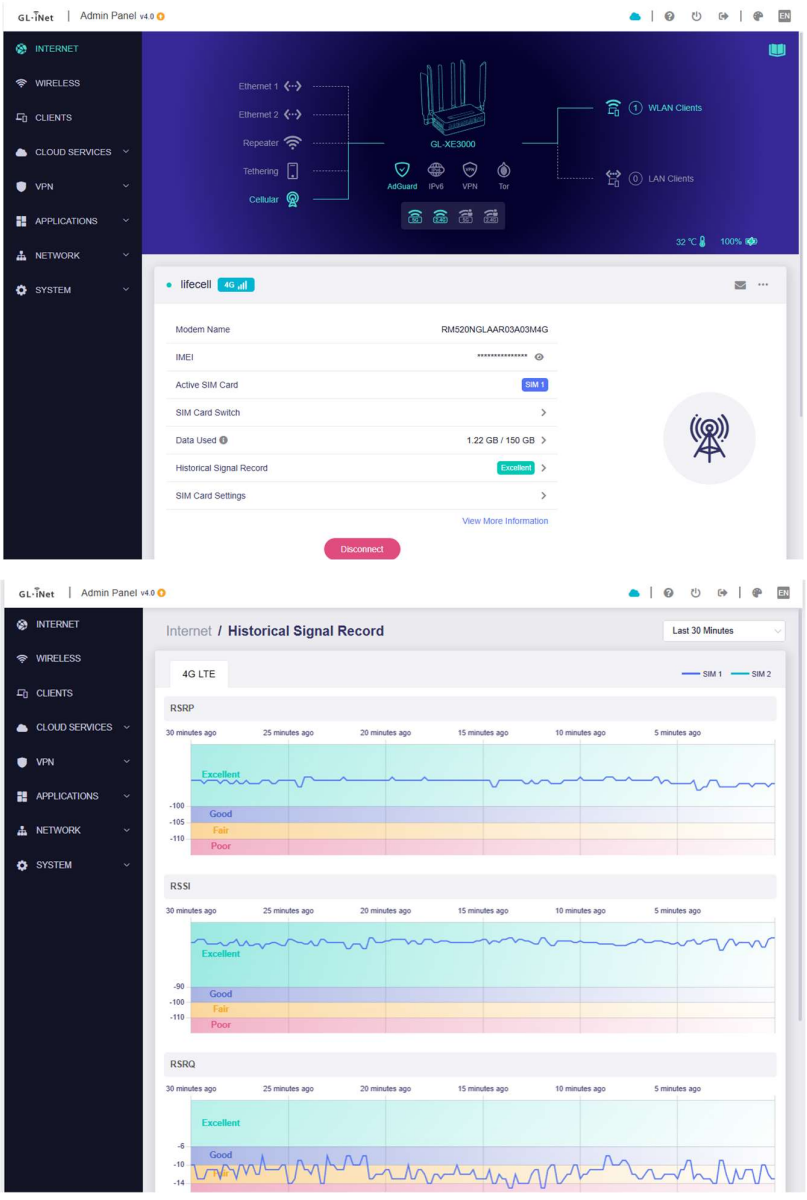


Рисунок 3.6 – Робота VPN при відмові основного каналу

Фізична компактність і мобільність пристрою відкривають можливості для розгортання у практично будь-яких умовах, включаючи:

— тимчасові об’єкти;

— польові середовища;

— транспортні засоби;

— віддалені локації без розвиненої інфраструктури.

Там де традиційні серверні рішення або є економічно недоцільними, або взагалі не можуть бути реалізовані через відсутність необхідних ресурсів, при цьому розгортання не потребує окремих серверних приміщень, складної кабельної інфраструктури чи додаткового обладнання, що значно спрощує процес впровадження та знижує поріг входу для використання таких технологій.

Практичне значення подібних характеристик проявляється у сценаріях, пов’язаних із роботою в умовах блекаутів, організацією тимчасових мереж на будівельних майданчиках, забезпеченням зв’язку у мобільних офісах або транспортних засобах, а також у системах моніторингу та віддаленого адміністрування, де критично важливо зберігати постійний доступ до інфраструктури незалежно від зовнішніх умов, у результаті чого апаратний VPN-шлюз забезпечує значно вищий рівень відмовостійкості, автономності та безперервності роботи порівняно з класичними серверними підходами, що робить його більш придатним для експлуатації в сучасних нестабільних середовищах.

Пропускна здатність та ресурсна ємність. Порівняння пропускної здатності та ресурсної ємності різних апаратних платформ традиційно базується на припущенні, що серверні системи архітектури x86 мають суттєво вищу продуктивність у порівнянні з вбудованими рішеннями на базі ARM або MIPS, які характеризуються:

— обмеженими обчислювальними ресурсами;

— меншою тактовою частотою процесора;

— обмеженим обсягом оперативної пам’яті.

Однак поява протоколу WireGuard змінює цей баланс завдяки особливостям його реалізації, що дозволяють ефективно використовувати навіть ресурсообмежені пристрої без суттєвих втрат у швидкодії [31].

Архітектурна оптимізація WireGuard базується на виконанні більшості операцій безпосередньо у просторі ядра Linux, що усуває необхідність частих перемикань між "kernel space" та "user space", зменшуючи накладні витрати на обробку пакетів, при цьому мінімалістичний обсяг коду та використання сучасних криптографічних алгоритмів дозволяють досягти високої швидкості шифрування та дешифрування даних із мінімальним навантаженням на центральний процесор, унаслідок чого знижується затримка передачі пакетів і підвищується загальна пропускна здатність VPN-тунелю навіть на пристроях із відносно скромними технічними характеристиками.

Практичні результати тестування підтверджують ефективність такого підходу, оскільки в умовах реальної експлуатації зафіксовано стабільну швидкість передачі даних на рівні близько 50 Мбіт/с і вище, що супроводжується відсутністю значних втрат пакетів і стабільною роботою сервісів, чутливих до затримок, включаючи потокове відтворення відео у форматі 4K та завантаження великих обсягів даних через захищений тунель, при цьому обчислювальні ресурси маршрутизатора не досягають критичних значень навантаження, що свідчить про ефективне використання апаратної платформи.

У контексті порівняння з традиційними VPN-рішеннями, зокрема з OpenVPN, різниця стає ще більш помітною, оскільки обробка трафіку в OpenVPN відбувається у "user space", що супроводжується більшими накладними витратами, додатковими затримками та підвищеним навантаженням на процесор, унаслідок чого для досягнення аналогічного рівня продуктивності необхідне значно потужніше апаратне забезпечення, що прямо впливає на вартість розгортання та енергоспоживання системи.

Отримані результати дозволяють зробити висновок, що навіть за умов використання ARM-процесора маршрутизатор здатний ефективно обробляти зашифрований трафік без формування вузьких місць у системі, забезпечуючи

комфортну роботу користувачів та стабільний доступ до ресурсів приватної мережі, при цьому відсутня необхідність у впровадженні окремого серверного вузла для обробки VPN-з'єднань, що у багатьох сценаріях робить таке рішення надлишковим як з технічної, так і з економічної точки зору [29].

З урахуванням вартості обладнання, складності адміністрування та енергоспоживання використання окремого VPN-сервера призводить до зростання витрат без пропорційного приросту продуктивності, тоді як маршрутизатор, що поєднує функції мережевого шлюзу та VPN-сервера, забезпечує достатній рівень пропускної здатності, компактність, простоту впровадження та ефективне використання доступних ресурсів, унаслідок чого реалізація VPN безпосередньо на граничному маршрутизаторі постає як технічно обґрунтоване та практично оптимальне рішення, що природно переходить до подальшого аналізу економічної доцільності та масштабованості такої архітектури.

3.3 Економічна доцільність та масштабованість проєкту

Комплексний аналіз економічної доцільності впровадження системи віддаленого доступу на базі апаратного VPN-шлюзу, реалізованого із використанням маршрутизатора класу GL.iNet GL-XE3000, передбачає оцінку сукупної вартості володіння, порівняння з традиційними комерційними рішеннями та визначення можливостей масштабування залежно від сценаріїв використання, при цьому особлива увага зосереджується на балансі між початковими витратами, експлуатаційними витратами та гнучкістю системи, що в сукупності формує уявлення про доцільність такого підходу як для індивідуального використання, так і для корпоративного середовища.

Аналіз вартості володіння (TCO) та ліцензійної чистоти. У традиційних корпоративних VPN-рішеннях структура витрат є багаторівневою та включає придбання:

— серверного обладнання;

— мережевої інфраструктури;

— ліцензій на програмне забезпечення;

— оплату підписок;

— витрати на технічну підтримку та регулярні оновлення.

Причому одним із найбільш суттєвих факторів виступає саме ліцензування, оскільки у більшості комерційних платформ кожен підключений користувач потребує окремої ліцензії, що призводить до лінійного зростання витрат із розширенням системи, а також накладає обмеження на кількість одночасних підключень, унаслідок чого навіть незначне масштабування інфраструктури може супроводжуватися суттєвими фінансовими витратами (див. рис. 3.7) [32].

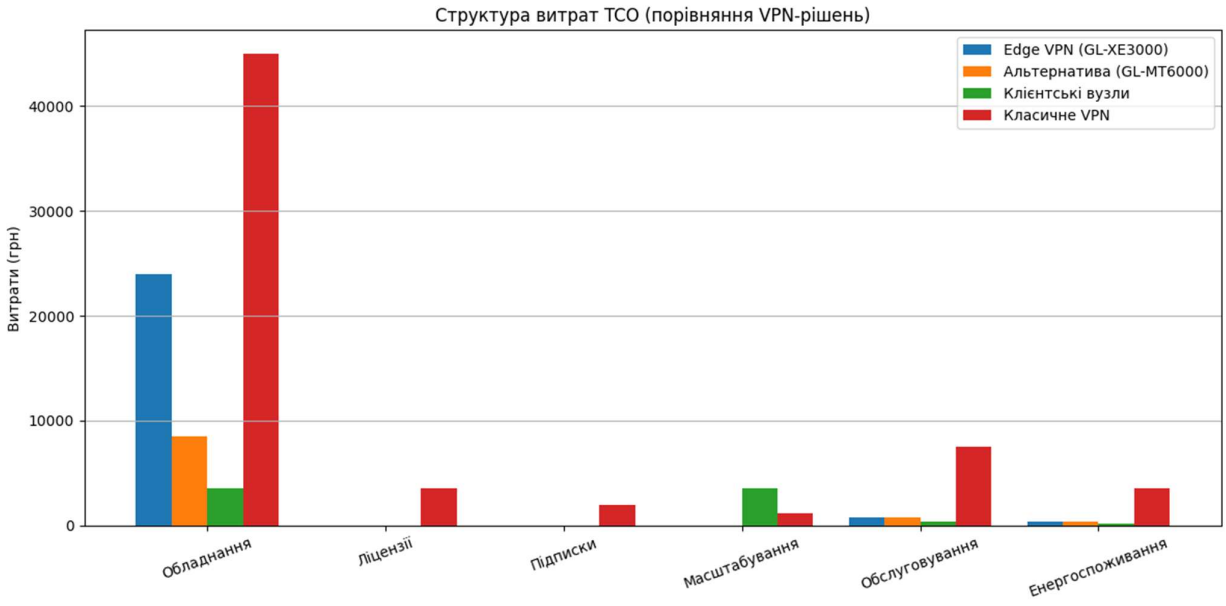


Рисунок 3.7 – Структура витрат TCO

На відміну від цього підходу, у реалізованій системі використовується програмне забезпечення з відкритим вихідним кодом, зокрема операційна система OpenWRT та протокол WireGuard, які не потребують ліцензійних платежів і можуть застосовуватися без обмежень щодо кількості користувачів, унаслідок чого витрати на програмну складову фактично дорівнюють нулю, а відсутність

залежності від постачальника дозволяє уникнути прив’язки до конкретного вендора та забезпечує повний контроль над системою.

З урахуванням практичної реалізації структура загальної вартості володіння формується переважно за рахунок одноразових витрат на придбання апаратного пристрою та базове налаштування, тоді як поточні витрати обмежуються споживанням електроенергії, оплатою інтернет-з’єднання та, за потреби, адміністративним обслуговуванням, причому відсутні витрати на ліцензії, підписки чи платні оновлення, що істотно знижує фінансове навантаження у довгостроковій перспективі [32].

Порівняльний аналіз демонструє, що у випадку використання апаратного VPN-шлюзу загальна вартість володіння є значно нижчою у порівнянні з комерційними рішеннями, при цьому масштабування системи не супроводжується додатковими витратами на ліцензування, а розширення кількості клієнтів або зміна конфігурації не потребує фінансових вкладень, що створює сприятливі умови для поступового розвитку інфраструктури без ризику різкого зростання витрат.

Гнучкість такого підходу дозволяє адаптувати систему під різні сценарії використання, починаючи від домашніх мереж і закінчуючи корпоративними середовищами, де важливими є як економічна ефективність, так і можливість швидкого масштабування без складних процедур узгодження та закупівель, унаслідок чого запропоноване рішення демонструє високу доцільність впровадження, поєднуючи мінімальні початкові витрати, відсутність ліцензійних обмежень та можливість подальшого розширення функціональності без суттєвих змін у базовій архітектурі системи.

Масштабування на базі модельного ряду вбудованих систем. У межах розгляду масштабованості системи віддаленого доступу на базі вбудованих рішень формується підхід, у якому апаратна складова безпосередньо пов’язана з можливістю адаптації до різних сценаріїв використання, при цьому використання OpenWRT як уніфікованої програмної платформи забезпечує перенесення однієї й тієї ж логіки конфігурації між різними пристроями без суттєвих змін, що дозволяє

будувати ієрархію вузлів різного рівня складності та продуктивності із збереженням спільної архітектури системи.

У цьому контексті доцільно розглядати декілька рівнів апаратної реалізації, які відрізняються не логікою роботи, а:

— ресурсами;

— мобільністю;

— сферою застосування.

При цьому найвищий рівень представлений мобільними граничними вузлами з розширеним функціоналом, де використовується маршрутизатор класу GL.iNet Puli AX GL-XE3000, що характеризується підтримкою мобільних мереж 4G/5G, наявністю вбудованого акумулятора та високою продуктивністю обробки VPN-трафіку, а також орієнтований на використання в польових умовах, критичній інфраструктурі або як автономний вузол доступу, хоча його вартість є відносно високою і може досягати приблизно 23999 гривень, що обмежує доцільність застосування у менш вимогливих сценаріях.

На наступному рівні формується більш збалансований підхід у вигляді стаціонарних офісних VPN-шлюзів, де можуть застосовуватись моделі на кшталт GL-MT6000 або Flint 2, які не мають вбудованого акумулятора, але забезпечують достатню обчислювальну потужність для стабільної роботи у постійному середовищі, при цьому зниження апаратної складності дозволяє зменшити вартість до приблизно 8000–9000 гривень, що робить такі рішення оптимальними для офісних мереж, домашніх інфраструктур або як центральний вузол VPN-доступу без необхідності мобільності.

Ще один рівень представлений компактними клієнтськими пристроями, такими як GL-MT3000 або GL-AXT1800 Slate AX, які орієнтовані на індивідуальне використання та мобільні сценарії, де важливими характеристиками виступають портативність, простота налаштування та можливість роботи у ролі VPN-клієнта, при цьому їхня вартість значно нижча і знаходиться в межах приблизно 3000–4000 гривень, що дозволяє масштабувати систему за рахунок великої кількості кінцевих точок доступу без значного фінансового навантаження (див. табл. 3.2).

Таблиця 3.2 – Порівняльний аналіз вартості володіння (TCO)

Витрати	Edge VPN (GL-XE3000)	Альтернатива (GL-MT6000 / Flint 2)	Клієнтські вузли (GL-MT3000 / Slate AX)	Класичне VPN-рішення (сервер)
Початкове обладнання	~24000 грн	~8000–9000 грн	~3000–4000 грн (за 1 пристрій)	~30000–60000 грн (сервер + мережа)
Ліцензії	0 грн	0 грн	0 грн	~2000–5000 грн/рік
Підписки	0 грн	0 грн	0 грн	~1000–3000 грн/рік
Вартість масштабування	0 грн	0 грн	~3000–4000 грн/користувач	~500–2000 грн/користувач
Обслуговування (рік)	~500–1000 грн	~500–1000 грн	~200–500 грн	~5000–10000 грн
Енергоспоживання (рік)	~300–500 грн	~300–500 грн	~100–200 грн	~2000–5000 грн
Загальні витрати за 1 рік	~25000 грн	~9000–11000 грн	~3500–4500 грн	~40000–80000 грн
Загальні витрати за 3 роки	~26000–28000 грн	~10000–13000 грн	~4000–6000 грн	~60000–120000 грн
Вартість 1 користувача (10 users)	~2500 грн	~1000 грн	~3500 грн (персональний вузол)	~4000–8000 грн

Об’єднання всіх цих рівнів в єдину систему стає можливим завдяки уніфікованій архітектурі, оскільки незалежно від обраного пристрою конфігурація WireGuard залишається ідентичною, а інтерфейси управління через веб-середовище та консоль OpenWRT забезпечують однаковий підхід до адміністрування, що спрощує підтримку, зменшує кількість помилок та дозволяє швидко інтегрувати нові вузли без необхідності перебудови всієї системи (див. рис. 3.8) [32-33].

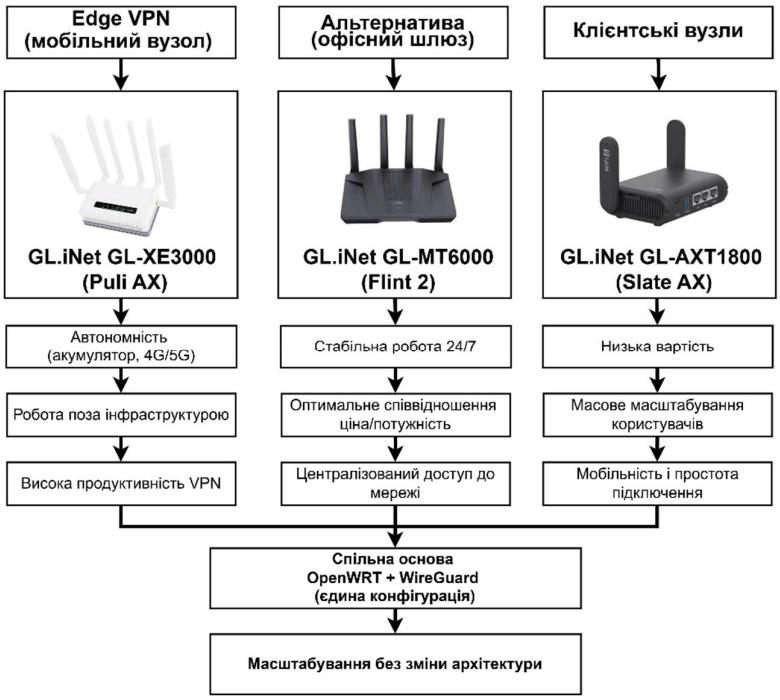


Рисунок 3.8 – Масштабування системи на різних пристроях GL.iNet

Додатковим аспектом виступає розширюваність функціоналу, оскільки платформа OpenWRT дозволяє встановлювати додаткові пакети та сервіси, що розширює можливості використання пристроїв далеко за межі лише VPN-доступу, включаючи мережевий моніторинг, фільтрацію трафіку, альтернативні VPN-протоколи або інтеграцію з іншими сервісами, що забезпечує довготривалий життєвий цикл обладнання та його адаптацію до нових задач без необхідності заміни апаратної бази.

У підсумку формується гнучка модель масштабування, де система може варіюватися від бюджетних клієнтських рішень до потужних мобільних вузлів із повною автономністю, при цьому логіка роботи, підходи до конфігурації та механізми безпеки залишаються незмінними, а відмінності зводяться лише до рівня продуктивності, мобільності та додаткових можливостей, що забезпечує високу економічну ефективність, універсальність застосування та здатність адаптації до різноманітних умов експлуатації без втрати цілісності архітектури системи.

Перспективи інтеграції в гібридні мережеві структури. У контексті подальшого розвитку системи віддаленого доступу формується підхід, що

передбачає інтеграцію у більш складні та гнучкі мережеві середовища, де особлива увага приділяється можливості розширення архітектури без суттєвої зміни її базових принципів, при цьому одним із найбільш перспективних напрямів виступає використання накладених мереж, які функціонують поверх існуючої інфраструктури та дозволяють організовувати з'єднання між вузлами незалежно від типу підключення або наявності публічних IP-адрес, що усуває необхідність у налаштуванні переадресації портів і значно спрощує процес розгортання [34].

У такій моделі мережевої взаємодії вузли можуть об'єднуватися в єдину логічну структуру навіть за умов знаходження за NAT або в середовищах із обмеженим доступом до мережевих ресурсів, а поєднання подібних накладених мереж із використанням WireGuard формує гібридну архітектуру, яка поєднує переваги захищених тунелів та динамічної топології, що дозволяє зменшити залежність від провайдерів, спростити адміністрування та забезпечити високу гнучкість при масштабуванні системи (див. рис. 3.9) [34].

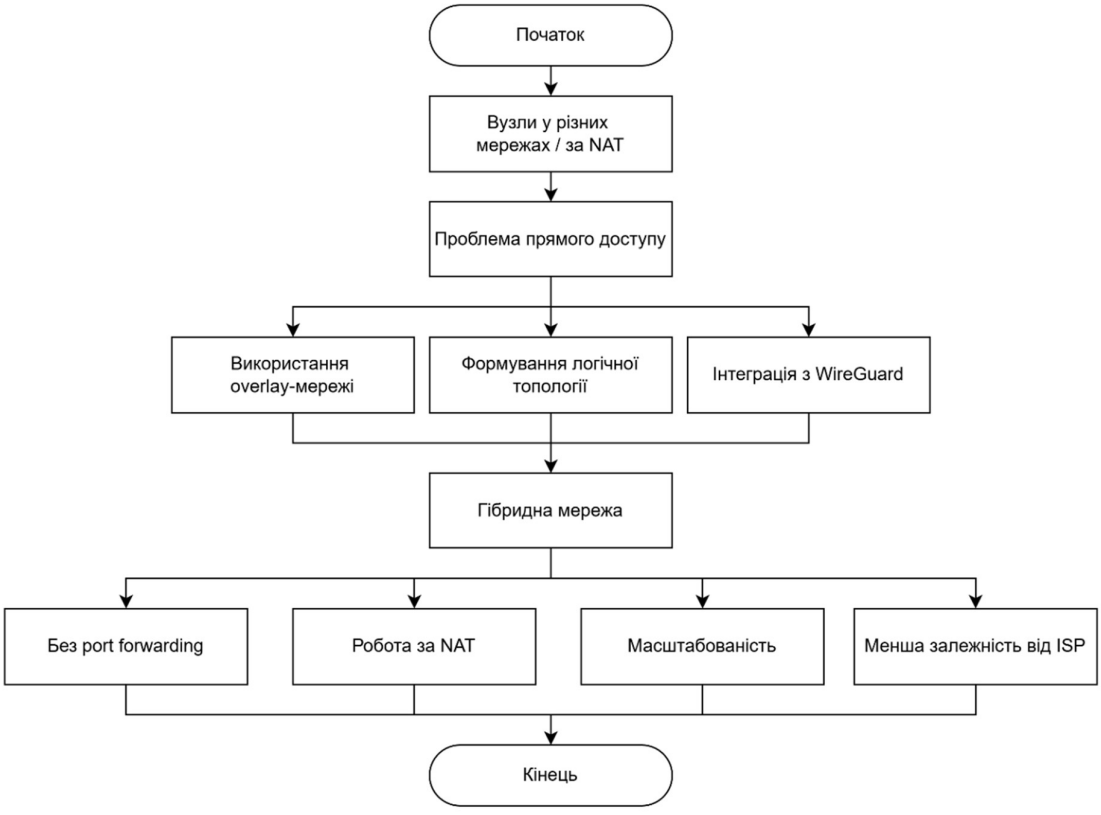


Рисунок 3.9 – Інтеграція з overlay-мережами

Додатковий вектор розвитку пов’язаний із застосуванням такої архітектури у сфері віддалених та розподілених систем, зокрема в інфраструктурах збору даних, де маршрутизатор може виконувати функцію шлюзу для пристроїв інтернету речей, забезпечуючи агрегацію телеметрії з датчиків у таких галузях як агросектор, промисловість або логістика, при цьому передача інформації здійснюється через захищений тунель із використанням мобільних мереж 4G або 5G до централізованих систем обробки, що забезпечує незалежність від локальної інфраструктури та дозволяє швидко розгортати такі рішення у будь-яких умовах.

Подальше розширення функціональності може включати автоматизацію процесів конфігурації, що передбачає генерацію параметрів підключення, централізоване управління користувачами та інтеграцію з системами ідентифікації, такими як LDAP або інші служби контролю доступу, що дозволяє підвищити керованість системи та забезпечити більш високий рівень безпеки при роботі з великою кількістю клієнтів.

Узагальнюючи підхід до перспектив розвитку, формується уявлення про систему як про гнучку платформу, яка поєднує економічну ефективність за рахунок відсутності ліцензійних обмежень, можливість масштабування без кардинальної перебудови архітектури та адаптивність до нових задач завдяки відкритості програмного середовища, а інтеграція з сучасними мережевими технологіями дозволяє використовувати її у складних інфраструктурних рішеннях різного масштабу, що забезпечує не лише актуальність у поточних умовах, але й значний потенціал для подальшого розвитку та впровадження у різноманітних сценаріях експлуатації.

ВИСНОВКИ

У результаті проєктування архітектуру віддаленого доступу інтегровано безпосередньо у граничний маршрутизатор. Це скоротило кількість мережевих переходів і спростило логіку обробки трафіку. Автономність пристрою гарантує стабільну роботу навіть без стаціонарного живлення чи провідного інтернету, а підтримка різних топологій дозволяє адаптувати систему для індивідуальних і розподілених мереж.

Розгортання підтвердило ефективність комбінованого налаштування через веб-інтерфейс та консоль OpenWRT. Такий підхід поєднує зручну базову конфігурацію з повним низькорівневим контролем: генерацією ключів, безпечною передачею клієнтських налаштувань через QR-коди та підтримкою тимчасових сесій без зміни основних параметрів.

Дослідження показало, що криптографічний обмін WireGuard забезпечує швидке з’єднання та стійкість до змін у мережі. Модель Cryptokey Routing об'єднує маршрутизацію з контролем доступу, що підвищує безпеку. Тестування підтвердило стабільність тунелю та високу пропускну здатність, достатню для потокового відео та передачі великих файлів.

Аналіз оптимізації довів переваги граничного маршрутизатора над традиційними серверами: зниження затримок, підвищення відмовостійкості та загальне спрощення інфраструктури. Економічна доцільність рішення зумовлена відсутністю ліцензійних витрат, а гнучкість платформи створює базу для подальшої інтеграції в складні гібридні середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is Remote Access? Cisco. URL: https://www.cisco.com/c/en/us/products/security/what-is-remote-access.html (дата звернення: 25.02.2026).
2. Remote Access VPN Overview. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-remote-access-vpn (дата звернення: 01.03.2026).
3. Enterprise Remote Access Use Cases. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/remote-access (дата звернення: 02.03.2026).
4. Network Security Requirements. NIST. URL: https://www.nist.gov/cyberframework (дата звернення: 04.03.2026).
5. What is a VPN? Cloudflare. URL: https://www.cloudflare.com/learning/network-layer/what-is-a-vpn/ (дата звернення: 05.03.2026).
6. IPSec VPN Explained. IBM. URL: https://www.ibm.com/topics/ipsec (дата звернення: 07.03.2026).
7. OpenVPN Documentation. OpenVPN Inc. URL: https://openvpn.net/community-resources/ (дата звернення: 07.03.2026).
8. SSL VPN Overview. F5 Networks. URL: https://www.f5.com/glossary/ssl-vpn (дата звернення: 10.03.2026).
9. Tunneling Protocols Explained. Microsoft Docs. URL: https://learn.microsoft.com/en-us/windows-server/remote/rras/vpn/vpn-tunneling (дата звернення: 11.03.2026).
10. Modern Cryptography for Networks. Cloudflare. URL: https://www.cloudflare.com/learning/ssl/what-is-encryption/ (дата звернення: 12.03.2026).
11. Network Architecture Basics. Cisco. URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html (дата звернення: 12.03.2026).
12. Authentication Servers Explained. Okta. URL: https://www.okta.com/identity-101/authentication/ (дата звернення: 15.03.2026).
13. Authentication vs Authorization. Auth0. URL: https://auth0.com/docs/get-started/identity-fundamentals (дата звернення: 16.03.2026).
14. Public Key Cryptography. IBM. URL: https://www.ibm.com/topics/public-key-encryption (дата звернення: 18.03.2026).
15. Firewalls and NAT Explained. Cisco. URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (дата звернення: 19.03.2026).
16. VPN Software Comparison. TechRadar. URL: https://www.techradar.com/vpn/best-vpn (дата звернення: 23.03.2026).

17. Open Source vs Commercial VPN. Comparitech. URL: https://www.comparitech.com/blog/vpn-privacy/openvpn-vs-wireguard/ (дата звернення: 01.04.2026).
18. VPN Protocol Comparison. NordVPN. URL: https://nordvpn.com/blog/vpn-protocols/ (дата звернення: 03.04.2026).
19. WireGuard Official Documentation. URL: https://www.wireguard.com (дата звернення: 03.04.2026).
20. OpenWRT Documentation. URL: https://openwrt.org/docs/start (дата звернення: 05.04.2026).
21. GL.iNet Router Docs. URL: https://docs.gl-inet.com (дата звернення: 05.04.2026).
22. Network Topologies Overview. Cisco. URL: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-topologies.html (дата звернення: 08.04.2026).
23. WireGuard Quick Start. URL: https://www.wireguard.com/quickstart/ (дата звернення: 10.04.2026).
24. QRencode Utility. URL: https://fukuchi.org/works/qrencode/ (дата звернення: 13.04.2026).
25. Linux Networking Tools. Red Hat. URL: https://www.redhat.com/en/topics/linux/what-is-linux (дата звернення: 17.04.2026).
26. WireGuard Protocol Whitepaper. URL: https://www.wireguard.com/papers/wireguard.pdf (дата звернення: 20.04.2026).
27. Cryptokey Routing Explained. WireGuard Docs. URL: https://www.wireguard.com/#cryptokey-routing (дата звернення: 22.04.2026).
28. Linux CLI Networking. DigitalOcean. URL: https://www.digitalocean.com/community/tutorials (дата звернення: 25.04.2026).
29. Network Monitoring Tools Overview. GeeksforGeeks. URL: https://www.geeksforgeeks.org/network-monitoring-tools/ (дата звернення: 27.04.2026).
30. Edge Computing Explained. IBM. URL: https://www.ibm.com/topics/edge-computing (дата звернення: 27.04.2026).
31. VPN Performance Comparison. WireGuard vs OpenVPN. URL: https://restoreprivacy.com/vpn/wireguard-vs-openvpn/ (дата звернення: 28.04.2026).
32. Total Cost of Ownership (TCO). Investopedia. URL: https://www.investopedia.com/terms/t/totalcostofownership.asp (дата звернення: 01.05.2026).
33. Embedded Systems Scaling. ARM. URL: https://www.arm.com/solutions/infrastructure (дата звернення: 02.05.2026).
34. Overlay Networks Overview. Cloudflare. URL: https://www.cloudflare.com/learning/network-layer/what-is-an-overlay-network/ (дата звернення: 04.05.2026).
35. Бережний С.В., Торошанко Я.І. Система віддаленого доступу до приватної інфраструктури на базі WireGuard для Edge та IoT середовищ. «Сучасний стан та перспективи розвитку IoT» : VII Науково-техн. конф., м. Київ, 20 квітня 2026 р. С.251-254.

36. Бережний С.В., Торошанко Я.І. Оптимізація та відмовостійкість VPN інфраструктури на базі WireGuard у розподілених мережах. «Застосування програмного забезпечення в ІКТ» : VII Всеукр. науково-техн. конф., м. Київ, 23 квітня 2026 р. (подано до публікації).

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра комп'ютерної інженерії



КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавра

НА ТЕМУ: «СИСТЕМА ВІДДАЛЕНОГО ДОСТУПУ ДО ПРИВАТНОЇ ІНФРАСТРУКТУРИ НА БАЗІ WIREGUARD»

Виконав студент групи КІД-41
Бережний Сергій Володимирович
Керівник кваліфікаційної роботи:
Торошанко Ярослав Іванович,
канд. техн. наук, доц., с.н.с.

Київ – 2026

Мета, об’єкт, предмет дослідження

Мета роботи – оптимізація та спрощення підключення користувачів до внутрішніх ресурсів приватної інфраструктури за рахунок використання сучасних криптографічних методів VPN-з’єднання та edge-архітектури

Об’єкт дослідження – організації захищеного віддаленого доступу до приватних мережевих ресурсів

Предмет дослідження – засоби та технології побудови, конфігурації та оптимізації VPN-систем на базі WireGuard і вбудованих мережевих платформ

Актуальність роботи

У роботі розглянуто теоретичні основи організації віддаленого доступу, принципи функціонування VPN-технологій, криптографічні механізми захисту трафіку та архітектурні підходи до побудови систем захищеного доступу. Проаналізовано сучасні протоколи, зокрема WireGuard, IPSec та OpenVPN, а також особливості їх реалізації, моделі маршрутизації, механізми автентифікації та контролю доступу, що дозволило обґрунтувати вибір оптимального рішення для побудови ефективної системи.

Окрему увагу приділено практичній реалізації системи автоматизованого підключення користувачів на базі маршрутизатора GL.iNet GL-XE3000 (Puli AX) з використанням OpenWRT та WireGuard. Реалізовано механізми генерації конфігурацій, передачі через QR-код, створення тимчасових сесій, а також алгоритми маршрутизації та управління доступом, проведено тестування продуктивності, моніторинг трафіку та оцінку ефективності, що підтвердило доцільність використання edge-підходу.

Обраний підхід (Edge VPN)

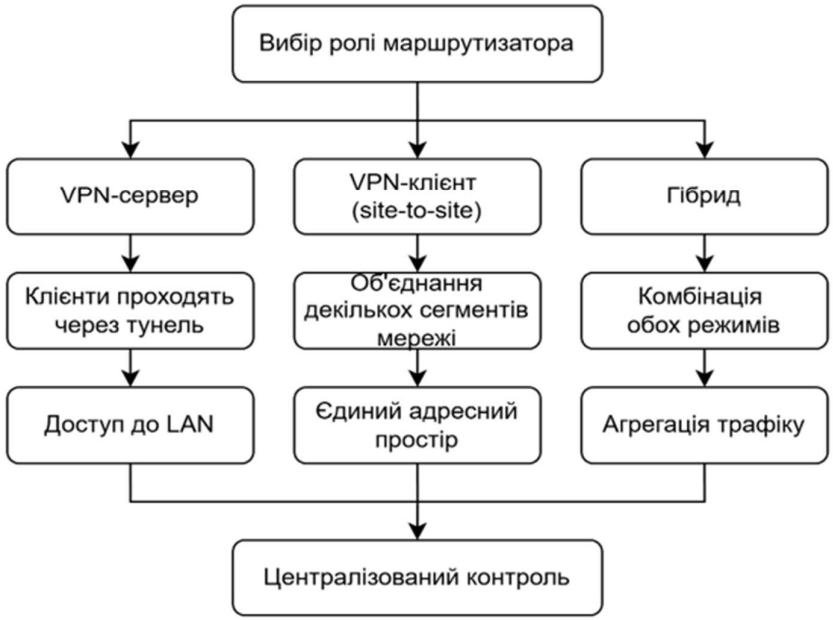


Рис. 2.3 – Концепція edge-підходу у VPN

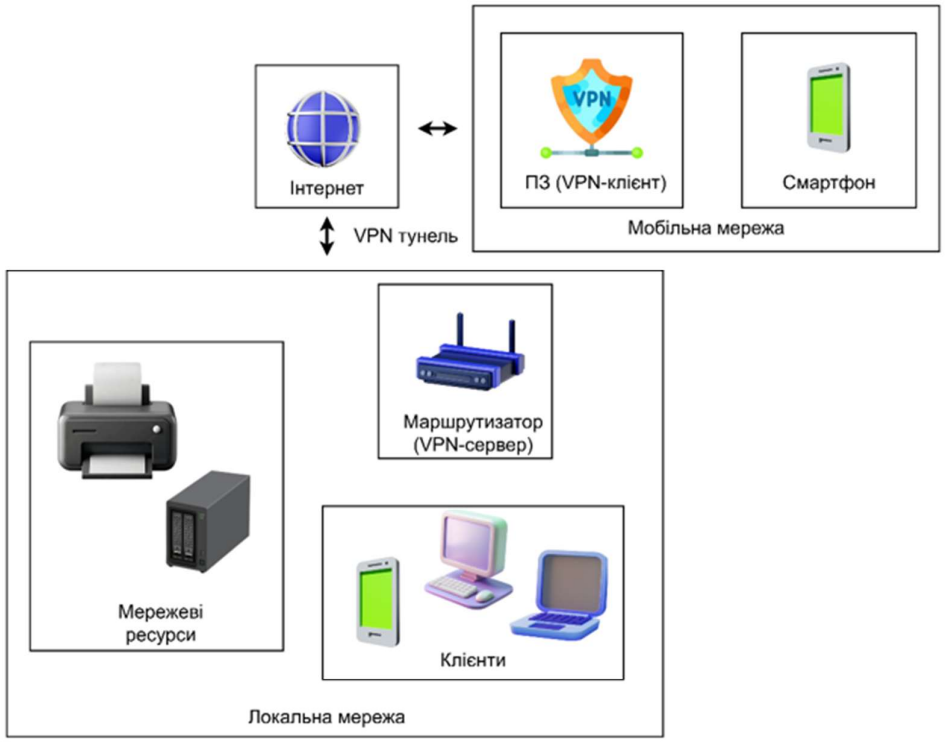


Рис. 1.6 – Взаємодія мережевих вузлів у VPN-системі

Архітектура системи

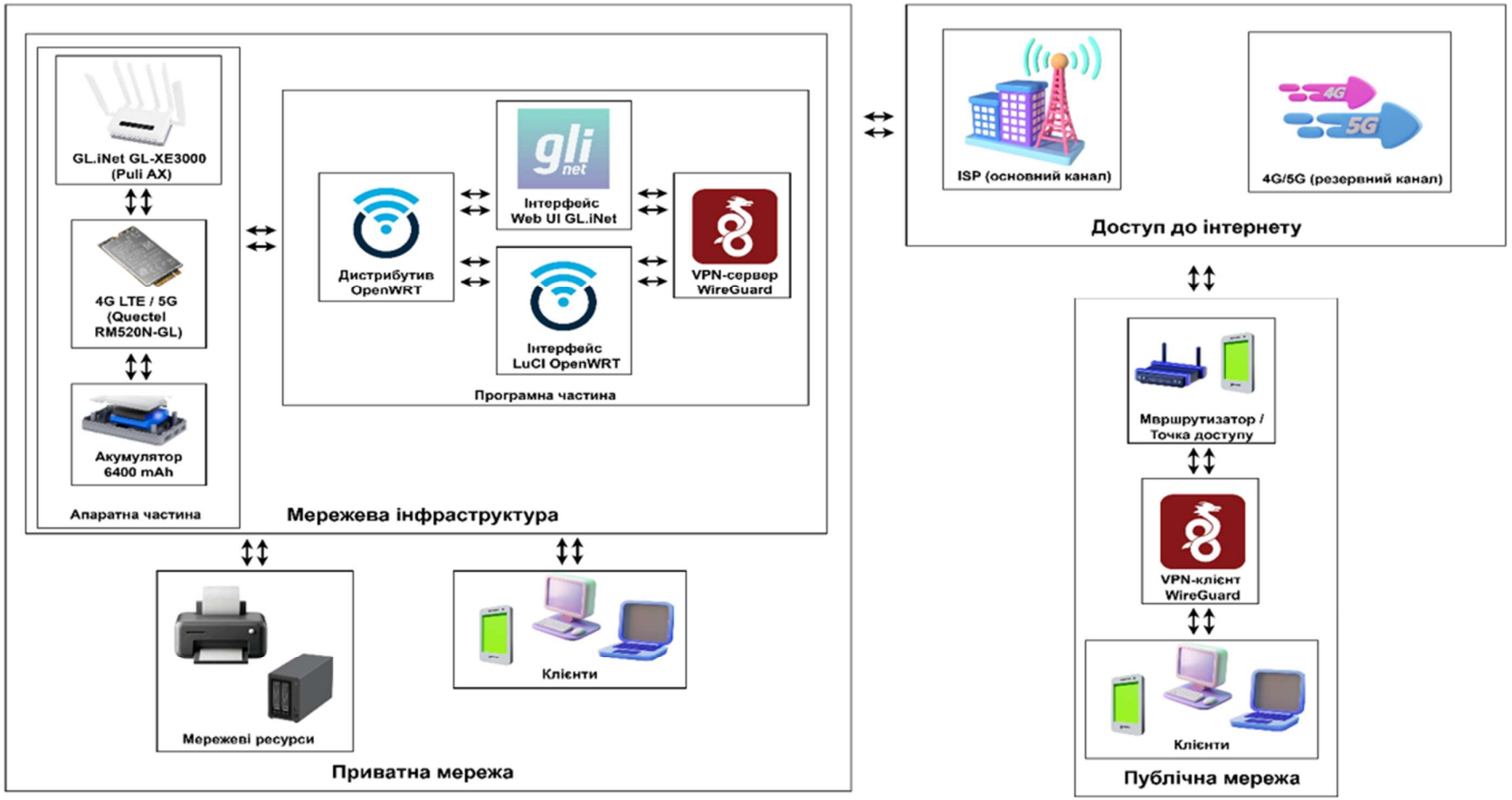


Рис. 2.2 – Загальна архітектура системи VPN-шлюзу

Апаратна платформа системи



Рис. 2.1 – Зовнішній вигляд маршрутизатора GL.iNet GL-XE3000

Табл. 2.1 – Технічні характеристики апаратної платформи VPN-шлюзу

Параметр	Значення
Модель	GL.iNet GL-XE3000 (Puli AX)
Процесор	ARM (quad-core)
Оперативна пам’ять	2 GB RAM
Накопичувач	8 GB eMMC
ОС	OpenWRT (Linux-based)
Підтримка VPN	WireGuard, OpenVPN
Мобільний зв’язок	4G LTE / 5G (Quectel RM520N-GL)
Wi-Fi	Wi-Fi 6 (802.11ax)
Ethernet	2× Gigabit LAN/WAN
Акумулятор	Вбудований (автономна робота)
USB	USB 3.0
Додатково	SIM-карта, failover, load balancing

Програмна платформа системи

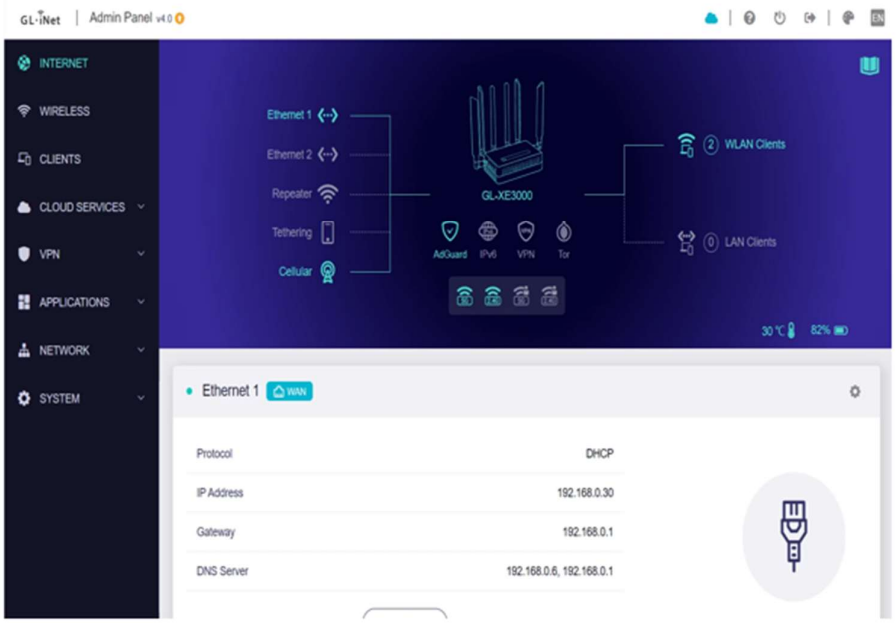


Рис. 2.5 – Інтерфейс Web UI GL.iNet

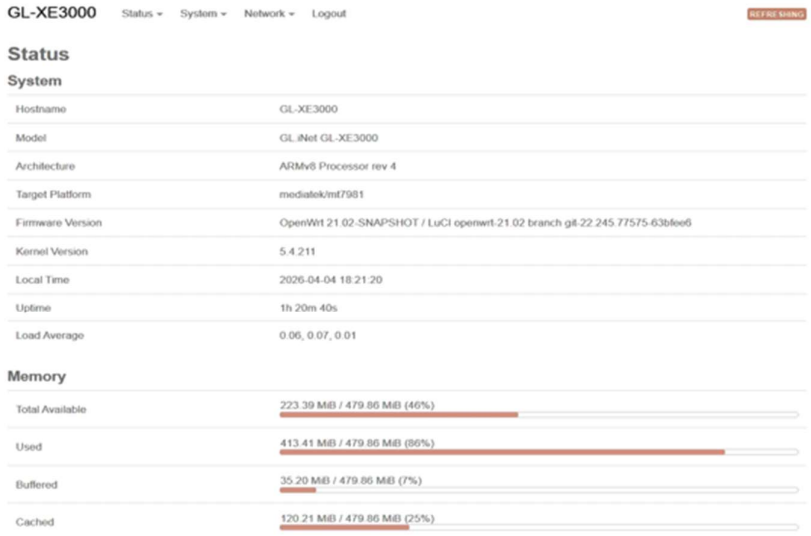


Рис. 2.4 – Інтерфейс LuCI OpenWRT

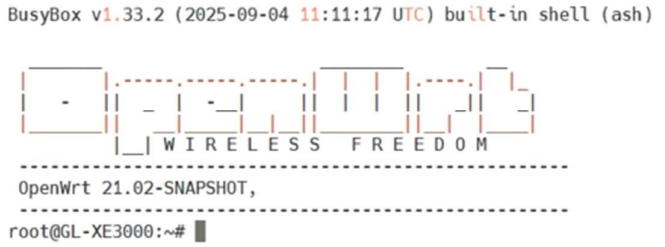


Рис. 2.7 – Підключення через SSH до маршрутизатора

Практична реалізація (налаштування)

```
root@GL-XE3000:~# mkdir wireguard && cd wireguard
root@GL-XE3000:~/wireguard# wg genkey | tee client_private.key | wg pubkey > client_public.key
root@GL-XE3000:~/wireguard# ll
drwxr-xr-x    2 root     root          3488 Apr  7 11:57 ./
drwxr-xr-x    1 root     root          3488 Apr  7 11:57 ../
-rw-r--r--    1 root     root            45 Apr  7 11:57 client_private.key
-rw-r--r--    1 root     root            45 Apr  7 11:57 client_public.key
```

Рис. 2.8 – Генерація ключів у терміналі

```
root@GL-XE3000:~/wireguard# cat client.conf
[Interface]
PrivateKey = [redacted]
Address = 10.0.0.2/32
DNS = 1.1.1.1

[Peer]
PublicKey = [redacted]
Endpoint = [redacted]:51820
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 25
```

Рис. 2.9 – Приклад конфігураційного файлу клієнта

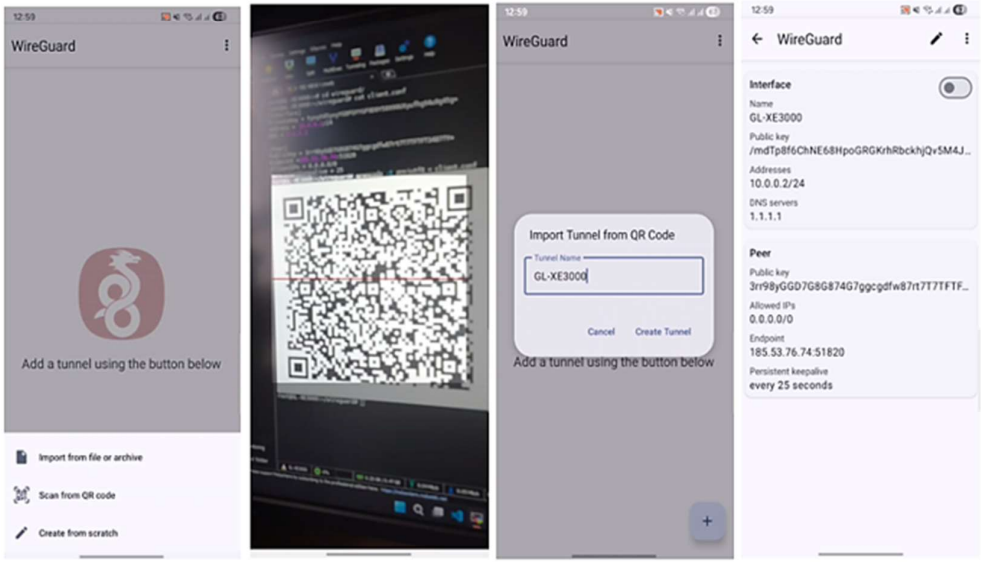


Рис. 2.11 – Сканування QR-коду у клієнтському додатку WireGuard



Рис. 2.10 – Генерація QR-коду в терміналі

Алгоритми встановлення з’єднання та маршрутизації

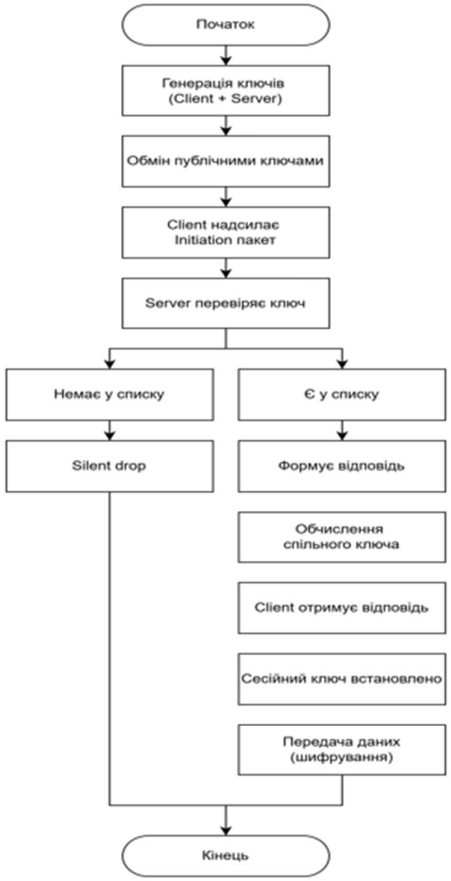


Рис. 2.12 – Алгоритм встановлення з’єднання (Handshake)

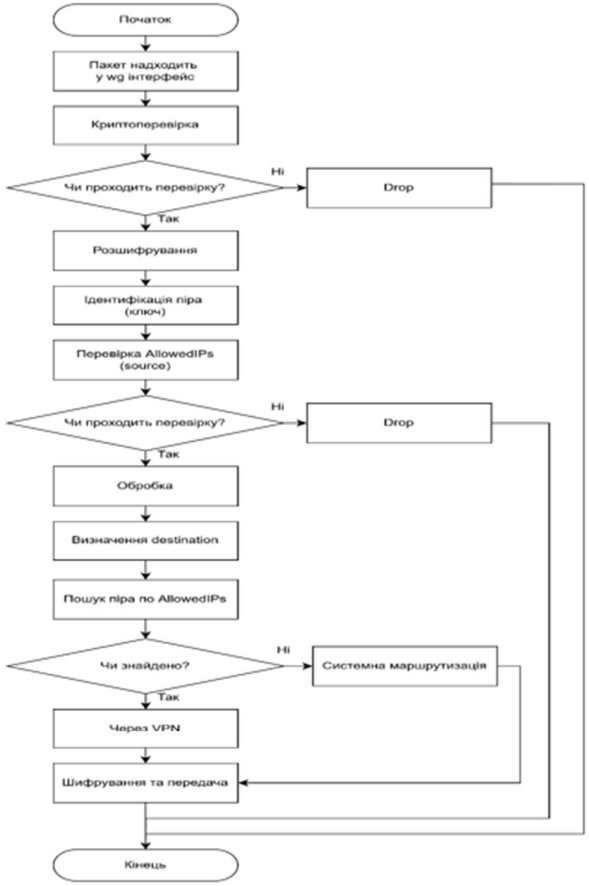


Рис. 2.13 – Алгоритм маршрутизації Cryptokey Routing (AllowedIPs)

Практичні результати

```
root@GL-XE3000:~/wireguard# wg show
interface: wgserver
  public key: [redacted]
  private key: (hidden)
  listening port: 51820
  fwmark: 0x8000

peer: [redacted]
  endpoint: [redacted]:5146
  allowed ips: 10.0.0.0/24
  latest handshake: 1 minute, 22 seconds ago
  transfer: 482.35 KiB received, 2.52 MiB sent
root@GL-XE3000:~/wireguard#
```

Рис. 2.15 – Вивід команди wg show

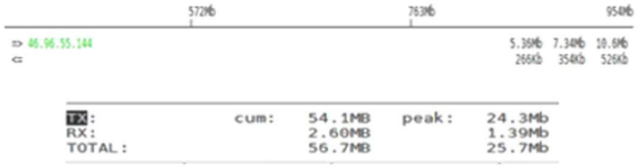


Рис. 2.19 – Навантаження мережі під час завантаження файла фіксованого об'єму 100 МБ

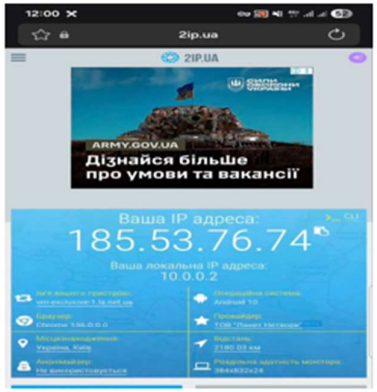


Рис. 2.16 – Перевірка IP-адресації клієнта

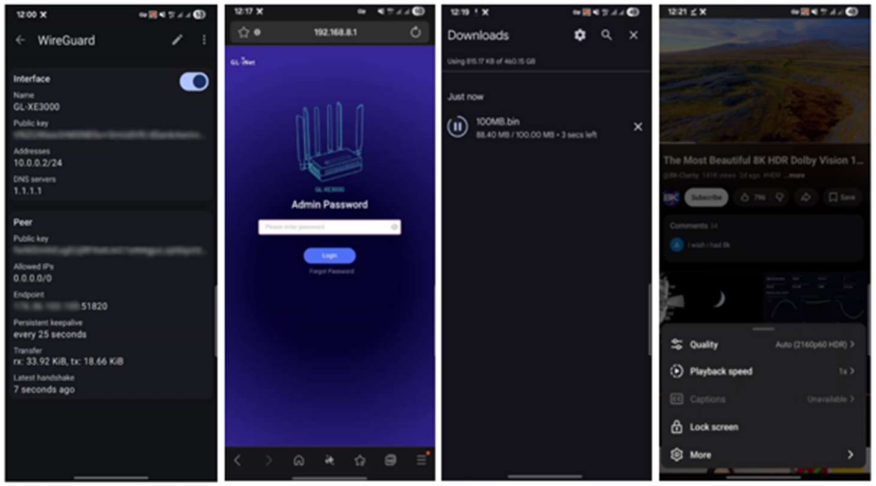


Рис. 2.18 – Отримання доступу та спрямування трафіку через VPN до приватної інфраструктури

Табл. 2.3 – Результати навантажувального тестування пропускної здатності

Сценарій	Швидкість (Мбіт/с)	Затримка (мс)	Втрати пакетів (%)	Стабільність
Завантаження файлу (100 МБ)	50–60	20–30	<1%	Висока
Стрімінг 4K	45–55	25–35	<1%	Висока
Web-серфінг	30–40	15–25	<0.5%	Висока
Пікове навантаження	до 70	30–50	1–2%	Середня
Idle (очікування)	–	<10	0%	Стабільна

Особливості обраної апаратної платформи



Рис. 3.5 – Робота VPN при зникнені електроенергії

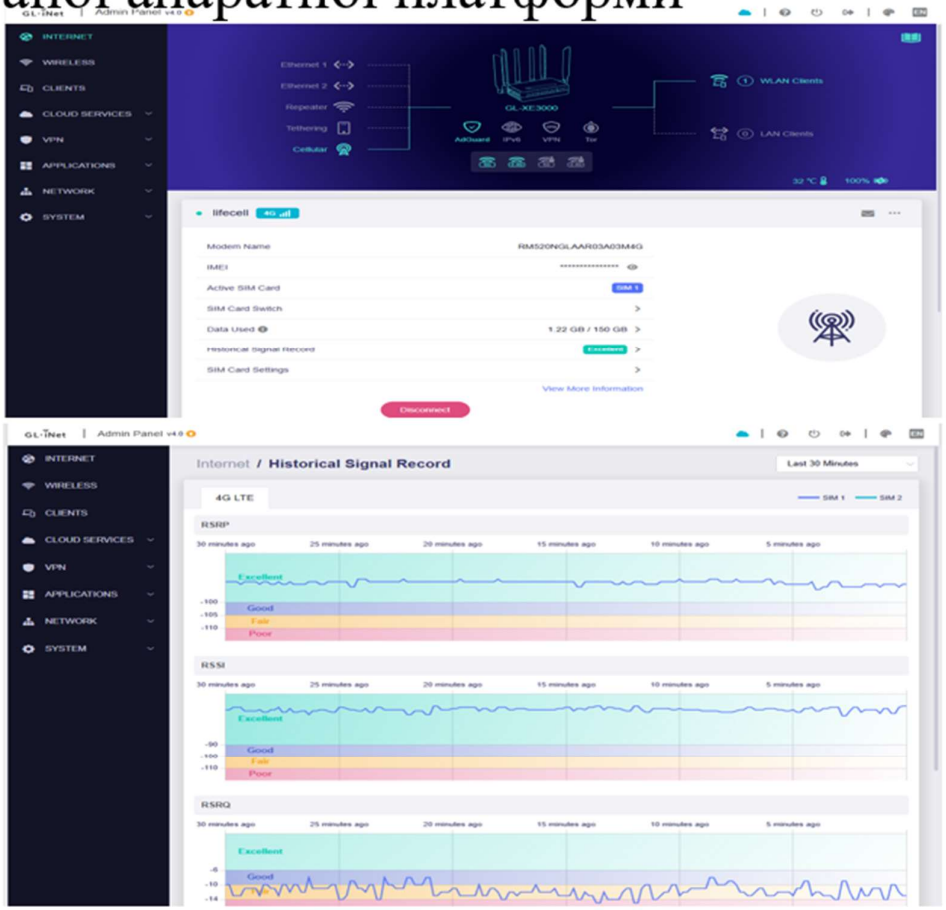


Рис. 3.6 – Робота VPN при відмові основного каналу

Виявлені проблеми та оптимізація

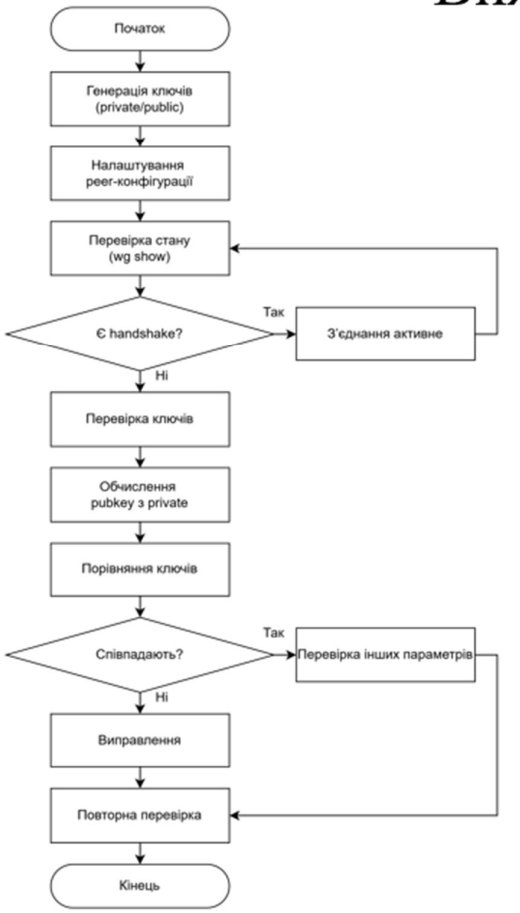


Рис. 3.2 – Верифікація криптографічних пар



Рис. 3.3 – Валідація мережевої адресації

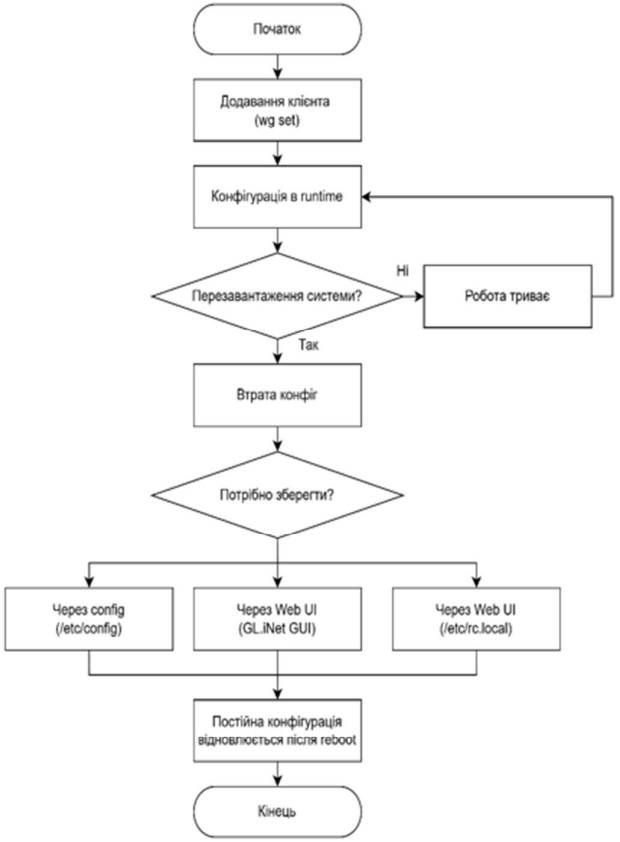


Рис. 3.4 – Синхронізація CLI-налаштувань з системними службами

Вартість володіння (ТСО)

Табл. 3.2 – Порівняльний аналіз вартості володіння (ТСО)

Витрати	Edge VPN (GL-XE3000)	Альтернатива (GL-MT6000 / Flint 2)	Клієнтські вузли (GL-MT3000 / Slate AX)	Класичне VPN-рішення (сервер)
Початкове обладнання	~24000 грн	~8000–9000 грн	~3000–4000 грн (за 1 пристрій)	~30000–60000 грн (сервер + мережа)
Ліцензії	0 грн	0 грн	0 грн	~2000–5000 грн/рік
Підписки	0 грн	0 грн	0 грн	~1000–3000 грн/рік
Вартість масштабування	0 грн	0 грн	~3000–4000 грн/користувач	~500–2000 грн/користувач
Обслуговування (рік)	~500–1000 грн	~500–1000 грн	~200–500 грн	~5000–10000 грн
Енергоспоживання (рік)	~300–500 грн	~300–500 грн	~100–200 грн	~2000–5000 грн
Загальні витрати за 1 рік	~25000 грн	~9000–11000 грн	~3500–4500 грн	~40000–80000 грн
Загальні витрати за 3 роки	~26000–28000 грн	~10000–13000 грн	~4000–6000 грн	~60000–120000 грн
Вартість 1 користувача (10 users)	~2500 грн	~1000 грн	~3500 грн (персональний вузол)	~4000–8000 грн

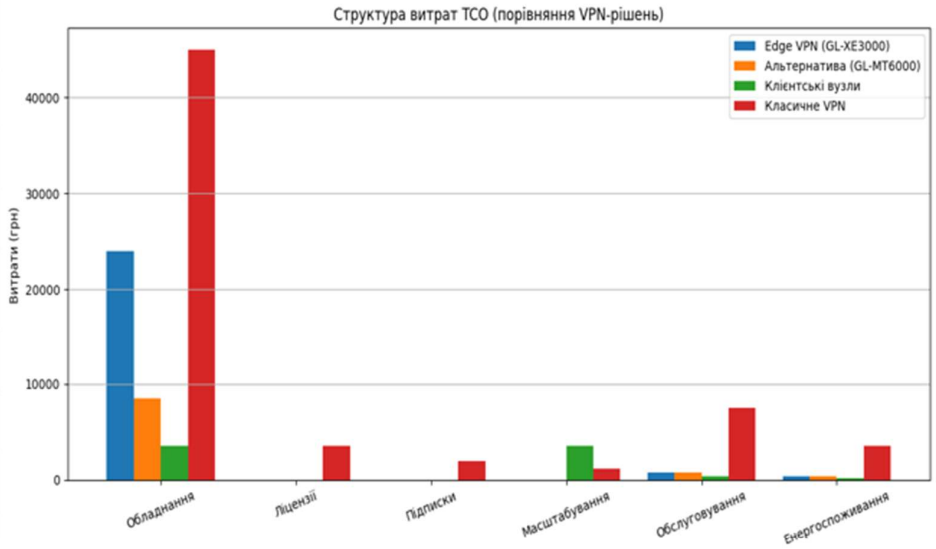


Рис. 3.7 – Структура витрат ТСО

Масштабування системи

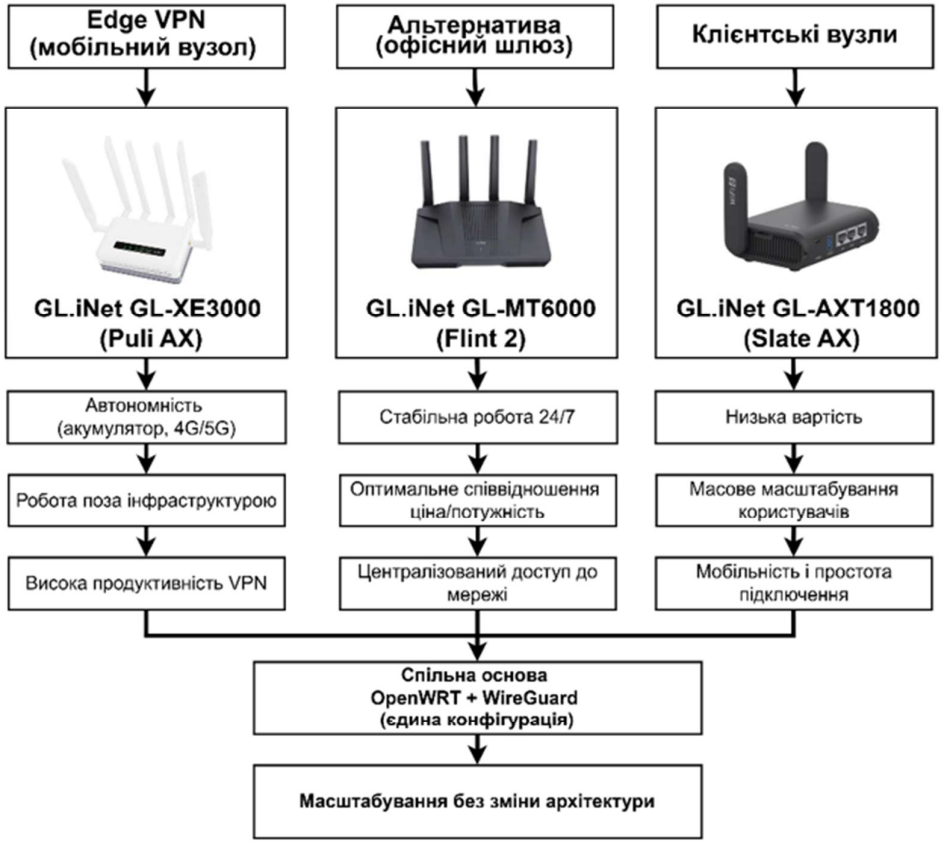


Рис. 3.8 – Масштабування системи на різних пристроях GL.iNet

Висновки

Запропоноване рішення реалізує VPN безпосередньо на граничному маршрутизаторі, що спрощує інфраструктуру, зменшує затримки та забезпечує автономну роботу. Комбіноване налаштування (Web UI + CLI) дозволяє поєднати зручність із повним контролем, включаючи швидке підключення клієнтів і підтримку тимчасових сесій.

Використання WireGuard забезпечує швидке та стабільне з’єднання, а Cryptokey Routing підвищує безпеку. У порівнянні з класичними VPN рішеннями досягнуто нижчу вартість, кращу масштабованість і простішу реалізацію.

Результати впровадження

1. Бережний С.В., Торошанко Я.І. Система віддаленого доступу до приватної інфраструктури на базі WireGuard для Edge та IoT середовищ. «Сучасний стан та перспективи розвитку IoT» : VII Науково-техн. конф., м. Київ, 20 квітня 2026 р. С.251-254.
2. Бережний С.В., Торошанко Я.І. Оптимізація та відмовостійкість VPN інфраструктури на базі WireGuard у розподілених мережах. «Застосування програмного забезпечення в ІКТ» : VII Всеукр. науково-техн. конф., м. Київ, 23 квітня 2026 р. (подано до публікації).