МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИРОДОКОРИСТУВАННЯ

ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

другого (магістерського) рівня вищої освіти

на тему:

«Проектування корпоративної комп'ютерної мережі організації з використанням VPN-технології»

Виконав: здобувач 6 курсу групи Іт-62

Спеціальності 126 «Інформаційні системи та технології»

(шифр і назва)

Баліцький В. С.

(Прізвище та ініціали)

Керівник: к.е.н., доцент Станько В. Ю.

(Прізвище та ініціали)

Рецензент: к.т.н., доцент Сиротюк С.В.

(Прізвище та ініціали)

ДУБЛЯНИ-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИРОДОКОРИСТУВАННЯ

ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Другий (магістерський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри_____
д.т.н., проф. А.М. Тригуба
"____"_____2024 р.

ЗАВДАННЯ

на кваліфікаційну роботу студенту
Баліцький Володимир Святославович

1. Тема роботи: «Проектування корпоративної комп'ютерної мережі організації з використанням VPN-технології»

   Керівник роботи Станько Володимир Юрійович, к.е.н., доцент
   Затверджені наказом по університету 12.09.2024 року № 616/к-с.

2. Строк подання студентом роботи 10.12.2024 р.

3. Початкові дані до роботи: 1. Вимоги до побудови інформаційних систем. 2. Науково-технічна і довідкова література. 3. Засоби створення, обладнання мова програмування. 4. Методика створення інформаційних систем.

4. Зміст розрахунково-пояснювальної записки:

   Вступ

   Аналіз стану корпоративних мереж, VPN технологій та завдання кваліфікаційної роботи.

   Обгрунтування та вибір обладнання та VPN протоколу для проектування корпоративної мережі.

   Побудова корпоративної комп'ютерної мережі з використанням vpn-технології

   Охорона праці та безпека у надзвичайних ситуаціях.

   Результати розробки системи аутентифікації користувача.

   Визначення економічної ефективності використання

   Висновки та пропозиції.

   Бібліографічний список.

5. Перелік графічного матеріалу: 1) Презентація із головними результатами кваліфікаційної роботи.

6. Консультанти з розділів:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3, 5	*Станько В.Ю., доцент кафедри інформаційних технологій*		
4	*Городецький І.М., доцент кафедри фізики, інженерної механіки та безпеки виробництва*		

7. Дата видачі завдання 12.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту	Строк виконання етапів роботи	Приміт-ка
1.	*Написання першого розділу та означення головних завдань роботи*	*12.09.2024 – 25.09.2024*	
2.	*Виконання другого розділу та формування головних показників для розрахунків*	*26.09.2024 – 10.10.2024*	
3.	*Виконання третього розділу, розрахунків та розробка листів*	*11.10.2024 – 22.10.2024*	
4.	*Написання розділу: «Охорона праці та безпека в надзвичайних ситуаціях»*	*23.10.2024 – 05.11.2024*	
5.	*Вартісна оцінка ефективності проектних пропозицій роботи*	*06.11.2024 – 17.11.2024*	
6.	*Завершення оформлення розрахунково-пояснювальної записки та аркушів графічної частини*	*18.11.2024 – 30.11.2024*	
7.	*Завершення роботи в цілому*	*01-10.12.2024*	

Студент _____ Баліцький В. С.
(підпис)

Керівник роботи _____ Станько В.Ю.
(підпис)

УДК 004.72:004.738.5

Проектування корпоративної комп'ютерної мережі організації з використанням VPN-технології.

Баліцький В.С. Кафедра інформаційних технологій – Дубляни, Львівський НУП, 2024.

Кваліфікаційна робота: 63 с. текст. част., 4 рис., 6 табл., 33 джерел.

Проведено глибоке дослідження технології VPN, що дозволило визначити її значущість і багатогранну роль у проєктуванні та створенні захищених комп’ютерних мереж. Особлива увага приділялася аналізу її застосування для протидії сучасним викликам у сфері інформаційної безпеки та забезпечення стабільності функціонування мереж.

Розглянуто ключові принципи її функціонування з урахуванням основних компонентів: тунелювання, аутентифікації та шифрування даних. Розділ також охоплює характеристику основних типів мереж VPN, їх функціональні властивості та різні підходи до реалізації цієї технології.

Здійснено масштабний комплексний аналіз поточного стану розвитку корпоративних мереж, VPN технологій та їхньої технологічної бази. Зокрема,

Результати детального дослідження та практичного впровадження проекту підтвердили важливість технології VPN як ключового інструменту для забезпечення конфіденційності передачі даних у комп’ютерних мережах сучасних корпоративних мережах.

перспективним і стратегічним напрямком для подальшого прогресу галузі. Отже, результати цієї роботи не тільки підкреслюють значущість досліджень у сфері захисту інформації, але й служать основою для посилення практичного впровадження та розширення впливу VPN-технологій.

Розроблено заходи щодо охорони праці.

Ключові слова: VPN технологія, протоколи, комп’ютерна мережа, Mikrotik, WireGuard, безпечне з’єднання.

Key words:. VPN technology, protocols, ,computer network, Mikrotik, WireGuard, secure connection.

ЗМІСТ

ВСТУП

В умовах стрімкого розвитку інформаційних технологій та глобальної інтеграції бізнесу забезпечення безпечної та ефективної передачі даних є важливим аспектом функціонування сучасних організацій. Використання комп'ютерних мереж стало необхідним інструментом для оптимізації процесів управління, комунікації та доступу до ресурсів. У той же час, ризики, пов'язані з порушенням конфіденційності інформації, зростають, оскільки обмін даними часто відбувається через загальнодоступні мережі, такі як Інтернет. В цьому контексті критичним стає питання створення надійних та безпечних корпоративних мереж із застосуванням передових технологій.

VPN (Virtual Private Network) – це технологія, яка забезпечує безпечний зв'язок через незахищені мережі, такі як Інтернет, шляхом створення віртуальних тунелів, що шифрують передані дані. Використання VPN у корпоративних мережах дозволяє компаніям створювати безпечні канали для обміну інформацією між віддаленими офісами, партнерами або співробітниками. У сучасних умовах, коли віддалена робота стає дедалі популярнішою, впровадження VPN-технологій стає не лише зручністю, а й необхідністю для збереження конкурентоспроможності компанії та захисту її ресурсів.

Актуальність проєктування корпоративної комп'ютерної мережі з використанням VPN-технологій визначається кількома факторами. По-перше, це забезпечення конфіденційності даних, особливо у випадку передачі комерційної або особистої інформації через Інтернет. По-друге, VPN дозволяє зменшити витрати на підтримку власних фізичних мережевих каналів зв'язку, використовуючи замість них доступні публічні мережі. Нарешті, віддалена робота, яка набула масового характеру через пандемію COVID-19, підкреслила важливість надійних рішень для безпечного підключення до корпоративних мереж з будь-якої точки світу.

Метою даної дипломної роботи є розробка проєкту корпоративної комп'ютерної мережі організації із застосуванням VPN-технологій. Основним

завданням є забезпечення безпечного доступу до корпоративних ресурсів для віддалених співробітників, а також зниження витрат на підтримку мережевої інфраструктури без втрати якості зв'язку.

Для досягнення цієї мети у роботі необхідно виконати наступні завдання:

1. Провести аналіз сучасних VPN-технологій, їх можливостей, переваг та недоліків, а також їх використання у корпоративних мережах Також необхідно розглянути протоколи, що використовуються для шифрування та передачі даних (IPsec, OpenVPN, SSL/TLS), та оцінити їх ефективність.

2. Вибрати оптимальні рішення для побудови безпечної корпоративної мережі на основі VPN, враховуючи специфіку організації, її розмір, кількість користувачів, географічне розташування офісів та вимоги до рівня безпеки даних. Вибір технологій і обладнання буде здійснюватися на основі аналізу доступних на ринку рішень, зокрема маршрутизаторів, фаєрволів та програмного забезпечення для створення віртуальних приватних мереж.

3. Розробити проєкт корпоративної мережі із застосуванням VPN, включаючи топологію мережі, схему підключень, налаштування обладнання, а також програмні рішення для шифрування даних та управління доступом. Важливо врахувати особливості обробки та маршрутизації трафіку через VPN, щоб забезпечити високу швидкість передачі даних та низьку затримку з'єднань.

Об'єктом дослідження є корпоративна комп'ютерна мережа організації, яка використовується для забезпечення внутрішнього зв'язку між офісами, обміну даними та доступу до ресурсів компанії. Предметом дослідження виступають VPN-технології та їх застосування для забезпечення захищеної передачі даних через загальнодоступні мережі.

У роботі застосовуються методи аналізу та синтезу інформаційних систем, порівняння технічних рішень, моделювання мережевих архітектур, а також методи оцінки продуктивності та безпеки мережі.

Практична цінність даної роботи полягає у створенні практичного рішення для проєктування та впровадження корпоративної мережі з використанням VPN-технологій, яке може бути застосоване в різних організаціях.

РОЗДІЛ 1.
АНАЛІЗ СТАНУ КОРПОРАТИВНИХ МЕРЕЖ ТА VPN ТЕХНОЛОГІЙ

1.1 Аналіз стану корпоративних мереж

1.1.1 Основні можливості корпоративних мереж

Корпоративна мережа виступає як інформаційна система, що надає можливість компаніям централізувати ресурси та забезпечувати їхнє спільне використання. Її ключові функції охоплюють такі важливі аспекти:

Підтримка колективної роботи. Корпоративна мережа створює умови для ефективної участі співробітників у спільних проектах, обміну документами та координації дій для досягнення загальних цілей. Збільшення продуктивності. Система надає швидший і точніший доступ до потрібної інформації та інструментів, що сприяє злагодженій і результативній роботі персоналу. Забезпечення безпеки даних. Завдяки контролю доступу та захисту інформації знижується ризик втрати даних і гарантується конфіденційність.

Оптимізація витрат. Використання спільних ресурсів в межах корпоративної мережі дозволяє заощаджувати на придбанні та підтримці IT-інфраструктури. Об’єднане використання апаратного забезпечення. Корпоративна мережа дає змогу компанії централізовано експлуатувати сервери, комутатори, маршрутизатори та сховища, замість придбання окремого устаткування для кожного підрозділу, що суттєво скорочує витрати. Спільне використання програмного забезпечення. Спільний доступ до програм дозволяє мінімізувати витрати на ліцензії та їх оновлення, охоплюючи такі засоби, як операційні системи, офісні додатки чи бази даних.

Централізоване адміністрування. Наявність єдиної команди системних адміністраторів спрощує управління мережею, скорочує витрати на її підтримку й забезпечує злагоджене функціонування.

Управління мережевим обладнанням. Адміністратори займаються налаштуванням, моніторингом і підтримкою обладнання, оновленням його програмного забезпечення та впровадженням політик безпеки. Забезпечення кіберзахисту та безпеки. Впровадження фаєрволів, антивірусних програм і систем запобігання загрозам гарантує безпеку корпоративного сегменту, зменшуючи ризики несанкціонованого доступу чи атак.

Моніторинг і аналіз мережевої активності. Використовуючи спеціалізовані інструменти, адміністратори оперативно виявляють аномалії в роботі мережі або проблеми перевантаження, миттєво усуваючи їх.

Допомога користувачам. Від налаштування підключень до відновлення паролів чи вирішення інших проблем із доступом – командна підтримка завжди готова оперативно надати допомогу.

Комунікації та додаткові сервіси. Корпоративна мережа пропонує єдиний доступ до email-систем, спільних сховищ, інструментів співпраці й додаткових послуг, що зменшує дублювання функцій у різних підрозділах і оптимізує витрати компанії на IT-забезпечення. Через інтеграцію обладнання й цифрових інструментів корпоративна мережа допомагає бізнесу ефективніше організовувати процеси, ухвалювати раціональні рішення й знизити витрати в конкурентному середовищі сучасного ринку.

Корпоративні мережі мають цілу низку вагомих переваг, які значно підвищують ефективність та продуктивність компанії. Однією з ключових переваг є можливість організації централізованого дистанційного навчання, що сприяє професійному розвитку співробітників і оптимізації витрат на навчальні заходи. Їх впровадження дозволяє значно знизити витрати на обслуговування мережі, водночас підвищуючи ефективність інвестицій у розвиток інфраструктури. Такі системи забезпечують прозорість процесів у компанії, контроль над використанням ресурсів і моніторинг роботи всіх відділів, що допомагає уникнути зайвих витрат та покращувати внутрішні процеси. Особливу увагу слід приділити можливостям підвищення безпеки та автономності, які пропонують корпоративні мережі. Вони сприяють збереженню

конфіденційності інформації та швидкому обміну актуальними даними між працівниками, що дозволяє оперативно приймати виважені рішення й адаптуватися до змін всередині компанії чи на ринку. Завдяки доступу до інформації в реальному часі навіть поза межами офісу співробітники можуть продуктивно виконувати свої обов'язки, а спільний доступ до ресурсів стимулює командну роботу та покращує комунікацію. Централізоване управління корпоративною інфраструктурою також відіграє важливу роль. Воно дозволяє оптимізувати адміністрування, впроваджувати єдині налаштування для всіх підрозділів компанії та гарантувати цілісність системи. Завдяки цьому адміністратори можуть централізовано контролювати роботу обладнання – від комутаторів і маршрутизаторів до бездротових точок доступу, що спрощує як початкову конфігурацію, так і подальшу підтримку мережі.

Моніторинг і аналітика також стають набагато ефективнішими завдяки централізації управління.

Збір даних із різних джерел дозволяє адміністраторам аналізувати пропускну здатність, виявляти несправності чи підозрілу активність і своєчасно вирішувати проблеми. Такий підхід збільшує стабільність системи та оптимізує її роботу. З точки зору безпеки мережа пропонує широкий спектр рішень.

Централізоване управління забезпечує ефективний контроль доступу до ресурсів, дозволяючи створювати політики безпеки, розподіляти права доступу та миттєво реагувати на потенційні загрози.

Автентифікація користувачів і авторизація доступу захищають інформацію від несанкціонованого користування, а застосування технологій шифрування оберігає дані від перехоплення під час передачі.

Додатковими засобами захисту виступають фаєрволи й інтрузивні системи виявлення вторгнень, які дозволяють своєчасно ідентифікувати підозрілу активність і блокувати зовнішні атаки. А інструменти для боротьби з шкідливими програмами надають змогу попереджати розповсюдження вірусів та зараження обладнання.

Особливо важливим є механізм резервного копіювання й відновлення даних. У разі виникнення аварій чи збоїв він забезпечує оперативну реконструкцію системи та збереження цілісності інформації, що критично важливо для стабільної роботи організації. Завдяки цим технологічним рішенням корпоративні мережі забезпечують комплексний підхід до безпеки й ефективного функціонування компанії в умовах сучасного динамічного бізнес-середовища.

Однією з ключових переваг корпоративних мереж є їхня масштабованість, яка дозволяє враховувати зростання та потреби організації. Це зокрема включає можливість додавання нових вузлів, збільшення пропускної здатності та адаптацію до зміни запитів користувачів. Додавання нових вузлів забезпечується шляхом встановлення додаткового обладнання та його інтеграції до існуючої інфраструктури. Це надає змогу динамічно реагувати на зміну потреб організації, забезпечуючи доступ новим користувачам та пристроям.

Збільшення пропускної здатності відбувається в процесі модернізації завдяки інсталяції нового обладнання з високою пропускною здатністю, оновленню комутаторів або розширенню каналів зв’язку. Це дозволяє підтримувати високу швидкість обробки даних і задовольняти вимоги зростаючої кількості користувачів.

Горизонтальна масштабованість реалізується через додавання фізичних ресурсів, таких як комутатори чи маршрутизатори, що сприяє рівномірному розподілу навантаження та покращенню загальної продуктивності системи.

Вертикальна масштабованість передбачає вдосконалення наявного обладнання чи використання оптимізованих протоколів для покращення ефективності роботи мережі. Віртуалізація відіграє важливу роль у масштабуванні корпоративних мереж і дає змогу більш раціонально використовувати ресурси через логічний поділ фізичної інфраструктури на віртуальні сегменти. Це також підвищує рівень безпеки та прискорює впровадження нових сервісів.

Серед інструментів віртуалізації важливе місце займають віртуальні приватні мережі (VPN), які створюють зашифровані тунелі для захищеної передачі даних між віддаленими користувачами або мережами через відкриті канали зв’язку, такі як Інтернет. VPN гарантує конфіденційність обміну інформацією незалежно від місця розташування пристроїв. Віртуальні локальні мережі (VLAN) дозволяють організувати логічний поділ фізичної інфраструктури, забезпечуючи об’єднання пристроїв чи користувачів в один сегмент незалежно від їх географічного розташування. VLAN спрощують управління трафіком, покращують безпеку системи та сприяють регулюванню доступу до ресурсів. Віртуалізація мережевих функцій (NFV) забезпечує перенесення основних мережевих функцій у віртуальне середовище через відокремлення їх від фізичного обладнання. Такий підхід значно підвищує гнучкість у керуванні ресурсами, знижує витрати на апаратне забезпечення та спрощує адміністрування сервісів.

Зниження витрат. Використання корпоративних мереж дозволяє зменшити витрати завдяки оптимізації інфраструктури, спільному використанню ресурсів і централізованому управлінню. Централізоване резервне копіювання даних. Корпоративні мережі забезпечують збереження важливої інформації на центральних серверах або мережевих сховищах, що підвищує стійкість до втрати даних через віруси, випадкове видалення або технічні несправності.

Централізоване зберігання. Усі дані розміщуються в одному місці — на серверах чи спеціалізованих пристроях зберігання. Такий підхід не лише спрощує управління інформацією, а й суттєво полегшує процес резервного копіювання.

Автоматизоване резервне копіювання. Центральна система може бути налаштована для автоматичного створення копій із різноманітних джерел, таких як файли, бази даних чи електронна пошта. Це забезпечує стабільність цього процесу та мінімізує ризики пропусків під час резервування.

Ієрархічне зберігання. Така структура використовує кілька рівнів: локальні копії, які доступні для швидкого відновлення, і зовнішні носії для

довготривалого зберігання інформації. Цей підхід дозволяє ефективніше розподіляти ресурси, одночасно підвищуючи надійність резервного копіювання.

Централізований доступ до резервних копій. Завдяки корпоративній мережі можна швидше й простіше організовувати доступ до резервних даних. Права доступу можна легко регулювати, дозволяючи відповідним працівникам або адміністраторам користуватися необхідними копіями.

Гнучка підтримка мобільності співробітників. Можливість підключення мобільних пристроїв у корпоративній мережі дає змогу працівникам отримувати доступ до ресурсів компанії незалежно від їхнього місцеперебування. Це покращує гнучкість роботи та сприяє продуктивності віддалених команд.

Підвищена надійність та доступність. Налаштування корпоративних мереж із використанням механізмів резервування і балансування навантаження гарантує стабільну роботу без перебоїв та безперервний доступ до ключових ресурсів підприємства.

Покращена комунікація. Корпоративні мережі забезпечують доступ до сучасних засобів спілкування, таких як електронна пошта, відеоконференції та чати, що сприяють швидкому обміну інформацією та колективному прийняттю рішень у команді. Централізоване управління користувачами. Управління правами доступу, автентифікацією та авторизацією користувачів здійснюється централізовано, що полегшує адміністрування облікових записів і забезпечує високий рівень захисту конфіденційної інформації всередині системи.

1.1.2 Призначення корпоративної мережі

Корпоративна мережа являє собою комплексну систему, що сприяє інтеграції та обміну даними між різноманітними додатками всередині організації. Вона працює як закрита внутрішня інфраструктура підприємства чи установи, заснована на протоколі TCP/IP і сучасних стандартах комунікацій, запозичених з Інтернету. Задля забезпечення стабільної роботи мережі

впроваджуються сервіси та програми, які ефективно доставляють інформацію кінцевим користувачам.

Наприклад, компанія може використати Web-сервер для розміщення внутрішніх оголошень, розкладів, а також інших робочих документів, доступ до яких співробітники отримують через веб-браузери. Такі Web-сервери здатні надавати послуги, аналогічні до тих, що пропонуються у глобальній мережі Інтернет. Зокрема, це може включати роботу з гіпертекстовими сторінками, які містять текстову інформацію, гіперпосилання, мультимедійні матеріали (зображення та звукові файли), та оброблення запитів користувачів для доступу до ресурсів чи баз даних. У корпоративному середовищі всі подібні служби публікації розглядаються як інтернет-сервіси незалежно від їхнього локального чи глобального розташування.

Як правило, корпоративна мережа є територіально розподіленою, поєднуючи різні офіси чи структурні підрозділи організації, що можуть бути віддалені один від одного на значну відстань. Її побудова суттєво відрізняється від створення локальних мереж.

Однією з основних задач є оптимізація передавання даних з мінімізацією їх обсягів, при цьому мережа повинна залишатися гнучкою і не обмежувати функціональність додатків чи якість обробки інформації. Процес проектування корпоративної інформаційної системи передбачає кілька ключових етапів, серед яких:

- Аналіз інформаційного забезпечення організації.

- Визначення архітектури системи та вибір апаратно-програмних засобів для її реалізації.

- Розробка або адаптація основних компонентів системи, включно з такими елементами:

- Система управління корпоративною базою даних.

- Засоби автоматизації бізнес-процесів і документообігу.

- Спеціалізовані програмні рішення.

- Системи підтримки прийняття рішень. Реалізація цих кроків забезпечує створення продуктивної корпоративної мережі, здатної задовольнити сучасні вимоги організації та підвищити її ефективність.

1.1.3 Технології, що використовуються в корпоративних мережах

Ethernet є найпопулярнішою технологією для передачі даних у локальних мережах (LAN), де використовуються кабелі для пересилання пакетів між пристроями. Wi-Fi забезпечує бездротовий доступ до мережі через радіохвилі, передаючи інформацію між пристроями й точками доступу. VLAN (Віртуальна Локальна Мережа) створює віртуальні сегменти всередині фізичної мережі, що дозволяє групувати пристрої за різними критеріями, підвищуючи безпеку та ефективність. VPN (Віртуальна Приватна Мережа) забезпечує захищені тунелі для передачі даних через незахищені мережі, такі як Інтернет, шифруючи інформацію для гарантії конфіденційності. Файрвол виступає як засіб безпеки, аналізуючи й фільтруючи мережевий трафік, блокуючи небажані дані та захищаючи від несанкціонованого доступу. Маршрутизація відповідає за вибір найкращих шляхів для передачі даних між сегментами мережі, де роутери визначають найефективніші маршрути. DHCP (Протокол Динамічного Конфігурування Вузлів) автоматизує налаштування IP-адрес і інших параметрів підключення, значно спрощуючи управління мережею. Active Directory надає централізоване управління ідентифікацією та доступом, дозволяючи створювати облікові записи та визначати політики доступу. Вона також забезпечує централізоване адміністрування завдяки механізмам аутентифікації й авторизації, впроваджуючи мережеві політики безпеки щодо паролів та контролю доступу. Active Directory використовує бази даних для швидкого доступу до інформації і забезпечує резервне копіювання. Інтеграція з продуктами Microsoft, як-от Exchange Server, SharePoint і Azure, робить її важливим елементом корпоративної інфраструктури і забезпечує єдину точку управління, спрощуючи управління ресурсами й підвищуючи безпеку в мережах.

1.2 Аналіз VPN технологій

1.2.1 Загальні дані

VPN (віртуальна приватна мережа) - це термін, що описує технологію створення захищеного з'єднання через ненадійні або загальнодоступні мережі шляхом тунелювання та криптографії.

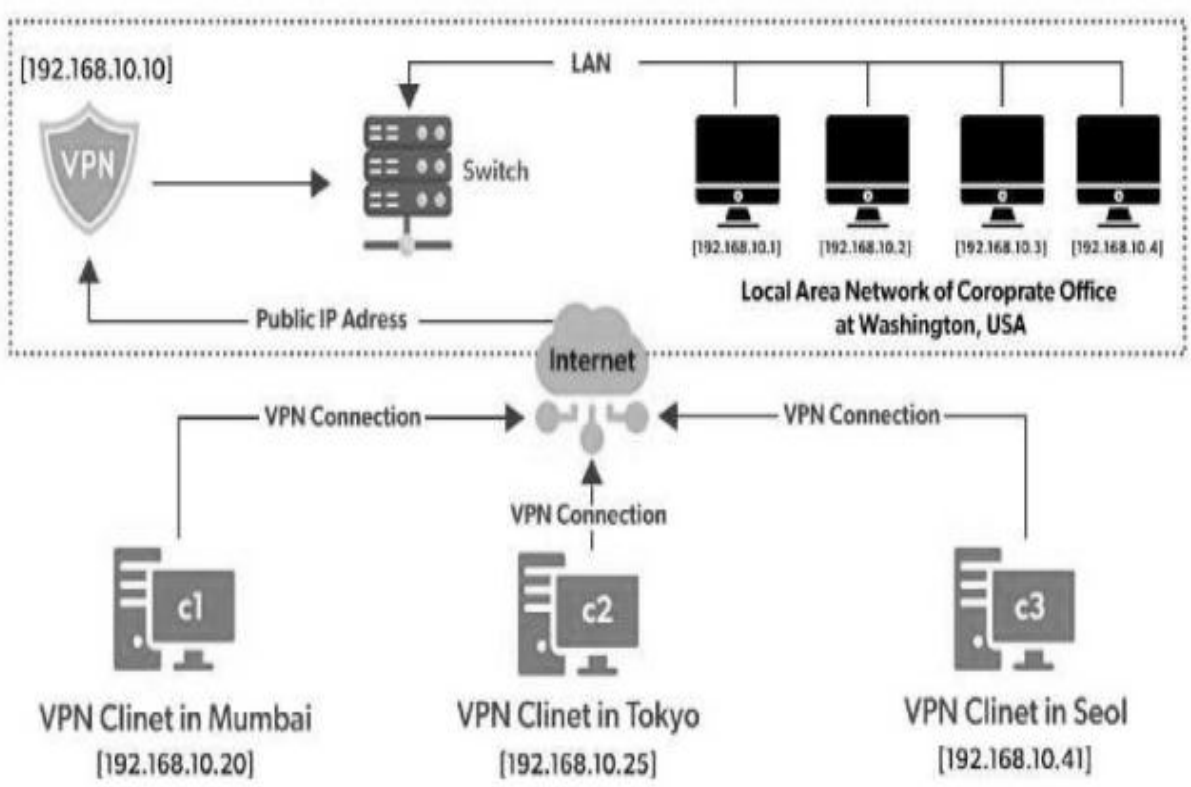

Рисунок 1.1 - Ілюстрація VPN

VPN (віртуальні приватні мережі) забезпечують можливість об'єднувати три типи вузлів: вузол до вузла, вузол до мережі та мережу до мережі. Ця технологія використовує Інтернет як транспортний засіб для передачі IP-трафіку, вирішуючи завдання підключення кінцевих користувачів до віддалених мереж або з'єднання між декількома локальними мережами. Основними компонентами VPN є канали глобальної мережі, захищені протоколи і маршрутизатори. Зазвичай VPN-пристрій розташовується між локальною мережею та Інтернетом з обох сторін з'єднання. Перед передачею даних через VPN вони потрапляють до однієї кінцевої точки та проходять через тунель до точки призначення. Цей

процес називають "тунелюванням" — створенням захищеного логічного тунелю у мережі Інтернет, який поєднує дві точки. Тунелювання маскує особисту інформацію, роблячи її недоступною для інших користувачів мережі. Перед входом у тунель всі дані шифруються, що забезпечує додатковий рівень безпеки.

Протоколи шифрування залежать від типу тунелювання, (рис 1.2) який підтримується конкретним VPN-рішенням. Одним із ключових критеріїв вибору VPN є набір автентифікаційних протоколів, які воно здатне підтримувати. Найпопулярнішим стандартом у цій сфері є сімейство X.509. Удосконалена автентифікація гарантує високий рівень захисту від несанкціонованого доступу. Завдяки цьому VPN стала основним елементом комплексних систем захисту інформації, які необхідні для функціонування державних, комерційних та приватних організацій як у межах офісу, так і віддалено.

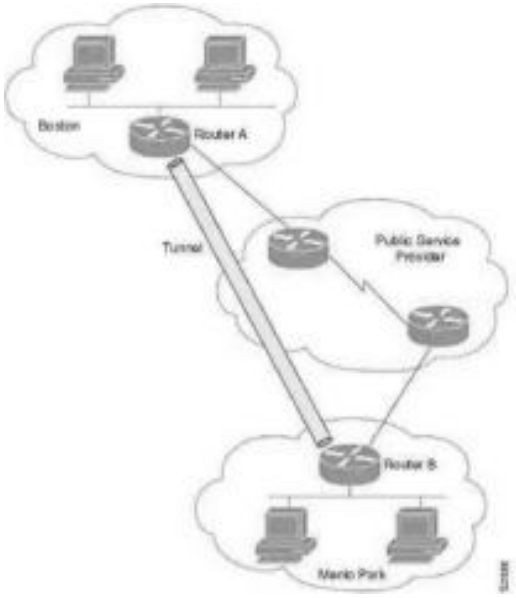

Рисунок 1.2 - Схема взаємодії мереж через тунель

Особливий попит на VPN зріс під час віддаленої роботи, спричиненої карантинними обмеженнями. Організації почали активно використовувати цю технологію для захисту переданих даних та безпечного підключення до корпоративних сервісів через Інтернет.

VPN має унікальні переваги у сфері організації мережевого доступу, зокрема усунення необхідності в комутованих з'єднаннях чи виділених лініях. За допомогою VPN користувач може отримати доступ до корпоративної мережі з будь-якої точки світу через Інтернет. Хоча ці дані передаються мережею загального доступу, вони залишаються захищеними завдяки шифруванню, де доступ до них має лише власник. Зокрема, одним із поширених алгоритмів шифрування є Triple DES, що використовує потрійне шифрування з трьома різними ключами. Таким чином, використання VPN дає змогу не лише забезпечити безпечне передавання даних, але й створити гнучку та функціональну інфраструктуру для сучасних організацій.

Достовірність даних забезпечується шляхом перевірки їхньої цілісності та ідентифікації користувачів, які використовують VPN. Це дозволяє переконатися, що інформація була доставлена до адресата без спотворення чи змін. Найпоширеніші алгоритми для забезпечення цілісності даних включають MD5 і SHA1. Далі система аналізує можливі зміни даних під час їх передачі мережею, з’ясовуючи, чи це було результатом зловмисних дій або випадкових помилок. Отже, основною метою створення VPN є забезпечення захищеного доступу через спеціальні тунелі між кількома локальними мережами або віддаленими користувачами. Для ефективної роботи VPN необхідно використовувати засоби шифрування трафіку як на вихідному, так і на вхідному етапах. Це може бути реалізовано як програмним способом, так і апаратно-програмними рішеннями, сумісними з будь-якими операційними системами, незалежно від того, чи мова йде про комп’ютер, чи мобільний пристрій. Таким чином, можна зробити висновок, що автентифікація та шифрування є невіддільними складовими безпечного з’єднання.

Безпечний віртуальний VPN забезпечує інтеграцію локальних мереж та комп'ютерів через відкриті зовнішні середовища передачі даних, створюючи єдину віртуальну корпоративну мережу з надійним захистом інформації, що циркулює всередині організації. При підключенні корпоративної локальної мережі до відкритої зовнішньої мережі існують такі потенційні ризики:

- Несанкціонований доступ (НСД) до даних компанії, що передаються відкритими каналами;

- НСД до внутрішніх ресурсів локальної мережі, який може бути здійснений після перехоплення доступу до мережі зловмисником. Захист даних у процесі передачі через відкриті канали ґрунтується на таких основних функціях:

- автентифікація учасників взаємодії;

- криптографічне шифрування переданих даних;

- перевірка точності та цілісності трансльованої інформації.

Ці функції є взаємопов'язаними й впроваджуються за допомогою методів криптографічного захисту інформації (КЗІ). Для запобігання НСД із зовнішнього середовища до корпоративних систем менеджменту (КСМ) застосовують міжмережеві екрани, які забезпечують безпеку інформаційного обміну шляхом фільтрації повідомлень. Міжмережевий екран функціонує на стику локальної та відкритої мереж. У випадку необхідності захисту окремого комп’ютера, підключеного до відкритої мережі, використовують спеціалізоване програмне забезпечення міжмережевого екрану .

Сучасний системний адміністратор регулярно налаштовує VPN-канали для співробітників, які працюють віддалено від мережі організації. Це можна продемонструвати, наприклад, на Рис. 1.1. Ще одним прикладом є VPN для двох офісних мереж, показаний на Рис. 1.2, де відбувається об’єднання окремих пристроїв або локальних мереж у єдину віртуальну мережу. Такий підхід забезпечує збереження цілісності та конфіденційності даних, що передаються.

Існує безліч способів і технологій для створення віртуальних тунелів, серед яких варто виділити такі основні:

1. L2TP - це транспортний протокол, який сам по собі не відповідає за шифрування чи захист конфіденційності даних. Його безпека забезпечується за рахунок використання інкапсульованих протоколів, найчастіше IPsec. У поєднанні з IPsec цей метод відомий як L2TP/IPsec.

2. IPSec - набір протоколів, що гарантують безпечну передачу даних на мережевому рівні. Такий підхід включає шифрування та інші методи захисту інформації, що передається між двома мережами.

3. OpenVPN - відкрите програмне рішення, підтримуване спільнотою розробників. Використовує криптографічну бібліотеку OpenSSL і пропонує декілька варіантів автентифікації, що робить його гнучким та надійним варіантом.

4. WireGuard - також проект з відкритим кодом. Його розробка спрямована на спрощення використання VPN, покращення продуктивності та зменшення можливих ризиків атаки. Технологія базується на сучасних методах шифрування та автентифікації.

Детальніше про кожну з цих технологій буде розглянуто далі.

1.2.2 L2TP

L2TP, хоча і функціонує подібно до протоколів канального (другого) рівня моделі OSI, фактично належить до сеансового (п’ятого) рівня. Він запозичує та доповнює переваги PPTP і L2F. Серед успадкованих особливостей — відсутність вбудованого механізму шифрування даних без використання додаткових технологій. У якості транспортного протоколу L2TP застосовує виключно UDP. Для забезпечення захисту інформації зазвичай використовують протоколи IPsec. У таких випадках можливе використання протоколів AH, ESP і IKE. Проте додатковий етап обробки даних, який виникає при цьому, може знижувати швидкість з’єднання.

Переваги, які вирізняють L2TP:

1. Висока гнучкість, легкість і швидкість налаштування зв’язку;

2. Універсальність — можливість адаптації до будь-яких методів шифрування;

3. Широка популярність і розповсюдженість протоколу, що спрощує його інтеграцію.

Ще однією перевагою L2TP є те, що клієнтські системи не потребують установлення додаткового програмного забезпечення для взаємодії з VPN-серверами. Базове ПЗ для роботи з цим протоколом зазвичай вже інтегроване в операційні системи, такі як Windows, macOS, iOS, Android та Linux.

1.2.3 IPsec

IPsec (або IP Security) — це комплекс протоколів, розроблений для створення захищених з'єднань у мережах. Він базується на стандарті IP, який визначає способи передачі інформації через Інтернет, але доповнює його шифруванням та автентифікацією для підвищення безпеки. Варто підкреслити, що IP сам по собі не входить до складу IPsec; натомість IPsec діє безпосередньо поверх нього, забезпечуючи підтримку транспортних протоколів, таких як TCP і UDP.

Ключові переваги IPsec включають:

1. Тунелі та VPN на основі IPsec забезпечують автентифікацію користувачів і шифрування даних, що запобігає несанкціонованому доступу до корпоративних мереж.

2. Шифрування даних у тунелях IPsec гарантує конфіденційність та цілісність інформації в процесі передачі між різними пристроями та мережами.

3. Захист мережевих даних досягається шляхом створення зашифрованих каналів зв’язку.

4. Швидка автентифікація отриманих даних дозволяє підтвердити, що вони приходять від довіреного джерела.

Шифрування в IPsec реалізується програмно для захисту вмісту даних. Платформа підтримує широкий спектр алгоритмів шифрування, серед яких AES, Blowfish, Triple DES, ChaCha та DES-CBC. Використовуються як симетричні, (рис 1.3) так і асиметричні методи (рис 1.4). Спочатку встановлюється з'єднання через асиметричне шифрування, після чого система переходить до використання симетричного шифрування для пришвидшення процесу передачі даних. IPsec

може працювати в двох режимах: тунельному (tunnel mode) і транспортному (transport mode). У тунельному режимі весь IP-пакет (як заголовок, так і корисне навантаження) шифрується і вкладається в інший IP-пакет. Цей режим забезпечує високий рівень безпеки. У транспортному режимі шифрується лише корисне навантаження пакета, залишаючи заголовок незміненим. Такий підхід є вигіднішим для надійних мереж, наприклад, для прямого з'єднання між двома пристроями. IPsec також слугує ефективним захистом від атак повторення (Replay Attacks), зокрема атак типу "Man-in-the-Middle". Для цього IPsec присвоює унікальні порядкові номери кожному пакету і перевіряє їх для визначення можливого дублювання або перехоплення даних під час маршрутизації. Для створення IPsec-тунелю обидва кінці з'єднання повинні мати налаштовані протоколи IPsec та ключі шифрування. Налаштування тунелів можливе за допомогою таких протоколів, як ESP, AH і IKE, які забезпечують різні рівні автентифікації та шифрування. Однією з найпоширеніших сфер застосування IPsec є VPN у екстранет-системах. Під час налаштування тунелів VPN із використанням IPsec необхідно дотримуватися специфічних процедур і практик забезпечення безпеки для досягнення максимального рівня захищеності. Налаштування IPsec-тунелів або VPN здійснюється через спеціалізоване програмне забезпечення. Воно може бути встановлене як на мережевому обладнанні, так і на персональних пристроях користувачів. Багато сучасних операційних систем, таких як Windows і MacOS, пропонують інтегровані засоби для налаштування IPsec і VPN, що дозволяє використовувати ці функції без додаткових інсталяційного ПЗ.

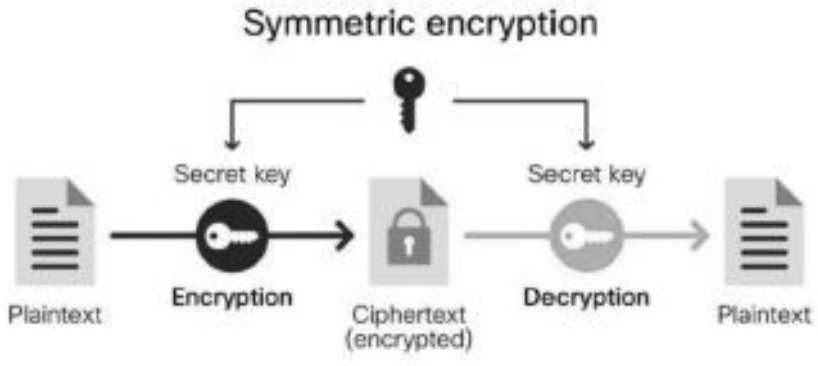

Рис. 1.3 - Симетричне шифрування

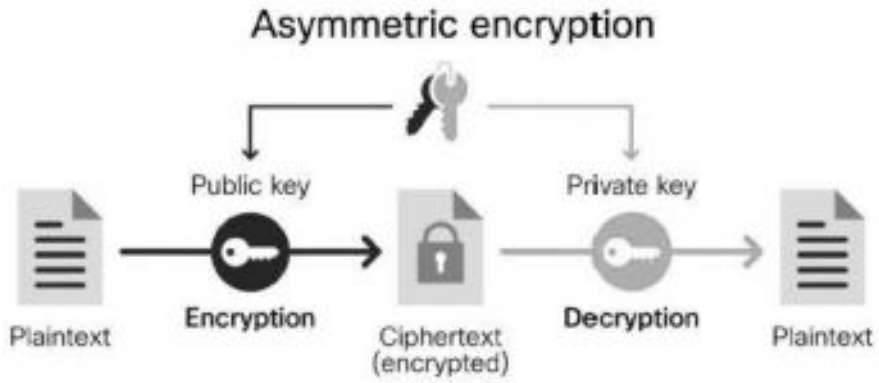

Рис. 1.4 - Асиметричне шифрування

1.2.4 OpenVPN

OpenVPN підтримує роботу з транспортними протоколами TCP та UDP і функціонує як у режимі точка-точка, так і клієнт-сервер. Він дозволяє створювати з'єднання між пристроями, що знаходяться за NAT або мережею з фаєрволом, без потреби в додаткових налаштуваннях. (рис 1.5)

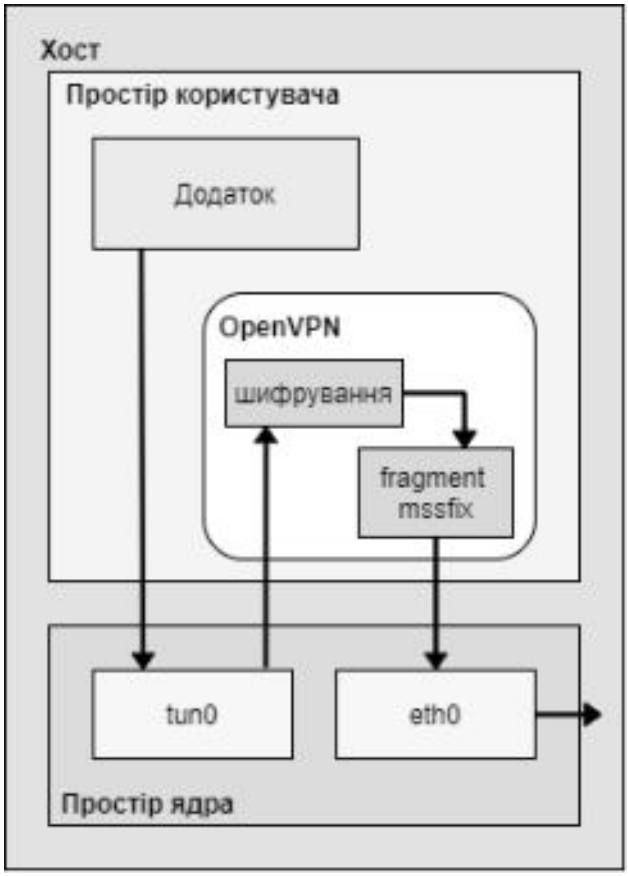

Рисунок 1.5 – Модель передачі трафіку від клієнта OpenVPN

Існують дві основні версії OpenVPN: Community Edition і Access Server. Перша є вільним і відкритим програмним забезпеченням, що виступає основою для другої версії. Access Server додає платні функції, такі як інтеграція з LDAP, SMB-сервер, веб-інтерфейс адміністрування та інші інструменти, які значно полегшують розгортання та управління.

Серед ключових переваг OpenVPN можна виділити:

1. Відкритий вихідний код і безкоштовність у базовій версії.

2. Простота встановлення та налаштування.

3. Наявність широкого спектра алгоритмів шифрування й аутентифікації користувачів.

4. Сумісність із великою кількістю операційних систем.

Однією з визначальних рис OpenVPN є можливість розширення функціоналу завдяки підтримці плагінів та користувацьких скриптів від сторонніх розробників. Окремо варто зазначити, що використання як TCP, так і UDP робить OpenVPN більш адаптивною альтернативою IPsec у випадках, коли провайдер блокує певні протоколи VPN. Однак потрібно враховувати, що при роботі з TCP продуктивність залишається стабільною лише за достатньої пропускної здатності мережі. Якщо ж пропускна здатність виявиться недостатньою, ефективність роботи системи різко знижується через відому проблему "TCP Meltdown Problem". Для шифрування й підписування трафіку OpenVPN застосовує власний формат HMAC, який може бути ввімкнений за бажанням для додаткового захисту з’єднання. За замовчуванням сервіс використовує бібліотеку OpenSSL для шифрування каналів даних і керування. OpenVPN також підтримує SSL/TLS та інші протоколи, але не сумісний із IKE, IPsec, L2TP чи PPTP. Програма має підтримку криптографічних ключів PKCS#11 і забезпечує апаратне прискорення процесів шифрування. OpenVPN підтримує IPv6 як усередині тунелю, так і зовні, під час встановлення з’єднання. Вона здатна працювати через більшість проксі-серверів (зокрема HTTP) та файрволів. Додатково є можливість створення IP-тунелів (TUN) на основі третього рівня або Ethernet-тунелів (TAP) на основі другого рівня моделі OSI, що дозволяє

передавати будь-який тип трафіку. Опціонально може використовуватись бібліотека стиснення LZO для зменшення об’єму даних у потоці.

1.2.5 WireGuard

WireGuard – це вільне та відкрите програмне забезпечення і протокол зв’язку, який проектувався із фокусом на спрощене використання, високу продуктивність і мінімізацію ймовірностей для атак.

Основними перевагами WireGuard є:

1. Вільний доступ і відкритий вихідний код.
2. Найвищий рівень безпеки завдяки використанню сучасних криптографічних алгоритмів.
3. Дуже швидке встановлення та підтримка з’єднань.
4. Простота адаптації до змін середовища (наприклад, перехід між Wi-Fi та стільниковими мережами).
5. Компактний і зрозумілий код для полегшення роботи з ним.

Як і OpenVPN, WireGuard підтримує розширення функціональності за допомогою сторонніх додатків і скриптів, проте саме цей протокол максимально ефективно використовує цю можливість. Виключення специфічних і складних операцій із ядра значно покращує стабільність та рівень безпеки роботи програми. На основі здобутого досвіду OpenVPN, WireGuard використовує виключно UDP, щоб уникнути недоліків TCP-over-TCP. Протокол підтримує IPv6 як всередині тунелю, так і поза ним, а також інтеграцію IPv4 та IPv6 один в одного. Він орієнтований лише на роботу з третіми рівнями моделі OSI. WireGuard базується на найпрогресивніших методах шифрування: X25519, ChaCha20, Poly1305, SipHash і BLAKE2s, при цьому є можливість додаткового симетричного шифрування через PSK. (таблиця 1.1)

Таблиця 1.1

Криптографічні алгоритми WireGuard

Алгоритми	Призначення
ChaCha20	Для симетричного шифрування
Po1y1305	Для автентифікації
CURVE25519	Для еліптичної кривої Діффі-Хеллмана
BRAKE2s	Для хешування
SipHash24	Для ключів хеш-таблиці
HKDF	Для отримання ключів
Perfect Forward Secrecy	Для захисту даних користувачів

Однією з ключових особливостей WireGuard є те, що він не встановлює постійного з'єднання. Автентифікація відбувається вже в першому запиті за допомогою хендшейку, в процесі якого створюються симетричні ключі для передачі даних. Таким чином, WireGuard демонструє поєднання сучасної технології шифрування, високої продуктивності та ефективного захисту від більшості потенційних загроз. (рис 1.6)

Рис 1.6 – Приклад роботи WireGuard

Цей механізм здійснює ротацію ключів кожні кілька хвилин, що дозволяє зберігати високий рівень секретності. Сервіс не відповідає неавторизованим запитам, залишаючи сервер «невидимим» для сторонніх клієнтів. Хендшейковий підхід також захищає від потенційних атак на сервіс, які спрямовані на перевантаження обробкою неавтентифікованих пакетів. Проте існує певний

ризик для атак повторення, де зловмисник може відтворити початковий запит хендшейка, примушуючи сервер знову генерувати ефемерний ключ і тимчасово відключати легітимного клієнта. Щоб мінімізувати подібні ризики, кожен перший запит містить мітку часу TAI64N. Сервер фіксує найновішу отриману мітку і автоматично ігнорує пакети із такою ж або більш старою міткою часу. Завдяки цьому зловмисники не можуть вплинути на активну сесію між клієнтом та сервером. Додатково використовується 64-бітний лічильник для забезпечення унікальності значень, що унеможливлює повторне використання або зміни порядку даних під час передачі.

РОЗДІЛ 2.
ОБГРУНТУВАННЯ ТА ВИБІР ОБЛАДНАННЯ ТА VPN ПРОТОКОЛУ ДЛЯ ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Порівняння та вибір VPN Протоколів

Основні характеристики найбільш популярних VPN-протоколів були ретельно проаналізовані, а результати цього аналізу систематизовані та представлені у таблиці 2.1. У ній наочно продемонстровані ключові особливості кожного протоколу, які дозволяють порівняти їх функціональні можливості, рівень безпеки, продуктивність та інші важливі параметри для подальшого вибору оптимального рішення.

Таблиця 2.1

Загальна характеристика VPN-протоколів

Критерії	L2TP/IPSec	OpenVPN	WireGuard
Рік випуску	1995 (IPSec), 1999 (L2TP)	2001	2015
Дизайн	Комплексний і складний	Складний	Простий і компактний
Доступність	Windows, Linux, macOS та ін.	Windows, Linux, macOS та ін.	Windows, Linux, macOS та ін.
Вбудовуваність	Windows, Linux, macOS та ін.	Ні	Linux
Блокування брандмауерами	Так	Малоймовірно	Малоймовірно
Налаштування	Швидке і легке	Гнучке, але складне	Негнучке, але просте

Під час вибору VPN-протоколу одним із ключових аспектів, на який слід звернути увагу, є рівень безпеки. (таблиця 2.2)

Проаналізувавши узагальнену характеристику, можна зробити такі висновки: найсучаснішу криптографію використовує WireGuard, він суворо контролює криптографічні примітиви і гарантує надійне шифрування пакетів даних, але цей протокол має деякі проблеми з конфіденційністю, для їх усунення необхідно виконувати додаткові налаштування VPN.

Таблиця 2.2

Характеристика безпеки VPN-протоколів

Критерії	L2TP/IPSec	OpenVPN	WireGuard
Вихідний код	У цій комбінації закритий	Відкритий	Відкритий
Автентифікація	За допомогою AH та ESP	Гнучка, TLS і сертифікати	Відкриті ключі, Po1y1305 для автентифікації
Шифрування	За допомогою ESP, AES-256 або інші шифри	Гнучке, AES-256 або інші шифри	ChaCha20 для симетричного шифрування
Цілісність	Хешування, різні алгоритми	Хешування, різні алгоритми	Хешування, BLAKE2S
Запобігання відтворенню	Поля порядкових номерів	64-бітні і 32-бітні ідентифікатори	96-бітні позначки часу TAI64N
Конфіденційність	Забезпечує, але підозрюється у зламі NSA	Забезпечує	Забезпечує, але має недоліки

OpenVPN, навпаки, пропонує гнучкі криптографічні алгоритми для автентифікації, шифрування та забезпечення цілісності даних, це дозволяє побудувати таку структуру безпеки, яка буде відповідати конкретній моделі загроз, цей протокол також забезпечує найкращу конфіденційність з усіх розглянутих протоколів.

Другим фактором є продуктивність (таблиця 2.3)

Таблиця 2.3

Характеристика продуктивності VPN-протоколів

Критерії	L2TP/IPSec	OpenVPN	WireGuard
Порт з’єднання	Фіксований порт UDP або TCP	Будь-який порт UDP або TCP	Будь-який порт UDP
Швидкість	Швидкий	Посередній	Дуже швидкий
Затримка	Середня	Найбільша	Найменша
Контекст виконання	У просторі ядра	У просторі користувача	У просторі ядра в Linux, у просторі користувача
Роумінг	Не підтримує	Не підтримує	Підтримує завдяки маршрутизації криптоключів
Стабільність	Стабільний	Дуже стабільний	Дуже стабільний

L2TP/IPSec загалом вважається надійним та безпечним, він використовує криптографічні алгоритми, які заслуговують на довіру, але цей протокол потенційно скомпрометовано NSA, тому він може викликати скептичне ставлення з боку прихильників конфіденційності.

Проаналізувавши , можна зробити такі висновки:

Найшвидшим з розглянутих протоколів є WireGuard, він використовує виключно порт UDP для з’єднань і може працювати у просторі ядра, а ще цей протокол підтримує роумінг пристроїв завдяки своїй концепції маршрутизації криптоключів. (рис 2.1)

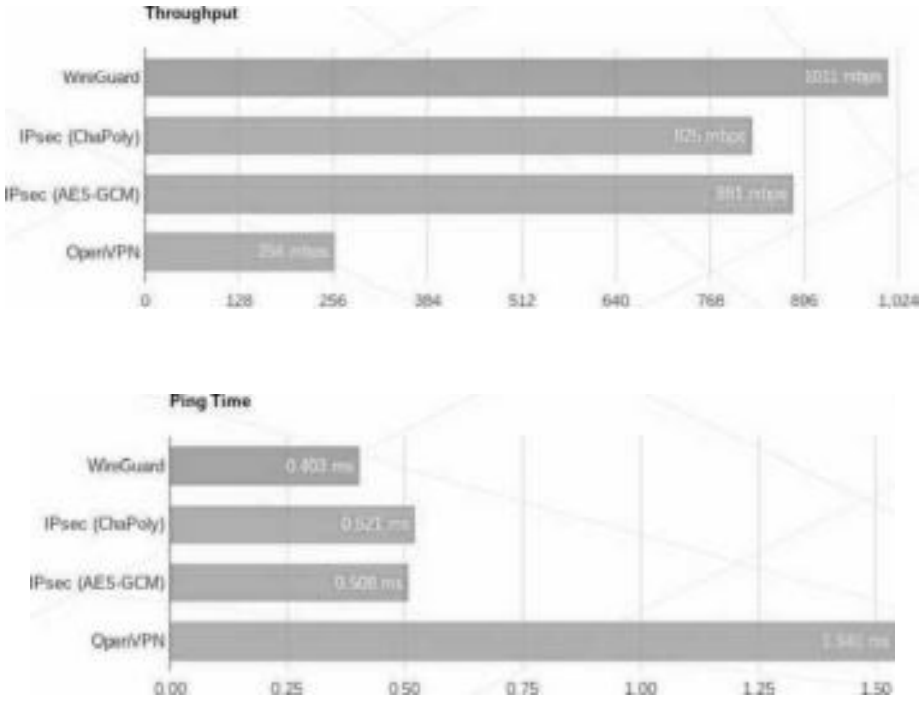

Рисунок 2.1 - Результати тестів продуктивності від розробників WireGuard

L2TP/IPSec так само демонструє непогані показники продуктивності, коли використовує порт UDP і працює в просторі ядра, але цей протокол має деякі виклики конфігурації, що можуть вплинути на його стабільність;

OpenVPN виявився не дуже швидким у порівнянні з іншими протоколами і єдиним, що працює виключно у просторі користувача, натомість цей протокол

забезпечує найкращу стабільність, навіть в ненадійних мережах, особливо, коли використовує порт TCP.

WireGuard – це інноваційний і високозахищений VPN-протокол, створений для оперативного та ефективного зв’язку між вузлами мережі. Будучи відносно новим, він уже отримав довіру серед спеціалістів із кібербезпеки завдяки своїй простоті, швидкодії та надійності. Цей протокол орієнтований на сучасні вимоги технологічного середовища, що робить його чудовим вибором для користувачів, які прагнуть мати безпечне VPN-рішення. Із самого початку WireGuard розроблявся для ядра Linux, однак сьогодні він став повністю кросплатформним і чудово функціонує на платформах Windows, macOS, BSD, iOS та Android.

На відміну від застарілих і менш ефективних протоколів, WireGuard пропонує швидкість роботи у поєднанні з посиленою безпекою. Завдяки інтеграції в ядро операційної системи, він працює ближче до апаратного забезпечення, що дозволяє прискорити процеси шифрування та дешифрування даних. Це є ключовим фактором, який надає WireGuard конкурентну перевагу серед інших VPN-протоколів.

У роботі WireGuard забезпечує створення зашифрованого тунелю між двома або більше мережевими інтерфейсами. Для автентифікації він використовує криптографічну систему з відкритим ключем. Кожен клієнт і сервер мають пару ключів: закритий ключ і відповідний відкритий. Відкритий ключ слугує для підтвердження автентичності клієнта чи сервера під час процесу рукостискання. Для встановлення спільного секрету між клієнтом і сервером WireGuard застосовує алгоритм обміну ключами Діффі-Геллмана на основі еліптичних кривих (ECDH). Цей спільний секрет використовують для генерації сеансових ключів, які забезпечують шифрування і дешифрування даних.

Протокол передбачає досконалу пряму секретність (PFS), створюючи унікальний набір сеансових ключів для кожного нового сеансу. Це гарантує, що навіть у разі компрометації ключів попередніх сеансів зловмисник не зможе їх використати для декодування інформації іншого сеансу. Також WireGuard має

високу стійкість до атак, включаючи методи грубої сили, диференціального або лінійного криптоаналізу.

Даний протокол застосовує передові криптографічні методи, зокрема Curve25519 для обміну ключами, ChaCha20 для шифрування і Poly1305 для створення коду автентифікації повідомлень (MAC). Криптографічний MAC є контрольним значенням, що генерується на основі секретного ключа і додається до передаваних даних. Після отримання даних MAC повторно обчислюється та порівнюється з отриманим значенням. У разі збігу значень підтверджується, що дані не зазнали змін під час передачі. В цілому, інтеграція алгоритмів криптографії з відкритим ключем та використання кодів автентифікації повідомлень у протоколі WireGuard забезпечує високий рівень захисту, гарантуючи як цілісність, так і безпечність передачі інформації.

Швидкість та ефективність: WireGuard створено з урахуванням мінімального впливу на навантаження центрального процесора, забезпечуючи високу продуктивність. Його лаконічний код та оптимізовані криптографічні алгоритми дозволяють досягати значно більшої швидкості порівняно з іншими VPN-протоколами, такими як OpenVPN та IPsec, і водночас надають підвищений рівень безпеки. (рис 2.2)

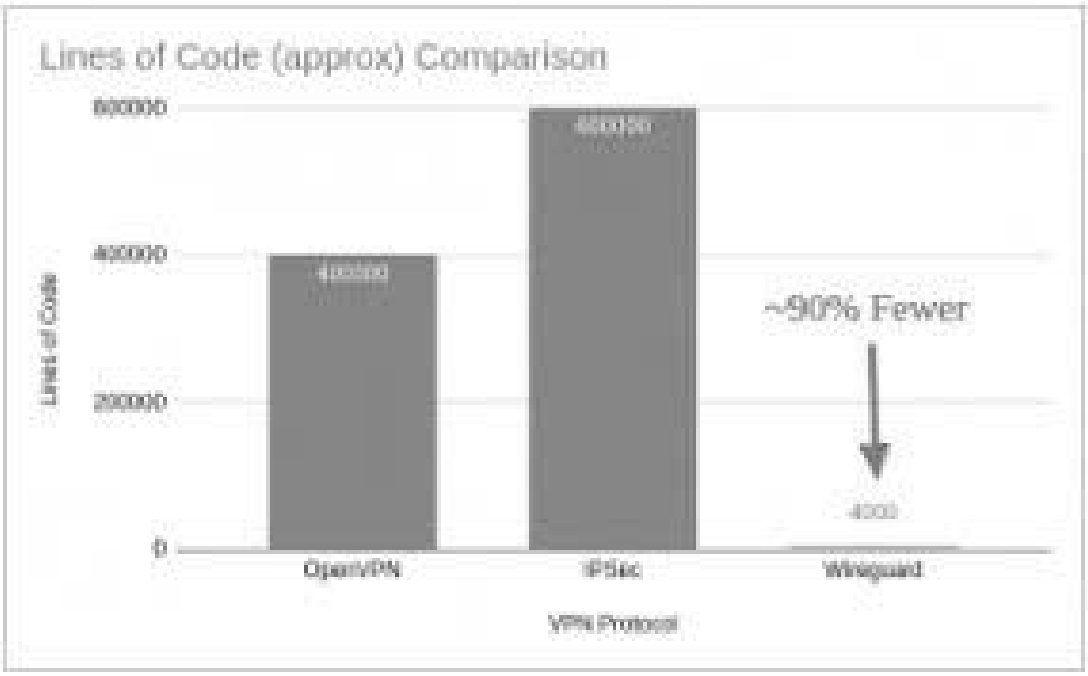

Рис 2.2 - Кількість рядків коду порівнянно з OpenVPN та IPSec

Процес розробки протоколу був спрямований на забезпечення стабільності роботи навіть у разі змін мережевого середовища. Завдяки цьому протокол здатний підтримувати з'єднання, наприклад, при переході з Wi-Fi на мобільний інтернет.

WireGuard пропонує низку важливих переваг, які роблять його популярним вибором як серед кінцевих користувачів, так і серед адміністраторів мереж. Серед основних переваг варто виділити:

Безпека: WireGuard застосовує сучасні криптографічні методи для захисту та забезпечення конфіденційності обміну даними між вузлами мережі. Завдяки використанню досконалої прямої секретності (PFS), навіть у разі компрометації секретного ключа зловмисник не зможе розшифрувати раніше передані або майбутні повідомлення.

Простота налаштування: WireGuard створений з акцентом на доступність, що робить його налаштування легким і зрозумілим. Конфігураційні файли мають просту структуру, а підтримка автентифікації на основі ключів значно полегшує управління проєктами, незалежно від їхнього масштабу.

Кросплатформність: WireGuard підтримується в різних операційних системах, зокрема Linux, Windows, macOS, BSD, iOS та Android. Це забезпечує його гнучкість і робить ідеальним вибором для використання в різноманітних IT-середовищах.

2.2 Вибір обладнання

2.2.1 PfSense

PfSense є дистрибутивом для створення міжмережевого екрану або маршрутизатора, побудованим на основі FreeBSD. Відомий своєю надійністю, pfSense пропонує функції, які зазвичай зустрічаються лише в дорогих комерційних рішеннях. Його налаштування виконується через зручний веб-інтерфейс, що дозволяє використовувати pfSense навіть без знань базової

системи FreeBSD. Зазвичай ці мережеві пристрої використовуються як периметрові брандмауери, маршрутизатори, DHCP/DNS-сервери та VPN технології у топології hub/spoke. Ця система може бути встановлена на більшості звичайних апаратних засобів, включаючи старі персональні комп'ютери та вбудовані системи. Завдяки веб-інтерфейсу процес налаштування і адміністрування спрощується навіть для користувачів з мінімальними знаннями мереж.

Для роботи з маршрутизатором зазвичай не потрібно використовувати термінал або редагувати конфігураційні файли. Оновлення програмного забезпечення також запускаються через веб-інтерфейс. pfSense виконує роль маршрутизатора та брандмауера і зазвичай налаштовано як DHCP та DNS сервери, точка доступу WiFi, та VPN сервер, усе це функціонує на одному апаратному пристрої. За допомогою вбудованого менеджера пакетів, користувачі можуть встановлювати сторонні пакети з відкритим кодом, такі як Snort або Squid, що робить pfSense популярним вибором для багатьох мережевих адміністраторів. PfSense не тільки є потужним і гнучким брандмауером і маршрутизатором, але також пропонує систему пакетів, що забезпечує операційній системі можливість легкого розширення та захисту від потенційних вразливостей.

Завдяки своєму гнучкому дизайну, pfSense може використовуватися як у невеликих домашніх маршрутизаторах, так і для управління цілою корпоративною мережею. У сучасних умовах pfSense все частіше замінює дорогоцінні корпоративні бренди, такі як CISCO, не тільки через свою безкоштовність, але через багатофункціональність і зрілість платформи. PfSense можна встановити на будь-якому обладнанні, включаючи старі комп'ютери з кількома мережевими картами. pfSense регулярно оновлюється і швидко виправляє проблеми безпеки до того ж надаючи повний контроль над мережею. (рис 2.3)

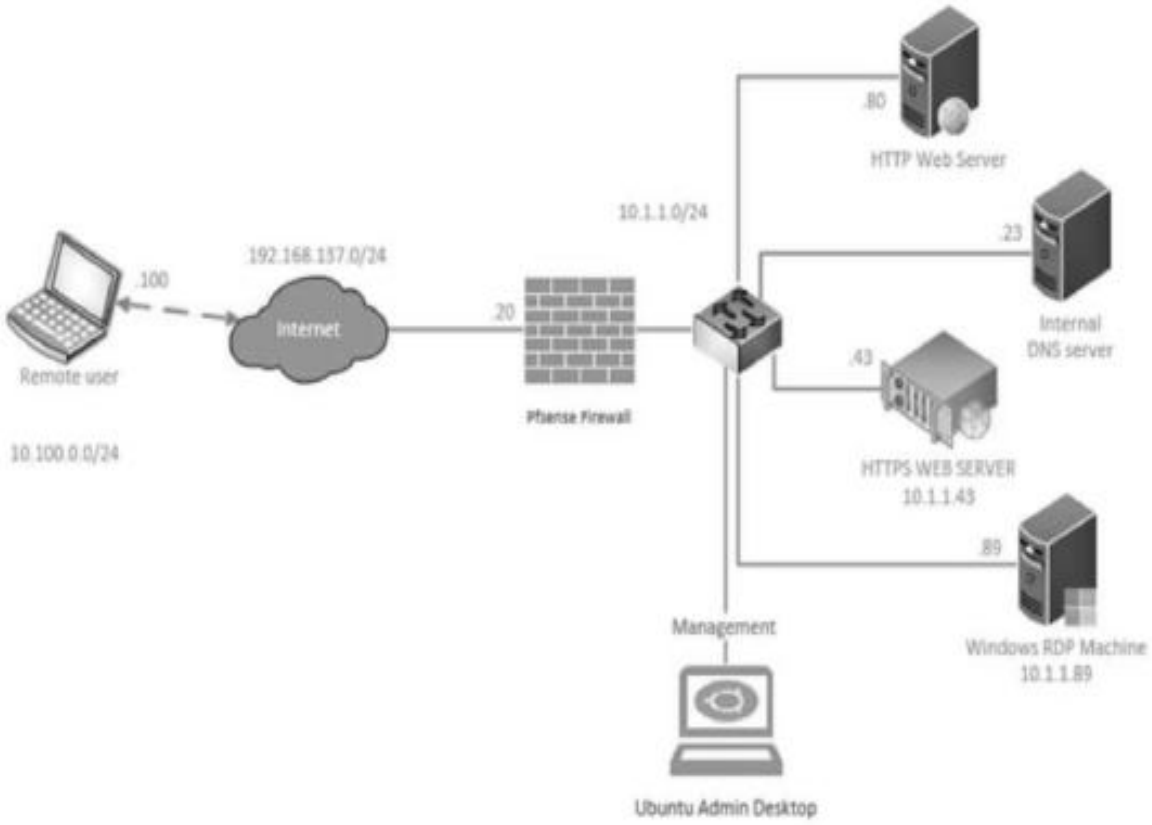

Рис. 2.3 Схема роботи мережевого екрану PfSense

2.2.2 Mikrotik

MikroTik — латвійська компанія, що спеціалізується на розробці мережевого обладнання та програмного забезпечення для нього. Її продукція позиціонується в напівпрофесійному сегменті, який суттєво перевершує за функціональністю та надійністю звичайні домашні маршрутизатори, такі як TP-Link, Xiaomi тощо. Обладнання цих брендів здатне задовольнити лише невибагливих користувачів, оскільки значно поступається за можливостями, потужністю та рівнем безпеки. Разом з тим, порівнювати MikroTik із професійними мережевими рішеннями теж непросто. Наприклад, Cisco славиться найвищим рівнем надійності, цілодобовою технічною підтримкою та рядом додаткових переваг. Проте, за функціональністю MikroTik майже не відстає від більш дорогого професійного обладнання.

Компанія впроваджує численні можливості у свої пристрої, такі як налаштування міжмережевих екранів, підтримка різних типів VPN, реалізація

роумінгу та багато іншого. Ключовим фактором при виборі залишається ціна: модель Wi-Fi роутер MikroTik hAP ac lite (RB952Ui-5ac2nD), яка є популярною, коштує близько $56. Серед конкурентів MikroTik можна виділити Ubiquiti, проте ця компанія акцентує увагу переважно на бездротових мережах: стабільному покритті, якісному роумінгу, реалізації технологій MIMO тощо. Водночас MikroTik забезпечує більшу гнучкість налаштувань для створення безпечних і відмовостійких мереж із широкими можливостями управління, що робить його більш стабільним у цьому сегменті. Саме тому компанія була обрана як об’єкт дослідження.

Також варто зазначити, що MikroTik продає RouterOS як окремий програмний продукт, адаптований до архітектури x86, що дозволяє розгортати його на власному обладнанні. Це створює додатковий простір для його використання у різних проєктах..

Підсумовуючи, MikroTik RouterOS є самостійною операційною системою та потужним засобом для вирішення широкого спектру мережевих завдань.

РОЗДІЛ 3.
ПОБУДОВА КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ VPN-ТЕХНОЛОГІЇ

3.1 Реалізація Wireguard сервера на платформі PfSense

3.1.1 Встановлення додаткового пакету

Перш ніж приступати до встановлення та налаштування WireGuard, дуже важливо належним чином підготувати pfSense. По-перше, потрібно перевірити перевірити версію pfSense і сумісність, оскільки WireGuard підтримується на pfSense версії 2.5.0 і новіших. Після підтвердження сумісності наступним кроком є встановлення пакета WireGuard. Для цього переходимо до розділу System - Package Manager - Available Packages, знаходимо пакет WireGuard та виконуємо його інсталяцію. (рис 3.1)

Рис 3.1- Встановлення пакету WireGuard

3.1.2 Налаштування

Для налаштування тунелю потрібно перейти у розділ VPN – WireGuard – Tunnels, та створити новий тунель: вказати назву (наприклад, tun_wg0), порт для прослуховування (зазвичай 51820) та згенерувати приватний ключ. (рис 3.2)

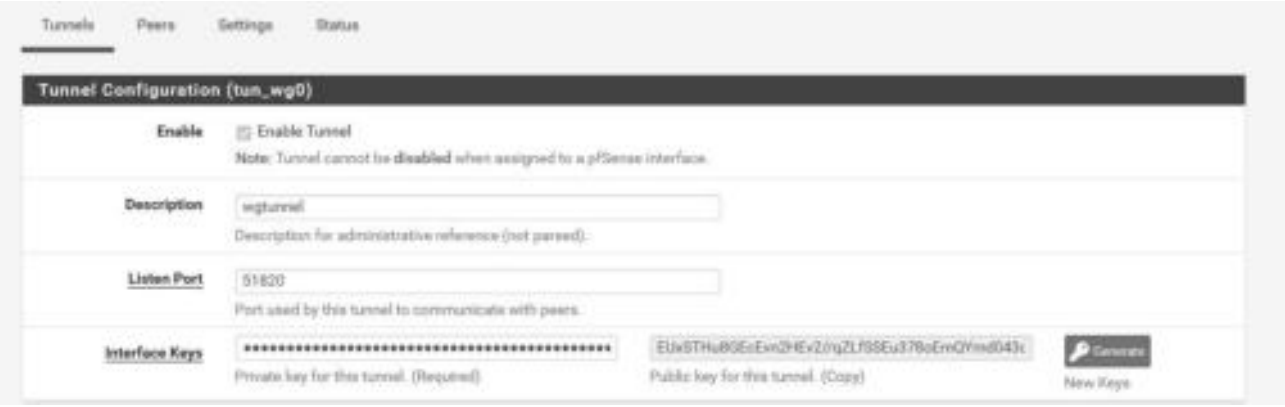

Рис 3.2 - Приклад створеного тунелю

Далі потрібно стоворити Peers, VPN – WireGuard – Peers (рис 3.3)

Рис 3.3 - Налаштування Peers

Тут можна вказати такі налаштування:

Tunnel – обираємо тунель з яким буде працювати даний Peer.

Description – вказуємо назву Peer.

Dynamic Endpoint – залишаємо активним, тому що користувач буде підключатись з різних місць

Keep Alive – У багатьох випадках клієнти VPN перебувають за NAT або брандмауером, які автоматично закривають "неактивні" з'єднання через певний час. Keep Alive дозволяє відправляти регулярні пакети, щоб запобігти цьому, Обираємо 10 сек.

Public Key – вставляємо публічний ключ клієнта-пристрою з якого буде підключення

Allowed IPs - вказуємо 10.10.20.0/24 , мережа нашого Wireguard тунеля

3.2 Налаштування клієнта WireGuard

3.2.1 Налаштування клієнта на основі обладнання Mikrotik

Налаштування клієнтської частини VPN на основі протоколу WireGuard для обладнання Mikrotik може здатися непростим на перший погляд, проте процес можна виконати без значних труднощів. Слід лише дотримуватися відповідних кроків і враховувати ключові налаштування та нюанси.

Перш за все, необхідно переконатися, що наше обладнання Mikrotik підтримує роботу з WireGuard. Для цього потрібно оновити операційну систему RouterOS до версії 7 або вище, оскільки підтримка WireGuard з’явилась саме в цьому випуску.

Для початку відкриваємо інтерфейс RouterOS (будь то WinBox чи веб-інтерфейс) і створюємо інтерфейс WireGuard. Це робиться в розділі IP → Interfaces. Нам потрібно натиснути кнопку додавання нового інтерфейсу і обрати тип WireGuard. Задати йому відповідну назву, наприклад wireguard1, для зручності використання у подальшій конфігурації.

Далі слід виконати налаштування параметрів WireGuard. У розділі налаштувань інтерфейсу вказуємо приватний ключ, який генерується автоматично через натискання значка оновлення поруч із полем. Зазначаємо порт, який використовуватиметься для підключення. (рис 3.4)

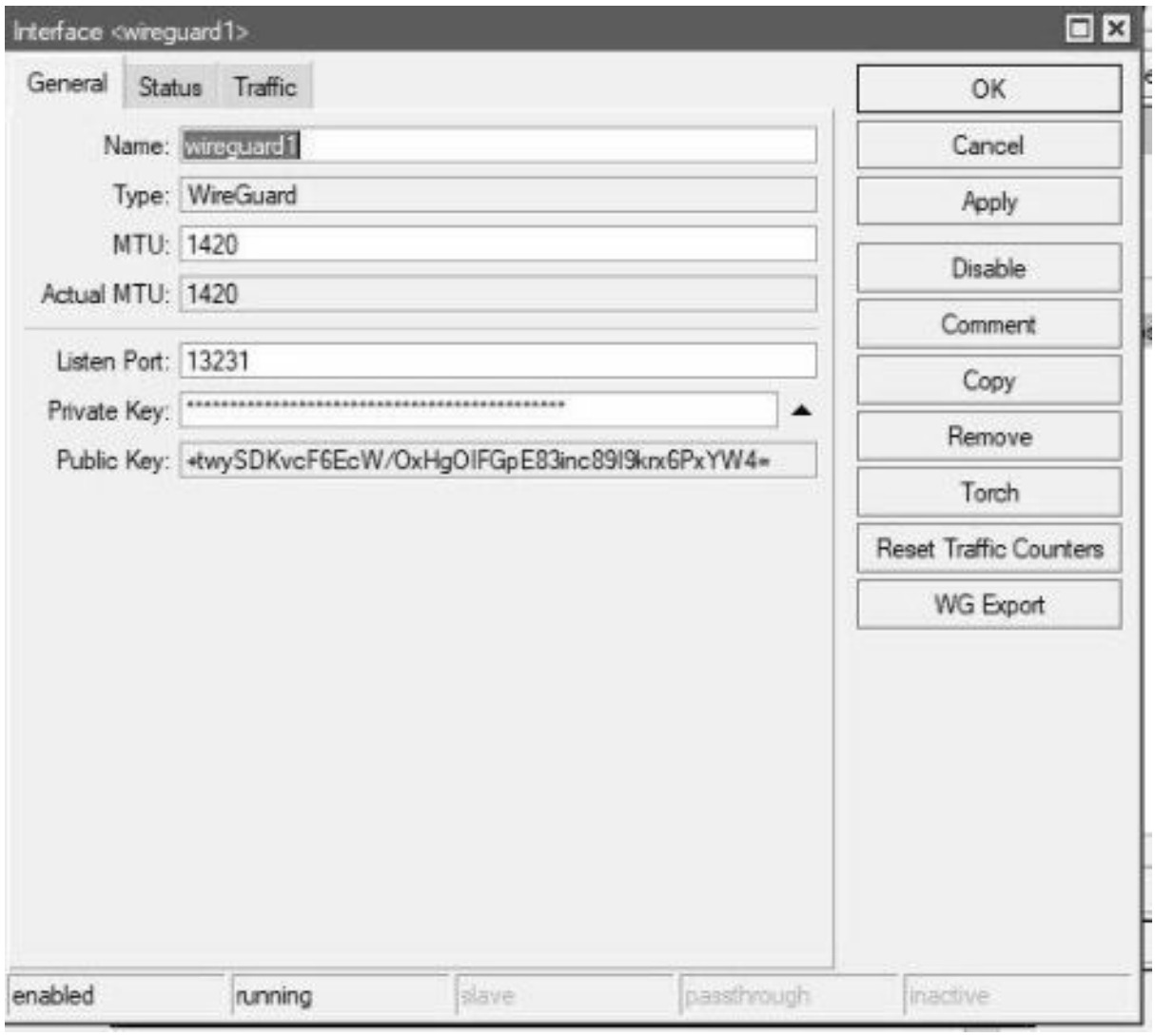

Рис. 3.4 - Створення інтерфейсу Wireguard

Наступним кроком є створення пірів (peers). Це список довірених вузлів, з якими обладанання Mikrotik може встановлювати зв'язок. Додаємо peer і вказуємо публічний ключ сервера WireGuard, адресу його кінцевої точки (endpoint), а також діапазон адрес, доступ до яких буде дозволений через цей VPN-з'єднання (Allowed IPs). (рис. 3.5)

Рис 3.5 Створення Peer

Далі потрібно задати IP-адресу для нашого WireGuard-інтерфейсу відповідна нашій мережевій архітектурі WireGuard сервера. Для цього переходимо в розділ IP - Address (рис 3.6)

Рис 3.6 – Задаємо адресу інтерфейсу

Після цього налаштовуємо маршрутизацію для передачі трафіку через інтерфейс WireGuard. Цей пункт передбачає додавання маршруту (Routes), де цільова підмережа маршруту повинна вказуватися у якості адреси, а інтерфейс або шлюз – інтерфейс WireGuard. (рис 3.7)

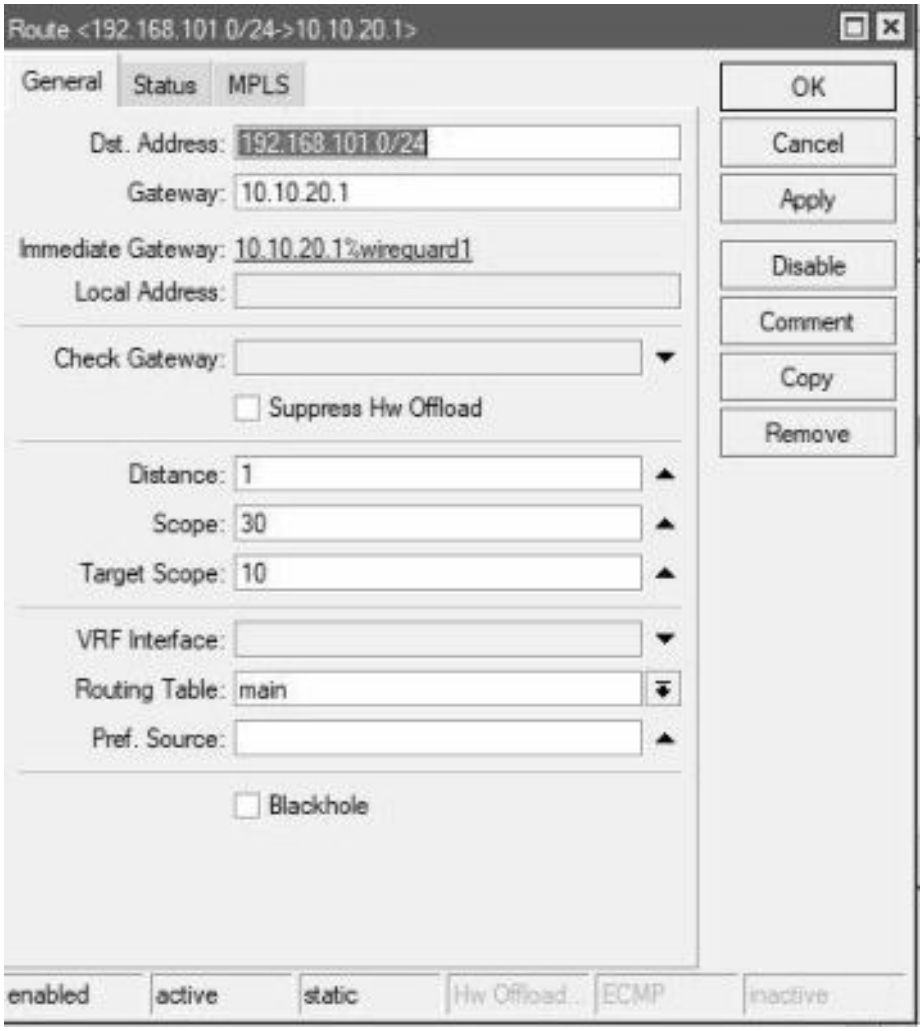

Рис 3.7 – Налаштування маршутів

Наостанок потрібно перевірити коректність налаштувань: що дані передаються коректно через новий тунель. (рис 3.8)

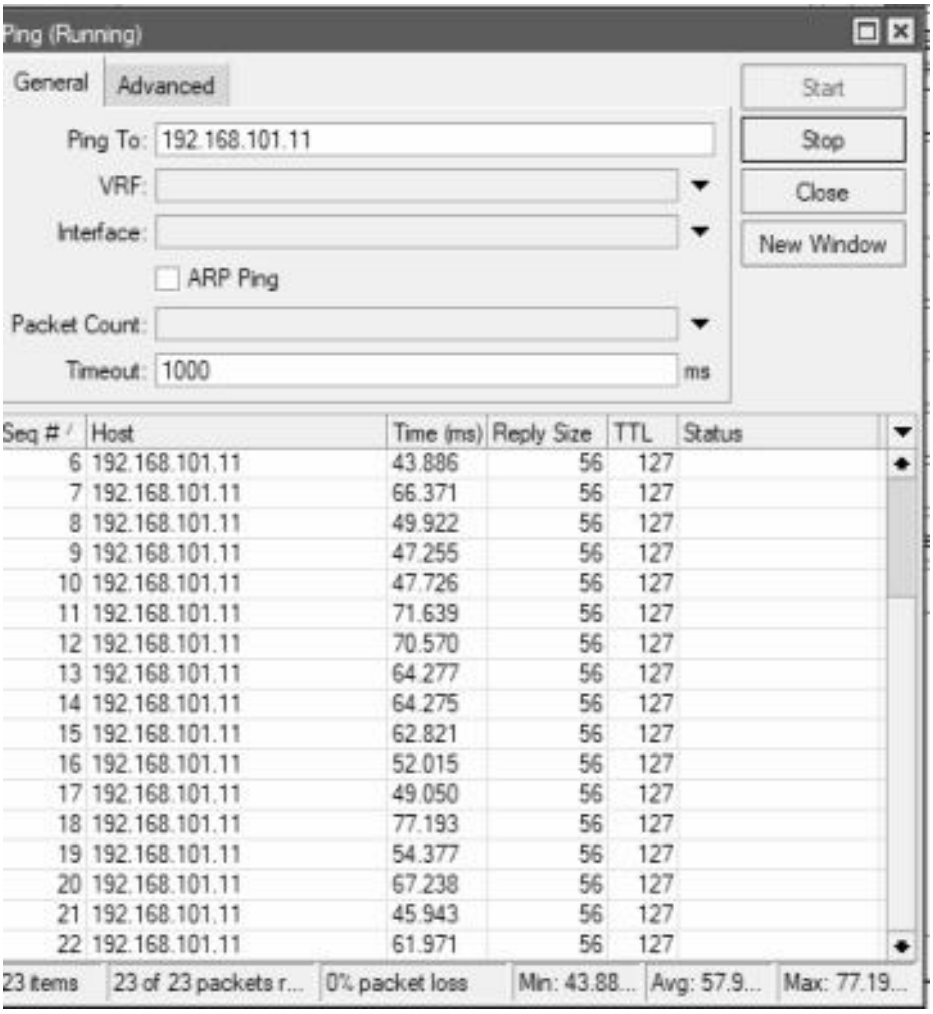

Рис 3.8 – Пінг робочого сервера який знаходиться за VPN

Таким чином, клієнт WireGuard успішно налаштований на обладнанні Mikrotik. Завдяки цьому ми отримаєм високий рівень захищеності з'єднання, а також мінімальні затримки і використання ресурсів у порівнянні з іншими VPN-протоколами.

3.2.2 Налаштування клієнта на основі операційної системи Windows

Щоб розпочати налаштування, спершу завантажте програму WireGuard з офіційного вебсайту. Після інсталяції та запуску додатка створіть новий тунель. (рис 3.9)

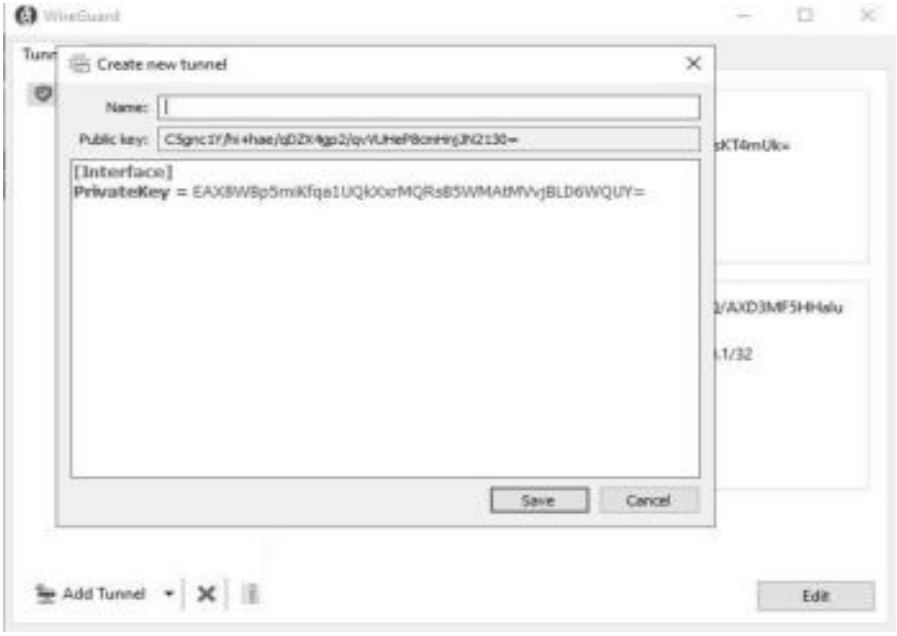

Рис 3.9 - Приклад пустого тунелю

Після того як дані були успішно внесені, ви отримуєте наступний результат з необхідними налаштуваннями:

Name (Назва тунелю) – це ім'я, яке ви обираєте для свого тунелю на власний розсуд, щоб легко ідентифікувати його серед інших конфігурацій.

PublicKey (публічний ключ тунелю) – цей елемент генерується автоматично програмним середовищем. Публічний ключ потрібно внести на стороні сервера WireGuard, оскільки він використовується для автентифікації з'єднання.

PrivateKey (приватний ключ) – також створюється автоматично і виступає критичним елементом налаштування безпеки. Він не потребує додаткового втручання або редагування.

Address (мережева адреса клієнта) – це IP-адреса клієнта, яка буде використовуватися у підмережі WireGuard. За замовчуванням вона повинна бути унікальною для кожного вузла у цій мережі.

PublicKey (публічний ключ сервера) – сюди необхідно вказати PublicKey сервера WireGuard, який був згенерований під час створення та налаштування тунелю на серверній стороні. Це дозволяє клієнту автентифікувати з'єднання з сервером.

AllowedIPs (список дозволених IP-адрес) – у цьому полі зазначаються підмережі або конкретні IP-адреси, до яких дозволяється надсилати трафік через встановлений тунель. Цей параметр визначає маршрутизацію даних через WireGuard.

Endpoint (кінцева точка з'єднання) – тут вводиться IP-адреса або DNS-ім'я сервера, а також порт WireGuard, який використовується для комунікації між сервером і клієнтом.

PersistentKeepalive (постійне підтримання з'єднання) – рекомендується встановити значення у 10 секунд. Це необхідно для забезпечення стабільної роботи тунелю особливо у випадках, якщо клієнт знаходиться за NAT або у мережах зі строгими обмеженнями з'єднань. Такі параметри забезпечують надійну роботу та стабільність вашого з'єднання через WireGuard. (рис 3.10)

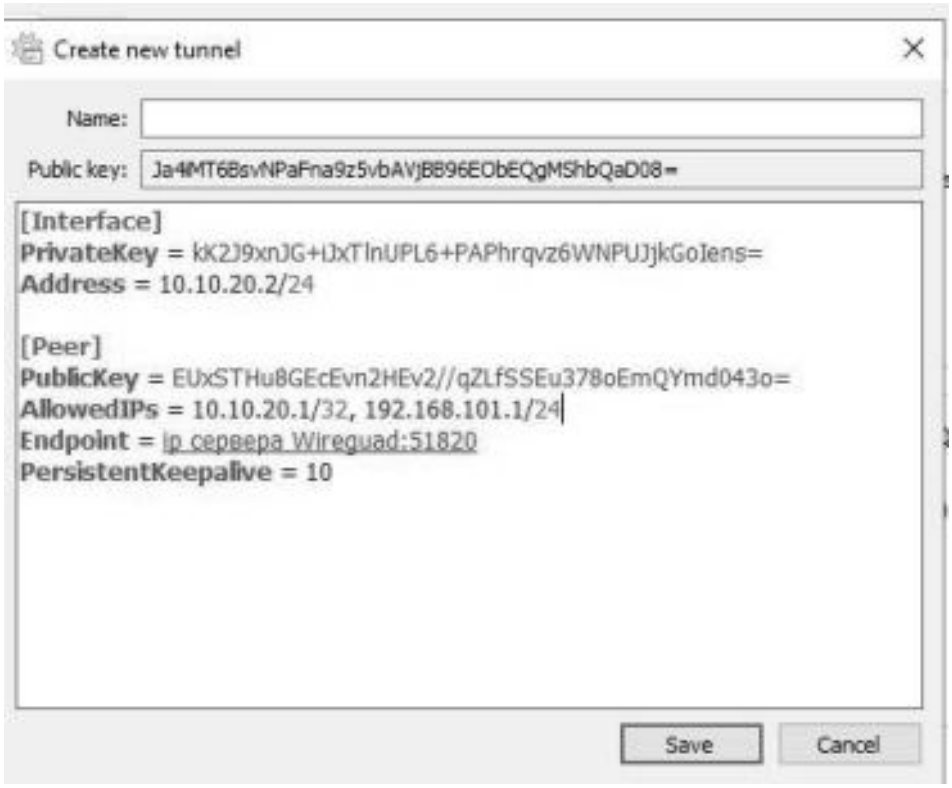

Рис 3.10 - Створення нового тунеля

Після завершення збереження налаштувань і успішного підключення до мережі, необхідно переконатися в наявності стабільного з'єднання з віртуальною машиною, яка має IP-адресу 192.168.101.11. Вона розташована у віддаленій

мережі, доступ до якої забезпечується через захищений тунель, створений за допомогою протоколу WireGuard. (рис 3.11) та відправка пакетів за допомогою програми iPerf (рис 3.12)

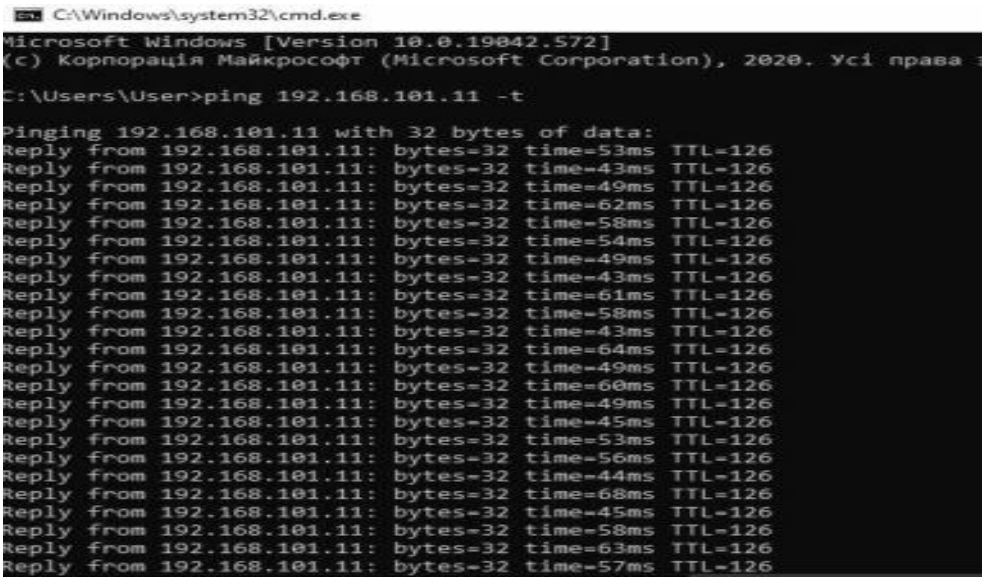

Рис 3.11 - Перевірка зв`язку з сервером

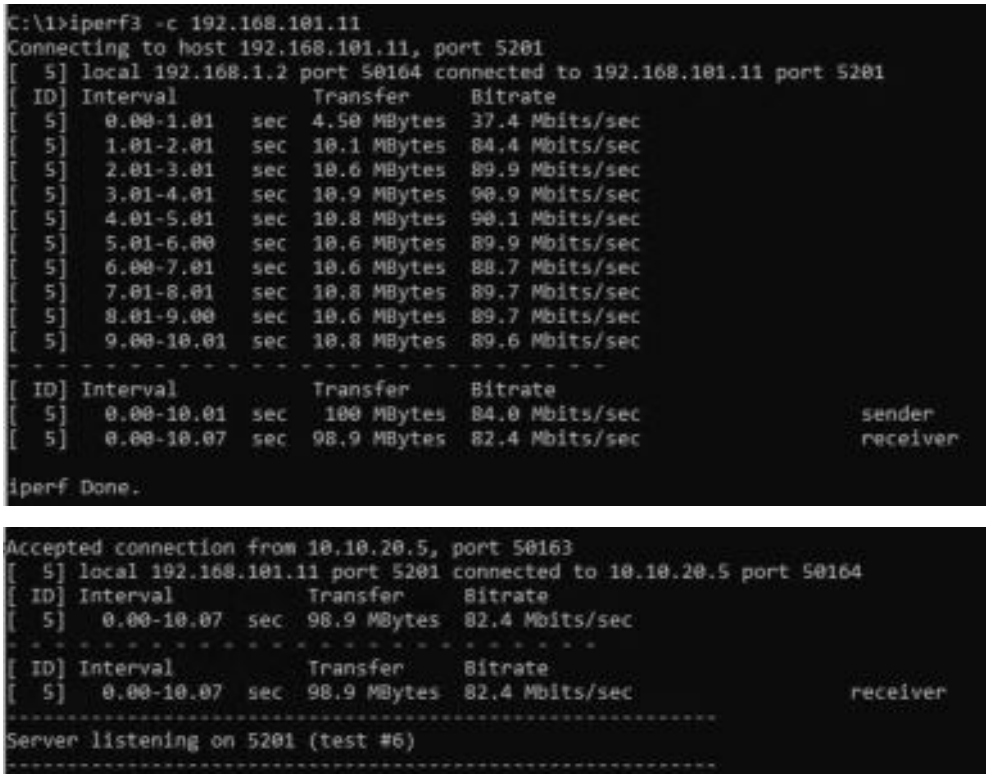

Рис 3.12 – Тестування швидкосты задопомгою утиліти iperf3

РОЗДІЛ 4.
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Аналіз небезпечних та шкідливих виробничих чинників під час роботи з комп’ютерною технікою та низьковольтним обладнанням

4.1.1 Комп`ютерна техніка

Однією з ключових особливостей сучасного розвитку суспільства є стрімке розширення сфер людської діяльності, у яких застосовуються інформаційні технології. Персональні комп'ютери отримали широке поширення, проте їх використання поставило на порядок денний питання збереження індивідуального та громадського здоров’я. Це вимагає вдосконалення існуючих практик та розробки нових підходів до організації робочих місць і впровадження профілактичних заходів для мінімізації негативного впливу комп'ютерів на здоров’я користувачів.

Охорона праці користувачів ПК потребує врахування трьох основних аспектів: соціального, психологічного та медичного. Соціальний аспект полягає у покращенні умов життя, роботи, відпочинку, харчування, побуту, а також у підвищенні рівня культури та розвитку інфраструктури і транспорту. Психологічний аспект акцентується на значенні психології праці для профілактики порушень здоров’я. Зокрема, створення гармонійних робочих колективів без внутрішніх конфліктів сприяє зменшенню нервово-психічної напруги, підвищенню працездатності й ефективності роботи. У користувачів комп’ютерів значну роль відіграє психоемоційний стрес, який проявляється у різному ступені практично у кожного.

Медичний аспект спрямований на попередження захворювань, пов’язаних із використанням ПК. Для цього застосовуються як заходи первинної профілактики (наприклад, професійний відбір), так і вторинної, яка дозволяє знижувати ризик перевтоми та надмірного напруження. Комплексні дії

спрямовані на відновлення нормальної роботи органів зору та опорно-рухового апарату. Щодо гігієнічних вимог до обладнання робочих місць із ПК, дизайн усіх елементів має відповідати принципам ергономіки з урахуванням особливостей конкретної діяльності. Робоче місце користувача повинно забезпечувати комфорт і правильну поставу. Розташування ПК відносно джерел природного освітлення слід організувати так, щоб світло поступало збоку, переважно з лівого боку. Варто дотримуватись таких відстаней: 1,2 м між боковими частинами комп'ютерів; 2,5 м від задньої сторони одного монітора до екрана іншого. Монітор повинен розташовуватись на оптимальній відстані 600–700 мм від очей, але не ближче ніж 600 мм, залежно від розміру шрифту й символів. Його нахил має бути таким, щоб забезпечити зручність огляду під кутом +30° відносно нормальної лінії погляду.

Клавіатура повинна знаходитись на робочій поверхні на відстані 100–300 мм від її краю. Її конструкція повинна включати опорний пристрій із матеріалу з високим коефіцієнтом тертя для запобігання ковзанню та дозволяти змінювати кут нахилу в межах 5–15°. Режими роботи і відпочинку для користувачів ПК також мають велике значення. Для підтримання здоров'я, профілактики професійних захворювань і забезпечення працездатності працівників передбачаються регламентовані внутрішньозмінні перерви. Вони включають короткі паузи в ті періоди, коли починають проявлятися об'єктивні та суб'єктивні ознаки втоми і зниження продуктивності.

Під час робочої зміни необхідно передбачити:

- Перерви на відпочинок і прийом їжі (обідні перерви).

- Перерви для особистих потреб та відпочинку, що відповідають трудовим нормам.

- Додаткові перерви для специфічних професій, враховуючи особливості їхньої діяльності. Згідно з класифікатором професій, розрізняють три основні групи:

1. Програмісти займаються роботою з комп'ютерами і документацією, яка вимагає інтенсивного обміну інформацією. Їхня діяльність пов'язана з

інтенсивним розумовим навантаженням і зоровою напругою. Вони працюють у вимушених позах і підлягають загальній гіподинамії з періодичним навантаженням на руки.

2. Оператори ЕОМ здійснюють обробку інформації, отриманої через дисплеї. Їхня робота уривчаста, з перервами для виконання інших завдань, відзначається середньою фізичною й нервовою напругою.

3. Оператори комп'ютерного набору виконують одноманітні роботи з документацією і клавіатурою. Робота вимагає високої швидкості введення даних і супроводжується фізичним напруженням рук, разом із загальною гіподинамією та напруженням зору.

Правила встановлюють такі режими праці та відпочинку для 8-годинної робочої зміни:

- Для програмістів: 15-хвилинна перерва щогодини роботи з комп'ютером.
- Для операторів: 15-хвилинна перерва що дві години.
- Для операторів набору: 10-хвилинна перерва після кожної години роботи.

Якщо виробничі умови не дозволяють дотримуватися таких перерв, тривалість безперервної роботи з комп'ютером не повинна перевищувати 4 години. При 12-годинній зміні перерви слід планувати аналогічно, а в останні 4 години — кожну годину по 15 хвилин. Деякі перерви бажано використовувати для комплексів вправ, рекомендованих у санітарних нормах роботи з комп'ютерами. Психофізіологічне розвантаження можна проводити сеансами аутогенного тренування, які включають психічну саморегуляцію і прості фізичні вправи. Рекомендується три періоди в кімнаті розвантаження: абстрагування від робочого середовища, заспокоєння та активізація. Сеанси можна проводити за загальною програмою через навушники, складаючи їх із двох 5-хвилинних періодів релаксації і підвищення працездатності. Вкінці пропонуються фрази самонавіювання для поліпшення настрою і почуття бадьорості. Після сеансу відчуття втоми знижується, а загальний стан покращується.

4.1.2 Низьковольтне обладнання

Аналіз потенційно небезпечних і шкідливих факторів, що виникають при експлуатації слабкострумового низьковольтного обладнання з напругою до 24 В, є критично важливим для попередження можливих ризиків і формування безпечних умов праці для співробітників. Незважаючи на те, що така напруга вважається порівняно низькою та менш небезпечною у порівнянні з високовольтними системами, існує низка специфічних загроз, які в жодному разі не слід ігнорувати. Серед основних небезпечних і шкідливих чинників, з якими можуть стикатися працівники під час роботи зі згаданим обладнанням, виділяються такі: можливість отримання електричного удару, термічний вплив на шкіру чи інші тканини, виникнення коротких замикань, які можуть призводити до займання або пошкодження обладнання. Крім того, електромагнітні поля, що випромінюються такими пристроями, можуть впливати на організм людини. Навіть за умов низької напруги та малих струмів порушення правил техніки безпеки здатне викликати опіки, механічні травми або в окремих випадках навіть негативно позначитися на роботі серцево-судинної чи нервової системи працівника при тривалому контакті.

Не менш важливими є й ергономічні аспекти, які впливають на загальну ефективність і комфорт виконання трудових обов’язків. Постійне перебування в незручному положенні, недостатнє освітлення робочого місця або відсутність належної організації умов праці можуть спричинити фізичне та психоемоційне перенапруження. Це може виражатися у вигляді втоми очей, погіршення зорової концентрації, зниження продуктивності, а також загального дискомфорту. До цього додається ризик несправності обладнання через використання неякісних деталей або нехтування регулярним технічним обслуговуванням, що значно підвищує ймовірність аварій чи непередбачених поломок.

Для зниження негативного впливу зазначених факторів та підвищення загального рівня безпеки необхідно забезпечити дотримання чіткого алгоритму заходів. Обов’язковими є використання засобів індивідуального захисту, таких як спеціальні гумові рукавички чи взуття з ізоляційною підошвою. Крім того, варто регулярно проводити технічну перевірку стану обладнання та усувати будь-які несправності на стадії їх виникнення.

Надзвичайно важливим є і навчання персоналу правилам використання таких систем, що дозволить зменшити людський фактор як один із джерел ризику. Запровадження вищезазначених заходів дає змогу створити надійне та безпечне середовище для співробітників. Це не лише захищає їхнє здоров'я, але й сприяє ефективній роботі та загальному підвищенню продуктивності підприємства.

4.2 Моделювання процесу виникнення травм та аварій

Моделювання процесу виникнення травм і аварій під час роботи з комп’ютерною технікою може стати ефективним інструментом для підвищення рівня безпеки й запобігання можливим негативним наслідкам.

Основні етапи проведення такого моделювання включають:

1. Розробка сценаріїв травм і аварій:

- Аналіз історії попередніх інцидентів і аварій на робочих місцях.

- Ідентифікація та опис потенційних сценаріїв небезпеки, що можуть спричинити травми або аварії.

2. Збір необхідних даних:

- Систематизація статистичних даних щодо зареєстрованих випадків травм і аварій. - Фіксація ризикових факторів і умов, що сприяють їхньому виникненню.

3. Визначення ключових факторів ризику:

- Вивчення впливу різноманітних факторів, таких як обладнання, працівники або навколишнє середовище, на можливість виникнення інцидентів.

- Виділення факторів, що збільшують ризик небажаних подій.

4. Розробка математичних моделей:

- Створення моделей, що відображають взаємозв'язки між чинниками ризику та ймовірністю виникнення травм чи аварій.

- Використання статистичних інструментів для аналізу зібраних даних і розрахунку ступеня ризику.

5. Перевірка і збалансування моделей:

- Тестування побудованих моделей на реальних прикладах інцидентів.

- Удосконалення моделей з урахуванням отриманого зворотного зв’язку та оновленої інформації.

6. Формування заходів безпеки:

- Розробка практичних рекомендацій і впровадження заходів для зменшення ризиків на основі результатів моделювання.

- Проведення навчань та інструктажів для підвищення обізнаності персоналу щодо безпеки.

7. Постійний моніторинг і аналіз:

- Регулярне відстеження показників безпеки на робочих місцях.

- Оновлення моделей і заходів відповідно до нововиявлених ризиків або змін у робочому середовищі. Застосування такого підходу дозволяє підвищити ефективність стандартів безпеки, зменшити ризики травм і аварій та створити більш захищене робоче середовище.

4.3 Розробка заходів щодо безпеки у надзвичайних ситуаціях

Забезпечення безпеки населення під час надзвичайних ситуацій включає комплекс заходів, спрямованих на запобігання, зменшення ризиків та мінімізацію наслідків можливих небезпек.

Це системний процес, який охоплює кілька ключових аспектів: Попередження та інформування:

- Розробка інтегрованих систем оповіщення, що використовують різноманітні комунікаційні канали, такі як сирени, текстові повідомлення чи соціальні мережі, для оперативного інформування людей про загрози.

- Проведення інформаційних кампаній, які поширюють знання серед населення про дії в умовах надзвичайних подій та розпізнавання потенційних небезпек.

Евакуація та укриття:

- Створення чітких планів евакуації для різних категорій об’єктів, як-от житлові райони, школи чи лікарні, і регулярне оновлення цих планів.

- Облаштування спеціалізованих укриттів, які забезпечують надійний захист людей у разі виникнення небезпеки.

Системи моніторингу та раннього виявлення:

- Постійний моніторинг погодних умов для своєчасного прогнозування стихійних явищ та інших природних лих.

- Впровадження технологій для ідентифікації потенційних загроз, таких як техногенні аварії або дії терористів.

Підготовка та тренування:

- Організація навчань та тренувань для звичайних громадян, аби надати їм необхідні навички реагування на критичні ситуації.

- Підвищення кваліфікації служб безпеки, зокрема рятувальників, медичних працівників та поліцейських, шляхом постійної підготовки.

Комунікація та координація:

- Заснування кризових центрів управління, які забезпечують спільну роботу різних відомств з метою швидкого реагування на надзвичайні події.

- Розбудова ефективних систем зв’язку, що гарантують безперебійний обмін даними між службами та з громадськістю.

Медична допомога:

- Оптимізація систем надання медичної допомоги постраждалим у надзвичайних ситуаціях шляхом модернізації інфраструктури і покращення координації роботи медичних установ. Для забезпечення ефективного захисту населення потрібен інтегрований підхід, який базується на співпраці усіх зацікавлених сторін, впровадженні сучасних технологій і регулярному оновленні існуючих стратегій. Лише за таких умов можна оптимально реагувати на швидкоплинні виклики сучасного світу.

РОЗДІЛ 5.
ВИЗНАЧЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ
комп'ютерної мережі

5.1 Розрахунок вартості використаного обладнання

Для побудови VPN мережі були використанний дистрибутив pFsense встановлений на сервері, роутер Miktorik. Бюджет витрат на матеріали та комплектуючі наведено в таблиці 5.1.

Таблиця 5.1

Бюджет витрат на матеріали та комплектуючі виробів

Назва	Вартість за 1 одиницю	Примітка
Оренда сервера та статичної IP адреси на хостингу Hetzner	1900 грн/місяць	Сервер: Intel i7-7700, 64 GB RAM, 2 шт - 512 GB SSD, 1 шт. - 2 TB HDD
Оренда ліцензії Windows Server 2022	1050 грн/місяць	
Mikrotik rb952ui	2000 грн	

На сервері інстальовано операційну систему Windows Server 2022, яка забезпечує основну платформу для роботи. На цій системі, за допомогою гіпервізора, розгорнуто віртуальну машину, на якій працює pFsense.

Використання гіпервізора дозволяє ефективно ізолювати роботу pFsense від основної операційної системи, створюючи окреме віртуальне середовище для виконання завдань, пов'язаних зі створенням маршрутизатора та мережевого брандмауера.

Технічні характеристики віртуальної машини pFsense:

Оперативна пам`ять - 1 GB.

Дисковий простір - 15 GB.

Ядра віртуального процесора – 2 шт.

Зважаючи на ще наявні вільні ресурси, сервер має потенціал для виконання додаткових завдань, зокрема може використовуватися як файлове сховище.

Окрім цього, він здатний слугувати платформою для розміщення інших типів сервісів, таких як поштовий сервер, веб-сайти та на інші потреби, що можуть виникнути. Для проведення тестування буде розгорнуто віртуальну машину з IP-адресою 192.168.101.11, яка слугуватиме умовним сервером підприємства.

5.2 Огляд вартості приватних VPN сервісів

Приватні VPN сервіси, як правило, пропонують різноманітні тарифні плани, адаптовані до потреб окремих користувачів і організацій. Базові пакети часто включають основні функції, такі як шифрування трафіку, захист даних, доступ до обмежених геолокацій і мінімальний набір серверів. Вартість таких пакетів здебільшого залишається на рівні економічно доступного розміру, що робить їх привабливими для більшості користувачів-початківців. Більш просунуті варіанти VPN-надань передбачають широкий спектр додаткових функцій: доступ до серверів із вищою швидкістю, підтримку кількох одночасних підключень, спеціалізовані протоколи безпеки та можливість використання на нетипових пристроях. Відповідно до цього ціни можуть варіюватися досить значно. Найчастіше такі сервіси мають гнучкий підхід до формування вартості – наприклад, щомісячна оплата може бути дорожчою порівняно з одноразовою передплатою на більший період, що дозволяє заощадити кошти у довгостроковій перспективі.

Здійснено аналіз та представлено вартість (таблиця 5.2) чотирьох популярних сервісів із їхніми бізнес-пакетами: Nordlayer, Perimeter81, Twingate і Proton.

Відповідно до представлених даних, організація та обслуговування VPN-мережі для компанії, яка налічує 10 працівників і потребує забезпечення віддаленого доступу, обійдеться принаймні у 5670 гривень за місяць.

Відповідно при реалізації технології WireGuard на ресурсах тестового нашого сервера вартість буде складати 2950 гривень.

Таблиця 5.2

Аналіз вартості послуг сторонніх VPN сервісів

Назва	Вартість за 1 користувача на місяць	Мінімальна кількість користувачів	Виділений сервер та статичну IP адресу
Nordlayer	294 грн	50	Включено у вартість
Perimeter81	672 грн	20	Включено у вартість
Twingate	420 грн	1	Додатково 1470 грн на місяць
Proton	420 грн	1	Додатково 1680 грн на місяць

Клієнти матимуть можливість підключатися як зі своїх робочих станцій, так і через спільний канал за допомогою роутера Mikrotik, на якому буде налаштовано клієнт WireGuard.

ВИСНОВКИ І ПРОПОЗИЦІЇ

У процесі виконання кваліфікаційної роботи було проведено глибоке дослідження технології VPN, що дозволило визначити її значущість і багатогранну роль у проєктуванні та створенні захищених комп’ютерних мереж. Особлива увага приділялася аналізу її застосування для протидії сучасним викликам у сфері інформаційної безпеки та забезпечення стабільності функціонування мереж.

Було здійснено масштабний комплексний аналіз поточного стану розвитку корпоративних мереж, VPN технологій та їхньої технологічної бази. Зокрема, досліджено відповідність можливостей і ресурсів актуальним вимогам часу.

Основний акцент зроблено на визначенні ролі комп'ютерних мереж у реалізації бізнес-процесів та досягненні високого рівня мобільності й гнучкості при виконанні завдань.. Зростаючі вимоги до забезпечення безпеки даних обумовлюють необхідність відповідати найвищим стандартам цієї галузі, особливо в умовах підвищеної вразливості до загроз кібератак.

Проведено всебічний аналіз основних концепцій VPN. Було розглянуто ключові принципи її функціонування з урахуванням основних компонентів: тунелювання, аутентифікації та шифрування даних. Розділ також охоплює характеристику основних типів мереж VPN, їх функціональні властивості та різні підходи до реалізації цієї технології.

Третій розділ цієї роботи повністю присвячений практичній реалізації захищеної мережі корпоративної мережі, у якому використовується технологія VPN. Цей етап охоплював комплексний підхід до вирішення поставлених завдань, починаючи з налаштування WireGuard сервера на основі pFsense, налаштувань обладнання Mikrotik та клієнта на операційній системі Windows, необхідного для забезпечення коректного функціонування мережі. Завершальним етапом виступила безпосередня реалізація практичних заходів із впровадження цієї технології в робоче середовище.

Четвертий розділ цієї роботи зосереджений на питаннях техніки безпеки, охорони праці та забезпеченні безпеки в надзвичайних ситуаціях. У ньому розглядається аналіз небезпечних і шкідливих виробничих факторів, які можуть виникати під час роботи з комп’ютерною технікою та низьковольтним обладнанням.

Проведено аналіз та виконано економічне обґрунтування доцільності впровадження технології на підприємстві.

Результати детального дослідження та практичного впровадження проекту підтвердили важливість технології VPN як ключового інструменту для забезпечення конфіденційності передачі даних у комп’ютерних мережах сучасних корпоративних мережах.

Завдяки аналізу стало очевидно, що VPN-технології відіграють критично важливу роль у галузі інформаційної безпеки.

На тлі зростання запитів на безпеку даних у сучасному світі IT та кіберзагроз можна стверджувати, що розвиток і вдосконалення VPN-технологій є перспективним і стратегічним напрямком для подальшого прогресу галузі. Отже, результати цієї роботи не тільки підкреслюють значущість досліджень у сфері захисту інформації, але й служать основою для посилення практичного впровадження та розширення впливу VPN-технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Побудова корпоративних мереж передачі даних. [Електронний ресурс] / Режим доступу: https://www.telesphera.net/blog/corporate-networking.html (дата звернення 12.10.2024)
2. Особливості побудови і використання сучасних корпоративних комп'ютерних мереж [Електронний ресурс] / Режим доступу:https://conferences.vntu.edu.ua/public/files/1/fitki_2017_netpub.pdf (дата звернення 18.10.2024)
3. Корпоративна мережа . [Електронний ресурс] / Режим доступу: http://surl.li/iaybm (дата звернення 12.10.2024)
4. Принципи побудови і призначення комп'ютерних мереж - [Електронний ресурс] / Режим доступу:http://surl.li/iadst (дата звернення 19.10.2024)
5. Загальні принципи побудови корпоративної мережі [Електронний ресурс] / Режим доступу:- https://studfile.net/preview/5470625/ (дата звернення 14.10.2024)
6. Сєдих В. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ //Інформаційні технології у науці, освіті, виробництві: збірник тез І Всеукраїнської науково-практичної Інтернет-конференції здобувачів вищої освіти і молодих учених, м. Маріуполь, 26 квітня 2018 р./Маріупольський державний університет; уклад. Тимофєєва ІБ, Дяченко ОФ-Маріуполь: МДУ, 2018.- 186 с. - 2018. С. 168.
7. Капу стін М. О. Порівняльний аналіз протоколів віртуальних приватних мереж. - 2023.
8. Аніщенко К. Я. КЛАСИФІКАЦІЯ ТЕХНОЛОГІЙ РЕАЛІЗАЦІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ // Київ. - С. 21 .
9. A Framework for IP Based Virtual Private Networks [Електронний ресурс] / Режим доступу:http://www.ietf.org/rfc/rfc2764.txt (дата звернення 10.11.2024)
10. Bollapragada V., Mohamed Kh., Wainner S. IPSec VPN Design. Cisco Press. (2005). 384 p.

11. Douglas Crawford. OpenVPN over TCP vs. UDP: what is the difference, and which should I choose? [Електронний ресурс] / Режим доступу:https://www.bestvpn.eom/blog/7359/openvpn-tcp-vs-udp-difference- choose/ (дата звернення 22.10.2024)
12. Harsh Kupwade Patil. Wireless Sensor Network Security: The Internet of Things [Електронний ресурс] / Harsh Kupwade Patil, Thomas M.Chen // Computer and Information Security Handbook. 2017. Third Edition, Chapter 18. - P. 317-337. - Режим доступу: https://www.sciencedirect.com/science/article/pii/B9780128038437000181. (дата звернення 20.10.2024)
13. IPSec - протокол захисту мережевого трафіку на IP-рівні. [Електронний ресурс] - Режим доступу до ресурсу: https://www.ixbt.com/comm/ipsecure.html (дата звернення 12.10.2024)
14. Сташевський О. С., Зелінська О. В. Застосування віртуальних приватних мереж //Прикладні аспекти сучасних міждисциплінарних досліджень. - 2022. - С. 209-211.
15. Хома И. ПЕРЕВАГИ ВИКОРИСТАННЯ ОБЛАДНАННЯ MIKROTIK ДЛЯ ПОБУДОВИ БЕЗДРОТОВИХ МЕРЕЖ //Vensky. - 2019.
16. WireGuard: Next Generation Kernel Network Tunnel [Електронний ресурс] / Режим доступу: www. URL: https://www.wireguard.com/papers/wireguard.pdf (дата звернення 2.10.2024)
17. Microsoft Security Advisory 2743314 [Електронний ресурс] / Режим доступу: www. URL: https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/ 2012/2743314?redirectedfrom=MSDN (дата звернення 17.10.2024)
18. Microsoft handed the NS A access to encrypted messages [Електронний ресурс] / Режим доступу: www. URL: https://www.theguardian.com/world/2013/jul/ll/ microsoft-nsa-collaboration-user- (дата звернення 17.10.2024)

19. Comparison of VPN Protocols at Network Layer Focusing on WireGuard Protocol [Електронний ресурс] / Режим доступу: www. URL: https://www.researchgate.net/publication/345681297 Paper-Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol Comparison (дата звернення 23.10.2024)
20. Performance Comparison of VPN Solutions [Електронний ресурс] / Режим доступу: https://core.ac.uk/download/pdf/322886318.pdf (дата звернення 20.10.2024)
21. WireGuard - Next Generation Secure Network Tunnel [Електронний ресурс] / Режим доступу: https://www.sstic.org/2018/presentation/WireGuard/ - (дата звернення 22.10.2024)
22. The New Cloudflare VPN: What It Is And Is Not [Електронний ресурс] / Режим доступу: https://openvpn.net/blog/what-is-cloudflare-vpn/ - (дата звернення 30.10.2024)
23. WireGuard VPN review: A new type of VPN offers serious advantages [Електронний ресурс] / Режим доступу: https://arstechnica.com/gadgets/2018/Q8/wireguard-vpn-review-fast-connections- amaze-but-windows-support-needs-to-happen/ (дата звернення 30.10.2024)
24. VPN Protocol Comparison: PPTP vs OpenVPN vs L2TP vs SSTP [Електронний ресурс] / Режим доступу: https://www.vpnuniversity.com/learn/vpn-protocols-compared-pptp-vs-openvpn- vs-12tp-vs-sstp - (дата звернення 30.10.2024)
25. OpenVPN Connect Client [Електронний ресурс] / Режим доступу: https://openvpn.net/vpn-client/- (дата звернення 28.10.2024)
26. What is WireGuard? Secure, simple VPN now part of Linux [Електронний ресурс] / Режим доступу: https://www.csoonline.com/article/3434788/what-is-wireguard-secure-simple-vpn- still-in-development.html (дата звернення 28.10.2024)

27. Fix: L2TP VPN issues (blocked / not responding) [Електронний ресурс] / Режим доступу: https://windowsreport.com/12tp-vpn-blocked/ - (дата звернення 14.10.2024)
28. What is OpenVPN? Is OpenVPN safe? [Електронний ресурс] / Режим доступу: https://www.comparitech.com/blog/vpn-privacy/what-is- openvpn/ - (дата звернення 14.10.2024)
29. How To Set Up WireGuard on Ubuntu 20.04 [Електронний ресурс] / Режим доступу: https://www.digitalocean.com/community/tutorials/how-to- set-up-wireguard-on-ubuntu-20-04 (дата звернення 12.10.2024)
30. RFC 3193: Securing L2TP using IPsec [Електронний ресурс] / Режим доступу: https://www.rfc-editor.org/rfc/rfc3193 (дата звернення 12.10.2024)
31. How IPsec works, it’s components and purpose [Електронний ресурс] / Режим доступу: https://www.csoonline.com/article/2117067/how- ipsec-works.html (дата звернення 18.10.2024)
32. AH and ESP protocols [Електронний ресурс] / Режим доступу:https://www.ibm.com/docs/en/zos/2.4.0?topic=ipsec-ah-esp-protocols (дата звернення 19.10.2024)
33. What is IPsec and how does it work? [Електронний ресурс] / Режим доступу: https://www.comparitech.com/blog/information-security/ipsec-encryption/ (дата звернення 20.10.2024)