МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Комп'ютерна інженерія»

Група: 2БКС-29

КВАЛІФІКАЦІЙНА РОБОТА

здобувача освіти денної форми навчання

БКС.29.20.000.КРБ

СЕРГЄЄВА
ВАЛЕРІЯ ВІТАЛІЙОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: **«Комп'ютерна інженерія»**

Група: **2БКС-29**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему: **Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю**

Проектний матеріал складається з пояснювальної записки на 74 сторінках та графічного (презентаційного) матеріалу на 15 аркушах (слайдах)

Виконавець _____ (Сергєєв В.В.)

Керівник проекту _____ (Кривченко А.А.)

Консультанти:

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувач кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ (Краснокутська К.Г.)

Захист «17» 06 2025 р. Протокол ЕК № 2

Оцінка ЕК 5 (відмінно) / 95

Секретар ЕК _____

АНОТАЦІЯ

Випускна кваліфікаційна робота присвячена дослідженню технологій побудови захищених каналів для організації VoIP-зв’язку з використанням віртуального приватного доступу та сучасних криптографічних методів. У роботі здійснено аналіз сучасних підходів до створення захищених каналів комунікації, а також досліджено особливості організації віртуального локального зв’язку (VPN) для передачі голосових даних у мережах з підвищеними вимогами до безпеки. Опрацьовано сучасні літературні джерела, що висвітлюють питання криптографії, шифрування мережевого трафіку та безпеки VoIP-зв’язку.

У проекті розглянуто методики налаштування та адміністрування OpenVPN як одного з ключових рішень для створення захищеного каналу передачі даних. Особлива увага приділяється аналізу впливу різних режимів шифрування на продуктивність VoIP-каналу, оцінці затримки і пропускної здатності при використанні відповідних криптографічних алгоритмів. Також у роботі розроблено та описано схему перехоплення VoIP-трафіку з метою аналізу стійкості криптографічних засобів захисту, а також підготовлено програмно-апаратне забезпечення для проведення експериментів із визначення залежності часу підбору шифрувального ключа від його довжини, що проводиться за допомогою методів прямого перебору та застосування райдужних таблиць.

Робота систематизує сучасні знання щодо організації захищених комунікацій за рівнями семирівневої моделі OSI та формує науково-обґрунтовану базу для подальшої оптимізації параметрів шифрування у VoIP-системах з метою підвищення рівня інформаційної безпеки в сучасному цифровому середовищі.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"28" 05 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачеві освіти *Сергєєву Валерію Віталійовичу*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю*

затверджена наказом по коледжу від "14" 11 2024 р. № 246

2. Термін здачі студентом кваліфікаційної роботи 20.06.25

3. Вихідні дані до роботи *1. Специфікації SIP-протоколу; 2. Порівняти існуючі протоколи VPN по рівнях мережевої моделі OSI та по їх функціям; 3. Реалізувати захист VoIP-зв'язку за допомогою VPN з шифруванням; 4. Реалізувати тунельний канал та здійснити віддалений доступ на базі протоколу PPTP; 5. Дослідити залежність часу підбору ключа шифрування RC4 у протоколі PPTP від його довжини; 6. Протестувати пропускну здатність каналу VoIP-зв'язку з VPN і шифруванням різних типів*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

Короткий огляд технологій захищеного зв'язку; Аналіз методів і засобів організації VoIP-зв'язку; Визначення видів загроз в мережі VoIP-зв'язку; Визначення методів захисту VoIP-зв'язку; Вибір технології захисту VoIP-зв'язку від несанкціонованого доступу; Вибір захищеного протоколу для шифрування VoIP-зв'язку; Аналіз роботи OpenVPN при організації VoIP-зв'язку; Аналіз надійності шифрування VoIP-зв'язку

5. Перелік графічного матеріалу (слайдів мультимедійної презентації) *Схема інтернет-трафіку з використанням VPS; Архітектура VPN для корпоративного застосування; Організація VPN для віддаленого користувача; Схема організації мережі VoIP-зв'язку на підприємстві; Схема перехоплення голосових пакетів шляхом прослуховування; Реалізація протоколу PPTP для тунелювання; Архітектура протоколу OpenVPN; Топологія мережі при тестуванні каналу VoIP-зв'язку з OpenVPN; Результати тестування впливу шифрування на продуктивність VoIP каналу у режимі OpenVPN; БСА перевірки та блокування небажаних IP-адрес; Результати підбору ключа шифрування; Залежність цінності інформації з VoIP-пакетів від часу*

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що їх стосуються

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний розділ	*Кривченко А.А.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання _____

Керівник роботи *Кривченко А.А.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Вступ. Аналіз технічного завдання	07.06.25	виконано
2.	Аналітичний огляд засобів безпеки інформаційних мереж	08.06.25	виконано
	на основі VPN. Вивчення протоколу VPN		
3.	Вивчення протоколів і алгоритмів захисту IPsec	09.06.25	виконано
4.	Порівняння протоколів захищених мереж, вибір найбільш	10.06.25	виконано
	відповідного		
5.	Адміністрування і реалізація захищеної мережі	11.06.25	виконано
6.	Налаштування VPN-серверу	12.06.25	виконано
7.	Дослідження надійності шифру RC4	13.06.25	виконано
8.	Проведення експерименту з дослідження часу підбору	14.06.25	виконано
	ключа шифрування RC4	15.06.25	виконано
9.	Аналіз роботи OpenVPN при організації VoIP-зв'язку	16.06.25	виконано
10.	Аналіз надійності шифрування VoIP-зв'язку	17.06.25	виконано
11.	Аналіз результатів тестування	18.06.25	виконано
12.	Розробка питань з охорони праці та техніки безпеки	19.06.25	виконано
13.	Підготовка матеріалів мультимедійної презентації	20.06.25	виконано

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 29. 20 000. 00 КРБ	Випускна робота		
А4			БКС 29. 20 000. 00 КРБ ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 29. 20 000. 00 КРБ		
Розробив		Сергєєв В.В.		10.06	Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю	Літ.	Аркуш 4 / Аркушів 74
Перевірив		Кривченко А.А.		10.06.		Н Д П	
Н. Контр.		Петрашова В.І.		10.06.25		ВСП "ОТФК ОНТУ" гр.2БКС-29	
Затверд.		Іванова Л.В.					

ЗМІСТ

ВСТУП

У сучасному світі інформаційних технологій зростання цифрової комунікації стимулює впровадження новітніх рішень для забезпечення безпеки передаваних даних. IP-телефонія, яка дозволяє здійснювати голосові дзвінки через мережу Інтернет, стає дедалі популярнішою як у корпоративному, так і в приватному секторі. Зі збільшенням обсягів голосової інформації та зростанням кількості кіберзагроз питання захисту VoIP-зв'язку набуває особливої актуальності. Ця робота присвячена аналізу методів захисту VoIP-зв'язку за допомогою віртуального тунелю, що дозволяє знизити ризики несанкціонованого доступу до передаваних даних.

Віртуальні приватні мережі (VPN) є ефективним засобом для створення захищених каналів зв'язку. Вони дозволяють організувати зашифроване з'єднання навіть через публічні мережі, таким чином забезпечуючи конфіденційність, цілісність та доступність інформації. У даній роботі буде розглянуто основні аспекти побудови VPN, включно з їх класифікацією, принципами функціонування та специфічними умовами, необхідними для забезпечення високого рівня захисту мережевої інфраструктури.

Особлива увага приділяється аналізу впливу криптографічних алгоритмів на якість роботи каналу зв'язку, що реалізовано на прикладі популярного інструменту OpenVPN. Дослідження включає вивчення параметрів шифрування, їх впливу на пропускну здатність мережі та ефективність використання складних криптографічних методів для захисту голосової інформації. Практична частина роботи містить налаштування OpenVPN серверу на базі операційної системи Ubuntu, а також розробку конфігурацій для клієнтського програмного забезпечення, що дозволить оцінити ефективність розробленої схеми захисту у реальних умовах.

Метою даної роботи є підвищення рівня захисту VoIP-зв'язку шляхом системного аналізу методів захисту інформації від несанкціонованого доступу, який може бути реалізований як навмисним впливом, так і в результаті природних чинників.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Короткий огляд технологій захищеного зв’язку

Забезпечення захищеності комунікацій набуває критичного значення. В мирний час близько 90% мережевого трафіку передається через мережі загального користування, що забезпечує масовість і доступність сервісів зв’язку.

Проте у військовий час ця частка знижується до приблизно 60%, оскільки розвиток власної інфраструктури в умовах інтенсивних технологічних змін є надзвичайно затратним завданням. Саме тому військові та інші критично важливі організації втрачають економічну можливість у повномасштабному впровадженні власного мережевого середовища і покладаються на мережі загального користування, використовуючи спеціальні засоби захисту для забезпечення надійного зв’язку.

Одним із найбільш поширених методів побудови захищених каналів є технологія VPN (Віртуальні Приватні Мережі), яка дозволяє створити безпечний тунель для передачі даних через загальнодоступні мережі.

Найпопулярнішим підходом у цій галузі є інкапсуляція мережевих протоколів (наприклад, IP, IPX, AppleTalk) у протокол PPP (Point-to-Point Protocol) з подальшою інкапсуляцією утворених пакетів у протокол тунелювання. Такий метод класифікується як тунелювання другого рівня, оскільки основним «пасажиром» тут виступає протокол другого рівня, що забезпечує високий рівень сумісності та гнучкості при інтеграції з різними мережевими технологіями.

Сучасні технології захищеного зв’язку не обмежуються лише тунелюванням другого рівня. Крім цього, широко використовуються протоколи IPSec для захисту мережевого рівня, SSL/TLS для забезпечення безпеки веб-трафіку (зокрема, HTTPS) та SSH для організації захищеного віддаленого доступу. Ці рішення базуються як на симетричних, так і на асиметричних методах шифрування, що дозволяє забезпечити комплексний підхід до конфіденційності, цілісності та автентичності передаваних даних у різноманітних умовах експлуатації мережевої інфраструктури.

1.1.1 Аналіз мети впровадження захищених каналів зв’язку

Сучасні інформаційні технології дозволяють здійснювати швидку передачу даних через глобальні мережі, проте зростання цифрових загроз вимагає ефективних заходів захисту інформації. Впровадження захищених каналів зв’язку є ключовим елементом забезпечення конфіденційності, цілісності та доступності даних як у корпоративному секторі, так і в умовах державного управління та оборони.

Одним із найбільш поширених рішень для організації безпечного зв’язку є використання технології VPN (Віртуальна Приватна Мережа). Вона дозволяє створити захищене з’єднання через Інтернет, що дає змогу користувачам з будь-якої точки світу отримати доступ до приватної мережі, знаючи відповідні аутентифікаційні дані (рис. 1.1).

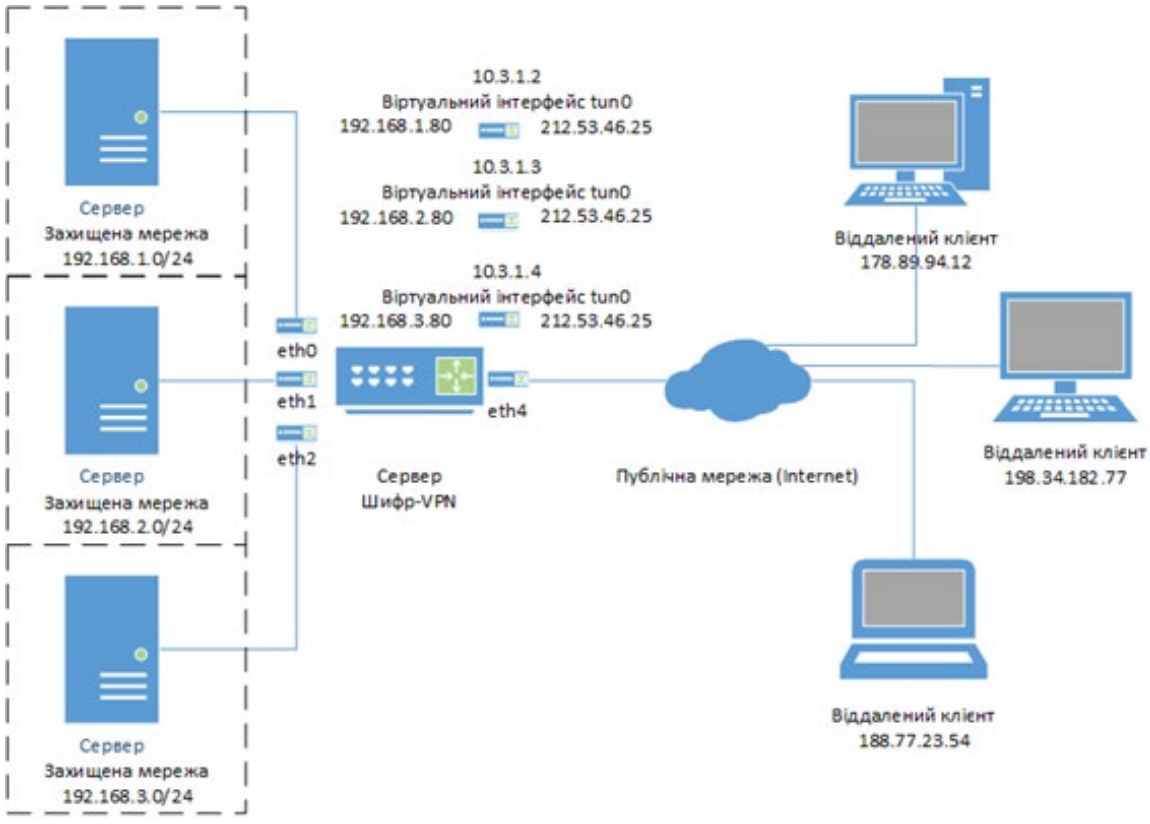


Рисунок 1.1. Архітектура VPN для корпоративного застосування

Основна мета впровадження VPN полягає у забезпеченні прозорого доступу до мережевих ресурсів, незалежно від географічного розташування користувача. Це робить VPN популярним рішенням серед дистанційних співробітників та організацій із територіально розділеною інфраструктурою (рис. 1.2).

Крім безпечного доступу до мережі, VPN також вирішує проблему конфіденційності обміну даними між віддаленими вузлами. При наявності великої кількості розподілених ресурсів та необхідності захисту інформації від перехоплення VPN стає оптимальним вибором. Завдяки застосуванню криптографічних алгоритмів та механізму тунелювання VPN-мережі значно знижують ризик зовнішнього втручання, забезпечуючи захист корпоративних, державних та приватних комунікацій. VPN також дозволяє створювати логічно єдине мережеве середовище для фізично розподілених користувачів (рис. 1.2). Це особливо корисно для мобільних співробітників, яким потрібен надійний доступ до централізованих даних. Використання VPN також спрощує управління мережевими ресурсами: замість зміни конфігурації всієї інфраструктури при зміні провайдера достатньо лише налаштувати шлюз під нові параметри.

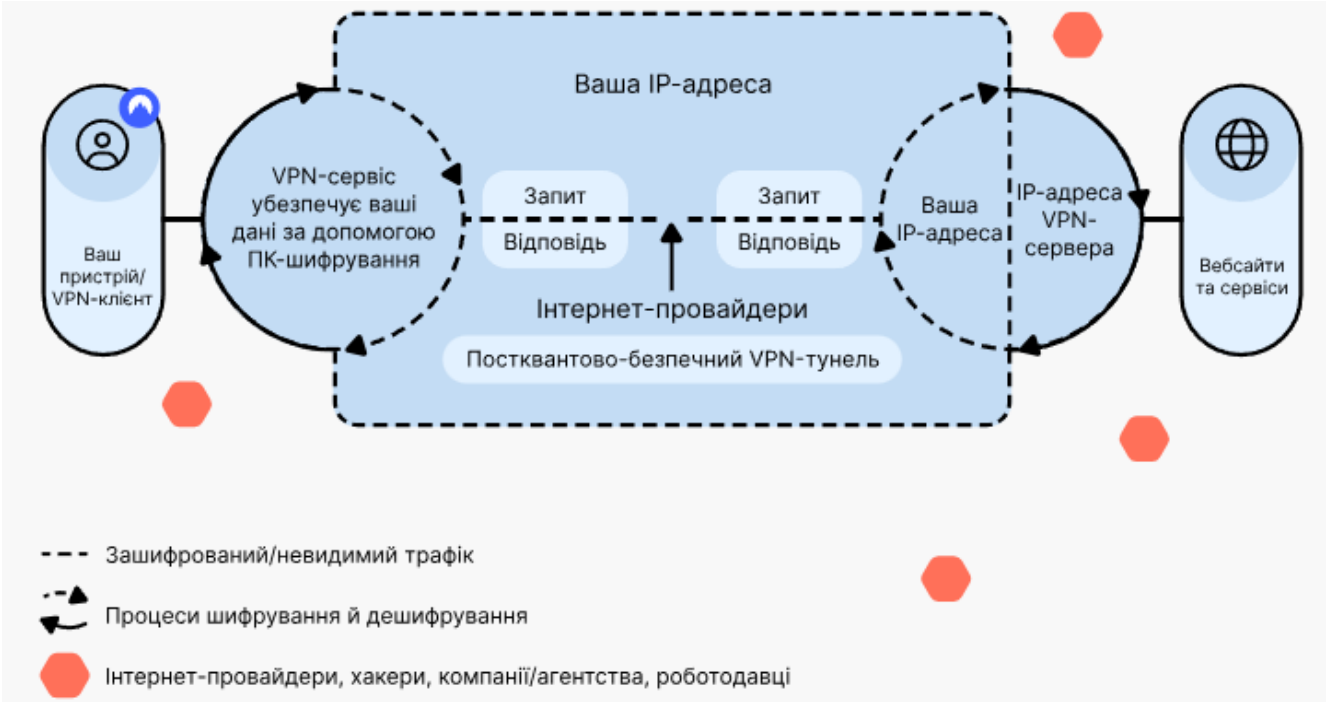


Рисунок 1.2. Схема підключення віддаленого користувача через VPN

Окрім безпеки та зручності, VPN є економічно вигідним рішенням для організації віддаленого доступу. Відсутність необхідності створення дорогих виділених мережевих каналів значно скорочує фінансові витрати, адже весь трафік передається через Інтернет, використовуючи захищені тунелі. Таким чином, VPN стає ефективним способом захисту даних у корпоративному середовищі, державних установах та особистих мережах.

1.1.2 Аналіз варіантів створення віртуального тунелю

Віртуальний тунель дозволяє інкапсулювати мережеві протоколи і забезпечувати захищену передачу даних через загальнодоступні мережі. Підхід до побудови VPN-тунелю базується на обов'язковій комбінації трьох компонентів: тунелювання, автентифікації та шифрування. Однак у процесі впровадження існує безліч варіантів реалізації цього механізму. Нижче подано перейняту класифікацію з переосмисленою структурою, що розглядає як апаратні, так і програмні підходи, а також їх гібридні рішення.

1. VPN на базі маршрутизаторів зі спеціальним криптографічним прискоренням. Маршрутизатори відіграють ключову роль у маршрутизації всього мережевого трафіку, що виходить із локальної мережі. Сучасні маршрутизатори, зокрема продукція Cisco Systems, інтегрують підтримку протоколів L2TP і IPSec, що дозволяє здійснювати інкапсуляцію даних на рівні мережі. У версіях програмного забезпечення, починаючи з IOS 11.3(3), ці пристрої забезпечують:

- Ідентифікацію та автентифікацію: Під час встановлення тунельного з'єднання відбувається обмін ключами за допомогою протоколів ISAKMP/Oakley.

- Шифрування всього IP-потоку: Шифрування може здійснюватися як програмно, так і за допомогою апаратних модулів, таких як Encryption Service Adapter (ESA), що знижує навантаження на центральний процесор і покращує пропускну здатність.

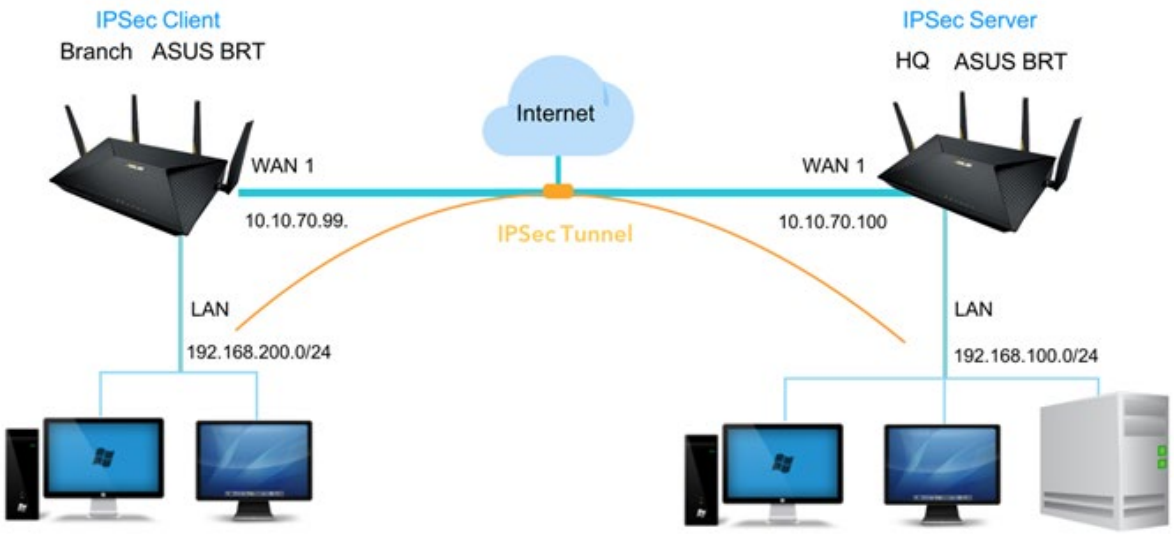


Рисунок 1.3. Приклад організації VPN-тунелю на базі маршрутизатора з апаратним шифруванням

Ці рішення підходять для організацій, де важлива висока пропускна здатність і масштабованість, оскільки апаратне прискорення дозволяє обробляти великий обсяг трафіку без затримок.

2. Спеціалізовані VPN-пристрої. Отримання високої продуктивності при захищеній передачі даних можливе за допомогою спеціалізованих апаратних засобів, розроблених виключно для реалізації VPN. Приклад такого пристрою — cIPro-VPN від компанії Radguard. Основні технічні особливості:

- Апаратне шифрування: Використання вбудованих криптопроцесорів забезпечує обробку даних на швидкості до 100 Мбіт/с.

- Підтримка стандартів: Пристрій працює за протоколами IPSec, ISAKMP/Oakley, а також підтримує трансляцію мережевих адрес, що дозволяє інтегрувати додаткові засоби захисту, наприклад, функції фаєрволу за допомогою додаткової плати.

Апаратні рішення оптимальні для мереж з високою інтенсивністю трафіку, де стабільність і швидкість мають першорядне значення.

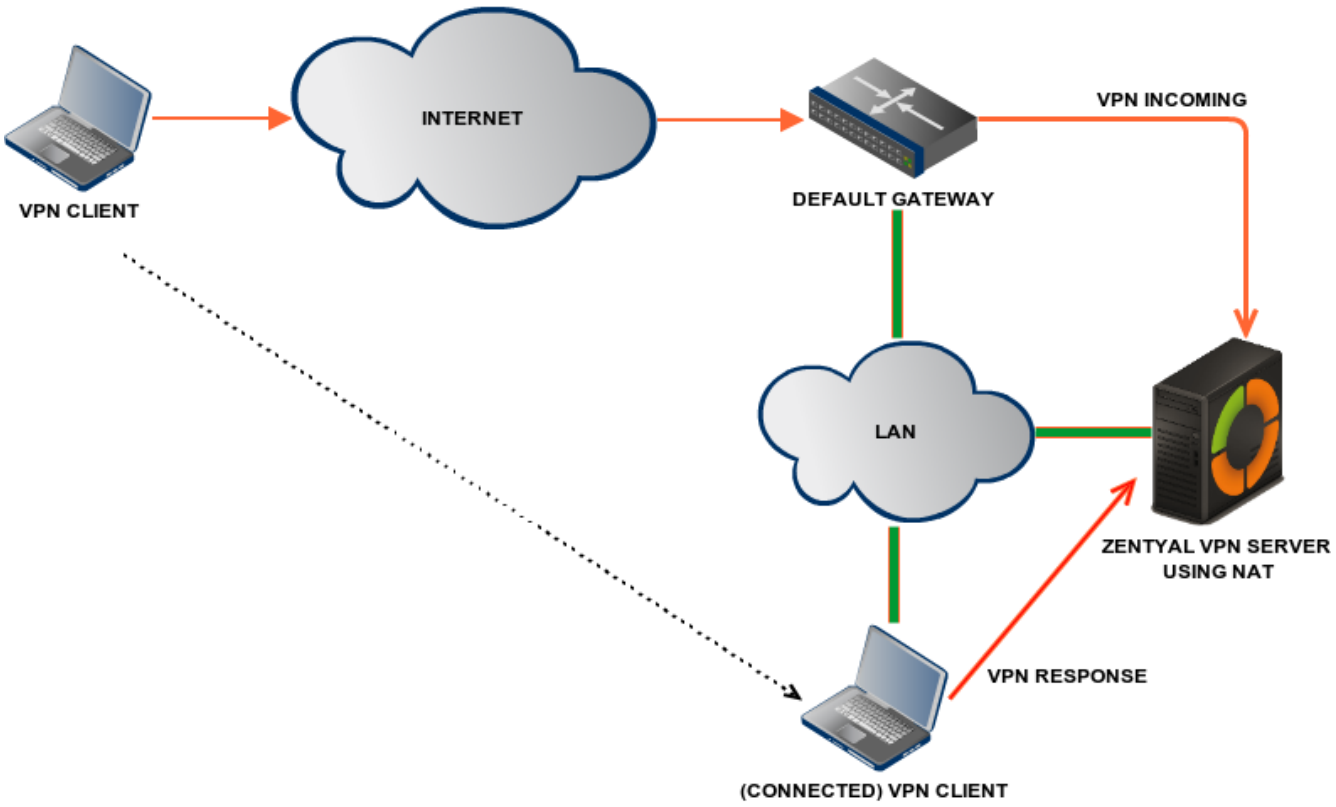


Рисунок 1.4. Схема побудови VPN за допомогою спеціалізованого апаратного пристрою

3. VPN на базі мережевих фільтрів (фаєрволів). Сучасні фаєрволи не обмежуються традиційним контролем доступу — вони часто реалізують можливості тунелювання та шифрування даних. Програмне забезпечення фаєрвола може містити модуль шифрування на базі стандартного IPSec. Трафік, що проходить через систему, шифрується і піддається аутентифікації, що дозволяє забезпечити захист даних у малих та середніх мережах. Однак продуктивність такого рішення сильніше залежить від апаратних ресурсів ПК чи серверу, на якому розгорнуто фаєрвол, тому воно підходить для мереж з помірною інтенсивністю трафіку.

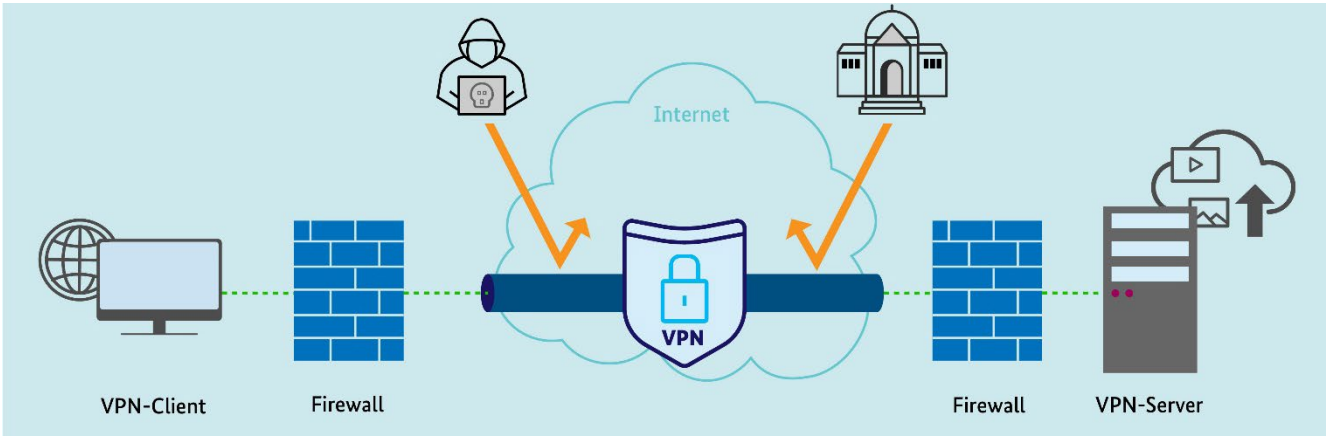


Рисунок 1.5. Архітектура VPN-тунелю на базі інтегрованого фаєрвола

4. Чисто програмні VPN-рішення. При обмежених бюджетах та необхідності високої гнучкості може бути використано програмні VPN-рішення. Приклади— комерційне програмне забезпечення, таке як iTop VPN, а також популярні open-source проекти (наприклад, OpenVPN). Технічні особливості:

- Алгоритми шифрування: Використання різних бітових ключів (від 32 до 256 біт) за алгоритмами на базі RC4 (хоча зараз часто застосовують більш сучасні алгоритми, як AES) забезпечує налаштування рівня безпеки;

- Інкапсуляція: Пакети зашифрованих даних інкапсулюються у нові IP-пакети, що передаються через загальнодоступну мережу;

- Контроль цілісності: Деякі рішення використовують алгоритм MD5 для перевірки цілісності отриманих даних.

Такі програмні рішення дозволяють швидко розгортати VPN, проте вони часто обмежені потужністю центрального процесора і можуть бути неефективними

при високій інтенсивності трафіку.

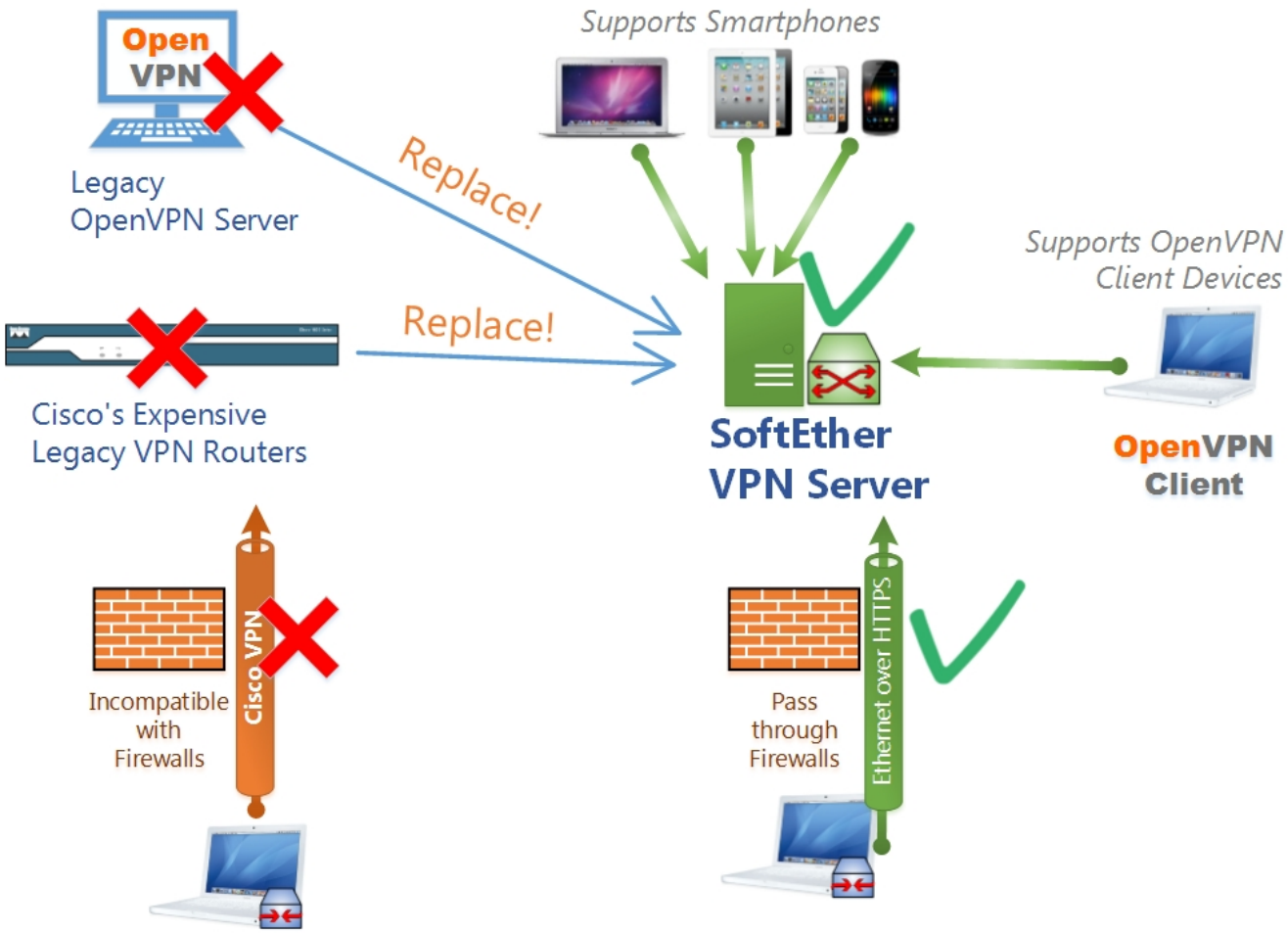


Рисунок 1.6. Схема програмного VPN-з’єднання

5. VPN, інтегровані в операційні системи. Інтегровані VPN-системи, наприклад, у сімействі Windows, надають можливість використання протоколів PPTP, SSTP або IKEv2. Основні риси:

- Інтеграція з користувацьким середовищем: VPN-рішення, вбудовані в операційну систему, використовують базу даних користувачів (Active Directory) для автентифікації, що спрощує управління.

- Простота налаштувань: Для таких систем необхідна лише конфігурація шлюзу, що робить їх доступними для компаній з уже існуючою Windows-інфраструктурою.

- Недоліки: Використання деяких протоколів (наприклад, PPTP із протоколом MPPE) має вразливості, а також обмежену підтримку динамічної зміни ключів під час з’єднання.

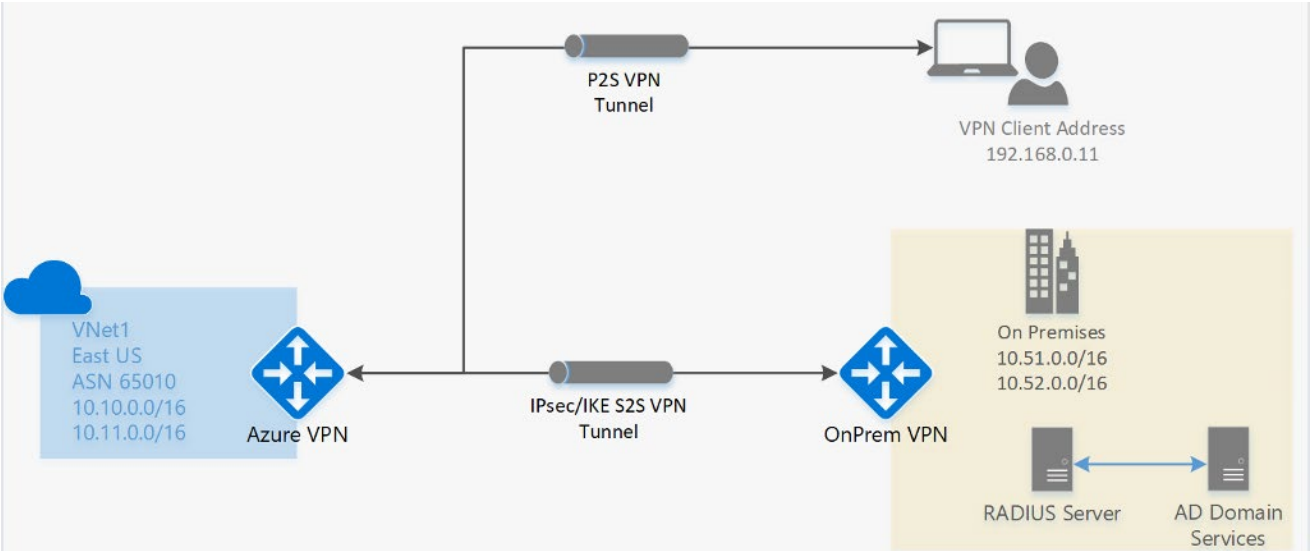


Рисунок 1.7. Схема VPN, інтегрованого в операційну систему

6. Гібридні підходи та додаткові варіанти. Сучасні мережеві рішення часто комбінують апаратні та програмні компоненти для досягнення оптимального співвідношення продуктивності і гнучкості. Наприклад, деякі маршрутизатори можуть мати апаратні модулі для прискорення криптографічних операцій, тоді як управління тунелями здійснюється з використанням програмних рішень. Такі гібридні конструкції дозволяють:

- Знизити навантаження на центральний процесор: Завдяки апаратному шифруванню окремі завдання делегуються спеціалізованим мікросхемам.

- Підвищити масштабованість: Гібридні рішення забезпечують більш плавне розширення мережі при зростанні обсягів трафіку.

- Гнучко адаптуватися до конкретних вимог: Поєднання різних алгоритмів шифрування та протоколів автентифікації дозволяє тонко налаштовувати рівень безпеки та продуктивності в залежності від умов експлуатації.

Аналіз варіантів створення віртуального тунелю демонструє, що ефективність реалізації VPN-технології безпосередньо залежить від правильного підбору апаратних та програмних засобів. Якщо основна вимога—це висока продуктивність і стабільність при великому обсязі трафіку, доцільно застосовувати апаратні рішення (маршрутизатори з апаратним шифруванням або спеціалізовані VPN-пристрої). У разі обмежених ресурсів або потреби гнучкої конфігурації оптимальним може стати використання чисто програмних рішень або інтегрованих

VPN-систем операційних систем. Кожен із розглянутих підходів вимагає ретельного аналізу з точки зору апаратних потужностей, криптографічних потреб і вимог до масштабованості. Сучасні гібридні рішення, що поєднують переваги обох підходів, дозволяють досягти високого рівня безпеки при збереженні оптимальної продуктивності мережі, що є критичним фактором у сучасному середовищі кіберзагроз.

1.2 Аналіз методів і засобів організації VoIP-зв'язку

Системи голосового зв'язку на базі Інтернет-протоколу (VoIP) радикально змінили спосіб організації телефонних дзвінків як у корпоративному, так і в приватному середовищі. Основним механізмом у цих технологіях є протокол SIP (Session Initiation Protocol), який використовується для сигналізації та керування сеансами зв'язку. Поняття SIP-телефону виступає синонімом VoIP-телефону або «програмного телефону», адже обидва типи дозволяють здійснювати виклики, використовуючи технологію передачі голосу за IP-протоколом.

1.2.1 Типологія SIP-телефонів

Апаратні SIP-телефони є спеціалізованими пристроями, що за зовнішнім виглядом нагадують традиційні телефони, але обладнані апаратними кодеками, модулями ехо-компенсації та іншими засобами для оптимізації голосової передачі. Вони забезпечують інтуїтивно зрозумілий інтерфейс і високу якість дзвінків завдяки апаратній оптимізації обчислювальних процесів. Апаратні рішення ідеально підходять для великих організацій, де стабільність і надійність зв'язку мають першорядне значення.

Використання програмних рішень (SIP-телефони, softphone) дозволяє перетворити будь-який комп'ютер, планшет або смартфон у VoIP-телефон. Для роботи потрібно лише встановлення відповідного програмного забезпечення, підключення телефонної гарнітури, мікрофона або використання вбудованої звукової карти. Програмний підхід забезпечує гнучкість, дозволяючи інтегрувати додаткові функції, наприклад, відеодзвінки, конференції та інші мультимедійні сервіси. При цьому зв'язок маршрутизується через SIP-сервер, який виконує роль

проксі та реєстратора учасників мережі.

1.2.2 Сеанс зв’язку за SIP-протоколом

Основна суть організації VoIP-зв’язку полягає у налагодженні та управлінні сеансами дзвінків між SIP-телефонами. Сеанс встановлення виклику зазвичай проходить за таким стандартним алгоритмом, який можна представити на схемі (рис. 1.8):

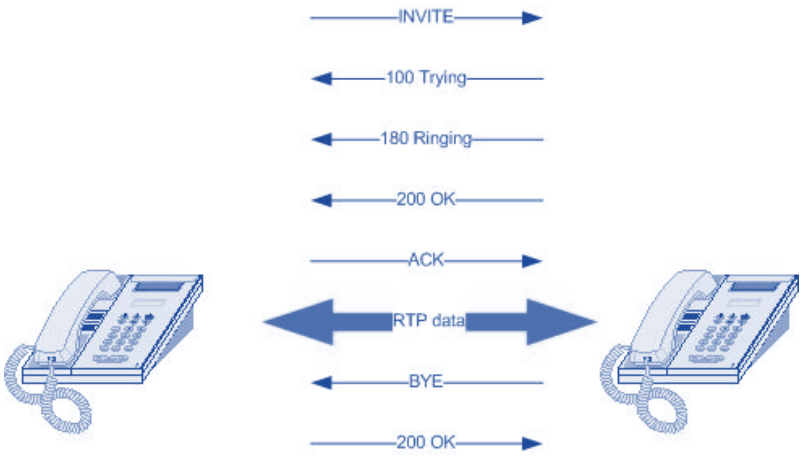


Рисунок 1.8. Організація сеансу зв'язку SIP

1. Ініціація виклику: Сторона, що ініціює дзвінок, надсилає SIP-запит INVITE до бажаного абонента. Запит містить інформацію про підтримувані кодеки, медіа-параметри за допомогою протоколу SDP (Session Description Protocol) та інші дані для встановлення з’єднання;

2. Початкове підтвердження: Отримувач виклику повертає тимчасову відповідь «100 Trying», яка сигналізує про початок процесу встановлення з’єднання;

3. Сигнал дзвінка: Далі, коли телефон, що викликається, починає сигналізувати про вхідний дзвінок, надійде відповідь «180 Ringing». Це дозволяє абоненту, який ініціював виклик, отримати інформацію про стан з’єднання;

4. Встановлення з’єднання: Після того як сторона, що викликається, піднімає трубку, SIP-сервер або телефон відправляє відповідь «200 OK», підтверджуючи готовність приймати з’єднання;

5. Підтвердження з’єднання: Ініціатор дзвінка надсилає SIP-повідомлення ACK для остаточного підтвердження. Після цього відкривається медіа-канал, який

використовує протокол RTP (Real-Time Transport Protocol) для передачі голосових даних;

6. Роз'єднання зв'язку: За завершенням сеансу одна зі сторін надсилає запит BYE, після чого інша сторона відповідає повідомленням «200 OK», що завершує з'єднання.

Цей процес забезпечує гнучкість у керуванні дзвінками, дозволяє проводити переговори, конференції та інтегрувати додаткові мультимедійні функції. Сучасні системи часто включають додаткові механізми NAT-трісверсу та адаптації мережевих протоколів (STUN, TURN, ICE), забезпечуючи стабільність зв'язку навіть у складних мережевих умовах.

1.2.3 Організаційні засоби та інтерфейс інтеграції з аналоговими мережами

Офісна міні-АТС утворює приватну телефонну мережу всередині організації, що дозволяє спільно використовувати обмежену кількість зовнішніх ліній для виходу в публічні телефонні мережі. Разом з розвитком VoIP-технологій з'явилися IP міні-АТС, які є програмними рішеннями для організації дзвінків через Інтернет. У цьому контексті розрізняють чотири типи міні-АТС:

1. Традиційні офісні міні-АТС;
2. Корпоративні віртуальні міні-АТС з аутсорсингом послуг;
3. IP міні-АТС;
4. Корпоративні віртуальні IP міні-АТС з аутсорсингом послуг.

IP міні-АТС дозволяють вирішувати завдання, які важко або економічно невигідно реалізувати з використанням аналогових систем. Вони забезпечують комплексну функціональність: від маршрутизації дзвінків до інтеграції з базами даних користувачів через SIP-сервер, що виступає як центральний елемент системи зв'язку.

Для забезпечення зв'язку між традиційними телефонними мережами (ТФЗК) та IP-телефонією використовуються спеціалізовані інтерфейси:

- Інтерфейс FXS (Foreign Exchange Station): Забезпечує підключення абонентського обладнання до телефонної мережі, постачаючи сигнал станції,

батарейне живлення та необхідну напругу для дзвінків. По суті, це «розетка», до якої підключається телефон.

- Інтерфейс FXO (Foreign Exchange Office): Служить приймачем сигналу телефонної лінії і встановлює зв'язок з аналоговим абонентським пристроєм. Ці порти мають індикацію стану дзвінка («трубка знята/на місці»), що дозволяє інтегрувати аналогові і цифрові системи.

Роз'єми FXS і FXO завжди працюють у парі, що забезпечує безперебійну взаємодію між аналоговими мережами загального користування та компонентами IP-телефонії.

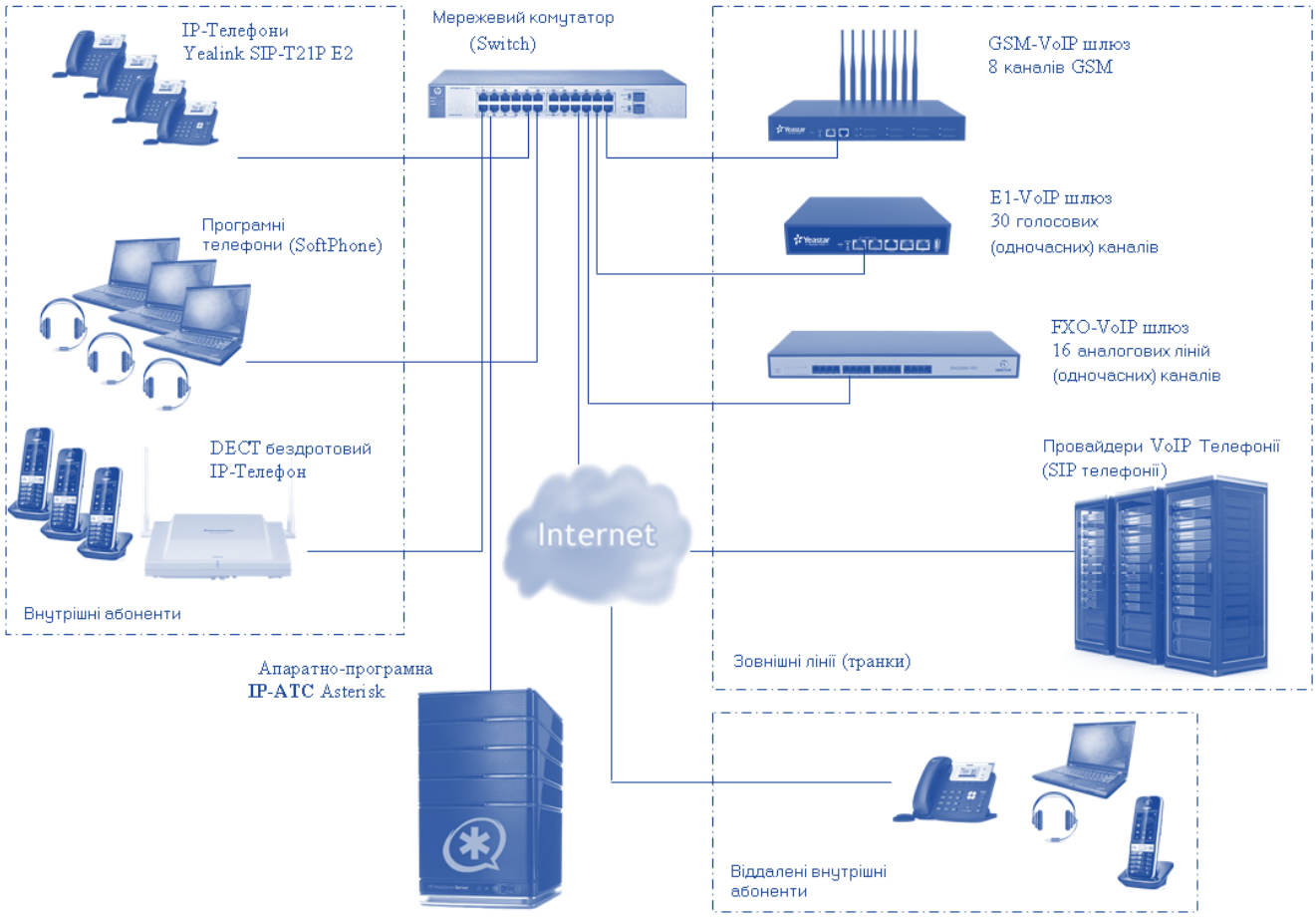


Рисунок 1.9. Схема організації мережі IP-телефонії на підприємстві

Ця схема (рис.1.9) відображає інтегровану мережеву інфраструктуру, де всі пристрої – від IP-телефонів та шлюзів до міні-АТС – з'єднані через комутатор. Особливу увагу приділяють вимогам якості обслуговування (QoS), що гарантує пріоритетну обробку голосового трафіку, мінімізуючи затримки, втрати пакетів і забезпечуючи високу якість зв'язку.

1.3 Визначення видів загроз в мережі VoIP-зв'язку

VoIP-системи передають голосові дані в режимі реального часу через IP-мережі, що створює специфічні вразливості, пов'язані із сигналізацією та передачою медіа-потоків. Безпосередній вплив атак вимірюється порушенням трьох основних характеристик безпеки: конфіденційності, цілісності та доступності. Нижче наведено конкретний опис основних видів загроз із додаванням статистичних даних, таблиць і порівнянь для подальшої візуальної інтерпретації.

1. Перехоплення голосових потоків (Eavesdropping). Незахищені або недостатньо захищені RTP-пакети можуть бути перехоплені, що дозволяє зловмисникам прослуховувати розмови та отримувати конфіденційну інформацію. За результатами деяких досліджень, до 30% інцидентів у VoIP-системах пов'язані саме з перехопленням голосових даних. Рис. 1.10 демонструє схему перехоплення голосових пакетів шляхом прослуховування.

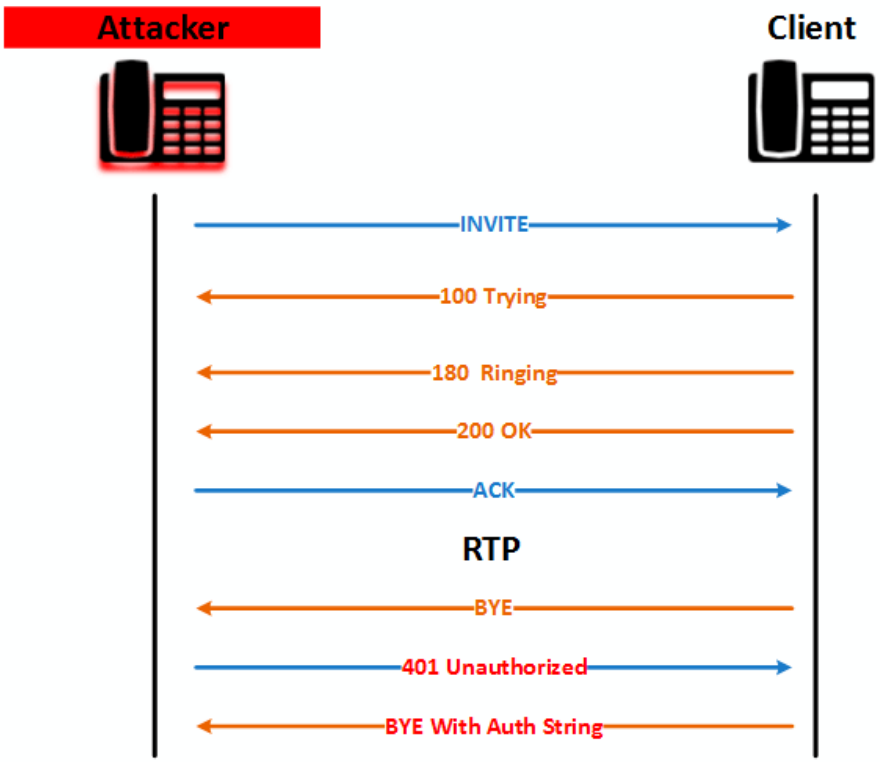


Рисунок 1.10 Схема перехоплення голосових пакетів шляхом прослуховування

2. Атаки на SIP-сигналізацію. Зловмисники можуть підроблювати SIP-повідомлення або втручатись у процес встановлення з'єднання, змінювати

параметри викликів або викрадати дані автентифікації. За статистикою, такі атаки зустрічаються приблизно в 25% випадків.

3. DoS/DDoS атаки. Атакуючі можуть перевантажувати SIP-сервери та медіа-шлюзи, що призводить до зниження пропускної здатності мережі або її повного виходу з ладу. Дослідження свідчать, що близько 35% інцидентів у VoIP-системах пов’язані з DoS/DDoS атаками. схему DoS-атаки, яка показує перевантаження серверів сигналізації масовим потоком запитів.

4. SPIT (Spam over IP Telephony). Масові небажані дзвінки, які ініціюються зловмисниками, створюють надмірне навантаження на сервери та можуть використовуватись для вторгнення в систему або для масового рекламного спаму. Цей тип загроз займає близько 10% від загального спектру атак.

5. Man-in-the-Middle (MITM) атаки. При MITM-атаках зловмисник вставляється між двома комунікаційними вузлами, що дозволяє йому модифікувати дані або навіть створювати фальшиві дзвінки. Статистично, такі інциденти становлять приблизно 20% загроз VoIP.

6. Програмні вразливості. Програмне забезпечення SIP-телефонів або серверів може містити недоліки, що дозволяють встановити шкідливий код або отримати несанкціонований доступ. Відсутність регулярних оновлень робить такі уразливості особливо небезпечними, що може призвести до комплексних атак із витоком даних.

Нижче наведено табл. 1.1, що узагальнює основні типи загроз в мережах VoIP, їх опис, орієнтовні статистичні дані та можливі наслідки.

Для кращого розуміння впливу кожного типу загроз на систему безпеки VoIP, наведемо ще одну таблицю, яка демонструє, як окремі загрози впливають на конфіденційність, цілісність та доступність (табл.1.2).

Ефективний захист мереж VoIP має базуватися на тотальному розумінні типів загроз, що впливають на систему, а також їх статистичної важливості. Зокрема, дані свідчать, що найбільш поширеними інцидентами є DoS/DDoS атаки та перехоплення голосових потоків, що вимагає впровадження сучасних криптографічних методів та механізмів автентифікації.

Таблиця 1.1. Порівняльна характеристика загроз VoIP-зв'язку

Тип загрози	*Опис*	*Статистика*	*Наслідки*
Перехоплення голосових потоків	Несанкціонований доступ до RTP-пакетів, що дозволяє прослуховувати дзвінки	~30% випадків	Витік конфіденційної інформації, порушення приватності
Атаки на SIP-сигналізацію	Підробка SIP-повідомлень, модифікація параметрів викликів	~25% випадків	Викрадення даних автентифікації, перенаправлення дзвінків
DoS/DDoS атаки	Перевантаження серверів сигналізації та шлюзів, що перешкоджає нормальній роботі системи	~35% випадків	Зниження доступності, повне відключення послуг
SPIT (Spam over IP Telephony)	Масові небажані дзвінки, що перевантажують систему	~10% випадків	Надмірне навантаження, втрати ресурсів, порушення якості обслуговування
MITM атаки	Вставляння зловмисника між комунікаційними вузлами з можливістю модифікації або блокування даних	~20% випадків	Модифікація голосових пакетів, створення фальшивих дзвінків
Програмні вразливості	Недоліки в програмному забезпеченні, що дозволяють встановлення шкідливого коду	–	Злом системи, витік даних, зміна параметрів роботи VoIP-систем

Таблиця 1.2. Вплив загроз на ключові параметри безпеки.

Загроза	*Конфіденційність*	*Цілісність*	*Доступність*
Перехоплення голосових потоків	Висока	Середня	Низька
Атаки на SIP-сигналізацію	Висока	Висока	Середня
DoS/DDoS атаки	Низька	Низька	Висока
SPIT	Середня	Середня	Середня
MITM атаки	Висока	Висока	Середня
Програмні вразливості	Висока	Висока	Висока

1.4 Визначення методів захисту VoIP-зв'язку

Сучасні технології VoIP використовують комп'ютерні мережі для передачі голосових даних, що забезпечує високу швидкість та економічність зв'язку. Проте ці мережі, побудовані на основі протоколів TCP/IP та UDP/IP, не є від природи захищеними від несанкціонованих атак. Зростання вимог до безпеки даних стимулює розробку комплексних методів захисту, які базуються на шифруванні, аутентифікації та тунелюванні.

1.4.1 Основні підходи та технології захисту

З метою створення ефективного захисту VoIP-систем вчені виділяють шість основних методів, спрямованих на створення перепон для зловмисників:

- Перешкода: застосування технічних засобів, що ускладнюють доступ до даних (наприклад, маршрутизація через спеціалізоване обладнання);
- Маскування: приховування реальної IP-адреси користувача або сервера для зменшення можливості ідентифікації цільових точок;
- Регламентація: встановлення чітких правил і політик доступу до мережевих ресурсів;
- Управління: моніторинг і контроль над доступом до мережевих ресурсів із використанням засобів логування та аудиту;
- Примус: застосування засобів захисту, що фізично або програмно блокують доступ неавторизованих користувачів;
- Спонукання: стимулювання відповідних поведінкових моделей у користувачів (наприклад, політика безпеки, навчання співробітників).

Незважаючи на різноманітність підходів, ключовим елементом захисту VoIP-зв'язку залишається технологія віртуально захищених мереж (VPN). VPN забезпечує створення зашифрованого «тунелю» між кінцевою точкою (наприклад, SIP-телефоном) та сервером VoIP або корпоративною мережею, що дозволяє ізолювати трафік від несанкціонованого доступу. На рис. 1.11 показана принципова схему VPN-тунелю, де дані між клієнтом і сервером зашифровані та проходять через відкриту мережу, забезпечуючи конфіденційність і цілісність інформації.

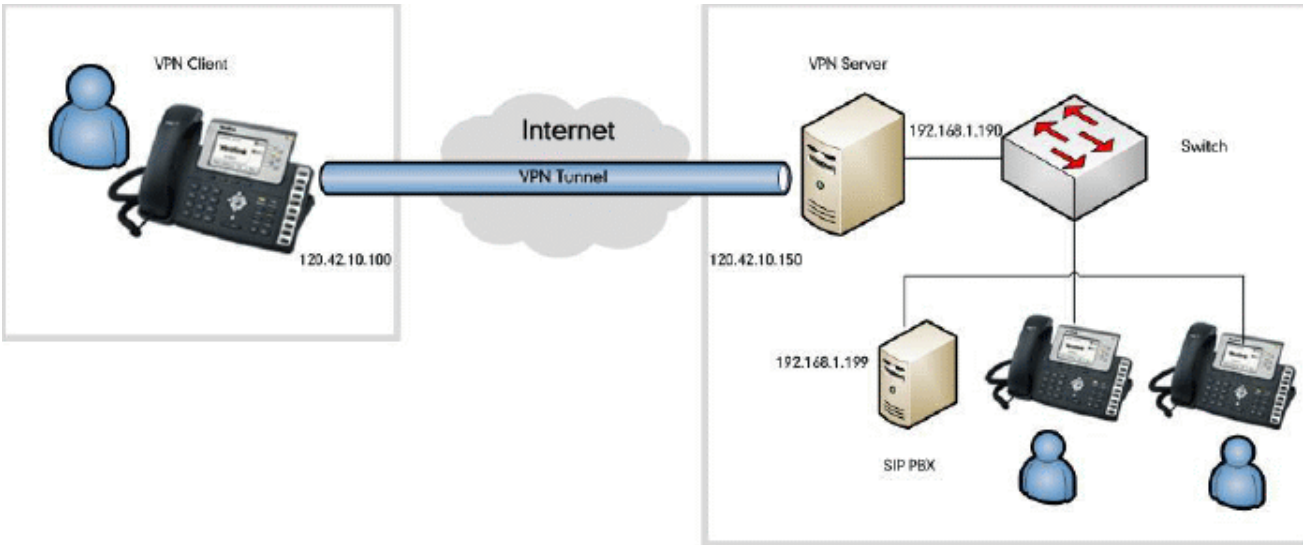


Рисунок 1.11. Схема захищеного каналу VoIP-зв’язку

1.4.2 Технічна реалізація методів захисту

Методи захисту VoIP-зв’язку реалізуються за допомогою комплексного використання криптографічних алгоритмів, протоколів тунелювання та систем аутентифікації. Серед основних технологій можна виділити:

1. VPN-тунелювання. Цей метод дозволяє організувати захищене з’єднання через загальнодоступну мережу, ізолюючи голосовий трафік за допомогою шифрування. Технологія VPN базується на інкапсуляції даних у захищену оболонку, що включає:

– Шифрування: Використання стандартних алгоритмів (AES, 3DES, тощо) для шифрування пакетів із голосовими даними;

– Аутентифікація: Перевірка автентичності клієнтів та серверів через протоколи, такі як IPSec або SSL/TLS.

Цей метод дозволяє приховувати реальну IP-адресу користувача, обмежувати доступ до системи та забезпечувати високий рівень захисту, що критично для корпоративних систем. На рис. 1.12 представлено загальний механізм інкапсуляції даних у віртуальному тунелі;

2. Використання криптографічних методів. Шифрування даних гарантує, що інформація залишається невідомою для третіх осіб, навіть якщо вона буде перехоплена. Сучасні криптосистеми застосовують комбінації симетричних і асиметричних алгоритмів для забезпечення:

– Конфіденційності: Дані перетворюються за допомогою сильних алгоритмів шифрування;
– Цілісності: Використовуються хеш-алгоритми (SHA-256, MD5) для перевірки немодифікованості даних;

3. Авторизація та аутентифікація. Для запобігання несанкціонованому доступу системи використовують суворі процедури перевірки достовірності. SIP-сервери, які здійснюють обробку викликів, впроваджують методи аутентифікації, такі як PAP, CHAP або MS-CHAP, що дозволяють гарантувати, що доступ отримують лише авторизовані користувачі;

4. Захист через маскування та фільтрацію. Розгортання мережевих фаєрволів і систем виявлення вторгнень (IDS/IPS) дозволяє здійснювати контроль над вхідним та вихідним трафіком, здійснюючи маскування реальних адрес і блокування спроб несанкціонованого доступу. Це підходить як для захисту внутрішніх мереж, так і для захисту кінцевих точок у VoIP-системах.

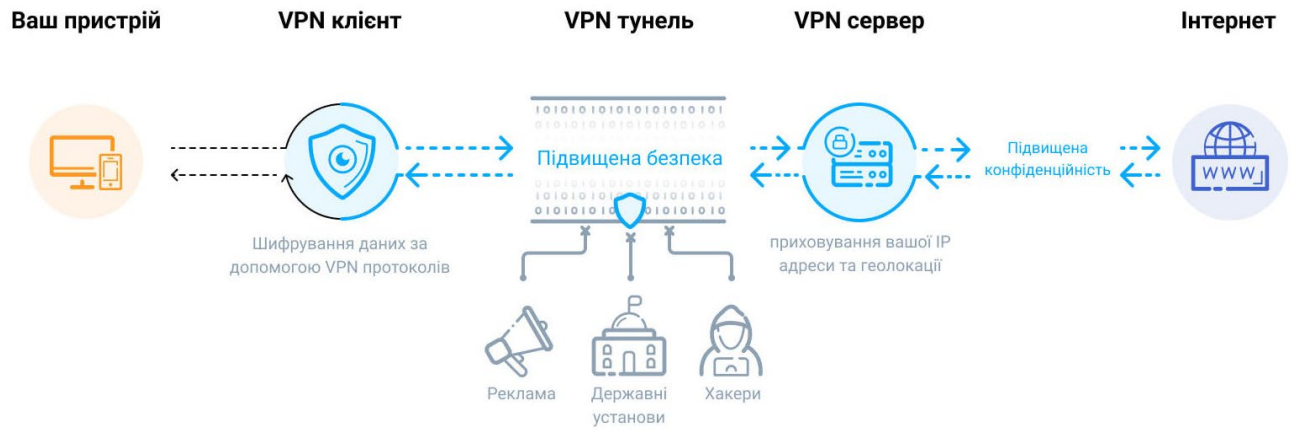


Рисунок 1.12. Схема тунельного шифрування в VPN

1.4.3 Порівняльна характеристика методів захисту

У табл.1.3 наведено результати порівняння основних методів захисту VoIP-зв'язку за ключовими показниками. Захист VoIP-зв'язку базується на комплексному застосуванні сучасних технологій, що включають тунелювання, криптографію та системи аутентифікації. Використання технології VPN є одним із найефективніших способів забезпечення безпеки, оскільки дозволяє створити зашифрований канал для передачі голосових даних через незахищені мережі.

Завдяки інтеграції криптографічних алгоритмів, методів маскування, регламентації доступу та контролю над трафіком, VoIP-системи отримують високий рівень захисту навіть при використанні стандартних мереж Internet.

Таблиця 1.3. Порівняльна характеристика методів захисту VoIP-зв'язку

Метод захисту	*Принцип*	*Переваги*	*Недоліки*
VPN-тунелювання	Інкапсуляція та шифрування даних через віртуальний тунель	Захищений канал на рівні мережі, приховування IP-адрес	Складність налаштування, додаткове навантаження
Криптографічне шифрування	Шифрування даних за допомогою алгоритмів (AES, 3DES)	Високий рівень захисту при перехопленні трафіку	Витрати на обчислювальні ресурси
Аутентифікація/ авторизація	Перевірка користувачів через протоколи SIP-аутентифікації	Забезпечення доступу лише для авторизованих користувачів	Можливі вразливості при застарілій реалізації
Маскування та фільтрація	Використання фаєрволів та IDS/IPS для контролю трафіку	Блокування несанкціонованих з'єднань, захист мережевої інфраструктури	Не вирішує проблему перехоплення даних на транспортному рівні

1.5 Вибір технології захисту VoIP-зв'язку від несанкціонованого доступу

Сучасні VoIP-системи базуються на передачі голосових даних через відкриті мережі Internet, що обумовлює необхідність застосування комплексних засобів захисту від несанкціонованого доступу. Основою для забезпечення безпеки є технології VPN, які побудовані на двох ключових підходах:

1. Технологія «тунелювання» (tunneling або encapsulation). Цей метод ґрунтується на інкапсуляції даних — в процесі тунелювання великі потоки даних розбиваються на менші пакети, які шифруються за допомогою сильних криптографічних алгоритмів і транспортуються по зашифрованому віртуальному каналу до кінцевого пункту. На рис. 1.13. представлено, як пакети даних, що містять голосову інформацію, інкапсулюються, шифруються і передаються через

загальнодоступну мережу, створюючи захищений «тунель». При цьому технологія тунелювання забезпечує не лише конфіденційність, але й певний рівень цілісності даних, проте самостійно вона не гарантує абсолютної безпеки. Слабкі місця тунельних протоколів можуть бути використані зловмисниками, якщо не застосовувати додаткові криптографічні заходи.

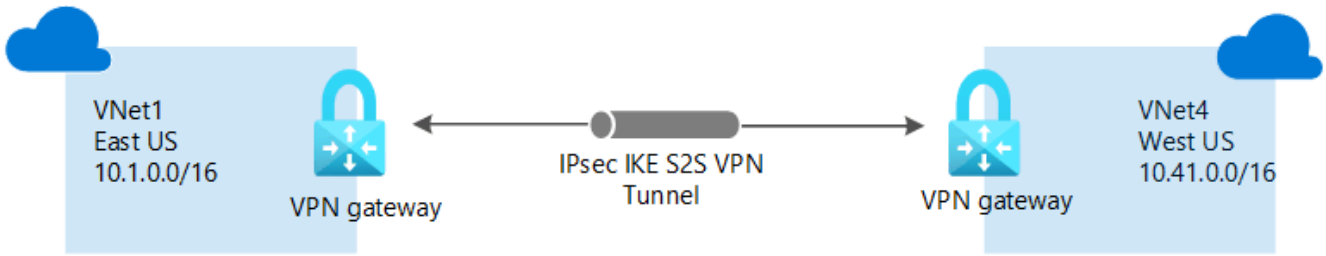


Рисунок 1.13. Тунельна схема організації VPN через IPsec/IKE

2. Технології аутентифікації та шифрування. Цей підхід забезпечує конфіденційність, цілісність і автентичність інформації шляхом використання криптографічних алгоритмів і методів цифрового підпису (електронного цифрового підпису, ЕЦП). До даних, що передаються, додається спеціальний блок даних, сформований за допомогою алгоритмів шифрування, який може бути дешифрований лише за допомогою особистого ключа, що проходить перевірку через відповідний відкритий ключ. Таким чином, навіть при перехопленні даних зловмисником, відновити їх правильний вміст без правильного ключа неможливо.

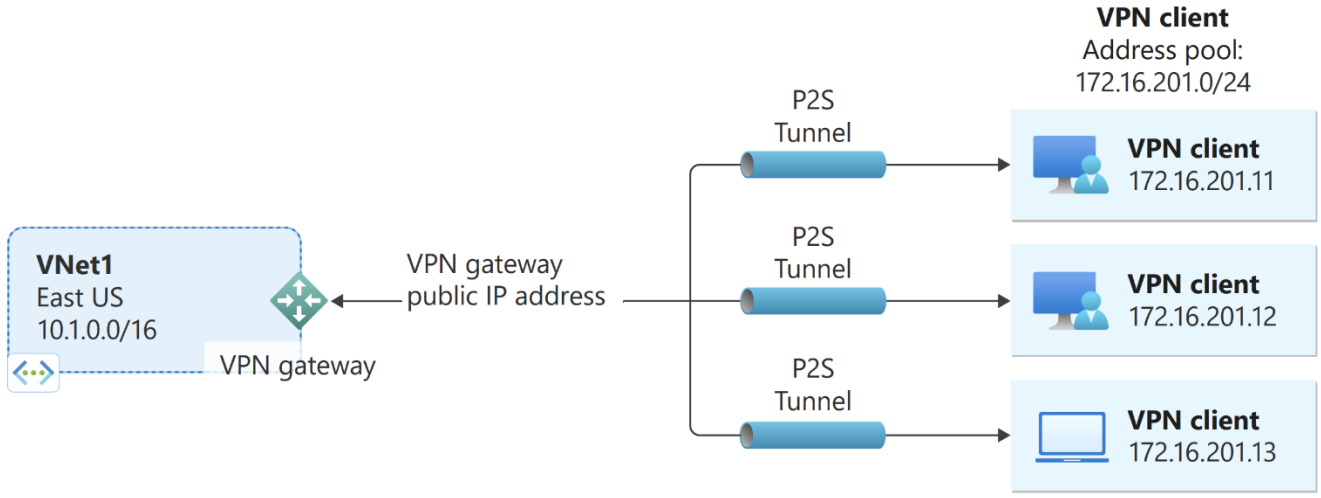


Рисунок 1.14. Схема підключення Remote Access VPN ("точка-мережа", P2S)

Рисунок 1.14. демонструє підключення «точка – мережа» (P2S) до VPN-шлюзу, яке дозволяє встановити безпечне з'єднання з вашою віртуальною мережею

на індивідуальному клієнтському комп'ютері. На рис.1.15 показано вміст IP-пакету при використанні віддаленого підключення за протоколом IPsec.

Рисунок 1.15. Тунельний режим IPsec

Вибір технології захисту базується на вирішенні двох ключових завдань:

1. Безпечне підключення до відкритих мереж. Забезпечення доступу виключно для авторизованих користувачів і запобігання несанкціонованому доступу до мережі;

2. Збереження автентичності та цілісності переданих даних. Гарантування того, що інформація у процесі передачі не змінюється і залишається достовірною.

Для захисту локальних мереж від зовнішніх загроз часто використовують брандмауери (firewall), які можуть бути поділені на персональні (для окремих комп'ютерів) та корпоративні (на шлюзі між Internet і локальною мережею). У комбінації з технологіями VPN вони дозволяють формувати захищене середовище для передачі конфіденційних даних, що є критично важливим для корпоративної інформаційної інфраструктури.

Таблиця 1.4. Порівняльна характеристика технологій захисту VoIP-зв'язку

Параметр	*Тунелювання*	*Аутентифікація/шифрування*
Принцип	Інкапсуляція даних у захищений тунель	Додавання криптографічного блоку даних та цифрового підпису
Основні переваги	Економічність, висока швидкість, можливість використання у WAN	Підвищена конфіденційність, гарантії цілісності та автентичності
Основні недоліки	Слабкі місця без додаткових криптографічних заходів	Вищі комп'ютерні витрати, складність налаштування
Застосування	Організація захищених з'єднань між мережами через Internet	Захист окремих каналів передачі даних; робота з цифровими підписами

У табл.1.4 показано узагальнення ключових параметрів технологій захисту VoIP-зв'язку. Вибір конкретного рішення залежить від низки факторів, зокрема:

- Продуктивність та швидкість передачі даних: VPN, побудовані на технології тунелювання, забезпечують економію каналів зв'язку і дозволяють підприємствам відмовитись від дорогих WAN- або Extranet-мереж;
- Сумісність між різними мережевими профілями: Використання стандартних протоколів дозволяє інтегрувати рішення VPN з різними типами мереж, забезпечуючи захист навіть між сайтами та компаніями з різними мережевими вимогами;
- Захист від несанкціонованого доступу: Комплексне рішення, що включає використання VPN, брандмауерів та систем контролю (IDS/IPS), дозволяє ефективно захищати як локальні, так і віддалені мережеві з'єднання.

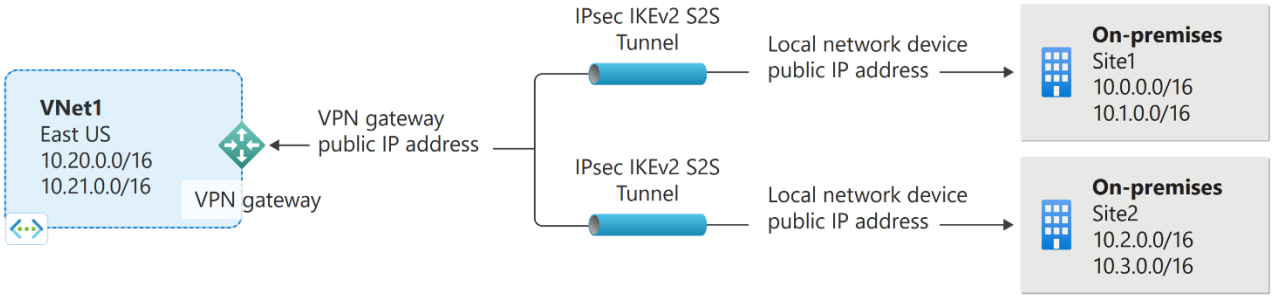


Рисунок 1.16. Тунельна схема організації VPN типу "мережа-мережа" (site-to-site)

Рис. 1.16 демонструє побудову захищеного з'єднання між офісними локаціями компанії за допомогою спеціалізованих маршрутизаторів. Підключення типу «мережа — мережа» (S2S) через VPN-шлюз — це підключення через VPN-тунель згідно з протоколом IPsec/IKE (IKEv1 або IKEv2). Підключення типу «мережа — мережа» можна використовувати для розподілених і гібридних конфігурацій. Для такого підключення потрібен VPN-пристрій, розташований у локальному середовищі з публічною IP-адресою, призначеною йому.

У шлюзі віртуальної мережі можна створити декілька VPN-підключень, як правило, до різних локальних сайтів. При роботі з кількома підключеннями необхідно використовувати тип VPN RouteBased. Оскільки кожна віртуальна мережа може мати лише один VPN-шлюз, доступну пропускну здатність шлюзу використовують усі підключення. Цей тип дизайну підключення іноді називають

«кількома сайтами».

Вибір технології захисту VoIP-зв’язку від несанкціонованого доступу у даній роботі базується на інтеграції двох основних підходів: тунелювання даних, яке забезпечує ефективну і економічну передачу інформації через зашифрований канал, та систем криптографічного захисту, що гарантує конфіденційність, цілісність і автентичність переданих даних за рахунок цифрових підписів та методів аутентифікації. Застосування комплексного підходу дозволяє суттєво підвищити рівень безпеки корпоративних VoIP-систем, забезпечуючи надійний захист інформації навіть у умовах використання незахищених мереж Internet.

1.6 Вибір захищеного протоколу для шифрування VoIP-зв’язку

Для забезпечення безпечного VoIP-зв’язку критично важливо обрати надійний протокол шифрування, який гарантує конфіденційність, цілісність та автентичність голосових даних, що передаються через відкриті мережі. Захищені VPN-тунелі, реалізовані на різних рівнях моделі OSI, дозволяють створити віртуальні канали для передачі даних, проте характеристика ізоляції і шифрування залежить від вибраного протоколу. Основні рівні моделі OSI, які використовуються для побудови мереж VPN — канальний, мережевий та транспортний рівні у побудові VPN, що слугують базою для впровадження методів шифрування VoIP-зв’язку. Протоколи VPN можна умовно розділити на два основних підходи:

1. Технологія тунелювання (інкапсуляція). Це механізм, за допомогою якого вихідний потік даних (зокрема, голосові дані) розбивається на менші пакети, що шифруються і передаються через загальнодоступну мережу за допомогою віртуального тунелю. Дані інкапсулюються всередину IP-пакету або спеціального заголовку, що забезпечує їх ізоляцію від атак із зовнішнього середовища. Один із найстаріших і найпоширеніших протоколів цієї групи – PPTP (Point-to-Point Tunnelling Protocol). На рис.1.17 представлено, як протокол PPTP інкапсулюється для передачі в IP-мережах. PPTP використовує стек протоколів TCP/IP, забезпечуючи високі показники швидкодії і сумісність з майже всіма пристроями навіть з обмеженими ресурсами. Проте, незважаючи на свою простоту та широке впровадження, PPTP має серйозні недоліки щодо безпеки, оскільки метод

шифрування і управління ключами в ньому є менш стійким до сучасних атак.

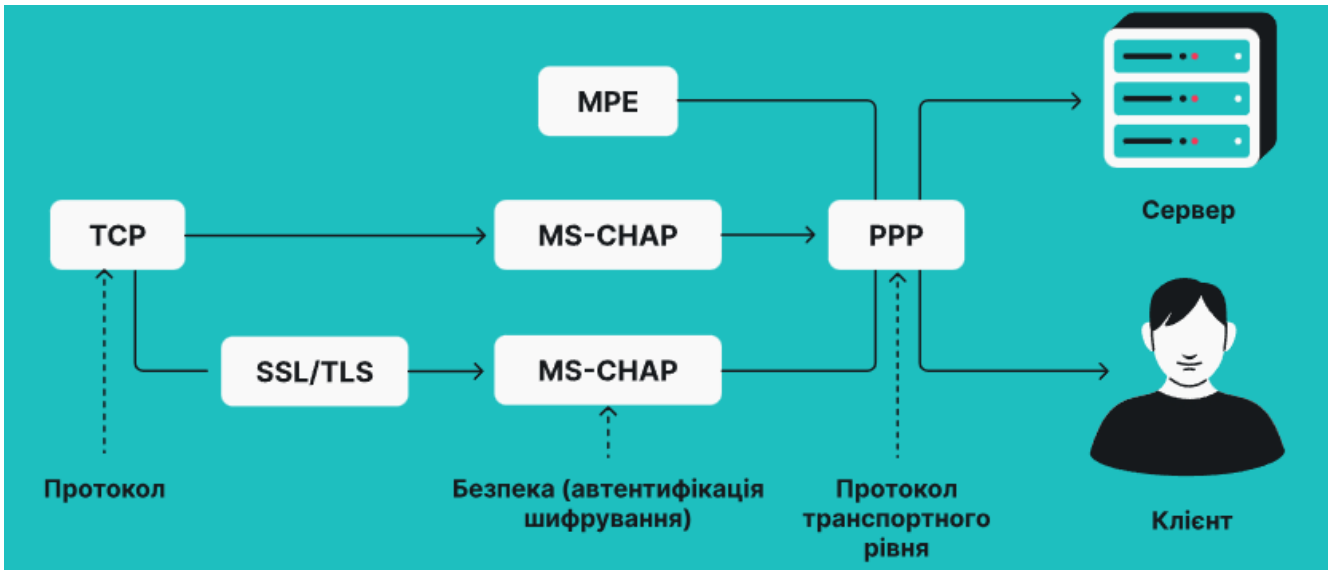


Рисунок 1.17. Реалізація протоколу PPTP для тунелювання

На рис.1.17 представлено, як дані спочатку інкапсулюються в кадри PPP, потім – у пакети GRE, а потім додається IP-заголовок. PPTP також характеризується тим, що для забезпечення базових функцій управління тунелем використовується окреме з'єднання, що обмежує рівень захищеності при безпосередній передачі пакетів.

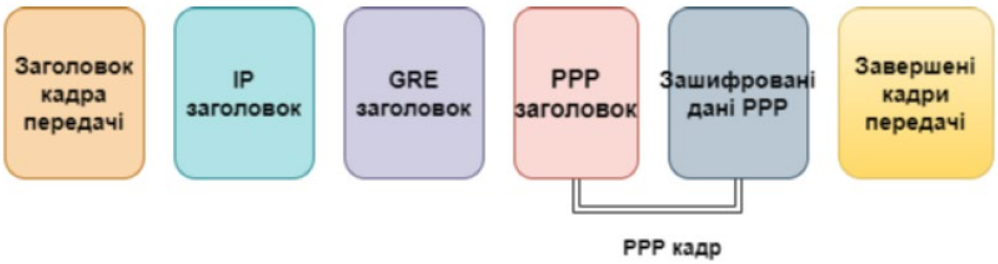


Рисунок 1.18. Схема пересилки даних по тунелю PPTP

2. Методи аутентифікації та шифрування. Другий підхід ґрунтується на комплексному використанні криптографічних методів для гарантування конфіденційності, цілісності та автентичності даних. За допомогою електронного цифрового підпису (ЕЦП) та сучасних алгоритмів (AES, 3DES тощо) до передачі зашифрованих пакетів додається додатковий блок даних, який може бути дешифрований лише за наявності відповідного особистого ключа, що підтверджується відкритим ключем. Цей рівень захисту може застосовуватись як у комбінації з тунелюванням, так і окремо.

На даний момент L2TP (Layer 2 Tunnelling Protocol), у комбінації з IPSec, вважається одним із найнадійніших рішень для побудови захищених VPN-каналів. L2TP поєднує переваги технологій PPTP і L2F (Layer 2 Forwarding) і забезпечує більш ґрунтовне шифрування за рахунок використання IPSec як базового механізму для транспортного шифрування.

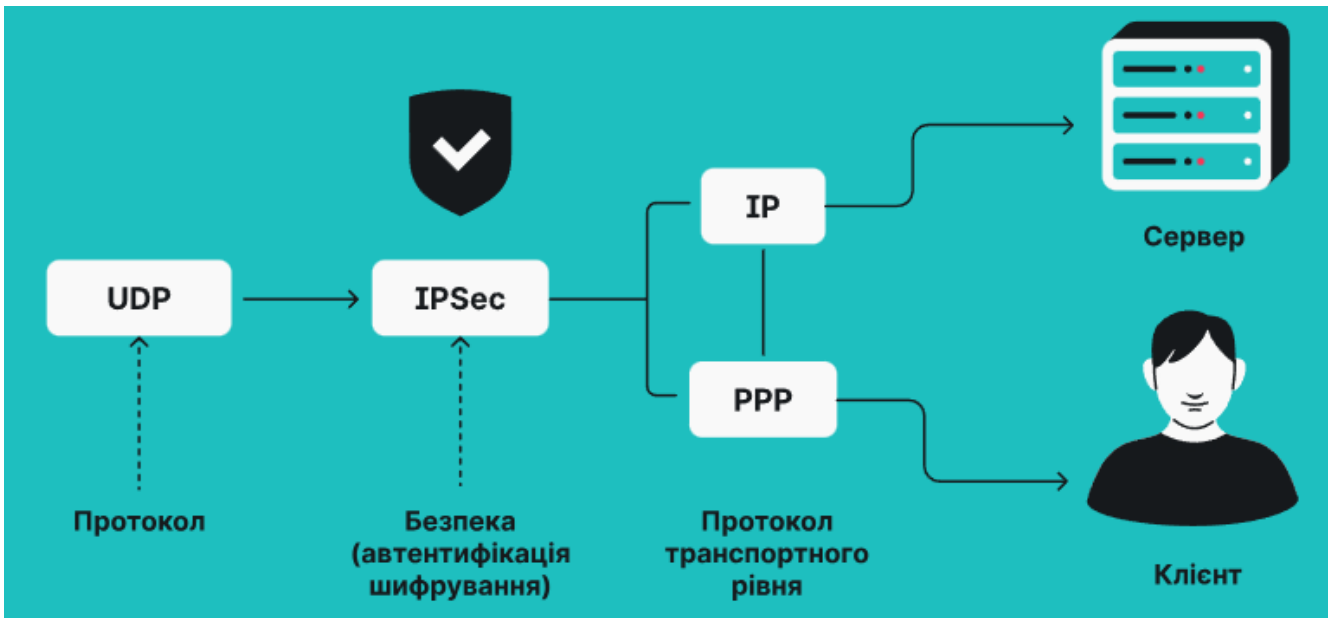


Рисунок 1.19. Архітектура протоколу L2TP

На рис.1.19 показано структурну схему, згідно з якою дані інкапсулюються протоколом L2TP із подальшим застосуванням IPSec для шифрування. Основна відмінність L2TP/IPSec від PPTP полягає в тому, що шифрування виконується на рейсі IPSec, що дозволяє гарантувати високий рівень криптографічного захисту. Проте дана комбінація вимагає більше ресурсів і може зменшувати швидкодію через подвійне інкапсуляцію (перш за все, внутрішнього протоколу тунелювання, а потім – зовнішнього IPsec-захисту).

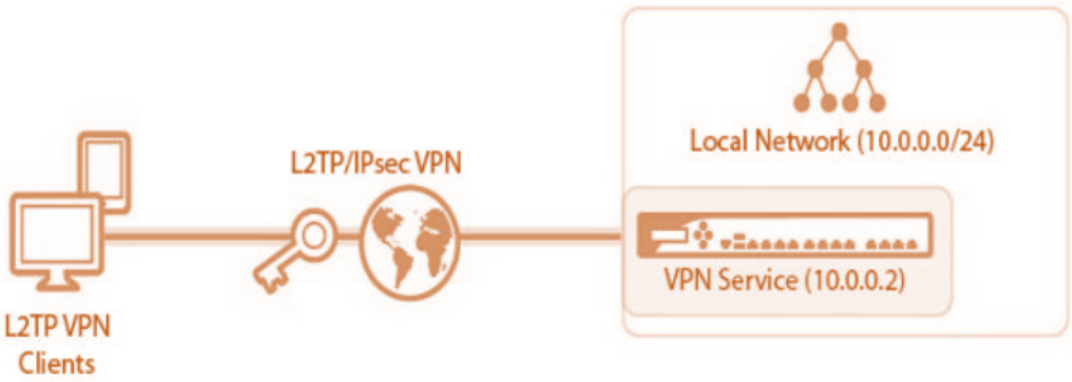


Рисунок 1.20. Структурна схема побудови тунелю на канальному рівні

На рис.1.20 показано логіку побудови тунелю з використанням L2TP для інкапсуляції і IPSec для шифрування даних. Для розширеного захисту мережевого трафіку, крім L2TP/IPSec, широко застосовують протокол IPSec на мережевому рівні. IPSec – це набір алгоритмів для шифрування даних, що працює поверх IP-протоколу. Він включає два основних механізми:

- Authentication Header (AH) – забезпечує автентифікацію і цілісність переданих даних;
- Encapsulating Security Payload (ESP) – відповідає за шифрування, конфіденційність і автентифікацію.

Крім того, для полегшення налаштування і високої сумісності з веб-додатками набуває популярності SSL VPN або TLS VPN. Ці протоколи використовують стандартні криптографічні засоби, інтегровані у веб-браузери, і забезпечують зручний доступ з персонального комп'ютера до мережевих ресурсів без необхідності складних налаштувань.

OpenVPN – це програмний продукт з відкритим вихідним кодом, що розповсюджується за ліцензією GNU General Public License (GPL). Він дозволяє встановити захищене VPN-з'єднання між комп'ютерами у локальній бізнес-мережі навіть через інфраструктуру загальнодоступного зв'язку. Основні технічні особливості OpenVPN:

- Шифрування та безпека: OpenVPN використовує бібліотеку OpenSSL та протоколи TLS/SSL для аутентифікації й асиметричного шифрування. Він підтримує 256-бітове шифрування, що гарантує високий рівень захисту. Крім того, даний протокол може працювати з різними алгоритмами шифрування, зокрема AES та Blowfish (проте наразі AES вважається найбільш надійним і широко використовується державними установами та секретними службами);
- Гнучкість підключення: Завдяки підтримці як TCP, так і UDP портів, OpenVPN може працювати навіть через HTTPS (наприклад, на порті TCP 443), що дозволяє обходити блокування портів, NAT та брандмауери. Це робить його особливо корисним у сценаріях віддаленого доступу;

- Механізми аутентифікації: Для встановлення з'єднання OpenVPN підтримує кілька методів аутентифікації – використання загального секретного ключа, цифрових сертифікатів або комбінації імені користувача з паролем. Такий підхід забезпечує двосторонню автентифікацію клієнтів і серверів;
- Продуктивність та масштабованість: Швидкодія роботи OpenVPN залежить від рівня шифрування, і в деяких випадках протокол може працювати навіть швидше за IPSec. Однак його встановлення та конфігурування є досить складним у порівнянні з, наприклад, L2TP/IPSec або PPTP. Серед переваг – скорочення оперативних витрат та можливість збільшення масштабів мережі без необхідності прокладання дорогих орендованих ліній.

На рис. 1.21 представлена узагальнена схема роботи протоколу OpenVPN з врахуванням підтримуваних алгоритмів шифрування, методів аутентифікації та можливості обходу NAT і брандмауерів.

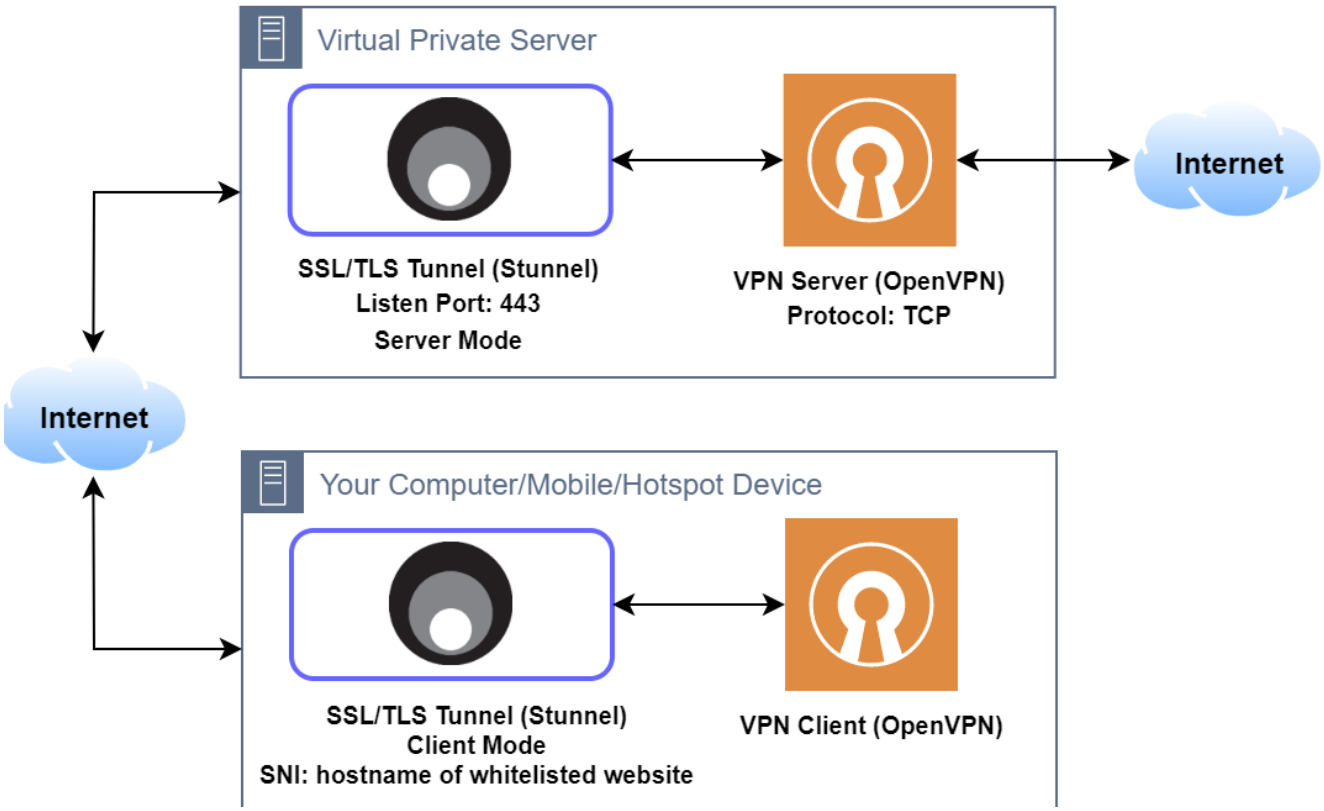


Рисунок 1.21. Архітектура протоколу OpenVPN

OpenVPN за рахунок використання сучасних криптографічних технологій (SSL/TLS, асиметричного шифрування) пропонує високий рівень захисту даних. Він є особливо привабливим рішенням для організацій, що потребують гнучкості в

налаштуванні та масштабній доступності, хоча налаштування системи вимагає досить високої кваліфікації.

IKEv2/IPsec – це сучасне рішення, яке виникло як вдосконалена заміна IKEv1, об’єднавши різні протоколи безпеки IPsec в один інтегрований механізм. Основні особливості IKEv2/IPsec:

- Пристосованість до мобільних технологій: IKEv2 був спеціально розроблений з урахуванням потреб мобільних пристроїв. Підтримка технології "мультихомінг" дає змогу безперебійно перемикатися між різними мережами (наприклад, з Wi-Fi на мобільний інтернет) без розриву VPN-тунелю;
- Висока швидкість та ефективність: IKEv2/IPsec відзначається швидкістю встановлення з’єднання та ефективністю роботи, що є важливим для застосувань, де час відгуку та безперервність зв’язку мають критичне значення. Однак з точки зору клієнтоорієнтованості іноді зустрічаються атаки типу «відмова в обслуговуванні» (DoS), засновані на фрагментації IP і використанні вироджених повідомлень;
- Обмін ключами та захист трафіку: Протокол використовує UDP порт 500 для обміну ключами, що виконується згідно з IKE, забезпечуючи самостійну автентифікацію та шифрування IP-трафіку. Метод шифрування здійснюється за допомогою комбінації протоколів AH та ESP, що гарантує як конфіденційність, так і цілісність переданих даних;
- Підтримка та складність налаштувань: Незважаючи на високі швидкісні характеристики, IKEv2/IPsec має певні недоліки: UDP порт 500 блокується набагато легше, ніж порти, що використовуються рішеннями на основі SSL (наприклад, SSTP або OpenVPN). Крім того, налаштування IKEv2 на сервері є досить складним, що може викликати потенційні проблеми з боку безпеки та сумісності на різних платформах.

На рис.1.21 показано, як здійснюється обмін ключами, встановлення тунелю та шифрування даних у системі IKEv2/IPsec, а також підкреслено переваги мобільності і швидкості.

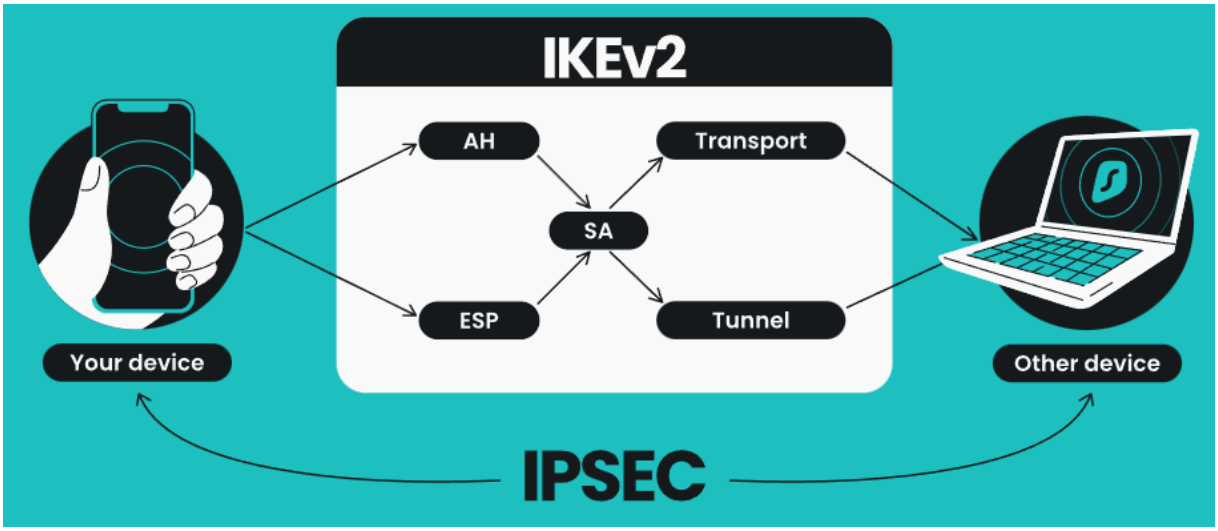


Рисунок 1.21. Архітектура і основні можливості IKEv2/IPsec

У табл.1.5 узагальнено основні характеристики протоколів, що використовуються для шифрування VoIP-зв'язку. Вибір захищеного протоколу для шифрування VoIP-зв'язку залежить від вимог до безпеки, сумісності з існуючою мережевою інфраструктурою та очікуваної продуктивності. Протокол PPTP, хоча і забезпечує високу швидкість і легкість впровадження, не відповідає сучасним вимогам до безпеки через слабкість криптографічних механізмів. Протокол L2TP у комбінації з IPSec є більш перспективним рішенням завдяки забезпеченню комплексного захисту, хоча і вимагає більше ресурсів. IPSec сам по собі демонструє високу надійність, проте налаштування може бути досить складним, а SSL/TLS VPN є зручним для інтеграції з веб-середовищами. IKEv2/IPsec є одним із найсучасніших і найшвидших протоколів, орієнтованих на стабільну роботу в умовах мобільних технологій. Проте для його ефективного використання необхідно враховувати особливості мережевого середовища та можливі загрози від DoS-атак. Цей протокол підійде для організацій, де важливим є швидке перемикання між мережами та висока надійність передачі захищених даних, хоча для його налаштування може знадобитися додаткова експертиза. Проведений аналіз дозволяє зробити висновок, що OpenVPN завдяки своїм характеристикам відповідає поставленому у даній роботі завданню: його налаштування, високий рівень безпеки та підтримка різноманітних складних алгоритмів забезпечують системі надійний захист.

Таблиця 1.5. Порівняльна характеристика протоколів шифрування для VoIP

Протокол	*Рівень OSI*	*Метод захисту*	*Переваги*	*Недоліки*
PPTP	Канальний (PPP)	Інкапсуляція через GRE, шифрування базового рівня	Швидкодія, простота реалізації, широка підтримка	Вразливість через слабку криптографію, обмежена цілісність
L2TP/IPSec	Канальний / Мережевий	Інкапсуляція L2TP + криптографіч-ний захист IPSec	Висока надійність, комплексний захист (конфіденційність, цілісність, автентичність)	Вища обчислювальна вартість, зниження швидкості
IPSec	Мережевий	AH/ESP, обмін ключами IKE	Повний захист IP-трафіку, гнучкі режими роботи (транспортування/ тунелювання)	Складність налаштування, можливе уповільнення через додаткове інкапсулювання
SSL/TLS VPN	Транспортний / Прикладний	Шифрування через SSL/TLS	Простота інтеграції з веб-браузерами, зручність для кінцевих користувачів	Залежність від правильності налаштувань, може бути менш ефективним для IP-трафіку
OpenVPN	Транспортний / Прикладний	Використання бібліотеки OpenSSL з протоколами TLS/SSL, підтримка роботи як через TCP, так і через UDP	Високий рівень захисту завдяки 256-бітовому шифруванню, гнучкість налаштувань, крос-платформеність, підтримка NAT traversal та масштабованість	Складність конфігурації, потенційно нижча швидкодія при високих рівнях шифрування, високі вимоги до обчислювальних ресурсів
IKEv2/IPSec	Мережевий	Аутентифікація та шифрування через AH/ESP з обміном ключами за протоколом IKEv2	Висока безпека, швидке відновлення з’єднання, мультихомінг, гнучке налаштування режимів роботи	Складність налаштування, можливість блокування UDP порту 500, піддатливість до DoS-атак

1.7 Аналіз роботи OpenVPN при організації VoIP-зв'язку

У сучасних мережах VoIP особливу увагу приділяють забезпеченню захищеності передаваних голосових даних. Один із найпопулярніших інструментів для організації безпечного VPN-з'єднання – OpenVPN, який як програмний продукт з відкритим вихідним кодом, здатний забезпечити високий рівень захисту за рахунок сучасних криптографічних методів. Основною метою є визначення, наскільки ефективно OpenVPN створює захищений канал для передачі голосових пакетів, забезпечує конфіденційність, цілісність і доступність даних, а також як його продуктивність і гнучкість налаштувань впливають на якість VoIP-зв'язку. Дослідження охоплює як теоретичні аспекти роботи OpenVPN (зокрема, його взаємодію з моделлю OSI та використання TLS/SSL для шифрування), так і практичну частину, що включає налаштування серверного та клієнтського оточення, інтеграцію з мережевими фаєрволами та оптимізацію мережевої конфігурації. Ключовими аспектами аналізу є:

- Безпека та криптографія: OpenVPN використовує сучасні криптографічні алгоритми (наприклад, 256-бітове шифрування на базі OpenSSL) для захисту переданих даних. Це дозволяє створити надійний «тунель», захищений від перехоплення та модифікації інформації;

- Продуктивність і гнучкість налаштування: Незважаючи на складність конфігурації, OpenVPN забезпечує високу ефективність передачі даних навіть в умовах проходження через NAT та брандмауери. Це важливо для організацій, що вимагають стабільного і швидкого захищеного доступу до VoIP-систем;

- Сумісність і масштабованість: Завдяки відкритості коду та широкій підтримці платформ, OpenVPN може бути інтегрований у різні мережеві середовища, що дозволяє організаціям безперешкодно масштабувати свій захищений зв'язок у разі збільшення кількості віддалених співробітників або розширення мережі.

Аналіз роботи OpenVPN охоплює тестування продуктивності, перевірку сумісності з мережевими засобами захисту та оцінку впливу алгоритмів шифрування на затримки та пропускну здатність VoIP-зв'язку.

1.7.1 Налаштування конфігурації OpenVPN

У цьому підрозділі розглядаються кроки з налаштування OpenVPN для організації захищеного VoIP-зв'язку, що включає встановлення необхідних пакетів, створення центра сертифікації (ЦС), генерацію серверних і клієнтських сертифікатів, налаштування конфігураційних файлів, мережевих параметрів і правил безпеки.

1. Підготовка оточення та встановлення OpenVPN

Перш за все, необхідно налаштувати сервер на базі Ubuntu, створити окремий (non-root) профіль користувача з привілеями sudo і налаштувати фаєрвол. Далі оновлюється список пакетів і встановлюються OpenVPN та easy-rsa:

sudo apt-get update

sudo apt-get install openvpn easy-rsa

Це гарантує, що програмне забезпечення встановлено і готове для подальшої конфігурації.

2. Створення центра сертифікації (ЦС)

Оскільки OpenVPN використовує TLS/SSL для шифрування трафіку між сервером і клієнтами, необхідно створити власний центр сертифікації. Для цього скористайтеся командою, що копіює шаблонну директорію easy-rsa до домашньої теки:

make-cadir ~/openvpn-ca

cd ~/openvpn-ca

3. Налаштування змінних ЦС

Треба відкрити файл vars у текстовому редакторі (наприклад, nano) і відредагувати необхідні змінні, які впливають на параметри створюваних сертифікатів:

nano vars

Необхідно змінити такі змінні, як:

- *export KEY_COUNTRY="US"*
- *export KEY_PROVINCE="NY"*
- *export KEY_CITY="New York City"*

- *export KEY_ORG="DigitalOcean"*
- *export KEY_EMAIL="admin@example.com"*
- *export KEY_OU="Community"*
- *export KEY_NAME="server"*

4. Створення центра сертифікації

Перебуваючи в директорії *~/openvpn-ca*, треба виконати команду для завантаження змінних:

source vars

Після цього процес створення ключа та сертифіката ЦС буде готовий до запуску. Таким чином, у вас з'явиться центр сертифікації, з якого можна буде видавати серверні та клієнтські сертифікати.

5. Генерація серверних сертифікатів, ключів і додаткових файлів

Треба виконати наступну команду для створення сертифіката та ключів для серверу:

./build-key-server server

Під час виконання процедури треба натиснути ENTER для прийняття значень за замовчуванням і, в кінці процесу, ввести *y* для підтвердження підпису сертифіката. Далі треба згенерувати ключі протоколу Діффі-Хеллмана:

./build-dh

І, нарешті, треба ствроити HMAC-підпис для підвищення безпеки, використовуючи команду:

openvpn --genkey --secret keys/ta.key

6. Створення клієнтських сертифікатів і пар ключів

Треба згенерувати сертифікат і пару ключів для клієнта. Для клієнта з іменем *client1*:

source vars

./build-key client1

Під час процесу треба ввести значення за замовчуванням, натискаючи ENTER.

7. Налаштування сервісу OpenVPN

Треба скопіювати всі згенеровані файли з директорії *~/openvpn-ca/keys* до директорії */etc/openvpn*:

cd ~/openvpn-ca/keys

sudo cp ca.crt ca.key server.crt server.key ta.key dh2048.pem /etc/openvpn

Далі треба скопіювати з прикладів базовий конфігураційний файл сервера:

gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz

| sudo tee /etc/openvpn/server.conf

8. Редагування конфігураційного файлу OpenVPN

Треба відкрити файл */etc/openvpn/server.conf:*

sudo nano /etc/openvpn/server.conf

Треба внести наступні налаштування:

- розкоментувати директиву *tls-auth* і додайте параметр *key-direction 0*:

  tls-auth ta.key 0

  key-direction 0

- в розділі, що відповідає за шифрування, розкоментувати рядок з *cipher AES-128-CBC* та додати рядок з *auth SHA256*:

  cipher AES-128-CBC

  auth SHA256

9. Налаштування мережевої конфігурації сервера

Щоб сервер міг коректно перенаправляти трафік, треба увімкнути IP-пересилання. Треба відкрити файл */etc/sysctl.conf*:

sudo nano /etc/sysctl.conf

Треба знайти та розкоментувати рядок:

net.ipv4.ip_forward=1

Після внесення змін треба застосувати їх командою:

sudo sysctl -p

10. Налаштування фаєрволу UFW для VPN

Треба визначити публічний мережевий інтерфейс команди:

ip route | grep default

Інтерфейс називається enp0s3. Треба відкрити файл */etc/ufw/before.rules:*

sudo nano /etc/ufw/before.rules

Треба додати на початок файлу відповідні правила для ланцюжка POSTROUTING у таблиці nat для приховування трафіку VPN (рис. 1.22).

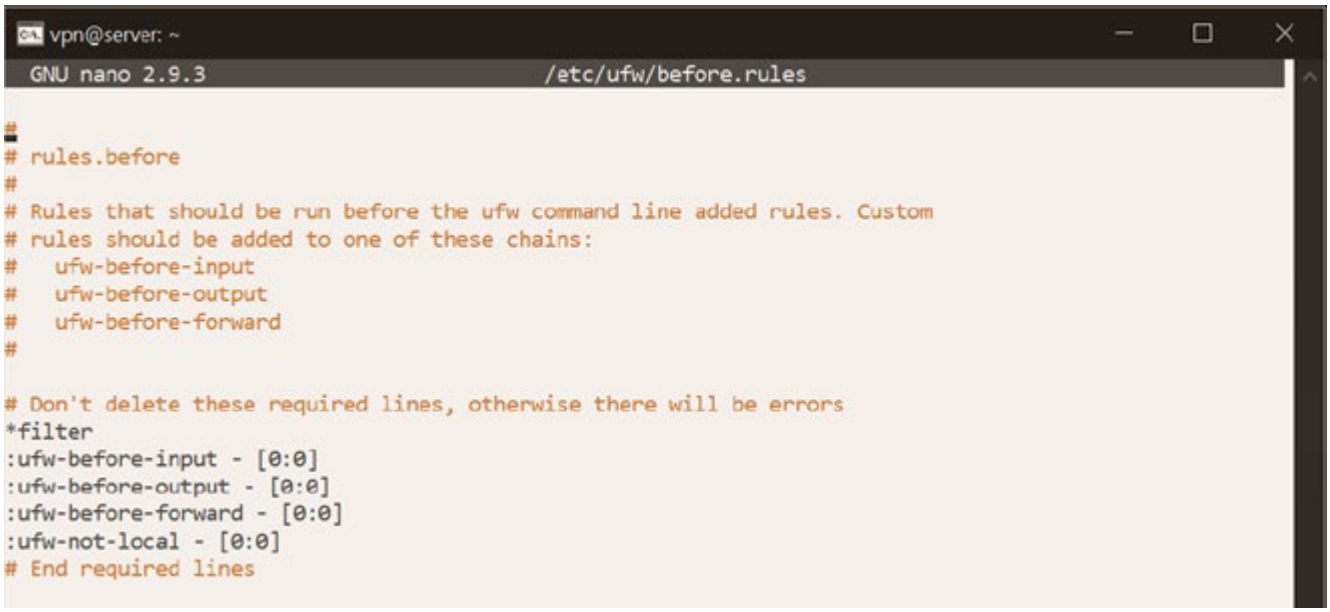


Рисунок 1.22. Налаштування правил для приховування трафіку VPN

Далі треба відкрити файл */etc/default/ufw* і змінити директиву DEFAULT_FORWARD_POLICY на ACCEPT:

sudo nano /etc/default/ufw

DEFAULT_FORWARD_POLICY="ACCEPT"

Необхідно дозволити прямий вхід для порту OpenVPN:

sudo ufw allow 1194/udp

sudo ufw allow OpenSSH

Треба перезавантажити UFW:

sudo ufw disable

sudo ufw enable

11. Запуск та перевірка роботи OpenVPN-сервера

Треба запустити OpenVPN-сервіс за допомогою *systemd*, вказавши ім’я файлу конфігурації (рис.1.23):

sudo systemctl start openvpn@server

sudo systemctl status openvpn@server

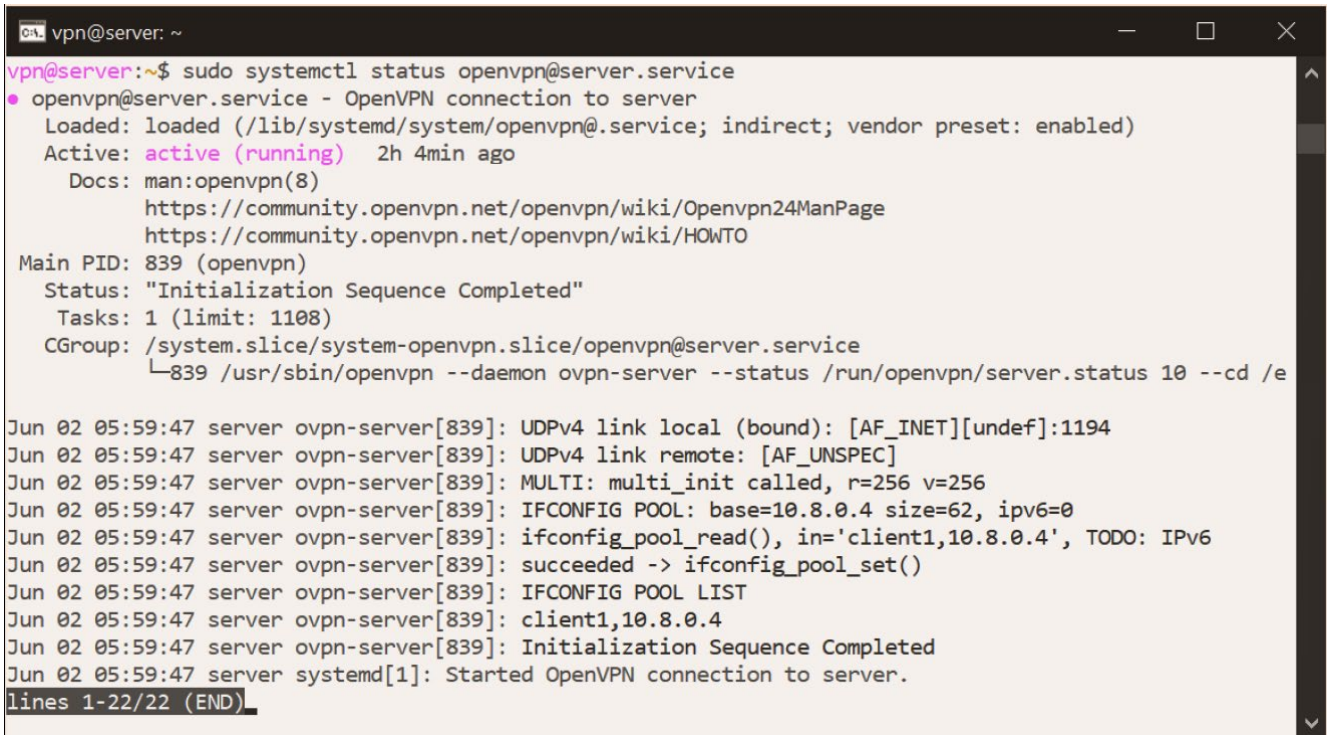


Рисунок 1.23. Перевірка статусу OpenVPN-сервера у терміналі

Треба переконатися, що інтерфейс *tun0* створений (рис.1.24):

ip addr show tun0

Рисунок 1.24. Стан інтерфейсу tun0 OpenVPN-сервера у терміналі

Далі необхідно налаштувати автоматичний запуск сервісу при завантаженні системи:

sudo systemctl enable openvpn@server

12. Створення конфігураційних файлів клієнта та встановлення з'єднання

Використовуючи приклад базової конфігурації, треба створити файл

конфігурації для клієнта, додавши в нього сертифікати ЦС, серверу та клієнта (рис.1.24).

```
client
dev tun
proto udp
remote 192.168.56.1 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher BF-CBC
auth SHA256
key-direction 1
verb 3
```

Рисунок 1.24. Конфігураційний файл для клієнта OpenVPN

Далі необхідно конфігурувати клієнтську машину (Windows 11) шляхом імпорту підготовленого файлу конфігурації. Після цього треба встановити з'єднання з VPN-сервером і перевірити нормальну роботу тунелю.

1.7.2 Аналіз впливу шифрування на канал VoIP-зв'язку у технології OpenVPN

Для оцінки впливу шифрування на продуктивність VoIP-каналу в рамках OpenVPN було проведено низку тестів у віртуальному середовищі VirtualBox, яке відтворює мережеву конфігурацію діапазону 192.168.56.0/24. У цьому середовищі, де один комп'ютер із Ubuntu виступає в ролі VPN-сервера, а хостовий пристрій – як клієнт, використовувалося програмне забезпечення Iperf для генерації трафіку та вимірювання параметрів зв'язку. Схема підключення (рис. 1.25) ілюструє топологію мережі, що використовується для тестування.

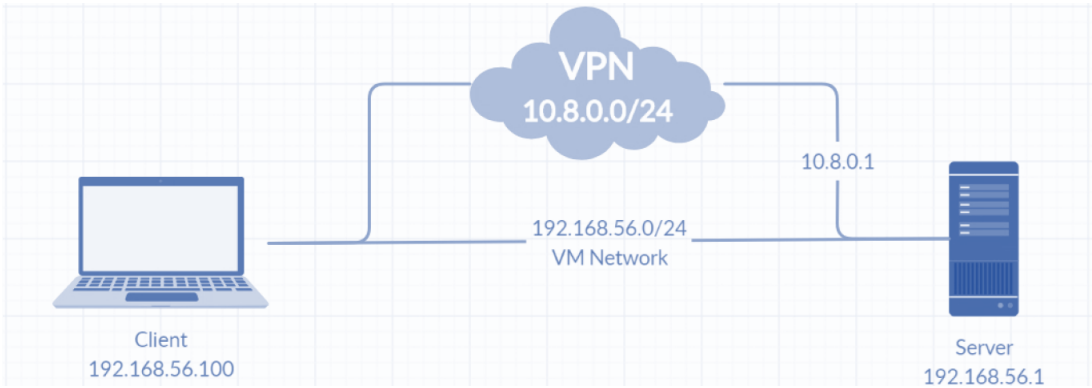


Рисунок 1.25. Топологія мережі при тестуванні каналу VoIP-зв'язку з OpenVPN

Першим етапом було виконано тестування без використання VPN-тунелю. За результатами тесту середня пропускна здатність складала 4.38 Гбіт/с, а середня затримка – 0.5 мс (рис. 1.26). Цей тест встановлює базовий показник ефективності мережевого каналу для VoIP-зв'язку у відсутності додаткових навантажень, пов'язаних із шифруванням.

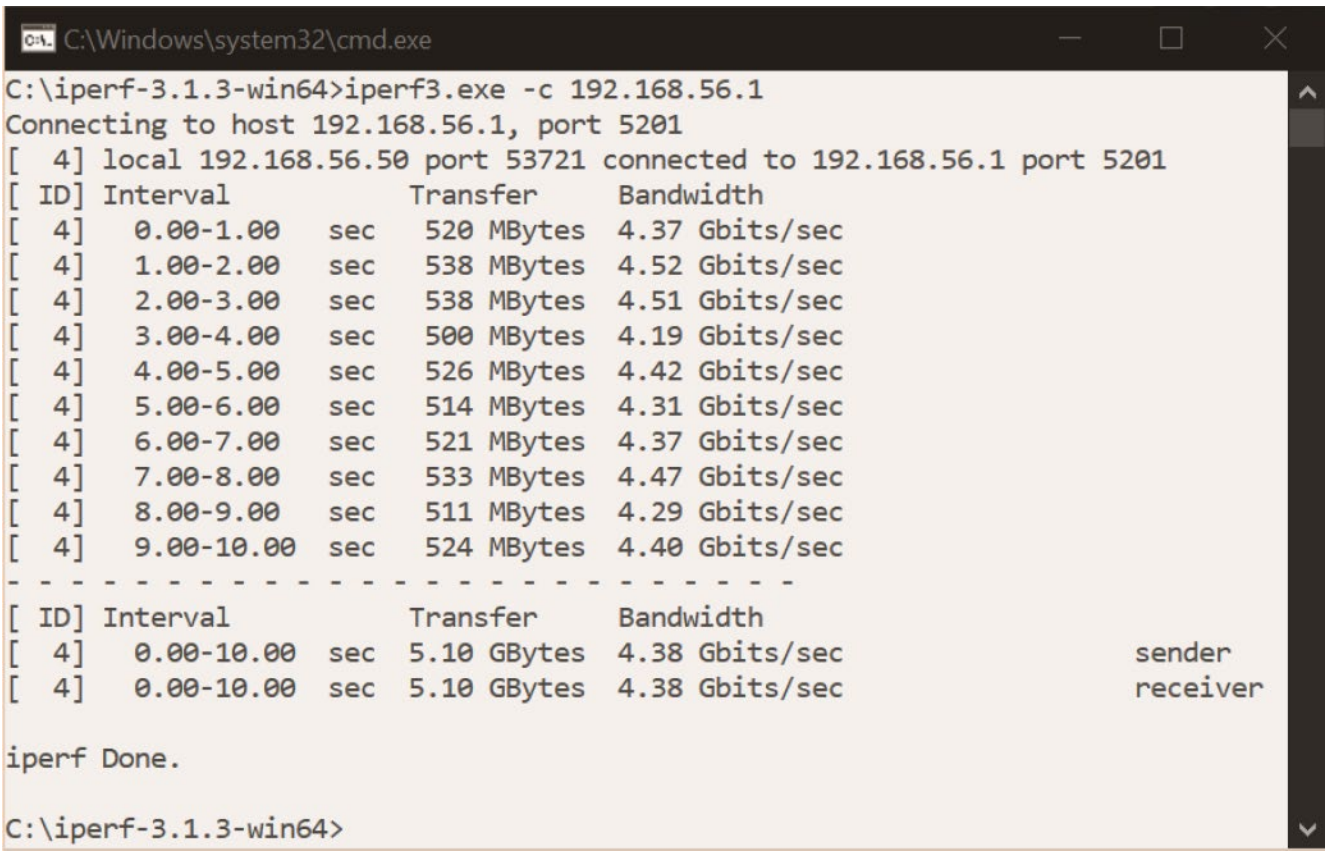
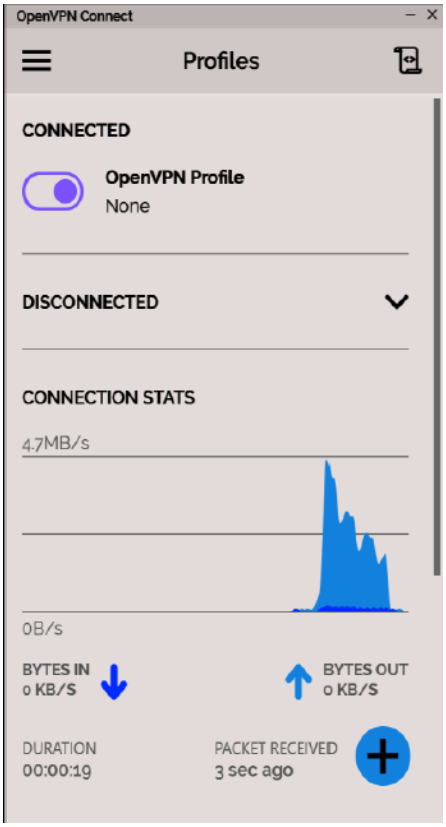


Рисунок 1.26. Тестування пропускної здатності VoIP-зв'язку без VPN (VM)

Наступним кроком було створення VPN-тунелю без застосування шифрування. Результати цього тесту показали зниження пропускної здатності до 231 Мбіт/с із зростанням затримки до 3 мс (рис. 1.27). Такий результат свідчить, що навіть базове тунелювання викликає падіння продуктивності через додаткову обробку даних. Подальше тестування було спрямоване на вивчення впливу різних алгоритмів шифрування. При використанні алгоритму DES-EDE пропускна здатність знизилася до 217 Мбіт/с, а середня затримка зросла до 3.2 мс (рис. 1.28). При застосуванні алгоритму BF-CBC спостерігалося ще більше зниження продуктивності – пропускна здатність упала до 210 Мбіт/с, а затримка приблизно досягла 3.5 мс (рис. 1.29).



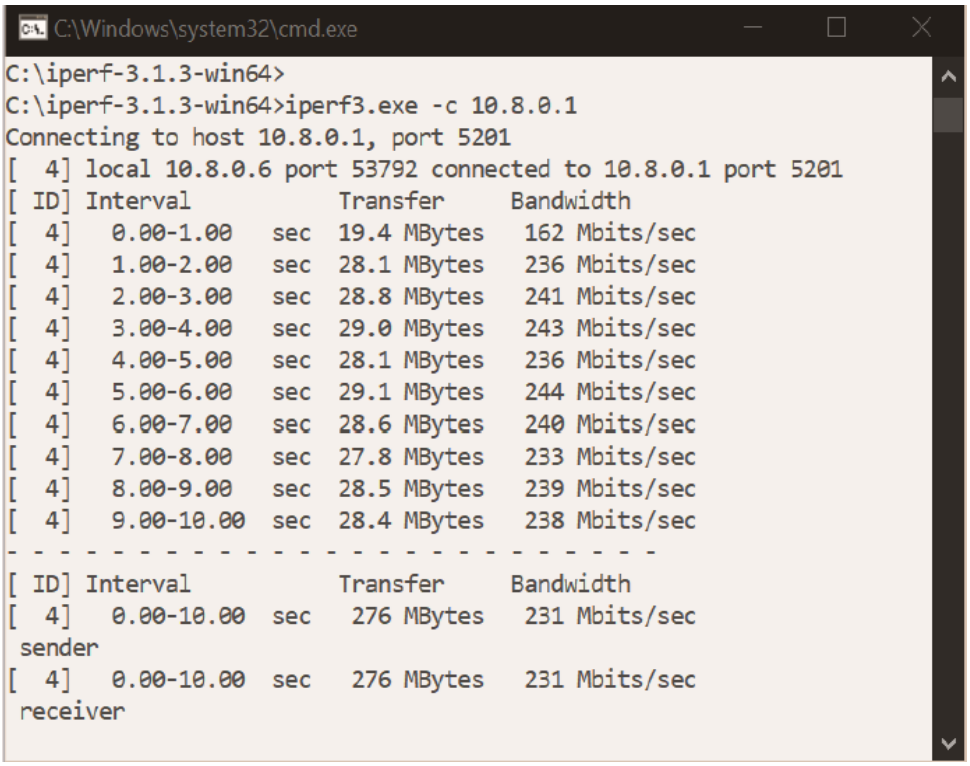
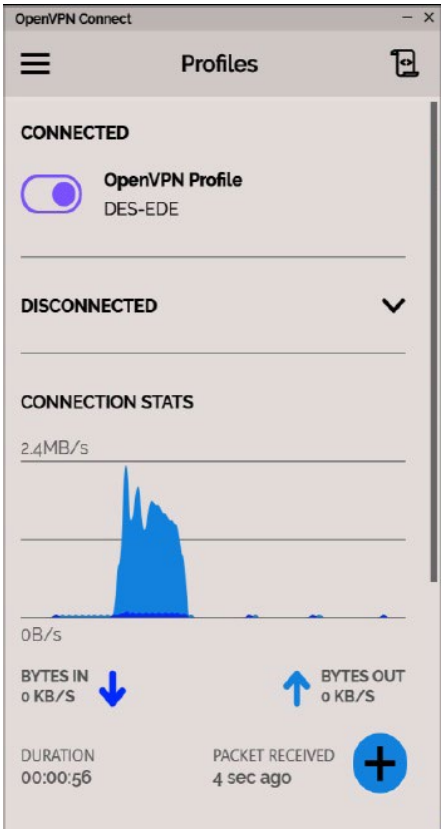


Рисунок 1.27. Тестування пропускної здатності VoIP-зв'язку з OpenVPN (без застосування шифрування)

Нарешті, найсучасніший і найбільш надійний алгоритм AES-256 забезпечував пропускну здатність близько 207 Мбіт/с із середньою затримкою 4 мс (рис. 1.30). Нижче наведено узагальнену таблицю з результатами тестів:



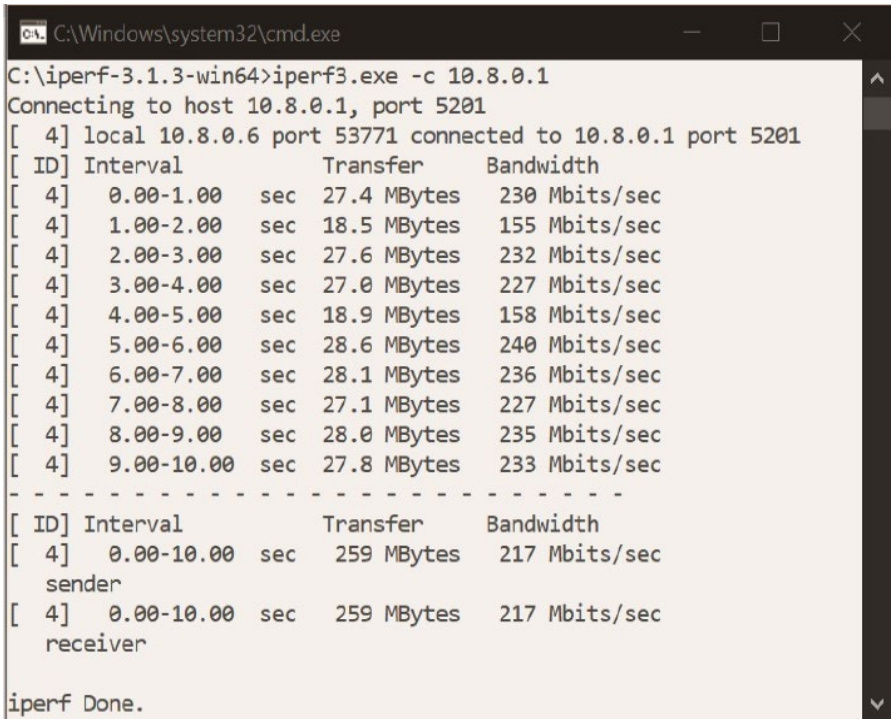
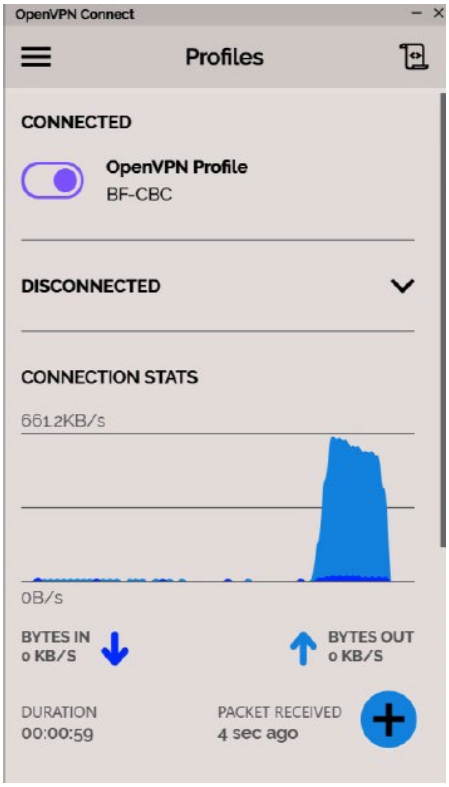


Рисунок 1.28. Тестування пропускної здатності VoIP-зв’язку з OpenVPN (з застосуванням шифрування за алгоритмом DES-EDE)

Проведені експерименти показали, що застосування шифрування не суттєво впливає на основні характеристики каналу VoIP-зв’язку. Чим сильніший алгоритм шифрування, тим нижчою є пропускна здатність та вищою – затримка.



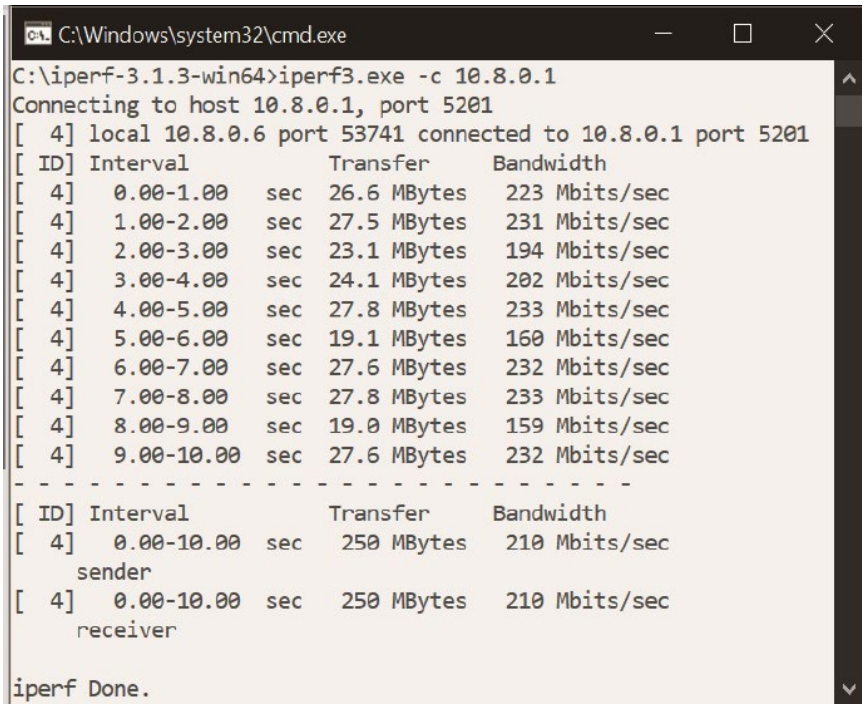
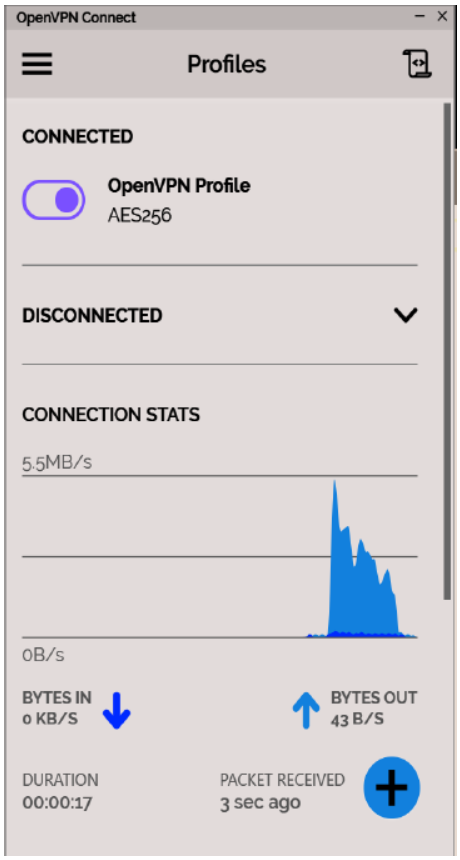


Рисунок 1.29. Тестування пропускної здатності VoIP-зв’язку з OpenVPN (з застосуванням шифрування за алгоритмом BF-CBC)

Проте, з точки зору безпеки, наприклад, шифрування AES-256 забезпечує надійний захист конфіденційних даних, що є критично важливим для захищеного VoIP-зв’язку. Результати тестів демонструють прийнятний компроміс між рівнем безпеки та продуктивністю: з використанням AES-256 спостерігається неістотне

зниження пропускної здатності до 207 Мбіт/с (порівняно з 213 Мбіт/с у базовому режимі), забезпечується сервіс високої надійності, що може задовольнити вимоги більшості корпоративних VoIP-систем.



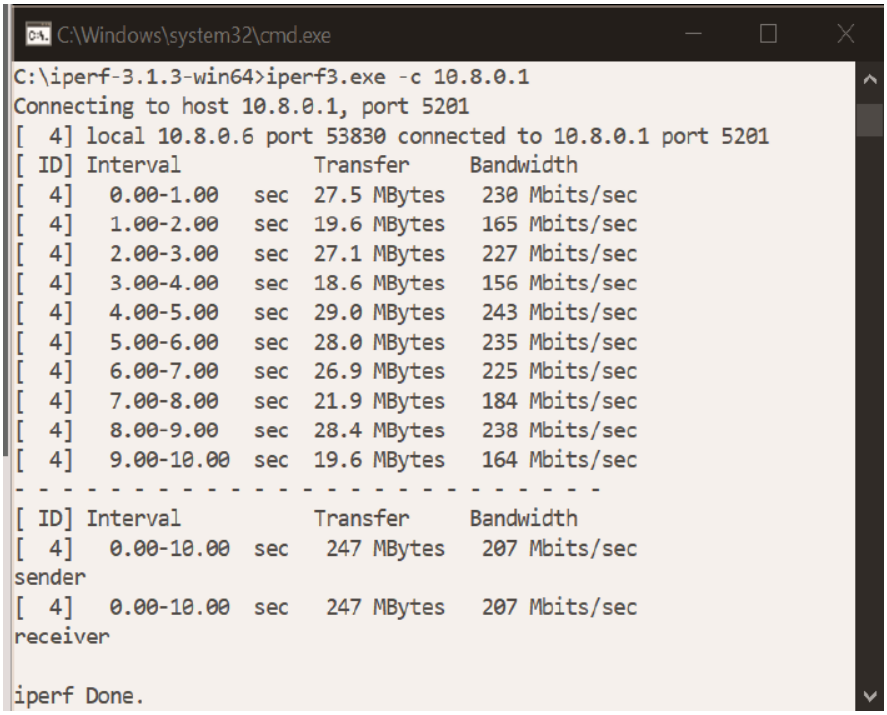


Рисунок 1.30. Тестування пропускної здатності VoIP-зв'язку з OpenVPN (з застосуванням шифрування за алгоритмом AES-256)

Таблиця 1.6. Результати тестування впливу шифрування на продуктивність VoIP каналу у режимі OpenVPN

Режим OpenVPN	*Пропускна здатність (Мбіт/с)*	*Середня затримка (мс)*
Без VPN-тунелю	4380	0.5
VPN-тунель без шифрування	213	3
VPN-тунель з шифруванням DES-EDE	217	3.2
VPN-тунель з шифруванням BF-CBC	210	3.5
VPN-тунель з шифруванням AES-256	207	4

Подальші дослідження можна спрямувати на оптимізацію налаштувань протоколу OpenVPN для зниження негативного впливу шифрування на швидкість передачі даних при збереженні високого рівня безпеки, а також на інтеграцію з мережевими засобами захисту для забезпечення адаптивної роботи мережі в умовах змінної навантаженості та мережевих аномалій. Проведений аналіз демонструє, що вплив шифрування на VoIP-зв'язок у технології OpenVPN проявляється у несуттєвому зниженні пропускної здатності та незначному зростанні затримки. При цьому рівень безпеки, досягнутий за допомогою сучасних криптографічних алгоритмів, виправдовує компроміс із показниками продуктивності «на практиці», оскільки забезпечує високий рівень захисту від несанкціонованого доступу до конфіденційних даних.

1.8 Аналіз надійності шифрування VoIP-зв'язку

У сучасних VoIP-системах питання захисту переданих голосових даних є надзвичайно актуальним, оскільки вони проходять через загальнодоступні мережі та можуть стати об'єктом атак. Надійність шифрування VoIP-трафіку безпосередньо впливає на конфіденційність, цілісність і доступність даних. В цьому розділі буде проведено аналіз стійкості різних криптографічних методів, що використовуються для захисту VoIP-зв'язку, зокрема тунельних протоколів і шифрувальних алгоритмів.

Одним із традиційних методів створення захищеного каналу є тунелювання

з використанням протоколів, таких як PPTP (Point-to-Point Tunneling Protocol), який реалізує шифрування Point-to-Point Encryption (PPE) на основі алгоритму RC4. RC4 є потоковим алгоритмом шифрування, що працює за принципом використання одного симетричного ключа для шифрування та розшифрування даних. Такий підхід дозволяє обробляти текстові дані побітово, поєднуючи кожен біт відкритого тексту з відповідним бітом ключа XOR-операцією. Однак, незважаючи на високу швидкість RC4, його вразливість до атак на повторювані ключі та прогнозовану генерацію потоків робить його ненадійним для використання у сучасних VoIP-системах.

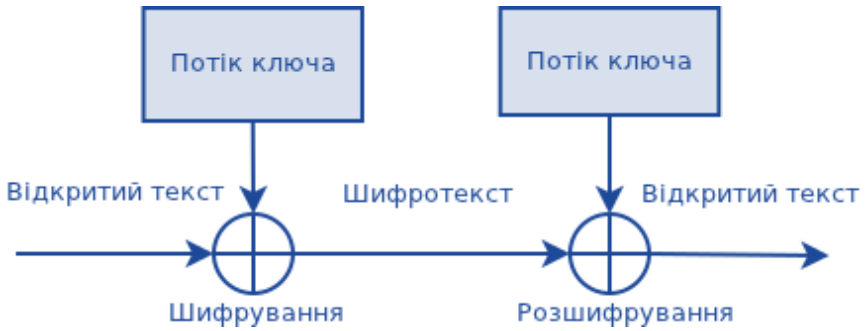


Рисунок 1.31. Структура потокового шифрування-дешифрування RC4

У сучасних рішеннях з шифрування голосового трафіку широко застосовуються алгоритми AES (Advanced Encryption Standard), Blowfish та Camellia, які забезпечують високий рівень безпеки за рахунок стійкості до криптоаналізу та складності розрахунків для зламування ключів. Проте більш потужне шифрування вимагає додаткових обчислювальних ресурсів, що може впливати на затримку передачі даних та пропускну здатність каналу зв'язку.

У рамках аналізу буде проведено порівняння криптографічних алгоритмів, що використовуються в OpenVPN та інших VPN-рішеннях для VoIP, а також оцінка їхньої ефективності в реальних умовах експлуатації. Буде розглянуто вплив довжини ключа (від 32 до 256 біт) на стійкість шифрування, а також проведено експериментальне дослідження продуктивності роботи голосового трафіку при використанні різних методів захисту. Узагальнені результати тестування дозволять визначити оптимальне рішення для забезпечення балансу між рівнем безпеки та ефективністю передачі голосових пакетів.

1.8.1 Підготовка схеми перехоплення та аналізу VoIP-трафіку

Для проведення аналізу надійності шифрування VoIP-зв'язку надзвичайно важливо організувати ефективну схему перехоплення трафіку, що дасть можливість дослідити, наскільки стійко захищені дані під час їх передачі через VPN-канали. У процесі технічного аудиту віртуальних приватних з'єднань фахівці використовують широкий спектр методів – від методів соціальної інженерії та пасивного прослуховування до активних кібератак різного типу. Одним із найбільш диференційованих підходів є атака «людина посередині» (MITM), коли зловмисник, виступаючи в якості проміжного ланцюжка, перехоплює мережевий трафік без відомості цільового користувача.

Рисунок 1.32. Схема атаки MITM з перехопленням та аналізом VoIP-трафіку

На рис.1.32 показано схему, за якою зловмисник знаходиться посередині зв'язку, що дозволяє перехопити, змінити чи перенаправити мережевий трафік. При такому підході перехоплення починається зі збору даних – зазвичай це дамп пам'яті маршрутизатора або комп'ютера, який оформлюється у форматі, наприклад, PCAPNG. Цей файл містить дані у шістнадцятковому вигляді та створюється за допомогою мережевого аналізатора, наприклад, Wireshark. Файл дозволяє майбутньому криптоаналітику ретельно вивчити вміст трафіку та спробувати витягти чи змінити критично важливу інформацію.

Особливим випадком є перехоплення трафіку, що передається через VPN-канал. У такому випадку дамп, отриманий за допомогою Wireshark, зашифрований алгоритмом, зазначеним у налаштуваннях VPN-серверу. У

досліджуваному сценарії аналізу надійності шифрування було отримано сім файлів, що містять однаковий мережевий трафік, але зашифровані різними ключами – з довжинами 32, 40, 56, 64, 72, 128 та 256 біт – при використанні алгоритму RC4 (Rivest cipher 4). Такий підхід дозволяє порівняти ефективність криптографічного захисту залежно від сили ключа, що є важливим для визначення оптимальної конфігурації безпечного з'єднання. БСА перевірки та блокування небажаних IP-адрес наведено на рис.1.33.

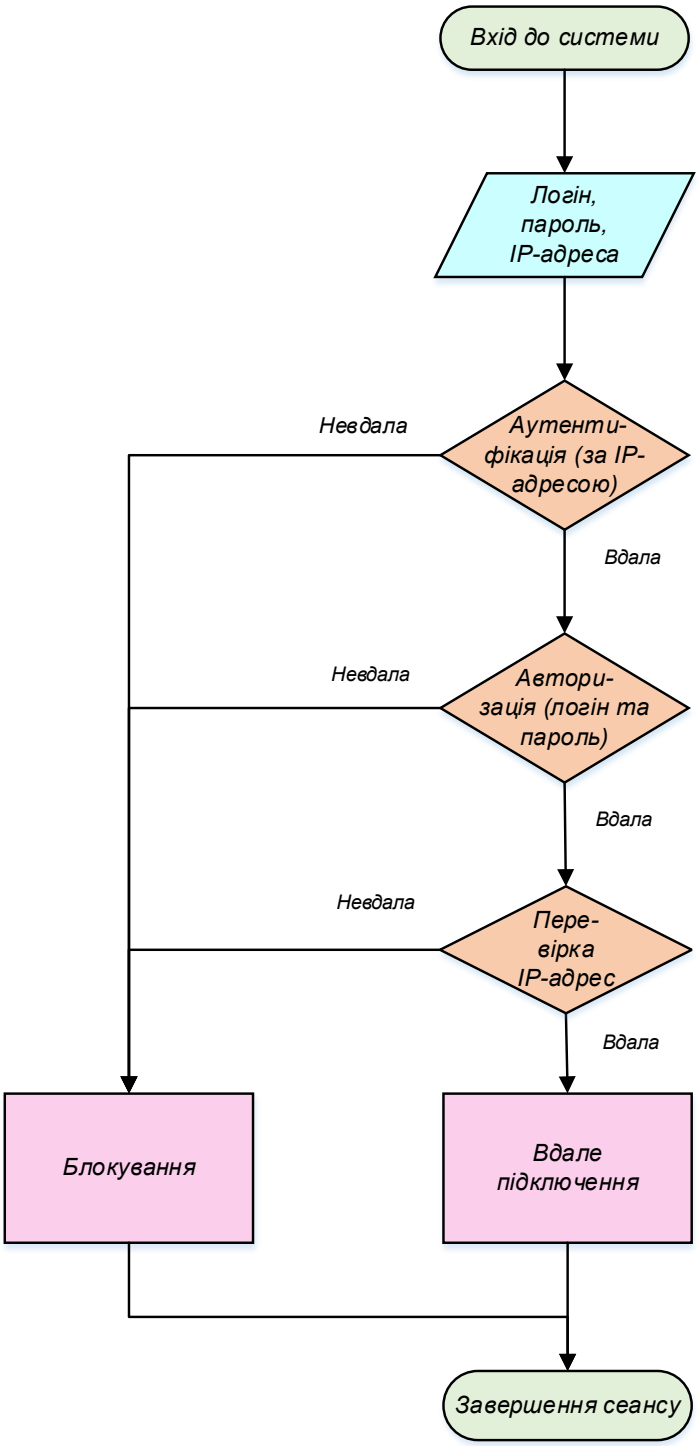


Рисунок 1.33. БСА перевірки та блокування небажаних IP-адрес

Програмну реалізацію конфігурації (dialplan) для Asterisk, який здійснює перевірку параметрів шифрування вхідного VoIP-з'єднання, наведено у Додатку А. Код перевіряє, чи вказано у SIP-заголовках належний статус використання VPN-шифрування, чи правильно задано алгоритм шифрування та чи відповідає довжина криптографічного ключа мінімальним вимогам. У випадку, якщо параметри не відповідають вимогам, виконується блокування дзвінка.

1.8.2 Підготовка програмно-апаратного забезпечення для проведення аналізу надійності шифрування VoIP-зв'язку

Для проведення комплексного експериментального аналізу впливу шифрування на VoIP-зв'язок необхідно створити сучасну програмно-апаратну платформу, яка забезпечує високий рівень обчислювальної потужності та гнучкість налаштувань. У дослідженні використано хмарний сервіс Caspio (PaaS Provider) для розгортання віртуального середовища, на базі якого експерименти проводяться з використанням операційної системи Kali Linux – дистрибутиву, оптимізованого для цифрової криміналістики та тестування проникнення. Для максимізації обчислювальної ефективності роботи алгоритмів підбору ключів, таких як прямий перебір із застосуванням програми ARCFOURdecrypt, обрано найсучасніше апаратне забезпечення:

- Процесор (CPU): Intel Core i9-14900K. Цей високопродуктивний процесор забезпечує високу багатопоточну продуктивність, що є критичним при виконанні прямого перебору шифрувальних ключів;

- Графічний процесор (GPU): NVIDIA GeForce RTX 4090. Завдяки підтримці технологій NVIDIA CUDA та оптимізованим алгоритмам обчислень, цей GPU значно пришвидшує операції з перебору ключів, що виконуються як у режимі прямого перебирання, так і за допомогою райдужних таблиць.

Програмне забезпечення дослідження включає два основних підходи до підбору ключа шифрування алгоритму RC4:

1. ARCFOURdecrypt: Цей інструмент виконує перебір ключів прямим методом із розподілом обчислювального навантаження між CPU та GPU. Завдяки використанню графічного процесора, обчислення проводяться набагато швидше,

що дозволяє точно визначити залежність часу підбору ключа від його довжини;

2. Rainbowcrpt: Програма, що реалізує підбір ключа за допомогою попередньо згенерованих райдужних таблиць. Використання цього методу дозволяє скоротити час пошуку з ймовірністю успіху від 85% до 99%, що дає можливість провести контрольований аналіз ефективності алгоритмічних методів перебору.

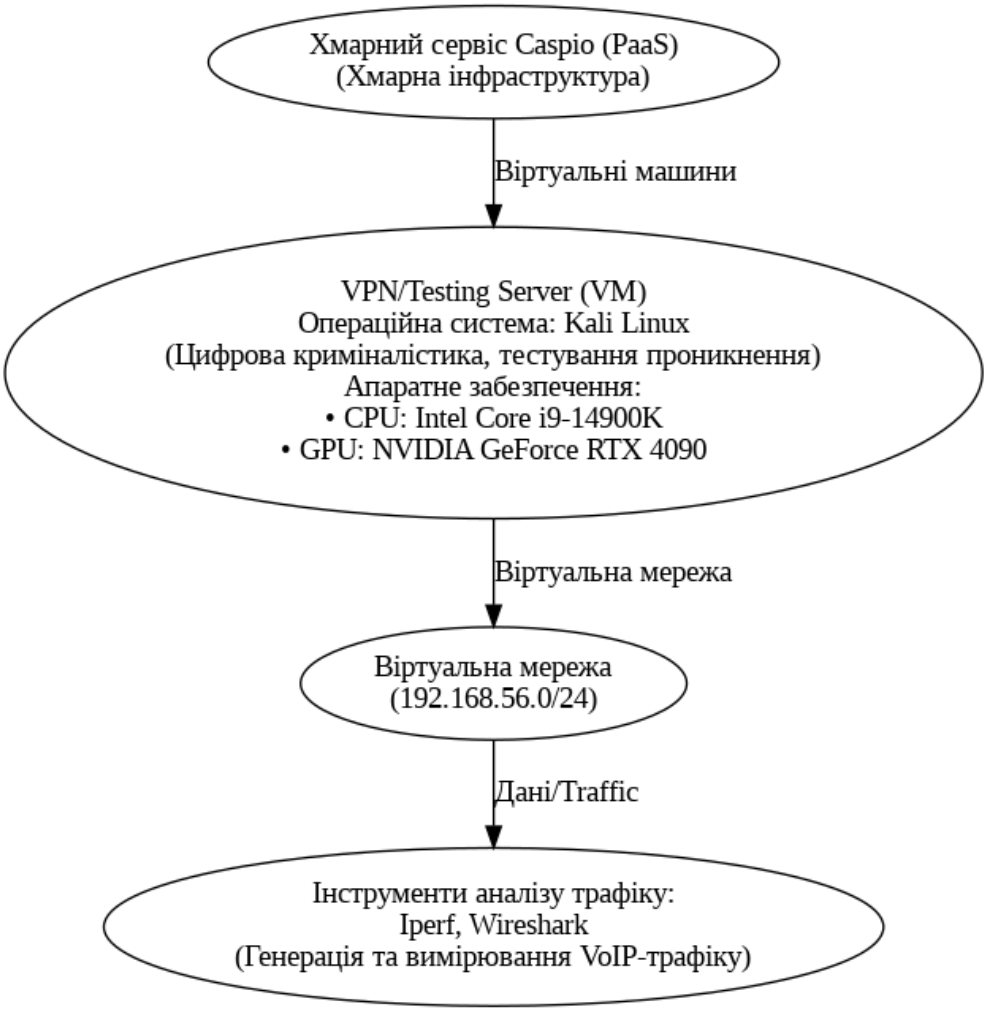


Рисунок 1.34. Схема середовища тестування на базі Caspio та Kali Linux

На рис. 1.34 показано топологію віртуальних машин, запущених на хмарному сервісі Caspio, де сервер із Kali Linux оснащено Intel Core i9-14900K і NVIDIA GeForce RTX 4090 для проведення обчислювальних експериментів.

Підготовка програмного забезпечення включає встановлення та налаштування драйверів GPU, зокрема NVIDIA CUDA Toolkit, що забезпечує підтримку сучасних обчислювальних модулів для графічного процесора. Встановлено також всі необхідні бібліотеки, зокрема OpenSSL, для роботи

криптографічних алгоритмів. Завдяки цьому, експерименти можна проводити на оптимізованій платформі з високою відтворюваністю результатів.

Налаштування системи було здійснено таким чином, щоб результати тестування (які включатимуть вимірювання часу підбору ключа шифрування RC4 при використанні ключів довжиною 32, 40, 56, 64, 72, 128 та 256 біт) були максимальними точними. Обрана обчислювальна платформа дозволяє не лише ефективно вимірювати час підбору, але і визначати вплив параметрів шифрування на загальну продуктивність VoIP-зв'язку у захищеній мережевій інфраструктурі.

1.8.3 Отримання результатів аналізу надійності шифрування VoIP

У цьому підрозділі проведено експериментальний аналіз залежності часу підбору ключа шифрування RC4 від довжини ключа за допомогою двох методів: прямого перебору та підбору за допомогою райдужних таблиць. Для прямого перебору виконувалося два раунди підбору ключів: перший – за допомогою обчислень на центральному процесорі (CPU) Intel Core i9-14900K, а другий – із використанням графічного процесора (GPU) NVIDIA GeForce RTX 4090. Методи перебору із застосуванням райдужних таблиць (Rainbowcrpt) проводилися у двох раундах, обидва на процесорі, оскільки цей метод базується на попередньо згенерованих даних і виконується виключно через CPU.

Таблиця 1.7. Підбір ключа шифрування за методом прямого перебору

Розрядність ключу	*Перший раунд (на CPU Intel Core i9-14900K), годин*	*Другий раунд (на GPU NVIDIA RTX 4090), годин*	*Усереднений час підбору, годин*
256 біт	–	–	–
128 біт	13,68	6,91	10,30
72 біт	6,76	3,40	5,08
64 біт	4,56	2,12	3,34
56 біт	2,26	1,04	1,65
40 біт	1,12	0,39	0,76
32 біт	0,74	0,19	0,47

Експерименти виконувалися у віртуальному середовищі, розгорнутому на хмарній інфраструктурі Caspio із використанням операційної системи Kali Linux, придатної для тестування проникнення та цифрової криміналістики. Як інструмент

вимірювання трафіку застосовували Iperf, а отримані результати були зібрані та проаналізовані для кожного методу перебору ключа.

Результати для методу прямого перебору наведено у таблиці 1.7. За рахунок сучасного апаратного забезпечення час підбору з використанням CPU значно скоротився порівняно з попередніми експериментами на старішому обладнанні, а застосування потужного GPU додатково пришвидшило цю операцію.

Як видно з таблиці, збільшення довжини ключа призводить до пропорційного збільшення часу підбору – наприклад, перебір 128-бітового ключа у середньому займає приблизно 10,3 годин, у той час як для 32-бітового ключа середній час знижується до 0,47 години. Результати для методу підбору за допомогою райдужних таблиць наведено у таблиці 1.8. Оскільки цей метод працює виключно на CPU, для обох раундів використовувалася потужність Intel Core i9-14900K. Оскільки метод не гарантує 100% відтворюваність результатів, деякі дані для деяких розрядностей відсутні, але за наявних даних видно, що також існує пряма залежність часу підбору від довжини ключа.

Таблиця 1.8. Підбір ключа шифрування за допомогою райдужних таблиць

Розрядність ключу	*Перший раунд (на CPU Intel Core i9-14900K), годин*	*Другий раунд (на CPU Intel Core i9-14900K), годин*	*Усереднений час підбору, годин*
256 біт	15,82	16,46	16,14
128 біт	11,64	–	11,64
72 біт	5,72	5,96	5,84
64 біт	3,76	3,90	3,83
56 біт	–	1,88	1,88
40 біт	0,94	0,76	0,85
32 біт	0,086	0,19	0,14

Як показує аналіз даних, є чітка пряма залежність – з підвищенням розрядності ключа зростає час, необхідний для його перебору. Наприклад, для райдужних таблиць 128-бітовий ключ підбирається за 11,64 години, а для 32-бітового – лише за 0,14 години. Ці дані демонструють, що крипто-аналітику знадобиться значно більше часу для перебору довгих ключів; це є одним із

аргументів на користь використання максимально довгих ключів для забезпечення високої безпеки VoIP-зв’язку, що передається через VPN-канали.

На рис. 1.35 наведено графік, який демонструє залежність цінності інформації від часу. Графік показує, що чим довше триває процес підбору ключа, тим меншу практичну цінність матиме перехоплена інформація – для криптоаналітика ефективність атаки зменшується з часом, оскільки інформація дедалі втратить свою актуальність. Зростання часу перебору ключа знижує економічну і стратегічну цінність інформації, що може бути отримана у випадку успішного перехоплення.

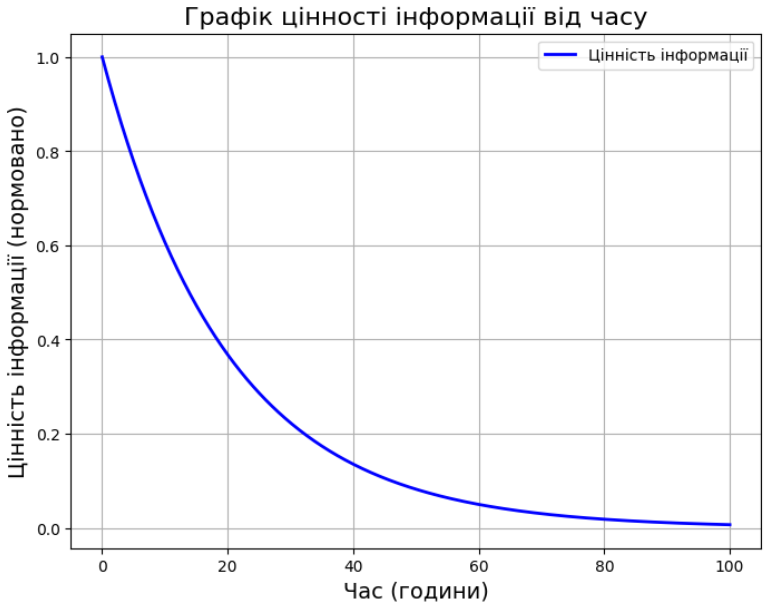


Рисунок 1.35. Залежність цінності інформації з VoIP-пакетів від часу

Проведений аналіз підкріплює висновок, що збільшення довжини ключа шифрування значно підвищує стійкість системи, хоча й впливає на продуктивність каналу VoIP. Результати експериментів свідчать про те, що для забезпечення максимальної надійності передачі даних через VPN-канали необхідно використовувати ключі максимальної довжини, які при цьому підтримують усі пристрої мережі. Отже, баланс між продуктивністю та високим рівнем безпеки є критичним, особливо враховуючи, що для криптоаналітика інформація стає менш цінною з кожною годиною затримки при підборі шифрувального ключа.

2 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Відповідно до Конституції України, громадянам забезпечується рівноправність у області праці, незалежно від національності і раси.

Умови праці впливають на здоров'я, працездатність і всебічний розвиток особи трудящого. Узагальнюючи приведені вище положення, можна зробити висновок, що чим вища культура виробництва, тим краще умови праці, а отже, забезпечуються здоров'я і безпека працівників.

Робоче місце користувача послуг захисту VoIP-зв’язку за допомогою віртуального тунелю складається з персонального комп’ютеру з програмним забезпеченням. Тому для нього застосовуються звичайні вимоги до організації робочого місця користувача персонального комп’ютеру.

2.1 Аналіз небезпечних і шкідливих факторів, що впливають на користувача ПК

До основних критеріїв забезпечення гігієни робочого середовища належать інтенсивність освітлення, температура повітря, вологість, рівень шумового забруднення, ступінь вібраційного впливу, токсичність, загазованість. Крім цього, враховується дія електростатичного поля та вплив як неіонізуючих, так і іонізуючих електромагнітних випромінювань.

2.2 Гігієнічні вимоги до виробничого середовища

Державні санітарні норми, зокрема ДСАНПіН 3.3.2.007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин», спрямовані на запобігання негативного впливу шкідливих чинників, що супроводжують роботу з візуальними дисплейними терміналами, на здоров’я працівників.

2.2.1 Вимоги до приміщення

Розміщення робочих місць із використанням ВДТ, ЕОМ і ПЕОМ заборонено у підвальних приміщеннях та на цокольних поверхах. Для кімнат, призначених для роботи з візуальними дисплейними терміналами, рекомендується орієнтувати вікна

у напрямку півночі або північного сходу. На вікнах повинні бути встановлені регульовані жалюзі або штори, що дозволяють їх повністю закривати для забезпечення оптимальних умов освітлення.

Планувальні рішення будівель і приміщень, де розташовано відеодисплейні термінали, мають відповідати вимогам ДСАНПіН 3.3.2.007-98. Для робочого місця програміста передбачено мінімальну площу не менше 6 кв. м та об’єм приміщення не менше 20 куб. м. Крім того, стіни приміщень повинні бути пофарбовані матовою фарбою, а в приміщеннях з ВДТ обов’язково мають бути передбачені зони для відпочинку та психологічного розвантаження.

2.2.2 Освітлення

Для забезпечення належного освітлення приміщення, де працює програміст, застосовується комбінована система, що поєднує природне освітлення із додатковим штучним світлом. Загальне оздоблення простору виконується за допомогою газорозрядних ламп типу ЛД. Згідно з встановленими нормами, для робочого місця, на якому здійснюються високоточні операції (де мінімальний розмір об'єкта розрізнення становить 0,3–0,5 мм), необхідна освітленість рівномірно має досягати 300 лк. В цілому, ці вимоги щодо освітлення забезпечені.

2.2.3 Шум

У робочих приміщеннях основним джерелом шумового навантаження є звуки, що генеруються ПЕОМ. Крім того, значну частину шуму створюють джерела електромагнітного походження – це коливання компонентів електромеханічних пристроїв під впливом змінних магнітних полів. До того ж, в приміщеннях виникає структурний шум, який випромінюють поверхні конструктивних елементів (стіни, перекриття, перегородки) у звуковому спектрі частот. Для зниження або усунення негативного впливу шуму доцільно ізолювати робочі зони, розташовуючи їх у частинах будівлі, що знаходяться в глибині та ведуть своїми вікнами у двір – таким чином мінімізується вплив міського шуму. Крім цього, необхідно регулярно перевіряти герметичність корпусів комп’ютерної техніки та своєчасно здійснювати заміну вентиляторів охолодження.

2.3 Вимоги до організації робочого місця працівника

Конструкція робочого місця користувача комп'ютера, з урахуванням розташування сидіння, засобів керування та засобу відображення інформації, розроблена згідно з антропометричними, фізіологічними та психологічними вимогами, а також відповідно до специфіки виконуваної роботи. Робоче меблеве обладнання повинно бути оснащене можливістю індивідуального регулювання, що дозволить адаптувати його під зріст кожного користувача й підтримувати оптимальну, зручну поставу. Робочий стіл рекомендовано обробляти матовим покриттям, що сприяє зменшенню небажаних відблисків. > > Розміщення дисплея організовано таким чином, щоб його верхня межа відповідала рівню очей, а відстань до екрану становила приблизно 70 см – що повністю входить у допустимий інтервал від 60 до 90 см. Частота мерехтіння екрану fмер дорівнює 100 Гц, що значно перевищує мінімальне рекомендоване значення у 70 Гц.

2.4 Мікроклімат

Показники мікроклімату, складу іонів у повітрі, а також рівень шкідливих речовин у робочих зонах, де використовуються ПК, мають відповідати вимогам ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».

Для підтримки нормативних значень мікроклімату та забезпечення оптимального співвідношення позитивних і негативних іонів слід передбачити установку пристроїв зволоження, штучної іонізації або кондиціювання повітря. Крім того, рівні інфрачервоного випромінювання не повинні перевищувати встановлених нормативних меж згідно з ГОСТ 12.1.005. Також вміст озону в робочій зоні не має перевищувати 0,1 мг/м³, оксидів азоту – 5 мг/м³, а концентрація пилу повинна залишатися в межах 4 мг/м³.

2.5 Електробезпека

Приміщення, де використовуються імпульсні джерела живлення згідно з ОНТП24-86 і ПУЕ-87, віднесено до категорії об'єктів, де ризик ураження персоналу електричним струмом не є підвищеним. Це пояснюється тим, що відносна вологість повітря не перевищує 75%, температура залишається нижчою

за 35°С, а хімічно агресивні середовища відсутні. Електроживлення обладнання організовано від двофазної мережі з заземленою нейтраллю, при напрузі 220 В і частоті 50 Гц, із застосуванням автоматичних пристроїв токового захисту.

В приміщенні обов'язково має бути встановлена схема заземлення. Ураження електричним струмом може виникнути у випадках: 1) при контакті з відкритими струмоведучими елементами; 2) при торканні неструмоведучих частин обладнання, які, через порушення ізоляції або інші причини, опинилися під напругою.

Відповідно до вимог ГОСТ-12.2.007.0-75 устаткування (за винятком ЕОМ II класу) відноситься до I класу та оснащене робочою ізоляцією згідно з ГОСТ 12.1.009-76. Підключення обладнання здійснено згідно з нормативами ПБЕ та ПУЕ, тому додаткових заходів щодо електробезпеки не вимагається.

2.6 Пожежна безпека

Основні принципи пожежної безпеки Пожежна безпека – це комплекс заходів, спрямованих на запобігання виникненню пожеж, мінімізацію їх наслідків та забезпечення безпечного евакуаційного процесу.

Фактори, що впливають на ризик виникнення пожежі:

- Несправність електромережі та електроприладів
- Використання горючих матеріалів
- Порушення правил зберігання легкозаймистих речовин.
- Недотримання інструкцій з пожежної безпеки.

Запобіжні заходи та система протипожежного захисту:

- Використання вогнестійких матеріалів у будівельних конструкціях.
- Регулярне технічне обслуговування електромережі та обладнання.
- Наявність засобів пожежогасіння: вогнегасники, системи автоматичного пожежогасіння.
- Розробка та дотримання плану евакуації у разі пожежі.
- Навчання персоналу правилам пожежної безпеки.

Робоче приміщення, що відповідає вимогам ПБЕ та ОНТП 24–86 у сфері вибухово-пожежної безпеки, класифікується як об’єкт категорії «В».

Відповідно до ПУЕ, для зниження ризику виникнення пожежі необхідно забезпечити комплекс заходів, зокрема: ретельну ізоляцію всіх струмоведучих проводів, що підключені до робочих місць, регулярний огляд та перевірку стану їх ізоляції, а також суворе дотримання норм безпечної експлуатації обладнання.

Для гасіння пожеж на робочому місці користувача ПК застосовують як вуглекислотні, так і порошкові вогнегасники.

– Вуглекислотні вогнегасники випускаються у варіанті ручних пристроїв (наприклад, ВВК-5);

– Порошкові вогнегасники представлені моделями ВП-2, ВП-5, ВП-10 та іншими

Рисунок 3.1. Засоби пожежогасіння ВП-5

З метою своєчасного оповіщення, на дільниці необхідно встановити протипожежну сигналізацію. Проходи та запасні виходи повинні бути вільними. Пожежний щит повинен розміщуватись в доступному місці та містити первинні засоби пожежогасіння (вогнегасник, лопату, відро, простирадло, ящик з піском)

ВИСНОВКИ

У результаті проведених досліджень встановлено, що застосування технологій захищених VPN-з'єднань, зокрема OpenVPN, дозволяє забезпечити високий рівень безпеки передачі VoIP-трафіку в умовах незахищених мереж. Експериментальна частина дипломної роботи довела, що інтеграція сучасних криптографічних алгоритмів, таких як AES-256, у поєднанні з належним тунелюванням гарантує конфіденційність, цілісність та автентичність голосових даних. Аналіз показав, що збільшення довжини ключа шифрування безпосередньо призводить до пропорційного зростання часу перебору ключа, що підтверджується як методом прямого перебору, так і підбором за допомогою райдужних таблиць. Водночас використання сучасного обладнання, зокрема процесора Intel Core i9-14900K та графічного процесора NVIDIA GeForce RTX 4090, дозволяє значно скоротити час виконання обчислювальних операцій, проте навіть у таких умовах підбір довгих ключів вимагає значних витрат часу, що робить атаки типу перебору майже неможливими з практичної точки зору.

Отримані результати демонструють, що компроміс між продуктивністю каналу та рівнем безпеки здатен забезпечити оптимальне функціонування системи VoIP-зв'язку, якщо використовувати максимально підтримувану довжину ключа шифрування. Експерименти з прямим перебором ключів і застосуванням райдужних таблиць виявили чітку залежність часу підбору від розрядності ключа, що надає можливість розробити рекомендації щодо оптимізації криптографічних налаштувань у корпоративних мережах. Аналіз графіка цінності інформації від часу також показує, що зростання часу підбору ключа суттєво знижує актуальність потенційно перехоплених даних, що є додатковим аргументом на користь застосування довгих ключів для підвищення стійкості системи до кібератак.

Проведене у кваліфікаційній роботі дослідження доводить, що інтеграція OpenVPN із сучасними криптографічними методами забезпечує ефективний захист VoIP-зв'язку, а також формує науково-практичну базу для подальшої оптимізації та масштабування систем безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Мельников В. Інформаційна безпека в Україні: сучасні виклики. – Київ: «Наукова думка», 2021.
2. Романюк О., Коваленко А. Кібербезпека в Україні: сучасний стан та перспективи розвитку. – Харків: «Фоліо», 2022.
3. Дягилев Л., Комаров М. Захист голосових комунікацій в IP-мережах. – Львів: «Видавництво Логос», 2021.
4. Петрова І., Савчук Г. Новітні технології безпеки в телекомунікаціях. – Одеса: «Одеська політехніка», 2020.
5. Добрянський В., Клименко Я. Віртуальні приватні мережі (VPN) та їх застосування у системах зв’язку. – Київ: Інститут інформаційних технологій, 2022.
6. Степаненко М. Теорія та практика захисту VoIP-зв’язку. – Харків: Харківський політехнічний інститут, 2021.
7. Заболотний Н., Куликова Л. Аналіз сучасних криптографічних алгоритмів для забезпечення інформаційної безпеки. – Київ: «Києво-Могилянська академія», 2022.
8. Мельничук І. Цифрова трансформація та кібербезпека: проблеми і рішення. – Київ: «Новий час», 2020.
9. Гордієнко О. Сучасні методи захисту інформації в цифровій епохі. – Дніпро: Дніпровський національний університет, 2021.
10. Коваль С. Безпека телекомунікаційних систем: теорія і практика. – Тернопіль: Тернопільський національний педагогічний університет, 2023.
11. OpenVPN Community Resources. OpenVPN Official Documentation, Інтернет-ресурс. Доступ: [https://openvpn.net/community-resources/how-to/]
12. Caspio Platform. Офіційний вебсайт Caspio, сервіс хмарних обчислень (PaaS). Доступ: [https://www.caspio.com/]
13. Microsoft PPTP Documentation. Технічна інформація щодо PPTP та алгоритму RC4 від компанії Microsoft. Доступ: [https://docs.microsoft.com/]

ДОДАТОК А. Програмна реалізація перевірки параметрів шифрування у VoIP-зв'язку (Asterisk)

```
exten => _X.,1,NoOp(Перевірка параметрів шифрування для дзвінка на розширення ${EXTEN})
 same => n,Set(ENCRYPT_STATUS=${SIP_HEADER(X-VPN-ENCRYPT)})
 same => n,Set(ENC_KEY=${SIP_HEADER(X-ENC-KEY)})
 same => n,Set(ENC_ALGO=${SIP_HEADER(X-ENC-ALGO)})
 same => n,Verbose(0,Статус шифрування: ${ENCRYPT_STATUS}, Ключ: ${ENC_KEY},
Алгоритм: ${ENC_ALGO})

 ; Перевірка, чи використовується VPN-шифрування (очікуємо, що заголовок X-VPN-ENCRYPT
дорівнює "YES")
 same => n,GotoIf($["${ENCRYPT_STATUS}" != "YES"]?unencrypted,1)

 ; Встановлюємо мінімально допустиму довжину ключа (наприклад, 128 біт)
 same => n,Set(MIN_KEY_LENGTH=128)
 same => n,Set(KEY_LENGTH=${LEN(${ENC_KEY})})
 same => n,Verbose(0,Довжина ключа шифрування: ${KEY_LENGTH})

 ; Якщо довжина ключа менша за мінімальну, блокувати дзвінок
 same => n,GotoIf($[${KEY_LENGTH} < ${MIN_KEY_LENGTH}]?badkey,1)

 ; Якщо параметри шифрування прийнятні, продовжити обробку дзвінка
 same => n,NoOp(Параметри шифрування відповідають вимогам)
 same => n,Dial(SIP/${EXTEN}@SecureOperator,60)
 same => n,Hangup()

; Блокування дзвінка через відсутність шифрування
exten => unencrypted,1,NoOp(Блоковано: не виявлено належного VPN-шифрування (X-VPN-
ENCRYPT=${ENCRYPT_STATUS}))
 same => n,Hangup()

; Блокування дзвінка через недостатню довжину ключа шифрування
exten => badkey,1,NoOp(Блоковано: надто коротка довжина шифрувального ключа
(KEY_LENGTH=${KEY_LENGTH}, мінімально допустимий=${MIN_KEY_LENGTH}))
 same => n,Hangup()
```

ДОДАТОК Б. Слайди мультимедійної презентації

ВИПУСКНА РОБОТА БАКАЛАВРА

Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю

Сергєєв Валерій, 2БКС-29

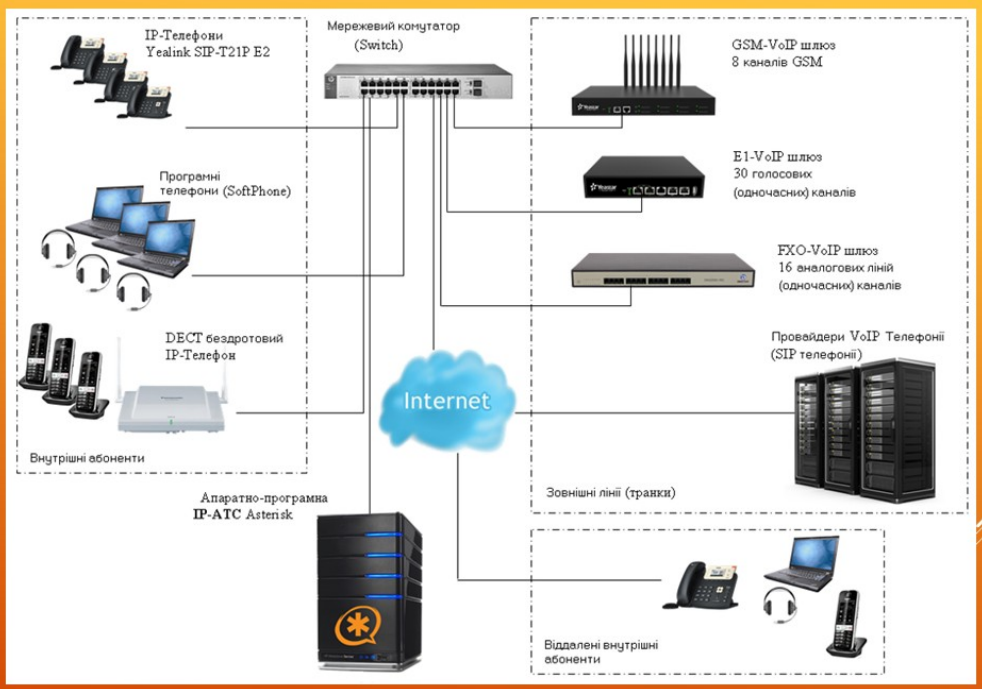


Схема організації мережі IP-телефонії на підприємстві

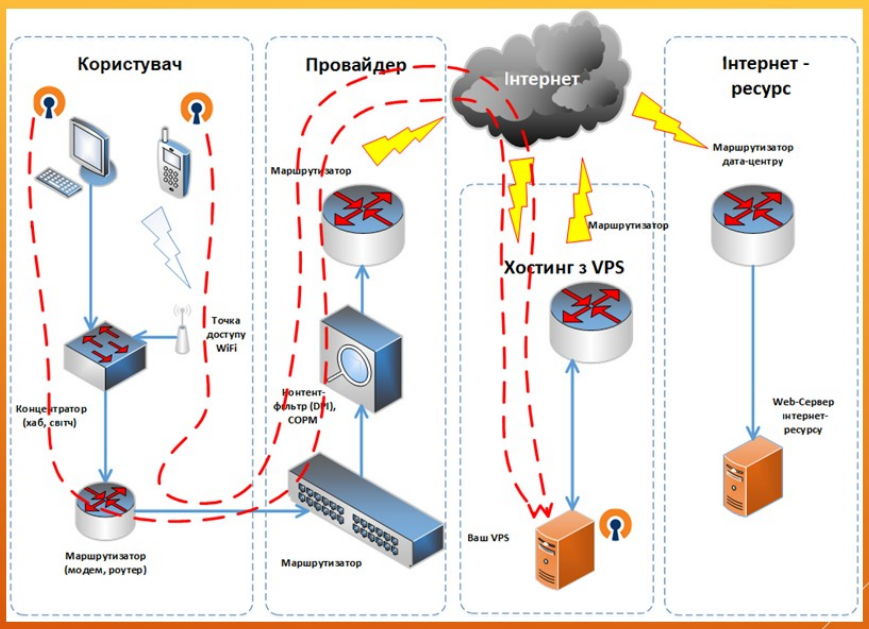
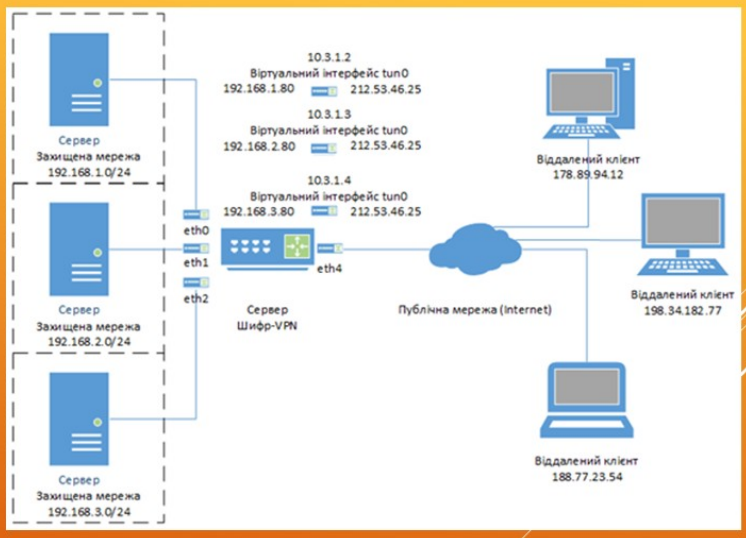
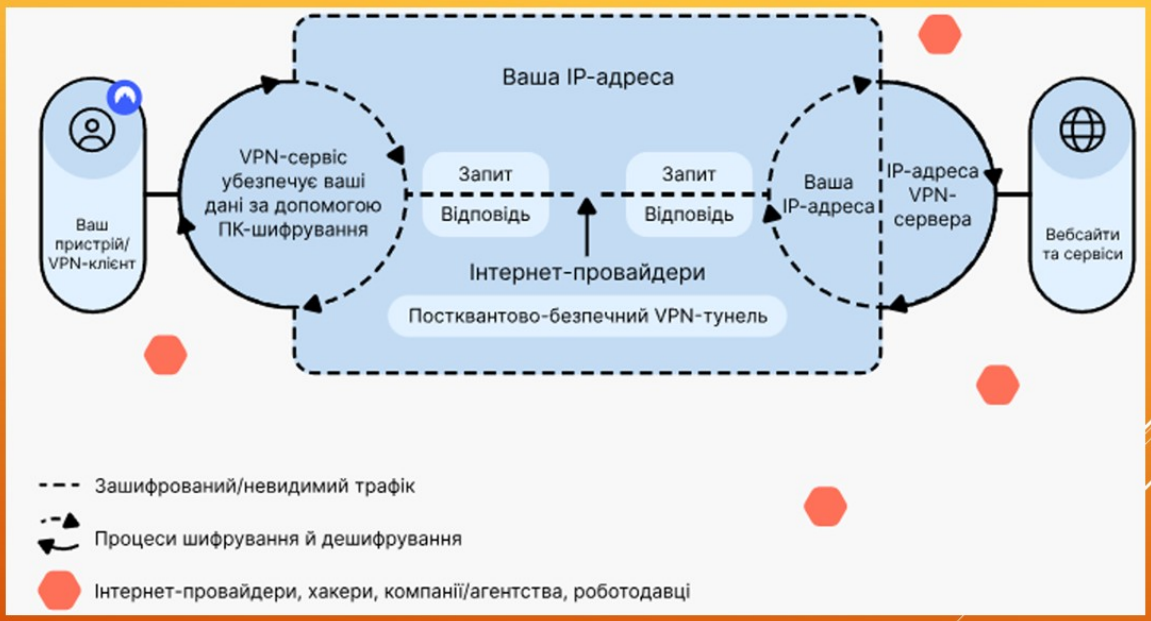


Схема інтернет-трафіку під час серфінгу у інтернет з використанням VPS

Загальна схема VPN-мережі для організацій



Архітектура VPN для корпоративного застосування



Організація VPN для віддаленого користувача

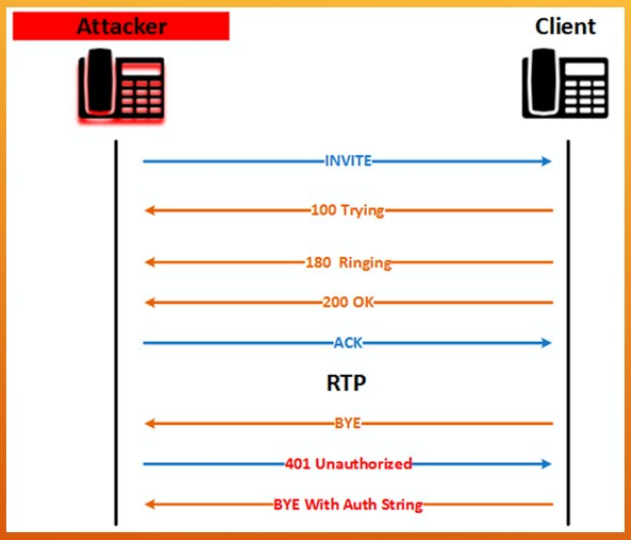
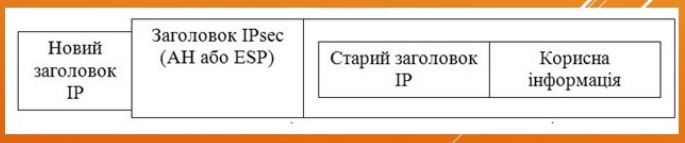
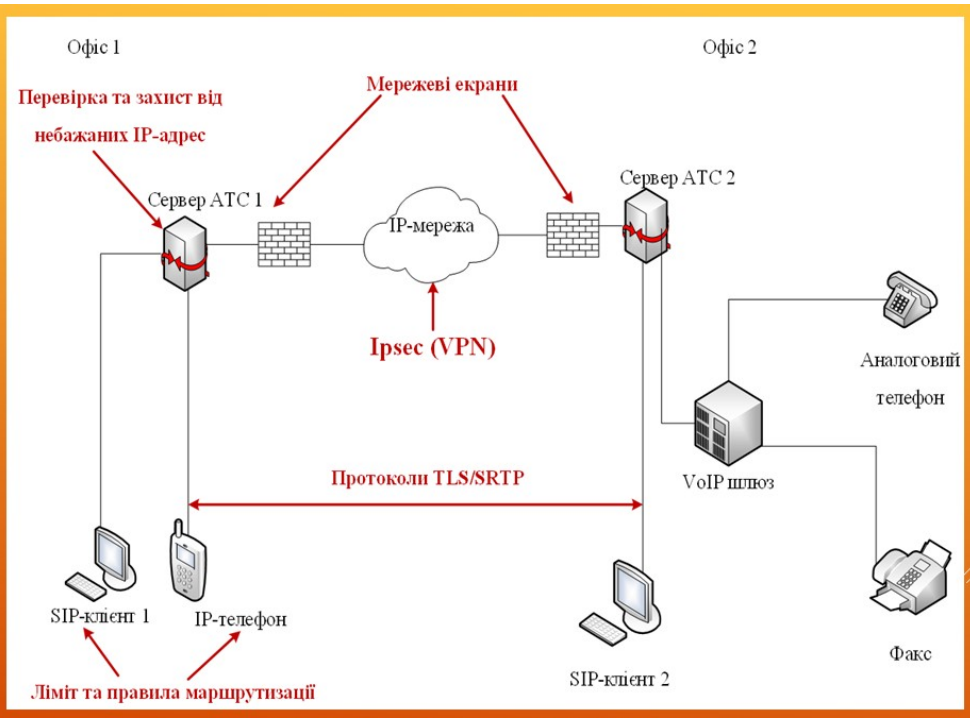


Схема перехоплення голосових пакетів шляхом прослуховування

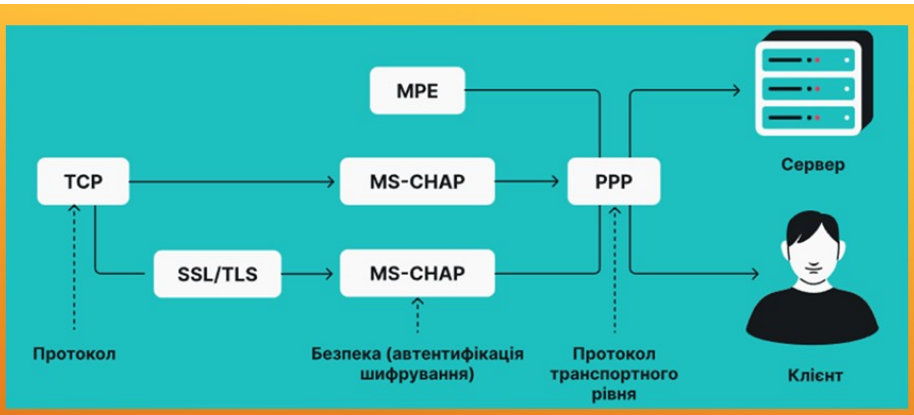
Транспортний режим IPsec



Тунельний режим IPsec

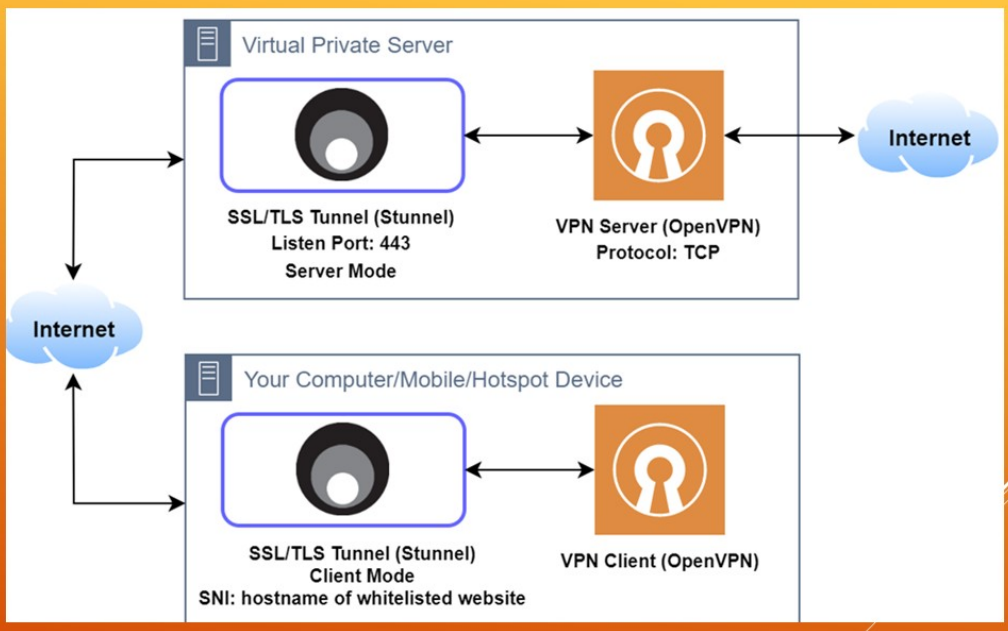


Система захисту VoIP-зв'язку

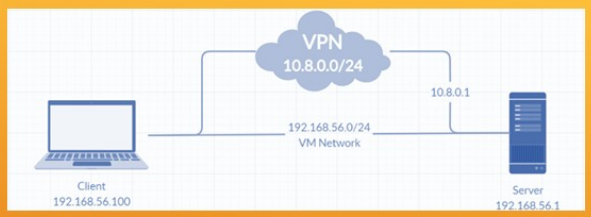


Реалізація протоколу PPTP для тунелювання

Схема пересилки даних по тунелю PPTP



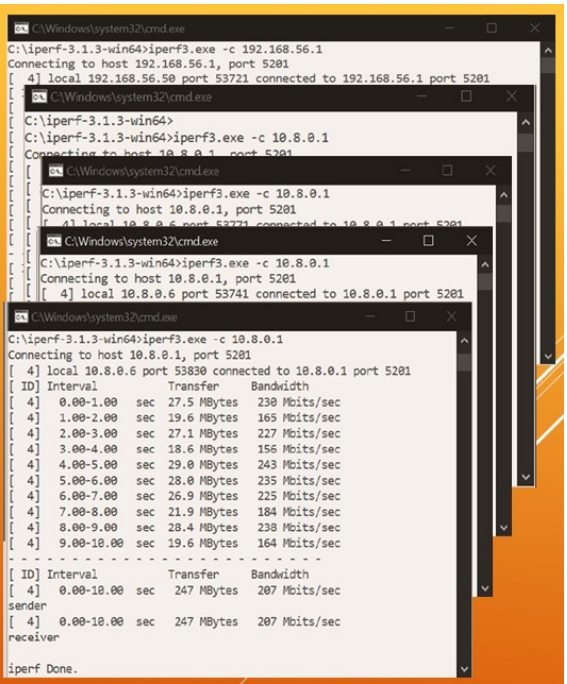
Архітектура протоколу OpenVPN



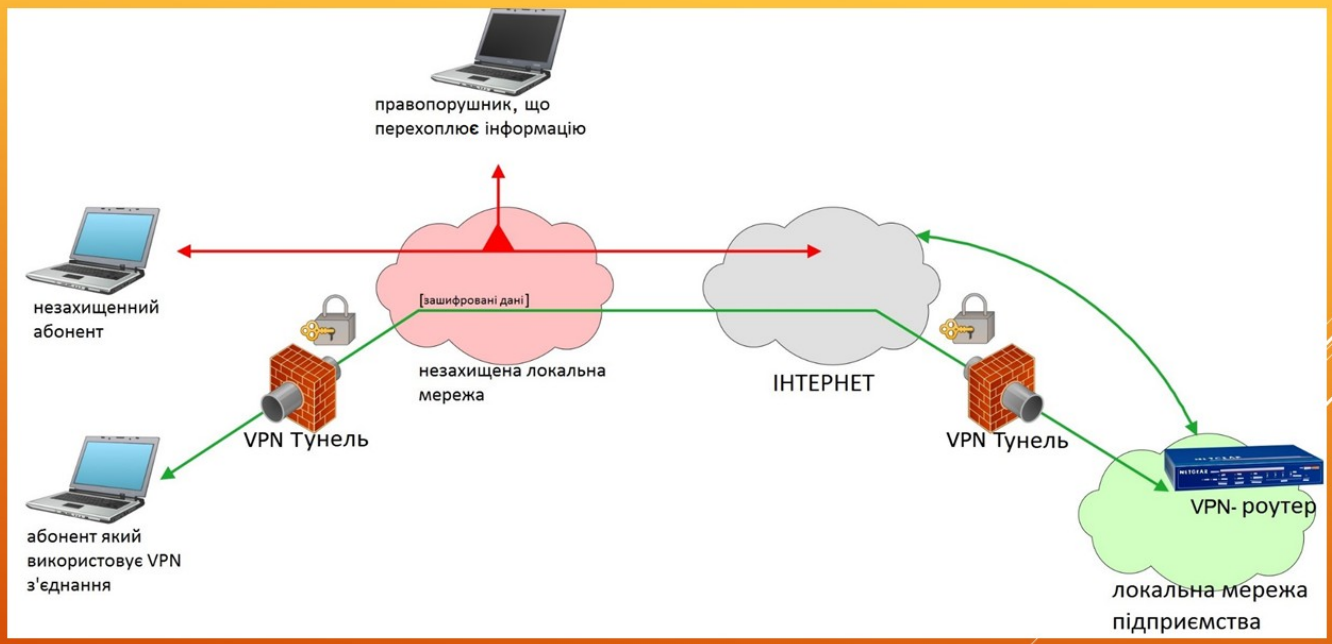
Топологія мережі при тестуванні каналу VoIP-зв'язку з OpenVPN

Режим OpenVPN	Пропускна здатність (Мбіт/с)	Середня затримка (мс)
Без VPN-тунелю	4380	0.5
VPN-тунель без шифрування	213	3
VPN-тунель з шифруванням DES-EDE	217	3.2
VPN-тунель з шифруванням BF-CBC	210	3.5
VPN-тунель з шифруванням AES-256	207	4

Результати тестування впливу шифрування на продуктивність VoIP каналу у режимі OpenVPN



Тестування пропускної здатності VoIP-зв'язку (+OpenVPN, +шифрування)



Ілюстрація атаки MITM (Man in the midle)

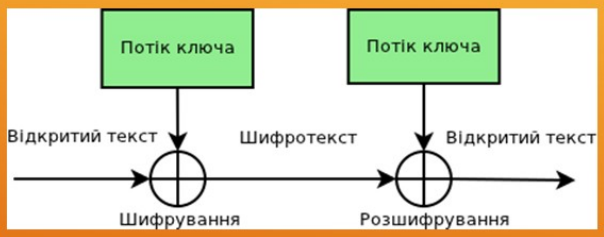


Схема шифрування-дешифрування пакетів даних за алгоритмом RC4

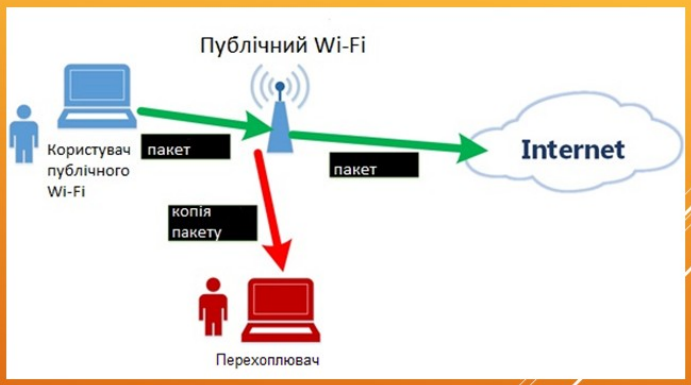
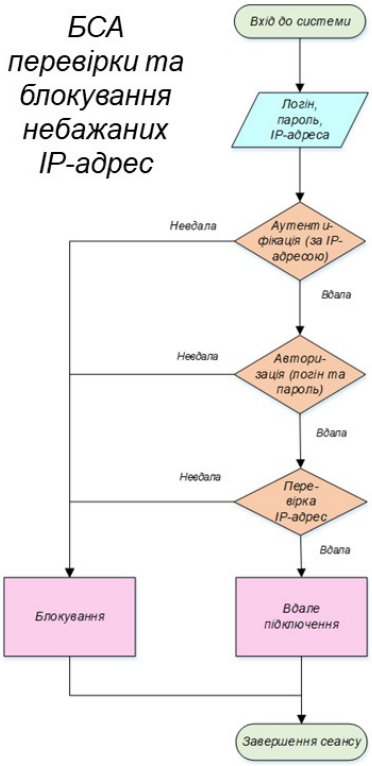


Схема атаки MITM з перехопленням та аналізом VoIP-трафіку

БСА перевірки та блокування небажаних IP-адрес



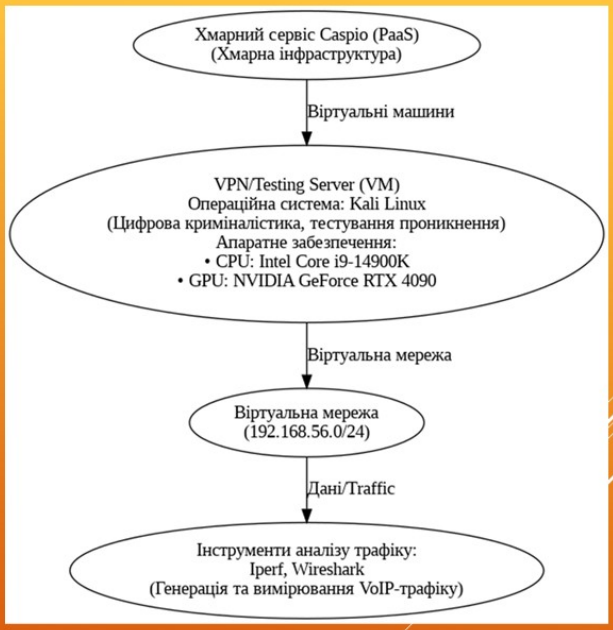


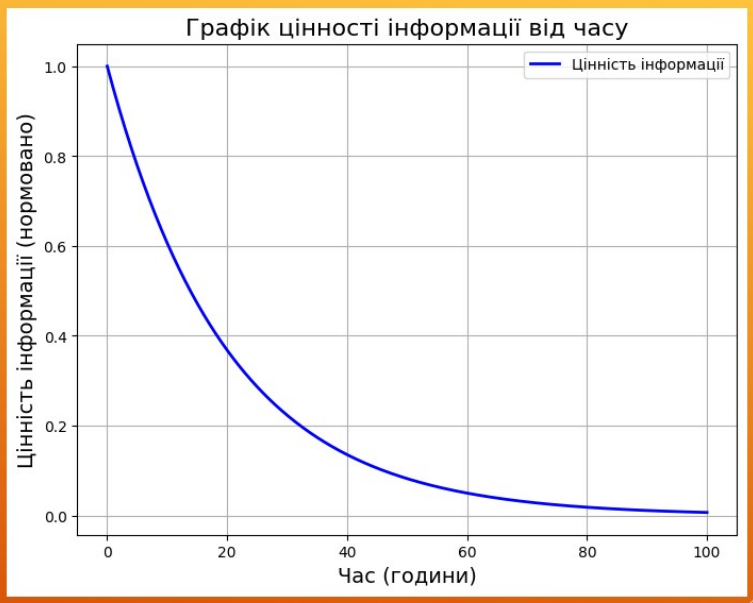
Схема середовища тестування на базі Caspio та Kali Linux

Розрядність ключу	Перший раунд (на CPU Intel Core i9-14900K), годин	Другий раунд (на GPU NVIDIA RTX 4090), годин	Усереднений час підбору, годин
256 біт	–	–	–
128 біт	13,68	6,91	10,30
72 біт	6,76	3,40	5,08
64 біт	4,56	2,12	3,34
56 біт	2,26	1,04	1,65
40 біт	1,12	0,39	0,76
32 біт	0,74	0,19	0,47

Результати підбору ключа шифрування прямим перебором

Розрядність ключу	Перший раунд (на CPU Intel Core i9-14900K), годин	Другий раунд (на CPU Intel Core i9-14900K), годин	Усереднений час підбору, годин
256 біт	15,82	16,46	16,14
128 біт	11,64	–	11,64
72 біт	5,72	5,96	5,84
64 біт	3,76	3,90	3,83
56 біт	–	1,88	1,88
40 біт	0,94	0,76	0,85
32 біт	0,086	0,19	0,14

Результати підбору ключа шифрування за допомогою Райдужних таблиць (Rainbow tables)



Залежність цінності інформації з VoIP-пакетів від часу

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу здобувача (здобувачки) освіти

відділення комп'ютерних систем

Сергєєва Валерія Віталійовича

(прізвище, ім`я та по батькові)

Спеціальність *123 "Комп'ютерна інженерія"*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Керівник кваліфікаційної роботи *Кривченко Анастасія Анатоліївна*

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи *Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю*

Обсяг розрахунково-пояснювальної записки *74* сторінок

Обсяг графічної (презентаційної) частини *15* аркушів (слайдів)

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаного кваліфікаційної роботи завданню

Представлена на рецензію кваліфікаційна робота бакалавра повністю відповідає меті випускної роботи та технічному завданню. Тематика кваліфікаційної роботи є актуальною для своєї галузі та присвячена аналізу методів захисту VoIP-зв'язку за допомогою віртуального тунелю.

б) характеристика виконання кожного розділу кваліфікаційної роботи

Кваліфікаційна робота складається зі вступу, двох розділів, висновків, переліку використаних джерел. У основному розділі виконано огляд технологій захищеного зв'язку; аналіз методів і засобів організації VoIP-зв'язку; визначення видів загроз в мережі VoIP-зв'язку; визначення методів захисту VoIP-зв'язку; Вибір технології захисту VoIP-зв'язку від несанкціонованого доступу; вибір захищеного протоколу для шифрування VoIP-зв'язку; аналіз роботи OpenVPN при організації VoIP-зв'язку; Аналіз надійності шифрування VoIP-зв'язку

в) оцінка якості виконання пояснювальної записки та графічної частини кваліфікаційної роботи

Графічна частина виконана на достатньо високому рівні у вигляді презентації із використанням офісного пакету Microsoft PowerPoint та Visio. Пояснювальна записка виконана охайно та у відповідності до норм оформлення документів із використанням офісного пакету Microsoft Word. Загальна якість виконання документації – добра, академічного плагіату ідей у роботі не виявлено

г) перелік позитивних якостей кваліфікаційної роботи *Робота порівнює численні підходи до організації захищених каналів VoIP-зв'язку. Вона включає аналіз як тунельних протоколів (PPTP, L2TP/IPSec), так і сучасних рішень на базі криптографії (OpenVPN, IKEv2/IPSec). Наявність таблиць порівняльної характеристики протоколів дозволяє чітко побачити переваги і недоліки кожного підходу.*

д) основні недоліки кваліфікаційної роботи *Варто було обговорити можливі обмеження експериментальної установки. Було б доцільно порівняти отримані результати з існуючими теоретичними моделями або попередніми дослідженнями. Це дозволить більш об'єктивно оцінити ефективність обраних методів захисту та надати рекомендації щодо оптимізації параметрів шифрування.*

Оцінка розрахункової частини *Відмінно*

Оцінка графічної частини *Добре*

Загальна оцінка *Відмінно*

Прізвище, ім'я, по батькові рецензента *к.т.н. Рудніченко Микола Дмитрович*

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

Підпис: _____

«*23*» *06* 2025 р.

ВСП «Одеський технічний фаховий коледж ОНТУ»

ВІДГУК

керівника про кваліфікаційну роботу бакалавра

Сергєєва Валерія Віталійовича

(прізвище, ім`я та по батькові)

Спеціальність *123 Комп'ютерна інженерія*

Освітньо-професійна програма *Комп'ютерна інженерія*

Тема кваліфікаційної роботи *Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю*

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки) *Випускна робота виконана відповідно технічному завданню. Пояснювальна записка до випускної роботи містить 74 сторінки. У пояснювальній записці виконано огляд та аналіз технологій побудови захищених каналів, описано технологію VPN, проведено аналіз методів захисту VoIP-зв'язку. Графічна частина складається з 15 слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра, розробку виконано у повному обсязі.*

б) Самостійність роботи *Протягом виконання випускної бакалаврської роботи Сергєєв Валерій поступово та послідовно виконувала всі етапи, проявила ініціативу у створенні загальної концепції та реалізації випускної роботи. Всі роботи вона виконувала самостійно, з оглядом на рекомендації керівника.*

в) Теоретична підготовка здобувача освіти

Сергєєв Валерій під час роботи над випускною бакалаврською роботою вивчив достатню кількість літературних джерел за даною тематикою.

Вважаю, що теоретична підготовка здобувача освіти добра і він готовий до захисту роботи.

г) Вміння розв`язувати виробничі і конструкторські питання на базі останніх досліджень науки і техніки, передових методів виробництва

Під час виконання роботи Сергєєв Валерій мав змогу самостійно приймати окремі рішення з виконання програмної частини роботи та показав вміння організовано працювати над поставленою задачею, складати та оформлювати презентацію проекту, користуючись сучасними комп'ютерними програмними засобами, такими як Caspio (PaaS Provider), ARCFOURdecrypt

Оцінка розрахункової частини *Відмінно*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Відмінно*

Прізвище, ім`я, по батькові *Кривченко Анастасія Анатоліївна*

Місце роботи і посада керівника роботи *ВСП "Одеський технічний фаховий коледж ОНТУ", викладач кафедри комп'ютерної інженерії, голова обласної методичної комісії викладачів комп'ютерної інженерії*

Підпис

«20» 06 2025 р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Сергєєв В.В.,
здобувач освіти гр. 2БКС-29, та

Кривченко А.А.,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю» (автор роботи – Сергєєв В.В., керівник роботи – Кривченко А.А.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Сергєєв В.В. /

Керівник _____ / Кривченко А.А./

«16» червня 2025 р.

ДОВІДКА

кафедри комп'ютерної інженерії
про допуск до захисту кваліфікаційної роботи
здобувача (здобувачки) освіти II курсу
відділення комп'ютерних систем групи 2БКС-29

Сергєєва Валерія Віталійовича

на тему *Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до кваліфікаційної роботи виконана з несуттєвими порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис) *20.06.2025* (дата) *Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 03.06.2025 р. значення коефіцієнту подібності в роботі становить 12,61%, коефіцієнт цитування – 0,93%.*

(підпис) *20.06.2025* (дата) *Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) кваліфікаційної роботи

здобувача (здобувачки) освіти *Сергєєва В.В.* (П.І.Б.)

проведена « *20* » *червня* 2025 р.

Висновки *Пояснювальна записка до кваліфікаційної роботи виконана у повному обсязі. Випускна кваліфікаційна робота відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Зав. кафедри КІ (підпис) *Іванова Л.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 6/3/2025
Дата редагування 6/3/2025

Документ прийнятий

Звіт подібності

метадані

Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Аналіз методів захисту VoIP-зв'язку за допомогою віртуального тунелю

Автор
Сергєєв Валерій Віталійович
Науковий керівник / Експерт
Кривченко Анастасія Анатоліївна

підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

КЦ

25
Довжина фрази для коефіцієнта подібності 2

12987
Кількість слів

105155
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		1
Інтервали	A→	0
Мікропробіли	·	0
Білі знаки		0
Парафрази (SmartMarks)	a	54

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	46 0.35 %
2	https://card-file.ontu.edu.ua/bitstreams/3c34e9ea-f695-4fe4-82de-a5c9314f822a/download	41 0.32 %
3	https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download	34 0.26 %
4	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	32 0.25 %
5	http://cpsm.kpi.ua/stud/bak/DP_BAK_KARAULOVA_LU.pdf	32 0.25 %

6	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	24 0.18 %
7	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	22 0.17 %
8	https://linoxide.com/configure-openvpn-ubuntu-16-04/	21 0.16 %
9	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	20 0.15 %
10	https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content	19 0.15 %

з домашньої бази даних (0.15 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Створення web-застосунку цифрового помічника з використанням Open AI [redacted] 5/28/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	19 (3) 0.15 %

з програми обміну базами даних (1.27 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Аналіз методів захисту інформації в мережі IP-телефонії [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	101 (11) 0.78 %
2	Технологія захисту інформаційної системи організації віддалених користувачів на базі VPN [redacted] 12/28/2023 State University of Telecommunications (ННІЗІ)	22 (3) 0.17 %
3	Способи захисту інформаційно- телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN [redacted] 12/21/2024 Ternopil Ivan Pul'uj National Technical University (кафедра кібербезпеки)	16 (1) 0.12 %
4	dm_2023_263_020 [redacted] 8/20/2024 O.M.Beketov National University of Urban Economy in Kharkiv (O.M.Beketov National University of Urban Economy in Kharkiv)	15 (1) 0.12 %
5	2015_805090301_Burshtyko_Anna_Volodymyrivna_24661 [redacted] 10/24/2024 National University "Lviv Politechnika" (National University Lviv Politechnika)	6 (1) 0.05 %
6	Дплом Шиян БСДМ-61.4 2003-конвертирован.pdf [redacted] 12/26/2019 State University of Telecommunications (ННІЗІ)	5 (1) 0.04 %

з Інтернету (11.20 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	636 (56) 4.90 %
2	**https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download**	**149 (7) 1.15 %**
3	http://www.scs.kpi.ua/sites/default/files/files/2017/%D0%91%D0%B0%D0%BA%D0%B0%D0%BB%D0%B0%D0%B2%D1%80%D0%B8/%D0%97%D0%B0%D1%97%D0%BA%D0%B0.doc	74 (9) 0.57 %

4	https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04	56 (6) 0.43 %
5	**https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download**	**54 (3) 0.42 %**
6	https://card-file.ontu.edu.ua/server/api/core/bitstreams/e86ba9fc-9135-43bb-922a-10bf0bce46b5/content	53 (5) 0.41 %
7	https://linoxide.com/configure-openvpn-ubuntu-16-04/	45 (3) 0.35 %
8	https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download	45 (4) 0.35 %
9	**https://card-file.ontu.edu.ua/bitstreams/3c34e9ea-f695-4fe4-82de-a5c9314f822a/download**	**41 (1) 0.32 %**
10	https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content	40 (6) 0.31 %
11	**http://cpsm.kpi.ua/stud/bak/DP_BAK_KARAULOVA_LU.pdf**	**40 (2) 0.31 %**
12	https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content	30 (2) 0.23 %
13	https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download	27 (3) 0.21 %
14	https://card-file.ontu.edu.ua/server/api/core/bitstreams/06e18d7b-ab24-4f6a-a89a-332bb9ca5ebb/content	22 (2) 0.17 %
15	https://ruvds.com/ru/helpcenter/kak-nastroit-openvpn-server-na-ubuntu-20-04/	22 (2) 0.17 %
16	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	19 (1) 0.15 %
17	https://dnaop.com/html/2297_2.html	15 (1) 0.12 %
18	https://noviello.it/ru/kak-ustanovit-openvpn-siervier-na-ubuntu-18-04-lts/	15 (2) 0.12 %
19	https://tecadmin.net/install-openvpn-server-ubuntu/	13 (2) 0.10 %
20	https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download	12 (1) 0.09 %
21	https://biblioteka.udhtu.edu.ua/wp-content/uploads/2020/11/4869_%D0%9C%D0%92_%D0%94%D0%9F_%D0%98%D0%A1_2019_%D0%9B.doc.pdf	12 (1) 0.09 %
22	https://card-file.ontu.edu.ua/bitstreams/d42aac6d-ab01-4a74-b9cb-ced2a9eff719/download	10 (1) 0.08 %
23	https://card-file.ontu.edu.ua/server/api/core/bitstreams/995bdcec-4e4d-4321-8070-4d6badcb8e49/content	10 (1) 0.08 %
24	https://arhivinfo.ru/1-33484.html	8 (1) 0.06 %
25	https://github.com/rozahp/openvpn-lxc	6 (1) 0.05 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Комп'ютерна інженерія»
Група: 2БКС- 29

КВАЛІФІКАЦІЙНА РОБОТА

здобувача **освіти денної форми навчання БКС.** 29.20.000.КРБ

СЕРГЄЄВА