Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Метод організації захищеного сегмента корпоративної мережі на основі моделі Zero Trust

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІ-21-6
Владислав ЛЮБЧИК
(власне ім’я, прізвище)

Спеціальність
123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп’ютерна інженерія
(повна назва освітньої програми)

Керівник: ас. Ірина ЧЕПУРНА
(посада, власне ім’я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім’я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Любчику Владиславу Олександровичу
(прізвище, ім’я, по батькові)

1. Тема роботи Метод організації захищеного сегмента корпоративної мережі на основі моделі Zero Trust

затверджена наказом по університету від “ 26 ” травня 2025 р. № 424 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 17 червня 2025 р.

3. Вхідні дані до роботи 1) концепція Zero Trust Architecture: основні принципи, технології реалізації; 2) технології захищеного зв’язку: VPN; 3) протоколи тунелювання: IPSec, OpenVPN, Wireguard, SSH, SSL/TLS; 4) управління ролями користувачів: RBAC; 5) методи експериментального та аналітичного моделювання захищеного сегмента мережі

4. Перелік питань, що потрібно опрацювати у роботі
1) аналіз проблеми та існуючих рішень;
2) принципи концепції моделі Zero Trust;
3) технології та протоколи захищеного зв’язку в мережах;
4) управління ролями та привілеями користувачів на основі RBAC;
5) організація захищеного сегменту на основі моделі Zero Trust;
6) висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

Слайд-презентація – 12 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень	27.05.25-30.05.25	
2	Вибір технології розробки та інструментальних засобів	31.05.25-03.06.25	
3	Розробка та тестування методу	04.06.25-06.06.25	
4	Оформлення матеріалів кваліфікаційної роботи	07.06.25-10.06.25	
5	Подання кваліфікаційної роботи керівникові	11.06.25-12.06.25	
6	Підготовка презентації та попередній захист	12.06.2025 – 13.06.2025	
7	Подання кваліфікаційної роботи на рецензування	14.06.25-16.06.25	

Дата видачі завдання " 26 " травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ас. Ірина ЧЕПУРНА
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 58 с., 12 рис., 5 табл., 3 дод., 34 джерела.

КОМП’ЮТЕРНА МЕРЕЖА, VPN, ПРОТОКОЛ, АРХІТЕКТУРА, ZERO TRUST, СЕГМЕНТАЦІЯ

Метою кваліфікаційної роботи є розробка методу організації захищеного сегменту корпоративної комп’ютерної мережі на основі моделі Zero Trust, яка забезпечує доступ до ресурсів відповідно до прав і привілеїв користувачів.

В ході виконання роботи проведено аналіз основних принципів концепції архітектури нульової довіри, сучасних технологій і протоколів захищеного з’єднання. Особливу увагу приділено застосуванню VPN, FreeRADIUS, LDAP та засобів багатофакторної автентифікації для забезпечення захищеного доступу до мережних ресурсів корпоративної мережі відповідно до рівня авторизації користувача.

Отримані результати підтверджують доцільність використання запропонованого підходу для задоволення високих вимог щодо захисту ресурсів корпоративної мережі від ризиків несанкціонованого доступу та витоку конфіденційної інформації.

ABSTRACT

Bachelor`s thesis: 58 pages, 12 figures, 5 tables, 3 appendicle, 34 sources.

COMPUTER NETWORK, VPN, PROTOCOL, ARCHITECTURE, ZERO TRUST, SEGMENTATION

The main goal of this thesis is to develop a method for organizing a secure segment of a corporate computer network based on the Zero Trust model, which provides access to resources in accordance with the rights and privileges of users.

In order to achieve this goal, an analysis of the basic principles of the Zero Trust architecture concept, modern technologies and secure connection protocols was conducted. Particular attention was paid to the use of VPN, FreeRADIUS, LDAP and multi-factor authentication tools to ensure secure access to network resources of a corporate network in accordance with the user's authorization level.

The results obtained confirm the feasibility of using the proposed approach to meet the high requirements for protecting corporate network resources from the risks of unauthorized access and leakage of confidential information.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IT – інформаційні технології

ВМ – віртуальна машина

ОС – операційна система

AAA – автентифікація, авторизація та облік (англ. Authentication, Authorization and Accounting)

AD – служба каталогів Active Directory (англ. Active Directory)

AES – стандарт симетричного шифрування (англ. Advanced Encryption Standard)

CCD – каталог клієнтських конфігурацій (англ. Client Configuration Directory)

CPU – центральний процесор (англ. Central Processing Unit)

DDoS – розподілена атака на відмову в обслуговуванні (англ. Distributed Denial of Service)

Dev – середовище розробки (англ. Development)

FIFO – черга з обслуговуванням у порядку надходження (англ. First In – First Out)

ICMP – протокол керування повідомленнями в інтернеті (англ. Internet Control Message Protocol)

IoT – інтернет речей (англ. Internet of Things)

IPsec – протокол захисту інтернет-протоколу (англ. Internet Protocol Security)

LDAP – протокол доступу до каталогів (англ. Lightweight Directory Access Protocol)

LTS – розширена підтримка версій (англ. Long-Term Support)

MFA – багатофакторна автентифікація (англ. Multi-Factor Authentication)

NAP – мережний вузол доступу (англ. Network Access Point)

NAT – трансляція мережевих адрес (англ. Network Address Translation)

NPS – сервер політик мережі (англ. Network Policy Server)

PAM – управління привілейованим доступом (англ. Privileged Access Management)

PKI – інфраструктура відкритих ключів (англ. Public Key Infrastructure)

PoLP – принцип найменших привілеїв (англ. Principle of Least Privilege)

Prod – промислове середовище (англ. Production)

RADIUS – служба віддаленої автентифікації (англ. Remote Authentication Dial-In User Service)

RAM – оперативна пам’ять (англ. Random Access Memory)

RBAC – модель контролю доступу на основі ролей (англ. Role-Based Access Control)

SSH – безпечна оболонка (англ. Secure Shell)

TCP – протокол керування передачею (англ. Transmission Control Protocol)

TLS – протокол захищеної передачі (англ. Transport Layer Security)

UDP – протокол користувацьких дейтаграм (англ. User Datagram Protocol)

VLAN – віртуальна локальна мережа (англ. Virtual Local Area Network)

VPN – віртуальна приватна мережа (англ. Virtual Private Network)

ВСТУП

Сучасний етап розвитку цифрового середовища супроводжується стрімким зростанням та ускладненням кіберзагроз. Це актуалізує потребу у впровадженні ефективних підходів до захисту конфіденційності, цілісності та доступності інформаційних ресурсів в корпоративних комп'ютерних мережах. Традиційні моделі периметрової безпеки, орієнтовані на довіру до внутрішнього середовища, втрачають свою ефективність в умовах динамічного поширення хмарних обчислень, віддаленого доступу, а також активного використання персональних та мобільних пристроїв.

Серед найбільш критичних загроз варто відзначити компрометацію облікових даних, інсайдерську активність та доступ через уразливості в захищених каналах комунікації.

У відповідь на зазначені виклики сформувалась концепція нульової довіри (Zero Trust), яка заперечує апріорну довіру до будь-якого елемента системи незалежно від його розташування або належності до внутрішнього середовища. Її ключовими принципами є постійна автентифікація та авторизація користувачів та пристроїв, безперервний моніторинг мережного трафіка з метою своєчасного виявлення потенційних загроз.

Для реалізації принципів концепції Zero Trust доцільно використовувати віртуальні приватні мережі (VPN), централізовані системи управління автентифікацією, політики доступу на основі ролей (RBAC) та принципу найменших привілеїв (PoLP). Реалізація цих механізмів сприяє підвищенню загального рівня безпеки та формуванню стійкої до зовнішніх і внутрішніх загроз інфраструктури.

Метою даної кваліфікаційної роботи є розробка методу організації захищеного сегмента корпоративної комп'ютерної мережі на основі моделі Zero Trust, що забезпечує захищений доступ до ресурсів корпоративної мережі на основі прав та привілеїв користувачів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Принципи концепції Zero Trust

Розвиток IT-інфраструктури, впровадження публічних хмарних сервісів та стрімке збільшення кількості мобільних користувачів призводить до збільшення кількості кіберзагроз, що дедалі стають більш складними [1-3]. В таких умовах інформаційні ресурси та конфіденційні дані користувачів стають вразливими перед несанкціонованим доступом та ризиком втрати критичних даних. При цьому традиційні моделі захисту, що передбачає захист периметра мережі, втрачають свою ефективність [4].

Традиційна архітектура безпеки фокусується на запобіганні зовнішньому вторгненню, проте в сучасних комп'ютерних мережах цього підходу вже недостатньо. Широке застосування віртуалізованих структур, децентралізація даних та розширення цифрового периметра призвели до формування нової парадигми безпеки, в основі якої лежить принцип постійної перевірки довіри – незалежно від місця походження запиту чи розташування ресурсу [5]. Умови, в яких мережний периметр більше не має чітких меж, вимагають динамічного підходу до захисту, коли кожен користувач, пристрій або сервіс має бути перевірений перед наданням доступу до будь-якого ресурсу. Така модель безпеки передбачає гнучке управління правами доступу, моніторинг поведінки та застосування контекстної інформації для прийняття рішень про авторизацію. Цей підхід швидко набирає поширення в організаціях по всьому світу як новий стандарт побудови безпечного IT-середовища, орієнтованого на зменшення ризиків та забезпечення стійкості до сучасних загроз.

Концепція архітектури нульової довіри (Zero Trust Architecture) на рисунку 1.1 базується на принципі «нічому не можна довіряти». Цей підхід було запропоновано Джоном Кіндервагом, аналітиком компанії Forrester

Research, у 2010 році у відповідь на зростання кількості внутрішніх та зовнішніх загроз, які класичні моделі мережної безпеки не могли ефективно нейтралізувати [6].

Рисунок 1.1 – Схема основного принципу концепції архітектури нульової довіри

Концепція архітектури нульової довіри (Zero Trust Architecture) ґрунтується на сукупності фундаментальних принципів, які забезпечують багаторівневий контроль доступу та підвищують рівень захищеності мережної інфраструктури. Зокрема, виділяють три базові принципи:

- обов'язкової автентифікації, що передбачає, що кожен запит на доступ до мережних ресурсів або даних розглядається як потенційно небезпечний, незалежно від його джерела. Навіть у випадках, коли ідентифікація користувача вже була здійснена раніше, система повторно ініціює процедуру аутентифікації, забезпечуючи таким чином постійний контроль і підтвердження особи;

- найменших привілеїв, що передбачає, що кожному користувачу або пристрою надаються виключно ті права доступу, які необхідні для виконання конкретних функцій або завдань. Такий підхід мінімізує можливості горизонтального переміщення в мережі у разі компрометації облікових даних та значно знижує ризик несанкціонованого доступу до критично важливої інформації;

- безперервного моніторингу, що базується на постійному зборі, аналізі та оцінці дій користувачів і системної активності в мережі. Завдяки використанню сучасних аналітичних інструментів та механізмів виявлення аномальної поведінки, забезпечується оперативне реагування на потенційні

інциденти безпеки, а також своєчасне виявлення загроз і мінімізація їх наслідків.

Концепція нульової довіри передбачає переосмислення традиційних підходів до забезпечення інформаційної безпеки, зокрема шляхом реалізації постійної верифікації доступу до ресурсів та принципу найменших привілеїв. Запровадження цієї моделі супроводжується низкою важливих переваг:

- підвищена прозорість доступу до ресурсів, яка передбачає детальну ідентифікацію, класифікацію та контроль усіх мережних ресурсів. Це дозволяє організаціям чітко фіксувати, хто саме, з якою метою та за яких умов отримує доступ до тих чи інших даних чи сервісів, що сприяє підвищенню рівня контролю та безпеки в інформаційному середовищі;

- зменшення площі атаки, що значно знижує ризики для організацій, оскільки унеможливлює або обмежує реалізацію атак, спрямованих на компрометацію мережного периметра;

- посилений моніторинг та реагування на інциденти, що забезпечується використанням додаткових засобів моніторингу, аналітики та автоматизованого реагування. Це забезпечує більш оперативне виявлення потенційних загроз і сприяє формуванню адаптивної та реактивної системи безпеки.

Разом з цим, впровадження архітектури нульової довіри супроводжується низкою обмежень:

- складність конфігурації, що призводить до труднощів з інтеграцією та налаштуванням окремих компонентів. Зокрема, не всі інформаційні системи підтримують реалізацію принципу найменших привілеїв, що є критично важливим для ефективного функціонування архітектури нульової довіри;

- уразливість до інсайдерських загроз, зокрема дій легітимних користувачів з компрометованими обліковими записами. Додаткові механізми, такі як управління привілейованим доступом (PAM), багатофакторна автентифікація (MFA) та ручна верифікація запитів, частково

можуть нівелювати цей ризик;

- залежність від політик та рішень адміністратора, оскільки будь-які помилки або недбалість у налаштуваннях можуть спричинити втрату доступу до ресурсів або створити вразливості в системі безпеки [7].

Таким чином, концепція архітектури нульової довіри формує нову модель захисту мережної інфраструктури сучасних ІТ-екосистем. Її базові принципи забезпечують багаторівневий контроль доступу та зменшують ризики несанкціонованих дій та витоку конфіденційної інформації, що забезпечує підвищений рівень безпеки в умовах розподілених мережних інфраструктур, динамічного доступу до ресурсів та зростаючої кількості кіберзагроз.

1.2 Архітектура моделі нульової довіри

Концепція архітектури нульової довіри передбачає комплексний підхід до забезпечення безпеки. Наукові дослідження в галузі мережної безпеки все частіше зосереджуються на вивченні та практичному впровадженні принципів архітектури нульової довіри в контексті побудови захищених сегментів мережної інфраструктури. Особливу увагу приділяють інтеграції цієї моделі з сучасними технологіями, такими як віртуальні приватні мережі (VPN), мікросегментація, багатофакторна автентифікація, а також інструментами адаптивного контролю доступу.

На рисунку 1.2 наведено схему реалізації основних принципів концепції архітектура нульової довіри для забезпечення надійного захисту, зменшення ймовірності компрометації ресурсів і даних, а також для ефективного реагування на загрози в реальному часі.

Рисунок 1.2 – Компоненти архітектури нульової довіри

Принципи архітектури нульової довіри включають такі основні компоненти:

- автентифікація та авторизація, що включає використання багатофакторної автентифікації та перевірку ідентифікації користувачів, пристроїв і застосунків, незалежно від того, чи знаходяться вони всередині або поза корпоративною мережею. В роботі [8] автори зазначають, що зловмисники використовують вразливості, що існують в апаратному, програмному та комунікаційному рівнях. Різні типи кібератак включають розподілену відмову в обслуговуванні (DDoS), фішинг, атаки типу «людина посередині», атаки за паролем, віддалені атаки, ескалацію привілеїв та шкідливе програмне забезпечення. Через атаки нового покоління та методи ухилення традиційні системи захисту, такі як брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення, списки контролю доступу тощо, більше не є ефективними у виявленні цих складних атак. Водночас в роботі [9] автори зазначають, що методи багатофакторної автентифікації є ефективним засобом підвищення рівня безпеки автентифікації в рамках моделі нульової довіри;

- мінімізація прав доступу, коли користувачі та пристрої отримують лише ті права доступу, які необхідні для виконання конкретних завдань, що знижує ризик несанкціонованого доступу або витоку інформації. Автори роботи

[10] підкреслюють, що організації можуть використовувати для покращення безпеки своєї мережі впровадження політик та процедур безпеки, зокрема контроль доступу, шифрування та протоколи автентифікації. Також в роботі [11] відзначено, що для підвищення рівня безпеки мережної інфраструктури бажано застосовувати принцип найменших привілеїв, який свідчить, що користувачам і процесам слід надавати лише мінімальний обсяг доступу, необхідний для виконання їх функцій, оскільки це запобігає небажаному доступу до конфіденційної інформації та ресурсів. Застосування списків контролю доступу також можуть гарантувати, що лише визначені користувачі можуть отримати доступ до певних ресурсів. Для запобігання небажаному доступу також можна використовувати шифрування даних;

- мікросегментація мереж дозволяє поділити мережі на менші ізольовані сегменти, доступ до яких суворо контролюється, що дозволяє знизити потенційний вплив атак та обмежити їх поширення всередині організації. В роботі [12] підтверджується, що методи сегментації широко використовуються в корпоративних комп'ютерних мережах. Зазначені методи передбачають сегментацію мережі на ізольовані кластери з обмеженим міжсегментним обміном, що мінімізує наслідки потенційних атак і підвищує захист конфіденційних даних від несанкціонованого доступу;

- контроль пристроїв та аналіз активності охоплює перевірку всіх пристроїв, що підключаються до мережі, моніторинг їх стану, актуальність програмного забезпечення, а також безперервний збір та аналіз даних про мережну інфраструктуру, трафік і поведінку користувачів для своєчасного виявлення аномалій і потенційних загроз. В дослідженні [13] вказується, що моніторинг кінцевих точок має вирішальне значення для забезпечення безпеки корпоративної мережі. Зниження ризиків несанкціонованого доступу та витоку критичної інформації досягається завдяки моніторингу в реальному часі;

- шифрування та безпечні канали зв'язку застосовуються в усіх комунікаціях в межах архітектури нульової довіри для забезпечення конфіденційності та цілісності даних. В роботах [14, 15] автори відзначають,

що для забезпечення конфіденційності та цілісності даних є ефективним застосування алгоритмів шифрування, які використовуються в VPN-рішеннях, включаючи AES та SSL/TLS. Робота OpenVPN з використанням протоколу SSL/TLS дозволяє інтегрувати політики контролю доступу на рівні груп користувачів, що значно знижує ризик несанкціонованого доступу до ресурсів корпоративної мережі. В роботі [16] детально описано можливості комерційних VPN-сервісів для захисту корпоративних мереж, де основний акцент зроблено на простоту у використанні та надійність шифрування даних. А також поряд з традиційними рішеннями для VPN, популярність набирають хмарні VPN-сервіси, які надають можливість швидкого розгортання та масштабування мережної інфраструктури. В роботі [17] описується, як хмарні рішення дозволяють бізнесу ефективно забезпечувати віддалений доступ до корпоративних ресурсів без необхідності підтримувати власну інфраструктуру. Проте, як зазначають автори, такі рішення часто стають менш контрольованими з точки зору безпеки, що може створювати додаткові ризики;

- централізоване управління доступом забезпечується впровадженням політик доступу, яке забезпечує гнучкий контроль та реагування на зміни в мережному середовищі. В роботах [18-20] автори зазначають, що централізоване управління доступом в межах архітектури нульової довіри реалізується шляхом впровадження політик доступу, зокрема політики найменших привілеїв та динамічного контролю. Це сприяє оперативному реагуванню на зміни в мережному середовищі, а також підвищує загальний рівень безпеки завдяки уніфікованому адмініструванню ідентичностей та довіри між постачальниками послуг.

Таким чином, ефективне впровадження Zero Trust Architecture в контексті побудови захищених сегментів комп’ютерних мереж вимагає комплексного підходу до реалізації її ключових компонентів, що дозволяє значно знизити ризик кіберзагроз та забезпечити високий рівень захисту корпоративної інфраструктури.

1.3 Постановка задачі

З огляду на стрімкий розвиток цифрових технологій, сучасні корпоративні комп'ютерні мережі повинні враховувати зростання кількості точок доступу, мобільних пристроїв, хмарних сервісів і загроз, пов’язаних з віддаленою роботою. В таких умовах стандартна модель захисту з єдиним периметром перестає бути ефективною, оскільки не здатна вчасно виявляти або блокувати загрози, що виникають як ззовні, так і всередині самої організації.

Метою дослідження є розробка методу організації захищеного сегмента корпоративної мережі на основі моделі Zero Trust, який забезпечує доступ до ресурсів корпоративної мережі на основі прав та привілеїв користувачів. Реалізація включає використання OpenVPN для створення шифрованого тунелю, FreeRADIUS як централізованого вузла автентифікації та RBAC для керування доступом відповідно до ролей користувачів, що дозволяє реалізувати концепцію архітектури Zero Trust в побудованому сегменті для підвищення рівня безпеки, захисту конфіденційних даних користувачів та ресурсів мережі від несанкціонованого доступу та витоку інформації.

2 МЕТОДИ ТА ТЕХНОЛОГІЇ РЕАЛІЗАЦІЇ ПРИНЦИПІВ КОНЦЕПЦІЇ ZERO TRUST

В сучасних умовах зростаючих кібератак концепція Zero Trust набуває особливої актуальності як один з провідних підходів до побудови захищеної інфраструктури IT-екосистем. Концепція Zero Trust базується на принципі «ніколи не довіряй, завжди перевіряй», згідно з яким жоден користувач, пристрій або процес не вважається апріорі надійним, незважаючи на те, що він може знаходиться у внутрішньому периметрі мережі. Це означає, що кожен запит до інформаційного ресурсу має проходити повну перевірку автентичності, авторизації та відповідності політикам безпеки, незалежно від місця походження запиту чи рівня попереднього доступу.

На відміну від традиційних моделей безпеки, що передбачають автоматичне надання довіри після входу до корпоративної мережі, в моделі Zero Trust запроваджено постійний контроль доступу, ізоляцію сесій та мінімізацію привілеїв, орієнтуючись на максимально можливу сегментацію середовища. Технології VPN, а також механізми багатофакторної автентифікації відіграють ключову роль в реалізації концепції Zero Trust, оскільки забезпечують захищене з’єднання, перевірку прав доступу та контрольований обмін трафіком між компонентами системи.

2.1 Методи реалізації принципів концепції Zero Trust

Забезпечення надійних та захищених каналів зв’язку є одним з ключових елементів реалізації моделі нульової довіри. Відсутність довіри за замовчанням до будь-якого користувача, який знаходиться навіть у внутрішньому периметрі корпоративної мережі, означає необхідність повної ізоляції мережного середовища від потенційних загроз, включаючи перехоплення даних, їх модифікацію або несанкціонований доступ до

ресурсів мережі. Використання сучасних протоколів тунелювання, які забезпечують конфіденційність, цілісність та автентичність переданої інформації, дозволяє забезпечити надійні та захищені канали передачі даних. Зокрема, IPsec, SSH, SSL/TLS, WireGuard та OpenVPN дозволяють створювати захищені логічні канали поверх відкритих або потенційно ненадійних мереж. Використання цих технологій в межах моделі Zero Trust забезпечує гранулярний контроль доступу, шифрування трафіку та мінімізацію ризиків витоку або компрометації даних на рівні мережної взаємодії.

Virtual Private Network (VPN) дає можливість створити захищений віртуальний канал поверх існуючої мережі, що гарантує шифрування та ізоляцію всього трафіку між двома кінцевими точками (рисунок 2.1). В рамках архітектури Zero Trust будь-який запит користувача на підключення спочатку повинен проходити перевірку ідентичності та авторизацію, а лише потім переходити до обміну даними. VPN-технології відповідають цим вимогам шляхом:

- шифрування та захисту від несанкціонованого перехоплення;
- контролю цілісності переданих пакетів;
- сегментації мережі шляхом створення ізольованих тунелів [21].

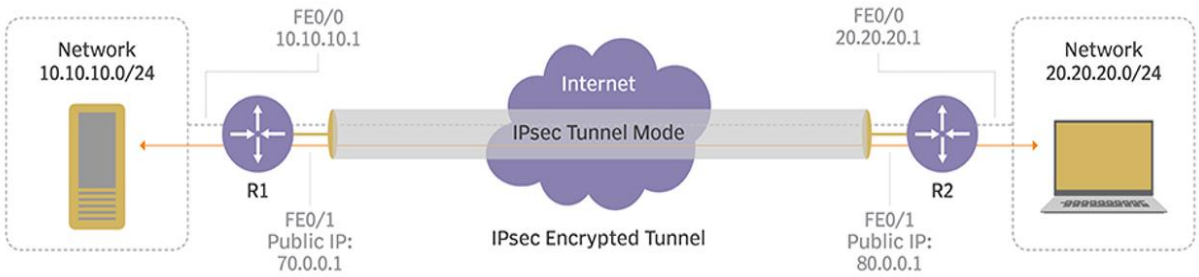

Рисунок 2.1 – Схема організації туленювання з протоколом IPSec

В сучасних комп’ютерних мережах виділяють такі основні типи VPN, кожен з яких має власні переваги та обмеження:

- Point-to-Point VPN дозволяє одному пристрою безпечно

підключатися до іншого. Такий VPN шифрує трафік між двома визначеними точками, захищаючи дані під час передавання і використовується, коли потрібно забезпечити безпечний зв’язок між двома фіксованими пристроями. Залежно від реалізації, тунелі Point-to-Point можуть працювати на канальному або мережному рівнях;

- Site-to-Site VPN встановлює тунель між двома мережними шлюзами, шифруючи весь трафік між цілими підмережами. Цей тип VPN часто застосовують банки та офіси для безпечної передачі транзакційних даних між різними локаціями без участі кінцевих пристроїв користувачів;

- Remote Access VPN дозволяє окремому пристрою безпечно підключитися до мережі. Завдяки тому, що пристрої отримують динамічну IP-адресу з пулу визначених адрес, це дозволяє застосовувати політики доступу на основі ідентичності, не прив'язаної до IP-адреси. На відміну від Point-to-Point, цей тип не вимагає постійного з'єднання між пристроями, оскільки користувач встановлює тунель до мережного шлюзу компанії. Це зручно для віддаленої роботи, адже працівник може отримати доступ до внутрішніх ресурсів компанії, ніби він фізично перебуває в офісі [22].

Шифрування відіграє ключову роль для VPN-технологій у забезпеченні конфіденційності, цілісності та достовірності переданих даних. Одним з найпоширеніших підходів до шифрування в VPN є використання алгоритму Advanced Encryption Standard (AES), який забезпечує високий рівень стійкості до криптографічних атак при помірному навантаженні на ресурси системи [23].

Алгоритм AES є симетричним блочним шифром, який застосовується для забезпечення конфіденційності інформації завдяки високій стійкості до криптографічних атак. AES передбачає три основні модифікації — AES-128, AES-192 та AES-256, де числове значення вказує на довжину криптографічного ключа у бітах. Збільшення довжини ключа підвищує рівень криптографічної стійкості, але водночас призводить до певного зниження швидкодії операцій шифрування та дешифрування [24].

Серед сучасних перспективних алгоритмів варто видокремити ChaCha20, який забезпечує високий рівень безпеки та продуктивності, особливо в умовах обмежених апаратних ресурсів. На відміну від традиційних рішень, ChaCha20 реалізує спрощену модель шифрування, яка не потребує складної інфраструктури сертифікатів, завдяки використанню пари відкритого та приватного ключів. Незважаючи на спрощений підхід, алгоритм зберігає високий рівень стійкості до атак шляхом мінімізації вразливих елементів в процесі обробки даних. [25]. Недоліками цього алгоритму є відсутність апаратного прискорення на більшості процесорів, на відміну від AES, який широко підтримується на рівні апаратного забезпечення, а також потреба в надійній генерації одноразового значення nonce, повторне використання якого може призвести до повної компрометації шифрування.

Автентифікація є ключовим етапом в процесі встановлення безпечного з'єднання, оскільки вона дозволяє ідентифікувати суб'єкта доступу – користувача або пристрій, який ініціює сеанс взаємодії з системою через тунель. Одним з найбільш надійних механізмів є двостороння автентифікація, за якої клієнт та сервер зобов'язані засвідчити свою автентичність один перед одним. Такий підхід зазвичай реалізується з використанням цифрових сертифікатів, зокрема стандарту X.509, що дозволяє забезпечити високий рівень довіри між сторонами та мінімізувати ризик несанкціонованого доступу до ресурсів мережі.

Для організації захищеного каналу зв'язку між пристроями мережі використовуються сучасні протоколи тунелювання, зокрема IPsec, SSL/TLS у складі OpenVPN, SSH та WireGuard. Кожен з них характеризується власними криптографічними підходами, рівнем продуктивності, масштабованістю та відповідністю принципам Zero Trust. В таблиці 2.1 наведено основні переваги та недоліки цих протоколів та їх відповідність ключовим вимогам архітектури нульової довіри.

Таблиця 2.1 – Порівняння протоколів тунелювання

Протокол	Переваги	Недоліки	Відповідність Zero Trust
IPsec	Висока продуктивність; підтримка апаратного прискорення	Складність конфігурації; обмеження в мобільних і динамічних мережах	потребує додаткових механізмів контролю доступу та автентифікації
SSH	Інтеграція автентифікації, шифрування та керування доступом на рівні сесії	не підтримує масштабування; потребує ручного адміністрування	придатний для точкових з’єднань, не підтримує динамічного керування доступом
WireGuard	Простота конфігурації; висока швидкість; сучасна криптографія	Відсутність підтримки TCP, сертифікатів, RADIUS, LDAP; обмежена масштабованість	відсутній вбудований механізм ролей та динамічного контролю
OpenVPN	Гнучкість; підтримка NAT, TCP, сертифікатів, LDAP/RADIUS, ролей та політик	складність налаштування та адміністрування;	підтримка багаторівневої автентифікації, контроль доступу

Протокол IPsec є широко застосовуваним у сценаріях Site-to-Site VPN для забезпечення стабільного та централізованого керованого зв’язку між двома фіксованими мережами. До його переваг відносять підтримку апаратного прискорення та високу сумісність з мережним обладнанням, зокрема маршрутизаторами та міжмережними екранами. Основними недоліками цього протоколу вважають високу складність конфігурації, залежність від зовнішніх служб для обміну ключами та обмежену гнучкість в мережах мобільного зв’язку та з динамічною маршрутизацією.

Протокол SSH широко застосовується для безпечного адміністрування

серверів, а також для створення захищених тунелів типу Point-to-Point між окремими пристроями. Основною перевагою протоколу є підтримка автентифікації, авторизації та шифрування. SSH застосовується в мережах з ручним управлінням доступом або в складі інших протоколів тунелювання для захищеного доступу до внутрішніх ресурсів. Він не підтримує централізоване управління політиками доступу та не призначений для масштабованих та сегментованих мережних інфраструктур, що обмежує його використання в сучасних корпоративних мережах.

До переваг протоколу WireGuard відносять простоту конфігурації в поєднанні з сучасними та стійкими криптографічними алгоритмами, що забезпечує простоту адміністрування та конфігурації. Проте основними недоліками WireGuard є відсутність підтримки TCP, сертифікатів, динамічного призначення IP-адрес, а також інтеграції з LDAP/AD, що обмежує його придатність в складних та масштабованих мережних інфраструктурах корпоративних мереж. Постійне збереження статичних IP-адрес для учасників пірів суперечить принципу збереження конфіденційності в концепції Zero Trust, через що цей протокол не використовують в корпоративних мережах, які застосовують архітектуру нульової довіри.

Протокол OpenVPN демонструє високу гнучкість та масштабованість. Що забезпечує його широке використання в корпоративних комп’ютерних мережах. Завдяки використанню TLS як транспортного протоколу, він підтримує передачу даних за протоколами TCP та UDP, що забезпечує сумісність з мережними фільтрами, NAT та фаєрволами. OpenVPN підтримує сертифікати, централізовану автентифікацію, зокрема, через RADIUS або LDAP, динамічне призначення IP-адрес та ведення детального журналювання подій, що відповідає ключовим принципам Zero Trust, зокрема політики найменших привілеїв, шифрування трафіку, багатофакторної автентифікації та оцінки кожного запиту [26–29].

Одним з ключових механізмів реалізації архітектури Zero Trust є мережна сегментація, яка забезпечує поділ мережі на ізольовані сегменти з

чітко визначеними політиками доступу. Основним підходом виступає логічний поділ мережі на підмережі, що дозволяє обмежити взаємодію між пристроями до принципу найменших привілеїв. Це зменшує поверхню атаки та дозволяє точково контролювати та перевіряти кожну сесію зв'язку.

Додатковим засобом досягнення сегментації є використання віртуальних локальних мереж (VLAN), які дають змогу об'єднувати пристрої в окремі логічні групи, незалежно від їх фізичного розташування (рисунок 2.2). Це дозволяє гнучко ізолювати користувачів відповідно до їх функціональних ролей та впроваджувати диференційовані політики контролю доступу на рівні кожного VLAN.

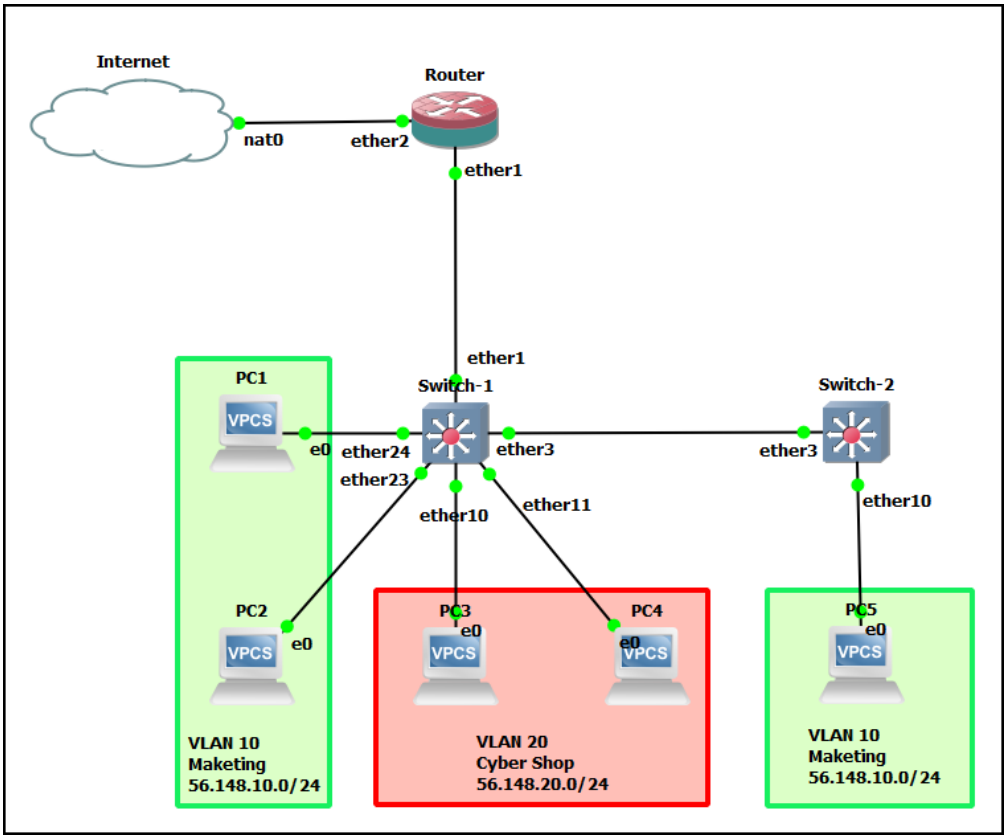

Рисунок 2.2 – Сегментація комп'ютерної мережі

В рамках Zero Trust архітектури така сегментація підкріплюється централізованою перевіркою політик доступу, включаючи ідентичність користувача або пристрою, геолокацію, тип запитуваного ресурсу, час доступу та рівень ризику. Таким чином пристрої, розташовані в одній VLAN

або підмережі, не мають автоматично довірених прав доступу один до одного без попередньої перевірки та авторизації.

Таким чином, мережна сегментація в Zero Trust моделі виконує лише функцію обмеження трафіку та є інструментом динамічного управління довірою, що суттєво підвищує рівень безпеки та стійкості корпоративної мережі до внутрішніх та зовнішніх загроз [30].

2.2 Методи управління правами та привілеями користувачів

Централізоване управління правами доступу та привілеями користувачів до ресурсів корпоративної мережі є важливим механізмом реалізації принципу найменших привілеїв в архітектурі нульової довіри. Такий розподіл доступу здійснюється з використанням моделі Role-Based Access Control (RBAC), що передбачає призначення дозволів на основі ролей та привілеїв користувачів відповідно до встановлених адміністратором політик доступу до ресурсів мережі. Це дозволяє забезпечити прозорість, гнучкість та контрольованість у наданні доступу до інформаційних ресурсів, знижуючи ризики неправомірного або несанкціонованого доступу.

Для реалізації моделі управління доступом використовується RADIUS сервер, який виконує функції обробки запитів на автентифікацію та передає VPN-серверу атрибути, які пов’язані з ролями користувачів. На основі цих атрибутів формується набір політик доступу до мережних ресурсів або окремих сегментів корпоративної мережі. Інтеграція механізмів RBAC з функціоналом RADIUS-серверу дозволяє впровадити динамічну авторизацію, забезпечуючи гнучке управління правами доступу в режимі реального часу під час кожного сеансу. Також це дозволяє реалізувати прозору взаємодію з системами управління ідентичностями, які є ключовими елементами Zero Trust-архітектури [31].

Логіка функціонування RADIUS серверу базується на трьох основних функціях: автентифікація, авторизація та облік. Автентифікація визначає

користувача або пристрій, який намагається отримати доступ, шляхом перевірки облікових даних, зокрема логіну та паролю, а в випадках більш суворого контролю – токену. Авторизація забезпечує дозвіл на виконання визначених дій користувачу після успішної автентифікації, зокрема доступ до певного сервісу чи ресурсу. Облік забезпечує фіксацію інформації про активність користувача, зокрема час входу, тривалість сесії, обсяг переданих даних. На рисунку 2.3 наведено узагальнену схему автентифікації через RADIUS сервер, яка може бути реалізована на хмарних платформах або в локальних корпоративних мережах. Під час ініціації VPN-з'єднання від користувача надходить запит на встановлення підключення до VPN-шлюзу, який виконує функції RADIUS-клієнта. Шлюз формує запит типу «Access-Request», що містить облікові дані користувача, зокрема пароль та логін, а також технічні параметри підключення, зокрема IP-адресу, порт з'єднання, та передає його на RADIUS-сервер, який розгорнуто на основі служби політик мережі. RADIUS-сервер після отримання запиту здійснює первинну автентифікацію через зовнішню систему управління обліковими записами, зокрема Active Directory. В разі успішної перевірки облікових даних, сервер ініціює процедуру багатофакторної автентифікації. Після підтвердження другої форми автентифікації формується відповідь у вигляді «Access-Accept» або в разі не підтвердження автентифікації формується відмова в доступі, яка повертається на VPN-шлюз. Таким чином, в разі успішної автентифікації встановлюється захищений тунель між користувачем та VPN-сервером, який дозволяє користувачеві безпечно взаємодіяти з корпоративною мережею та отримати доступ до визначених політикою доступу ресурсів мережі. [32].

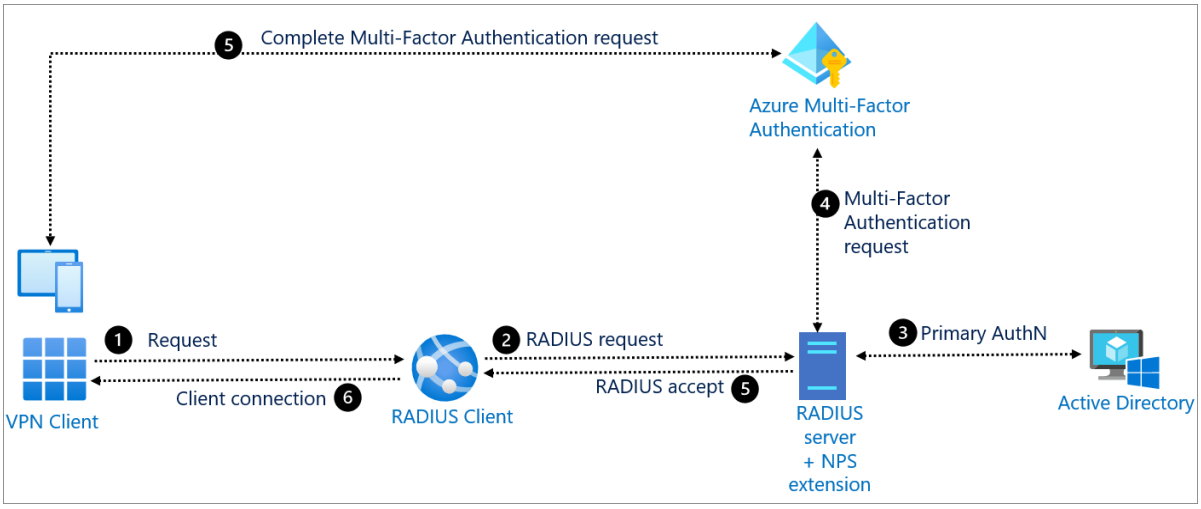

Рисунок 2.3 – Схема автентифікації через RADIUS сервер

В межах концепції Zero Trust рольовий підхід передбачає класифікацію користувачів за функціональними категоріями, кожній з яких призначається визначений набір дозволів і ресурсів, необхідних виключно для виконання службових обов'язків [33]. Проте в концепції архітектури нульової довіри авторизація не обмежена лише статичним розподілом ролей, також вона доповнюється контекстною оцінкою підключення, зокрема тип і стан пристрою, географічне розташування користувача, час доступу, операційна система користувацького пристрою, наявність відповідних сертифікатів, стан антивірусного ПЗ тощо. В разі виявлення потенційно ненадійного, незареєстрованого або скомпрометованого пристрою, система автоматично знижує рівень довіри до користувача, обмежуючи його доступ лише до тих ресурсів, що відповідають політикам доступу для звичайних користувачів або ініціює додаткові механізми автентифікації. Такий підхід забезпечує постійний контроль за кожним сеансом доступу. Це гарантує, що після успішної автентифікації, користувач не отримує автоматичного повного доступу, а кожен наступний запит підлягає повторній перевірці відповідно до його ролі та актуального рівня довіри. Таким чином інтеграція механізмів RBAC з технологіями захищеного зв'язку за допомогою служб RADIUS та LDAP або Active Directory, забезпечує гнучке, масштабоване та адаптивне управління правами доступу. Це дозволяє реалізувати основні принципи Zero

Trust, зокрема мінімізацію привілеїв, контекстно-залежну авторизацію та безперервний моніторинг активності користувачів.

Таким чином, впровадження архітектури Zero Trust вимагає всебічного та системного підходу, що охоплює вибір відповідних протоколів захищеного зв’язку, методів автентифікації, забезпечення безперервного моніторингу, верифікації кожного запиту на доступ, а також логічної сегментації мережної інфраструктури. Використання VPN-технологій є одним з ключових механізмів забезпечення безпечного доступу до ресурсів корпоративної комп’ютерної мережі. Зокрема, протокол OpenVPN, який може бути використаний для побудови захищених каналів зв’язку, підтримує централізовану автентифікацію, гнучке управління політиками доступу, інтеграцію із зовнішніми службами RADIUS та LDAP, а також надає широкі можливості для детального логування подій. Це робить OpenVPN ефективним інструментом для реалізації захищених комунікацій в корпоративних комп’ютерних мережах, побудованих на основі моделі Zero Trust. Також важливу роль в побудові такої архітектури відіграє мережна сегментація, яка забезпечує ізоляцію критично важливих ресурсів та контроль над міжсегментною взаємодією, що дозволяє мінімізувати ризики несанкціонованого доступу та витоку інформації.

3 РОЗРОБКА ЗАХИЩЕНОГО СЕГМЕНТА КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Моделювання захищеного сегменту корпоративної мережі

Моделювання захищеного сегменту корпоративної мережі виконувалось на основі аналізу апаратних вимог до побудови захищеного сегменту. Для розгортання VPN-серверу було використано хост-машину з операційною системою Ubuntu 20.04 LTS, процесором з щонайменше 1 ядром та максимальною частотою 2,9 ГГц. Об'єм ОЗУ залежить від кількості апаратних ресурсів, що надані віртуальній машині. З практичної точки зору, обсяг 2048 МБ ОЗУ забезпечує ефективне функціонування такої конфігурації, а рівень апаратних ресурсів дозволяє моделювати інфраструктуру, яку можна застосовувати в умовах малого та середнього бізнесу з можливістю масштабування за наявності апаратних ресурсів. Пропускна здатність каналу повинна становити не менше 1 Гбіт/с.

Для забезпечення захищеного зв'язку було налаштовано VPN- сервер на основі протоколу OpenVPN, який інтегрується з сервером автентифікації FreeRADIUS та службою каталогів LDAP для централізованого зберігання облікових записів. На рисунку 3.1 наведено схему реалізації захищеного сегмента корпоративної комп'ютерної мережі, де RADIUS-сервер є окремим пристроєм мережі, а VPN- сервер після проходження автентифікації ініціалізує з'єднання користувача з визначеним сегментом корпоративної мережі.

Додатково впроваджено багатофакторну автентифікацію з використанням одноразових кодів, що підвищує рівень безпеки доступу. Для розподілу прав та привілеїв користувачів та забезпечення контрольованого доступу до ресурсів корпоративної комп'ютерної мережі загальна кількість користувачів була поділена на групи: адміністратор, розробник та гість, які мають визначені дозволи на доступ до окремих ресурсів корпоративної мережі (рисунок 3.1). Розподіл ролей, привілеїв користувачів та їх дозволи на

доступ до окремих ресурсів наведені в таблиці 3.1.

Таблиця 3.1 – Розподіл ролей та привілеїв користувачів в захищеному сегменті корпоративної мережі

Роль	Рівень довіри	Права доступу	Ресурси мережі
Адміністратор	Високий	всі права	до всіх пристроїв мережі
Розробник	Середній	обмежені	192.168.1.10; 192.168.1.20
Гість	Низький	мінімальні	192.168.1.20

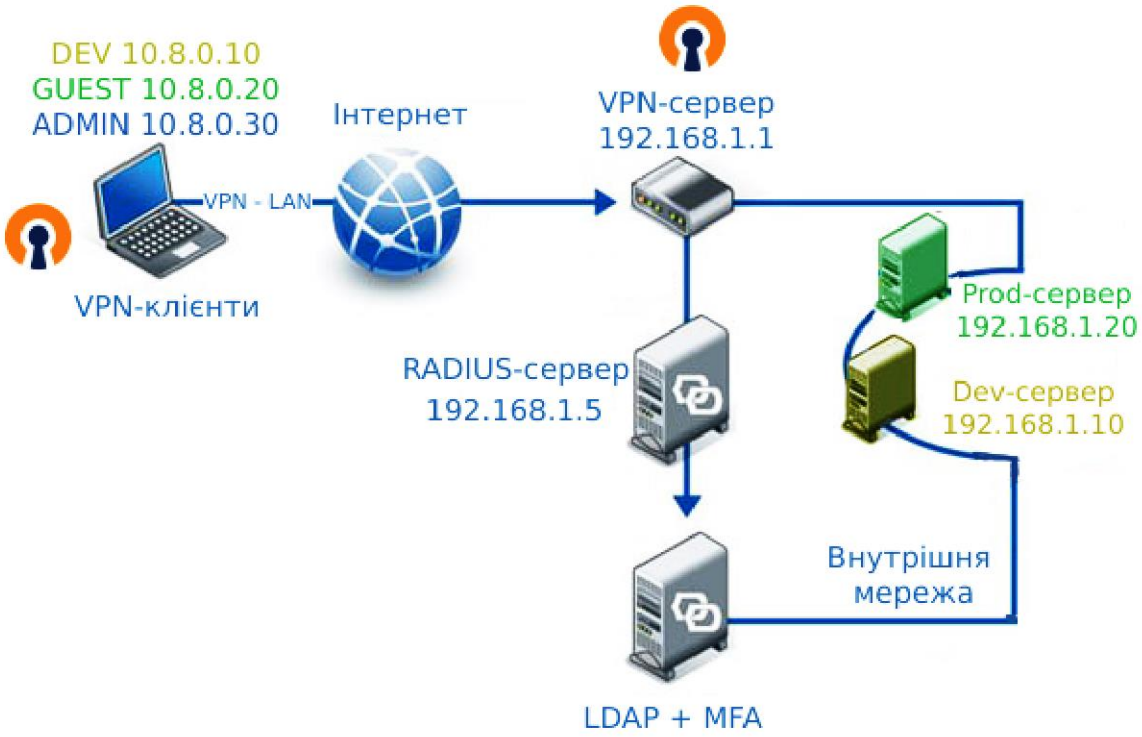

Рисунок 3.1 – Схема захищеного сегменту корпоративної комп’ютерної мережі

Доступ до захищеного сегменту корпоративної мережі 192.168.1.0/24 здійснюється через VPN-з’єднання на основі прав і привілеїв користувачів. Такий підхід дає змогу реалізувати ефективний контроль доступу та знизити

ризики несанкціонованого доступу до ресурсів мережі. Додатково було налаштовано правила доступу до ресурсів відповідно до встановлених прав користувачів. На рисунку 3.2 представлено розподіл ресурсів згідно з правилами та політиками доступу в межах захищеного сегмента. Користувачі, які мають права адміністратора, отримують доступ до всіх ресурсів мережі, тоді як інші групи користувачів мають доступ лише до визначених адміністратором ресурсів.

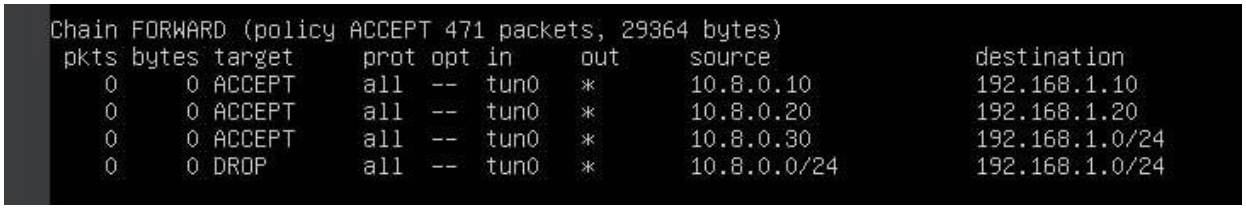

Рисунок 3.2 – Політики доступу до десурсів захищеного сегмента корпоративної мережі

Для забезпечення захищеного зв’язку в конфігураційному файлі VPN-сервера були додані опціонально порт з’єднання, алгоритм шифрування та протокол, за яким здійснюється передача даних в тунелі. Основні налаштування VPN-сервера наведено в конфігураційному файлі (лістинг 3.1).

Лістинг 3.1 – Конфігурація server.conf

```
port 1194
proto udp
dev tun0

# SSL/TLS
ca /etc/openvpn/easy-rsa/pki/ca.crt
cert /etc/openvpn/easy-rsa/pki/issued/server.crt
key /etc/openvpn/easy-rsa/pki/private/server.key
dh /etc/openvpn/easy-rsa/pki/dh.pem

# TOPOLOGY
topology subnet
server 10.8.0.0 255.255.255.0  # Clients' VPN-pool

# RADIUS
plugin /usr/lib/openvpn/radiusplugin.so
/etc/openvpn/radiusplugin.cnf
```

```
client-config-dir /etc/openvpn/ccd

keepalive 10 120
persist-key
persist-tun
verb 3
```

Для реалізації перевірки облікових даних через RADIUS-сервер було використано плагін radiusplugin. Основні налаштування наведено в конфігураційному файлі (лістинг 3.2).

Лістинг 3.2 – Конфігурація RADIUS-сервера

```
authorize {
    filter_username
    preprocess
    chap
    mschap
    digest
    suffix
    eap {
        ok = return
    }
    ldap
    if ((ok || updated) && User-Password && !control:Auth-Type)
    {
        update {
            control:Auth-Type := pam
        }
    }
    expiration
    logintime
    pap
    Autz-Type New-TLS-Connection {
        ok
    }
}
authenticate {
    Auth-Type PAP {
        pap
    }
    Auth-Type PAM {
        pam
    }
}
```

Після завершення налаштувань було здійснено тестування працездатності VPN-сервера, який забезпечує встановлення з’єднання з користувачем

відповідно до призначеної ролі та рівня привілеїв (рисунки 3.3, 3.4).

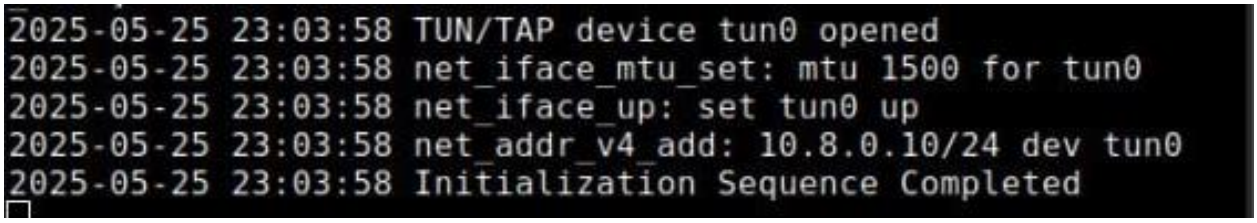

Рисунок 3.3 – Успішне підключення користувача devuser до визначених його роллю ресурсів

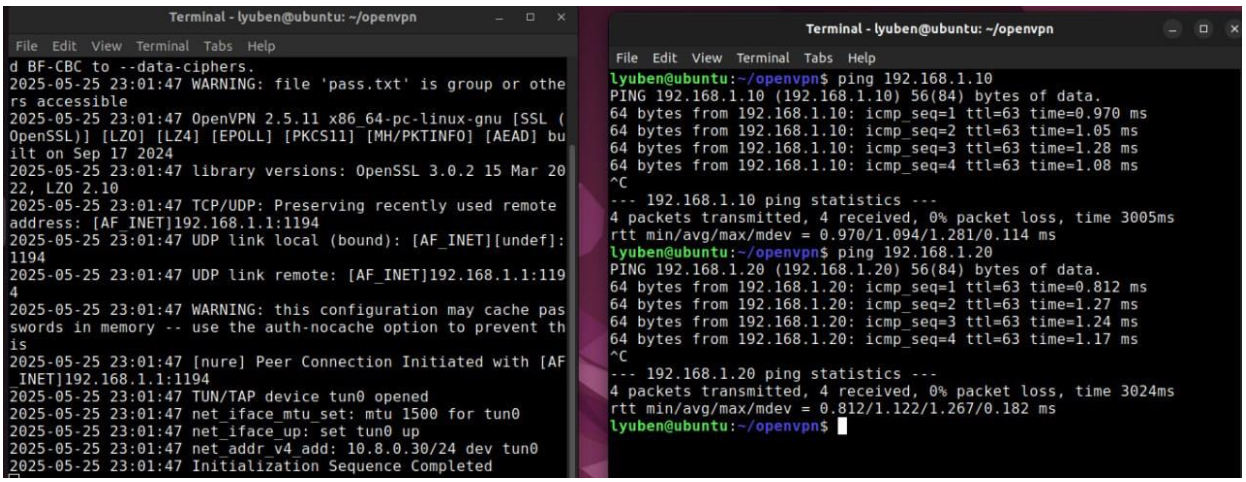

Рисунок 3.4 – Успішне підключення користувача adminuser до визначених його роллю ресурсів

Додатково було проведено тестування на використання скомпрометованих даних користувача для перевірки механізмів авторизації та автентифікації (рисунок 3.5). В результаті тестування було визначено невірні облікові дані користувача, що призводить до відмови в доступі до ресурсів корпоративної комп’ютерної мережі.

Після налаштування VPN-з'єднання було здійснено детальний аналіз роботи даної мережної моделі за допомогою програмного засобу Wireshark. Загальний час спостереження склав 12,89 хв. На рисунку 3.6 наведено вміст потоку TCP-пакетів, який показує спотворення вмісту пакетів через шифрування, що підтверджує передачу даних через налаштоване VPN-з'єднання. За результатами досліджень було отримано наступні дані

ключових параметрів аналізу, які наведено в таблиці 3.2.

```
lyuben@ubuntu:~/devuser$ sudo openvpn --config dev.ovpn
2025-05-25 23:04:34 --cipher is not set. Previous OpenVPN version defaulted to BF-CBC as fal
lback when cipher negotiation failed in this case. If you need this fallback please add '--d
ata-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2025-05-25 23:04:34 WARNING: file 'pass.txt' is group or others accessible
2025-05-25 23:04:34 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [
PKCS11] [MH/PKTINFO] [AEAD] built on Sep 17 2024
2025-05-25 23:04:34 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2025-05-25 23:04:34 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.1:1
194
2025-05-25 23:04:34 UDP link local (bound): [AF_INET][undef]:1194
2025-05-25 23:04:34 UDP link remote: [AF_INET]192.168.1.1:1194
2025-05-25 23:04:34 WARNING: this configuration may cache passwords in memory -- use the aut
h-nocache option to prevent this
2025-05-25 23:04:35 [nure] Peer Connection Initiated with [AF_INET]192.168.1.1:1194
2025-05-25 23:04:36 AUTH: Received control message: AUTH_FAILED
2025-05-25 23:04:36 SIGTERM[soft,auth-failure] received, process exiting
lyuben@ubuntu:~/devuser$
```

Рисунок 3.5 – Відмова в доступі до ресурсів користувача зі скомпроментованими обліковими даними

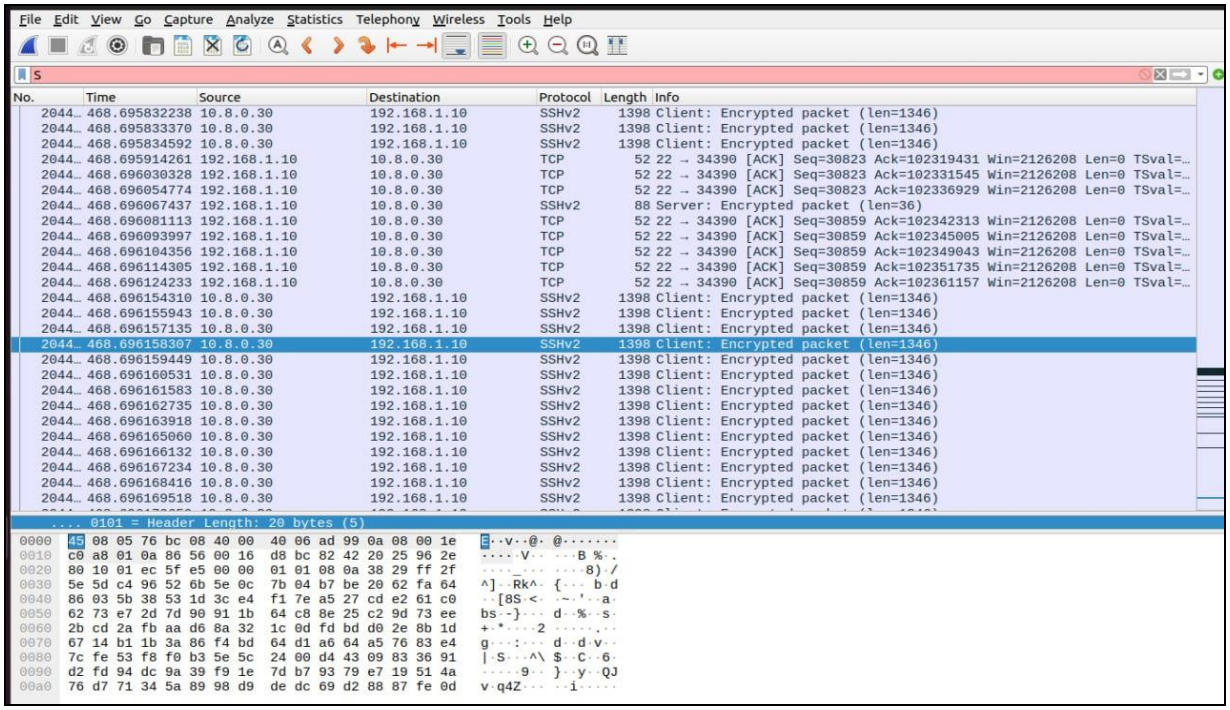

Рисунок 3.6 – Візуалізація шифрованого потоку TCP-пакетів VPN-тунелю в Wireshark

Таблиця 3.2 – Результати досліджень моделі захищеного сегменту

Параметр	Значення
Коефіцієнт завантаження (ρ)	0.9
Середня кількість запитів у системі (L)	9.12
Середня кількість у черзі (Lq)	8.19
Середній час перебування запиту в системі (W), с	0.0676 с
Середня кількість у черзі (Lq)	8.19

В результаті проведеного тестування підтверджено, що організований захищений сегмент корпоративної мережі відповідає принципам архітектури Zero Trust. Реалізація всіх ключових етапів, зокрема ідентифікації, автентифікації, авторизації та маршрутизації, була здійснена з використанням OpenVPN, FreeRADIUS, LDAP та Google Authenticator. Завдяки впровадженню рольової моделі доступу (RBAC), мережної сегментації та фільтрації за IP-адресами забезпечено надійну ізоляцію ресурсів та контроль доступу відповідно до ролей користувачів.

3.2 Аналітичне моделювання роботи захищеного сегменту мережі

Для оцінки ключових показників ефективності захищеного сегменту корпоративної комп'ютерної мережі, до складу якого входить VPN-сервер та RADIUS-сервер, інтегрований з LDAP-службою автентифікації, було застосовано модель системи масового обслуговування типу M/M/1 [34]. Ця модель дозволяє проаналізувати навантаження на підсистему автентифікації при підключенні клієнтів до VPN в режимі реального часу. В моделі передбачено, що користувацькі запити на встановлення VPN-з'єднання надходять до RADIUS-сервера з середньою інтенсивністю λ=10 зап/с, що

відповідає середньому числу одночасно активних користувачів, які звертаються до ресурсів захищеного сегменту корпоративної комп'ютерної мережі. Інтенсивність обслуговування, тобто вихідного потоку, становить $\mu = 15$ зап/с, що враховує процес автентифікації, встановлення захищеного сеансу з'єднання та обробку надісланих пакетів.

Коефіцієнт завантаження системи ρ дозволяє оцінити ступінь завантаженності системи. Робота системи вважається стабільною за умови $\rho < 1$. Коефіцієнт завантаження системи обчислюється як:

$$\rho = \frac{\lambda}{\mu}, \tag{3.1}$$

де λ – інтенсивність вхідного потоку запитів, од;

μ – інтенсивність вихідного потоку запитів, од.

Середня кількість запитів L показує кількість запитів, які одночасно знаходяться в системі, в черзі та на обслуговуванні. Цей показник вказує на завантаженість системи в будь-який момент часу і розраховується як:

$$L = \frac{\lambda}{\mu - \lambda}, \tag{3.2}$$

де λ – інтенсивність вхідного потоку запитів, од;

μ – інтенсивність вихідного потоку запитів, од.

Середня кількість запитів в черзі L_q показує кількість запитів, які надійшли до системи, але очікують обробку в черзі. Цей показник відображає наявність затримок в системі до початку обслуговування запитів і може бути пов'язаний з затримками, що викликані обмеженою пропускною здатністю сервера, високим навантаженням системи або нерівномірністю надходження запитів. Зростання цього показника збільшує час очікування користувачів на

обслуговування, що знижує якість обслуговування. Показник середньої кількості запитів в черзі розраховується як:

$$L_q = \frac{\lambda^2}{\mu(\mu - \lambda)^2}, \tag{3.3}$$

де λ – інтенсивність вхідного потоку запитів, од;

μ – інтенсивність вихідного потоку запитів, од.

Середній час перебування запиту в системі W важливий для оцінки загальної затримки в системі. Він враховує час, який запит проводить в системі в очікуванні обробки та безпосередньо час обслуговування. Середній час перебування запиту в системі розраховується як:

$$W = \frac{1}{\mu - \lambda}, \tag{3.4}$$

де λ – інтенсивність вхідного потоку запитів, од;

μ – інтенсивність вихідного потоку запитів, од.

Окремо аналізується середній час в черзі W_q. Цей показник демонструє чутливість системи до зміни інтенсивності трафіку:

$$W_q = \frac{\lambda}{\mu(\mu - \lambda)^2}, \tag{3.5}$$

де λ – інтенсивність вхідного потоку запитів, од;

μ – інтенсивність вихідного потоку запитів, од.

За результатами моделювання було отримано наступні результати, що наведені в таблиці 3.3 та побудовано графік залежності середньої затримки системи від кількості користувачів, які одночасно перебувають в системі

(рисунок 3.7). Графік демонструє, що зі збільшенням кількості користувачів, які одночасно проходять автентифікацію під час підключення, навантаження на систему суттєво зростає, що призводить до збільшення затримок у обробці запитів.

Таблиця 3.3 – Результати аналітичного моделювання

Показник	значення
Коефіцієнт завантаження системи	0.67
Середня кількість запитів у системі, од	2.00
Середній час перебування в системі, с	0.2000
Середня кількість запитів у черзі, од	1.33
Середній час очікування в черзі, с	0.1333

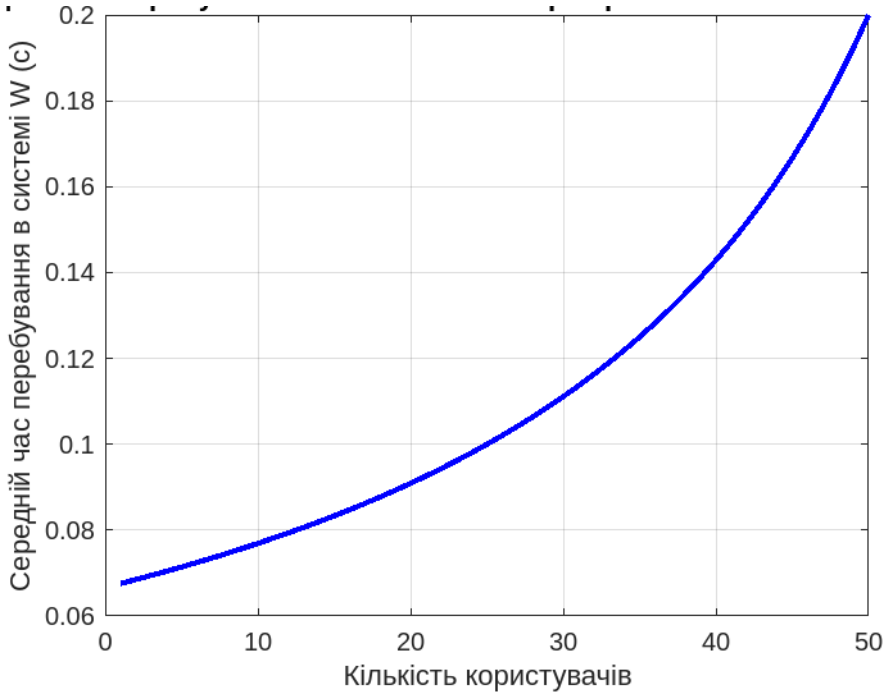

Рисунок 3.7 – Графік залежності середньої затримки від кількості користувачів в системі

Таким чином, результати аналітичного моделювання підтверджують ефективність реалізованого підходу до побудови захищеного сегменту

корпоративної комп'ютерної мережі з використанням VPN-сервера, централізованої автентифікації через RADIUS-сервер в інтеграції з LDAP та Google Authenticator. Результати аналітичного моделювання доводять доцільність запропонованої архітектури, яка поєднує принципи мережної сегментації, рольової авторизації та багатофакторної автентифікації відповідно до концепції Zero Trust.

На основі результатів аналітичного та експериментального моделювання захищеного сегменту корпоративної комп'ютерної мережі з реалізацією VPN, RADIUS-сервера та LDAP, які наведено в таблиці 3.4, встановлено, що система демонструє ефективну роботу в умовах підвищеного навантаження.

Таблиця 3.4 – Результати моделювання і тестування моделі захищеного сегменту корпоративної мережі

Показник	аналітичне моделювання	тестування
Коефіцієнт завантаження системи	0.67	0.9
Середня кількість запитів у системі, од	2.00	9.12
Середній час перебування в системі, с	0.2000	8.19
Середня кількість запитів у черзі, од	1.33	0.0676
Середній час очікування в черзі, с	0.1333	8.19

За результатами тестування встановлено, що розгорнута модель функціонує в умовах підвищеного навантаження, зумовленого впровадженням механізмів багатофакторної автентифікації та авторизації в середовищі з обмеженими апаратними ресурсами. Незважаючи на зростання загальної затримки обробки запитів, система демонструє стабільність функціонування. Підвищений час відповіді пояснюється додатковими обчислювальними витратами, пов'язаними з процесами автентифікації, авторизації, а також шифрування та дешифрування даних. Отримані

результати свідчать про працездатність запропонованої архітектури в умовах високого навантаження та обмежених обчислювальних можливостей.

Отримані результати підтверджують, що запропонована архітектура з використанням OpenVPN в поєднанні з FreeRADIUS та LDAP забезпечує високий рівень безпеки, що відповідає концепції Zero Trust, та ефективність обробки запитів при реальному навантаженні. Такий підхід може бути рекомендований для впровадження в корпоративних мережах з підвищеними вимогами до захисту від ризиків несанкціонованого доступу та витоків інформації.

ВИСНОВКИ

В кваліфікаційній роботі розроблено та реалізовано метод побудови захищеного сегменту корпоративної комп’ютерної мережі на основі моделі Zero Trust, яка передбачає відсутність апріорної довіри до будь-яких користувачів або пристроїв, незалежно від їх розташування в мережі. Запропонований метод забезпечує високий рівень захисту від несанкціонованого доступу та витоків інформації завдяки диференційованому підходу до надання доступу на основі ролей та привілеїв користувачів.

Запропонований метод передбачає організацію захищеного сегмента корпоративної мережі з використанням OpenVPN в поєднанні з FreeRADIUS та LDAP для централізованої автентифікації та авторизації користувачів, а також Google Authenticator для впровадження двофакторної автентифікації. Це дозволило реалізувати механізми ізоляції ресурсів та контроль доступу згідно з принципами Zero Trust.

На основі аналітичного та експериментального моделювання підтверджено ефективність запропонованої моделі в умовах підвищених вимог до безпеки. Результати тестування в режимі реального часу свідчать про стабільну та безперебійну роботу системи в умовах підвищеного навантаження. Запропонований підхід може бути рекомендований для використання в корпоративних комп’ютерних мережах, які функціонують в умовах підвищених вимог до забезпечення конфіденційності та цілісності інформації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. New Microsoft guidance for the CISA Zero Trust Maturity Model | Microsoft Security Blog. URL: https://www.microsoft.com/en–us/security/blog/2024/12/19/new–microsoft–guidance–for–the–cisa–zero–trust–maturity–model/ (date of access: 03.05.2025).

2. YESIN, V. I.; VILIHURA, V. V.; UZLOV, D. Y. Огляд існуючих моделей та основних принципів нульової довіри. Radiotekhnika, 2024, 217: 39–54.

3. Tsai M., Lee S., Shieh S. W. Strategy for implementing of zero trust architecture // IEEE Transactions on Reliability. – 2024. – Т. 73. – №. 1. – С. 93–100.

4. KODAKANDLA, Naveen. Securing Cloud–Native Infrastructure with Zero Trust Architecture. Journal of Current Science and Research Review, 2024, 2.02: 18–28.

5. What is Zero–Trust Architecture? A Guide to Blockchain Security BeInCrypto. URL: https://beincrypto.com/learn/zero–trust–architecture–guide. (date of access: 07.05.2025).

6. Хе, Ю., Хуан, Д., Чен, Л., Ні, Ю. та Ма, Х. (2022). Опитування щодо архітектури нульової довіри: виклики та майбутні тенденції. Бездротовий зв'язок та мобільні обчислення , 2022 (1), 6476274.

7. Архітектура нульової довіри: основні принципи, компоненти, плюси та мінуси [Електронний ресурс] / Syteca – 2025. – Режим доступу до ресурсу: https://syteca.bakotech.com/ua/blog/zero_trust_security_model (дата звернення: 03.05.2025).

8. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 2023; 12(6):1333. https://doi.org/10.3390/electronics12061333

9. J. Jose Diaz Rivera, A. Muhammad and W.-C. Song, "Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication," IEEE Open Journal of the Communications Society, vol. 5, pp. 2792–2814, 2024, doi: 10.1109/OJCOMS.2024.3391728

10. Arogundade, O. R. (2023). Network security concepts, dangers, and defense best practical. Computer Engineering and Intelligent Systems, 14(2).

11. Mubeen, M., Arslan, M., & Anandhi, G. (2022). Strategies to Avoid Illegal Data Access. Journal of Communication Engineering & Systems, 12(3), 29-40p.

12. A Al-Ofeishat, H., & Alshorman, R. (2023). Build a secure network using segmentation and micro-segmentation techniques. International Journal of Computing and Digital Systems, 16(1), 1499-1508.

13. Ганусяк С. І. Моніторинг систем кінцевих точок в SOC. ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «ЦИФРОВА ТРАНСФОРМАЦІЯ КІБЕРБЕЗПЕКИ» : зб. тез доп. Всеукр. науково-практ. конференція, м. Київ, 26 квіт. 2024 р. Київ, 2024. С. 23–26.

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

15. ВІНТЕНКО, Борис, et al. Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно–керуючих систем АЕС, важливих для безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024, 3.23: 111–131.

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

17. Santhanamahalingam S., Alagarsamy S., Subramanian K. A study of cloud-based VPN establishment using network function virtualization technique.

2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 20–22 October 2022. 2022. URL: https://doi.org/10.1109/icosec54921.2022.9951894.

18. FERNANDEZ, Eduardo B.; BRAZHUK, Andrei. A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces, 2024, 89: 103832.

19. HELLSTRÖM RYCKERT, Astrid. Zero Trust in Private Home Networks: A Sociotechnical Perspective on Implementing Zero Trust to Enhance Home Network Security. 2025.

20. MEHRA, Taresh. The Critical Role of Role–Based Access Control (RBAC) in securing backup, recovery, and storage systems. International Journal of Science and Research Archive, 2024, 13.1: 1192–1194.

21. ВЕРХОВСЬКИЙ, Ігор; ТКАЧОВ, Віталій. Методи побудови віртуальних тунелів extranet-систем. Scientific review, 2023, 4.89: 22-40.

22. LAWO, Daniel Christian, et al. Wireless and Fiber-Based Post-Quantum-Cryptography-Secured IPsec Tunnel. Future Internet, 2024, 16.8: 300.

23. ТКАЧОВ, В. М.; ЧЕПУРНА, І. С.; ФЕСЕНКО, Т. Г. МЕТОД МУЛЬТИРІВНЕВОГО VPN-ТУНЕЛЮВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІДДАЛЕНОГО ДОСТУПУ ДО ВУЗЛІВ ЕКСТРАНЕТ-МЕРЕЖІ. Вісник Херсонського національного технічного університету, 2024, 3 (90): 299-308.

24. БГАНЦОВ, Євгеній. Шифрування даних. Опис та структура алгоритму симетричного шифрування AES. 2023.

25. JOHANSSON, Vincent. A Comparison of OpenVPN and WireGuard on Android. 2024.

26. What is SSH? [Електронний ресурс] / Secure Shell (SSH) protocol. Cloudflare – 2025. – Режим доступу до ресурсу: https://www.cloudflare.com/learning/access-management/what-is-ssh/ (дата звернення: 15.05.2025)

27. SONG, Qi, et al. Classification of IPSec VPN Encrypted Traffic Based on a Hybrid Method. In: Proceedings of the 2024 2nd International Conference on

Electronics, Computers and Communication Technology. 2024. p. 204-209.

28. What is IPsec (Internet Protocol Security)? [Електронний ресурс] / TechTarget. – 2025. – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security (дата звернення: 12.05.2025)

29. MASTER, Alexander; GARMAN, Christina. A WireGuard Exploration. 2021.

30. HARMENING, Jim. Virtual private networks. In: Computer and Information Security Handbook. Morgan Kaufmann, 2025. p. 979-992.

31. PRADNYA, Umbarje. RADIUS Based Authentication. 2021.

32. RADIUS authentication with Microsoft Entra ID. Microsoft URL: https://learn.microsoft.com/en-us/entra/architecture/auth-radius (date of access: 19.05.2025)

33. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,23 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с.

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