ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І. І. МЕЧНИКОВА

(повне найменування закладу вищої освіти)

Факультет математики, фізики та інформаційних технологій

(повне найменування факультету)

Кафедра інформаційних технологій

(повна назва кафедри)

Кваліфікаційна робота

на здобуття ступеня вищої освіти «Бакалавр»

«Проектування системи захисту інформаційної мережі з використанням захищених з'єднань IPSec VPN»

(тема кваліфікаційної роботи українською мовою)

«Designing an information network protection system using secure IPSec VPN connections»

(тема кваліфікаційної роботи англійською мовою)

Виконав: здобувач денної форми навчання

спеціальності 122 Комп'ютерні науки

(код, назва спеціальності)

Освітня програма Комп'ютерні науки

(назва)

МУДРЯК Матвій Павлович

(прізвище, ім'я, по-батькові здобувача)

Керівник к.т.н., доцент Фразе-Фразенко О.О. _____

(науковий ступінь, вчене звання, прізвище, ініціали) (підпис)

Рецензент к.т.н., начальник ІОЦ ОНЕУ, Домаскін О.М.

(науковий ступінь, вчене звання, прізвище, ініціали)

Рекомендовано до захисту:
Протокол засідання кафедри
Інформаційних технологій
№ ___ від ___ _____ 2025 р.

Завідувачка кафедри

_____ КАЗАКОВА Надія

(підпис) (прізвище,ім'я)

Захищено на засіданні ЕК № _____
протокол № ___ від _____ 2025 р.

Оцінка _____ / _____ / _____

(за національною шкалою/шкалою ECTS/ бали)

Голова ЕК

_____ КОПИЧЕНКО Іван

(підпис) (прізвище,ім'я)

Одеса 2025

АНОТАЦІЯ

У бакалаврській кваліфікаційній роботі розглядається питання підвищення рівня інформаційної безпеки корпоративних мереж шляхом впровадження захищених з’єднань IPSec VPN. Метою роботи є проєктування, реалізація та перевірка системи захисту інформаційної мережі підприємства з використанням протоколів IPSec, що дозволяють створювати зашифровані тунелі між віддаленими вузлами.

У ході дослідження проаналізовано сучасні кіберзагрози та методи захисту, досліджено архітектуру та протоколи IPSec (AH, ESP, IKEv1/2), розглянуто методи шифрування та автентифікації. Розроблено топологію мережі у середовищі Cisco Packet Tracer, здійснено налаштування тунельних з’єднань, реалізовано сегментацію мережі та маршрутизацію. Проведено тестування системи, оцінено її ефективність і потенціал масштабування.

Результати роботи мають прикладну цінність у галузі захисту інформації, зокрема в умовах віддаленої роботи, використання хмарних сервісів і підвищених вимог до кібербезпеки в малих організаціях..

ABSTRACT

The bachelor's qualification thesis focuses on enhancing corporate network security through the implementation of IPSec VPN protected connections. The aim of the study is to design, implement, and test an information protection system for an enterprise network using IPSec protocols, which enable the creation of encrypted tunnels between remote nodes.

The research includes the analysis of modern cyber threats and defense tools, exploration of IPSec architecture and protocols (AH, ESP, IKEv1/2), and an overview of encryption and authentication methods. A secure network topology was developed in Cisco Packet Tracer, including VPN tunneling configuration, static routing, and network segmentation. System testing was conducted to assess efficiency and scalability.

The results of this work have practical value in the field of information security, especially in the context of remote work, cloud services usage, and increasing cybersecurity demands for small organizations.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

Аналіз потенційних вразливостей інформаційної системи – це систематичний підхід до виявлення та оцінки можливих слабких місць в системі, які можуть бути використані для несанкціонованого доступу чи атак.

Інформаційна безпека – стан захищеності інформації від несанкціонованого доступу, спотворення або знищення.

Управління правами доступу – процес встановлення та контролю доступу користувачів до ресурсів.

Authentication Header – протокол автентифікації в рамках IPSec.

DMZ (демілітаризована зона) – окрема частина мережі, в якій розміщуються публічно доступні ресурси (веб-сервери, FTP, DNS). DMZ відокремлена від внутрішньої корпоративної мережі та служить буфером, що знижує ризик прямого проникнення атакуючих до внутрішніх ресурсів.

Encapsulating Security Payload – протокол шифрування та автентифікації в IPSec.

Identity and Access Management – система управління ідентифікацією та доступом користувачів.

IDS (Intrusion Detection System) – система виявлення вторгнень, що аналізує мережевий трафік або події в системі для виявлення підозрілої активності або ознак кібератак. IDS виконує моніторинг у реальному часі, однак сама по собі не блокує загрози, а лише повідомляє адміністратора.

Internet Key Exchange – протокол обміну ключами та встановлення параметрів безпеки для IPSec.

Internet Protocol Security – набір протоколів для забезпечення безпеки мережевих з'єднань.

IPS – система запобігання вторгнень, яка не лише виявляє шкідливу активність, а й автоматично блокує її на основі заздалегідь визначених політик. Є логічним розвитком IDS з розширеними можливостями втручання у трафік.

MFA (багатофакторна автентифікація) – метод підтвердження ідентичності користувача шляхом використання щонайменше двох із трьох можливих факторів: знання (пароль), володіння (токен, телефон) та біометрія (відбиток пальця, розпізнавання обличчя).

Secure Sockets Layer – криптографічний протокол для захисту передавання даних у мережі.

Security Assertion Markup Language – протокол обміну аутентифікаційними і авторизаційними даними.

Single Sign-On – механізм автентифікації, який дозволяє користувачу входити до кількох систем з однією парою облікових даних.

Transport Layer Security – наступник SSL, протокол для забезпечення захисту даних при передачі через мережу

Virtual Private Network – віртуальна приватна мережа, яка дозволяє створювати захищене з’єднання через Інтернет.

VLAN – віртуальна локальна мережа, що дозволяє логічно об’єднувати пристрої в окремі сегменти незалежно від їх фізичного розміщення. VLAN підвищує безпеку і керованість мережевої інфраструктури, дозволяючи ізолювати трафік між підрозділами організації.

ІБ – інформаційна безпека.
УПД – управління правами доступу.
AH – authentication header.
DMZ – demilitarized zone.
ESP – encapsulating security payload.
IAM – identity and access management.
IDS – intrusion detection system.
IKE – internet key exchange.
IPS – intrusion prevention system.
IPSEC – internet protocol security.
MFA – multi-factor authentication.

SAML – security assertion markup language.

SSL – secure sockets layer.

SSO – single sign-on.

TLS – transport layer security.

VLAN – virtual local area network.

VPN – virtual private network.

ВСТУП

Сучасне інформаційне суспільство характеризується стрімким розвитком комп’ютерних технологій, активною цифровізацією бізнес-процесів, зростаючим використанням хмарних рішень та глобальною інтеграцією інформаційних ресурсів. Ці процеси стимулюють створення все складніших інформаційно-комунікаційних систем, значна частина яких функціонує в середовищі відкритих мереж, таких як Інтернет. Водночас постійно зростає кількість кіберзагроз, які ставлять під сумнів безпечність зберігання, обробки та передавання інформації у цифровому середовищі.

Метою кваліфікаційної роботи бакалавра є розробка, реалізація та перевірка працездатності системи захисту інформаційної мережі підприємства шляхом впровадження захищених з’єднань IPSec VPN, що дозволить підвищити рівень інформаційної безпеки, забезпечити безпечну передачу даних і зменшити вразливість до зовнішніх мережевих загроз.

Для досягнення поставленої мети у роботі необхідно виконати наступні завдання:

– провести аналіз сучасних загроз та засобів захисту інформаційних мереж;
– дослідити принципи побудови VPN, зосередивши увагу на архітектурі та протоколах IPSec;
– обґрунтувати доцільність використання Cisco Packet Tracer для моделювання IPSec-з’єднань;
– розробити мережеву топологію з підтримкою VPN-захисту;
– реалізувати конфігурацію тунельних з’єднань між віддаленими вузлами;
– провести тестування, аналіз ефективності та працездатності впровадженого рішення;
– оцінити рівень захищеності побудованої системи та можливість її масштабування.

Об’єкт дослідження – інформаційна мережа підприємства в умовах загроз мережевої безпеки.

Предмет дослідження – методи захищеної передачі даних з використанням протоколу IPSec VPN та їх практична реалізація у віртуальному середовищі.

У роботі повинні застосовуватися такі методи дослідження:

– аналіз наукових та нормативних джерел у сфері кібербезпеки;
– симуляційне моделювання у середовищі Cisco Packet Tracer;
– експериментальне тестування захищених тунелів;
– порівняльний аналіз продуктивності системи до та після впровадження IPSec.

Особливо актуальним питання забезпечення інформаційної безпеки стає в умовах масового переходу на віддалений режим роботи, широкого впровадження мобільного доступу до корпоративних ресурсів, використання SaaS-рішень та розвитку індустрії 4.0. Порушення цілісності, конфіденційності або доступності інформації може призвести до значних фінансових втрат, порушення безперервності бізнесу або освітнього процесу, а також негативних репутаційних наслідків. Як наслідок, у глобальній практиці простежується активне впровадження засобів криптографічного захисту, зокрема – віртуальних приватних мереж (VPN).

На тлі цих тенденцій технологія IPSec VPN є однією з найбільш ефективних і широко підтримуваних платформ для забезпечення захищеної передачі даних. Вона дозволяє створювати шифровані тунелі між географічно розподіленими вузлами мережі, використовуючи алгоритми автентифікації, шифрування та перевірки цілісності. IPSec підтримується більшістю сучасних операційних систем, маршрутизаторів і мережевих пристроїв, включаючи Cisco, що робить її універсальним і масштабованим рішенням.

Незважаючи на широкий розвиток засобів захисту, питання практичного впровадження VPN-рішень в умовах обмежених ресурсів (наприклад, в освітніх установах або невеликих підприємствах) залишається відкритим.

Саме тому в межах цієї роботи обґрунтовується, моделюється та реалізується система захисту інформаційної мережі підприємства з використанням IPSec VPN у навчальному середовищі Cisco Packet Tracer. Такий підхід дозволяє дослідити не лише теоретичні, а й практичні аспекти конфігурування, налаштування та тестування захищених мережевих з’єднань, що має високу прикладну цінність.

Дана кваліфікаційна робота бакалавра складається з 43 сторінки, 8 рисунків, 13 таблиць та 17 джерел посилання.

1 АНАЛІЗ КОНЦЕПЦІЙ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ МЕРЕЖ

1.1 Поняття інформаційної безпеки

Інформаційна безпека (ІБ) – це стан захищеності інформації, при якому забезпечується її конфіденційність, цілісність та доступність. У широкому сенсі це також комплекс організаційних, технічних і програмних заходів, спрямованих на запобігання несанкціонованому доступу до інформації, її спотворенню, знищенню чи витоку [1].

До основних принципів інформаційної безпеки (рис. 1.1) належать:

– конфіденційність (Confidentiality) – забезпечення доступу до даних лише авторизованим користувачам;
– цілісність (Integrity) – гарантія того, що інформація не була змінена чи пошкоджена несанкціоновано;
– доступність (Availability) – безперебійний доступ до інформації, сервісів та ресурсів у дозволених межах.

Рисунок 1.1 – Основи інформаційної безпеки

Система захисту інформації повинна забезпечувати дотримання базових принципів – конфіденційності, цілісності та доступності – на всіх рівнях функціонування інформаційної інфраструктури: фізичному, мережевому, програмному та організаційному. Фізичний рівень охоплює захист доступу до обладнання, серверів, дата-центрів і робочих місць. Мережевий рівень відповідає за безпечну передачу даних між вузлами мережі, зокрема шляхом фільтрації трафіку, шифрування та сегментації. Програмний рівень включає захист операційних систем, прикладного програмного забезпечення, баз даних і служб. Організаційний рівень базується на нормативних документах, політиках, регламентах, а також навчанні персоналу і процедурах реагування на інциденти. Ефективна система інформаційної безпеки має бути багаторівневою і спиратися на комплексний підхід, що поєднує технічні засоби з управлінськими рішеннями. Лише така модель дозволяє забезпечити надійний захист інформації в умовах динамічних і зростаючих кіберзагроз.

1.2 Типові загрози інформаційним мережам

У сучасних інформаційних мережах загрози класифікуються за різними ознаками, серед яких одним із ключових критеріїв є джерело походження. За цією ознакою загрози поділяються на внутрішні та зовнішні (табл. 1). Розуміння характеру цих загроз є критично важливим для формування ефективної стратегії захисту інформаційної інфраструктури. Внутрішні загрози виникають усередині самої організації, часто через доступ, який мають співробітники, підрядники або обслуговуючий персонал до внутрішніх систем і ресурсів. Вони можуть бути навмисними та ненавмисними. Зумисними (навмисними) – здійснені працівниками, які мають злісні наміри, наприклад, саботаж, крадіжка даних, несанкціоноване розкриття конфіденційної інформації, або діяльність на користь конкурентів.

Випадковими (ненавмисними) – результат необережності або помилок персоналу: неправильна конфігурація мережі, помилкова відправка даних, нехтування політиками безпеки, відкриття фішингових листів тощо.

Зовнішні загрози надходять із зовнішнього середовища і, як правило, реалізуються через мережеві атаки з Інтернету, атакуючих програм або кібер-злочинців (див. табл. 1.1). Зовнішні загрози можуть бути спрямовані на:

– отримання несанкціонованого доступу до систем;
– перехоплення або підміну даних;
– руйнування або порушення роботи інформаційних сервісів;
– нанесення шкоди репутації організації.

Таблиця 1.1 – Основні категорії загроз в інформаційних мережах

Категорія загрози	Опис	Типові приклади
Перехоплення трафіку	Незаконне прослуховування або аналіз мережевого трафіку з метою отримання конфіденційної інформації.	Sniffing, ARP-spoofing, перехоплення паролів у відкритих Wi-Fi
Несанкціонований доступ	Отримання доступу до мережі, систем або даних без дозволу адміністратора.	Brute-force, експлуатація вразливостей у службах доступу (SSH, RDP), атаки через вразливості ПО
Зміна або підміна даних	Модифікація переданих пакетів, порушення цілісності даних.	Man-in-the-Middle (MITM), DNS Spoofing, Packet Injection
Відмова в обслуговуванні	Порушення доступності мережевих сервісів через навмисне перевантаження.	DoS/DDoS-атаки, SYN Flood, UDP Flood
Соціальна інженерія	Маніпуляції з користувачами з метою отримання доступу або інформації.	Фішинг, підроблені сайти, скам-листи, телефонні шахрайства
Зловмисне програмне забезпечення (Malware)	Програми, що порушують цілісність або контроль над системою.	Трояни, віруси, шпигунське ПЗ, ransom-ware
Інсайдерські загрози	Дії працівників або партнерів, які мають легальний доступ до мережі.	Несанкціоноване копіювання файлів, витік даних, саботаж
Фізичні атаки	Фізичне знищення, крадіжка або підключення до обладнання.	Відключення живлення, підключення USB-диска з вірусом

На рис. 1.2 представлено найпоширеніші типові загрози у структурованому вигляді.

Рисунок 1.2 – Найпоширеніші типові загрози

Наслідки реалізації загроз в інформаційних мережах можуть бути різноманітними та мати серйозний вплив як на окремі системи, так і на функціонування організації загалом. Одним із найпоширеніших наслідків є порушення конфіденційності, що проявляється у витоку паролів, фінансової або персональної інформації користувачів і працівників. Не менш критичним є порушення цілісності даних, коли внаслідок зловмисних дій змінюється або спотворюється важлива інформація, наприклад, бухгалтерські записи, медична документація або службові звіти.

Ще однією серйозною проблемою є втрата доступності, яка може призвести до припинення роботи окремих сервісів або навіть повної зупинки діяльності установи. Такі збої часто тягнуть за собою фінансові втрати – організація змушена витрачати кошти на відновлення працездатності систем, усунення наслідків інцидентів, впровадження додаткових заходів безпеки, а також може зазнати штрафних санкцій з боку контролюючих органів.

Крім того, значного удару може зазнати ділова репутація: витік або компрометація даних, особливо конфіденційної чи персональної інформації,

призводить до втрати довіри з боку клієнтів, партнерів і акціонерів, що може мати довготривалі негативні наслідки для бізнесу або установи.

1.3 Засоби захисту інформаційних мереж

Захист інформаційних мереж – це складне завдання, яке потребує застосування комплексу взаємопов'язаних технічних, програмних та організаційних рішень. Основна мета – гарантувати конфіденційність, цілісність та доступність інформації, а також мінімізувати ризики реалізації типових загроз. Ефективна система захисту повинна бути побудована за принципом багаторівневої оборони, де кожен рівень виконує конкретні функції безпеки.

Ключові засоби захисту інформацінйих мереж представлено на рис. 1.3.

Рисунок 1.3 – Найпоширеніші типові загрози

Мережеві екрани (фаєрволи) є першою лінією оборони, що здійснює контроль і фільтрацію мережевого трафіку на основі заданих правил доступу [2]. Вони можуть бути апаратними або програмними і здатні:

– блокувати небажані порти або IP-адреси;
– обмежувати доступ до певних сервісів або ресурсів;

– створювати демілітаризовані зони (DMZ) для захисту публічних серверів.

Системи виявлення та запобігання вторгнень (IDS/IPS) забезпечують глибокий аналіз трафіку в реальному часі, що дозволяє виявляти підозрілу активність, характерну для мережевих атак (сканування портів, DoS, спроби експлуатації вразливостей) [3].

– IDS (intrusion detection system) – лише сповіщає адміністратора про потенційну загрозу;
– IPS (intrusion prevention system) – може автоматично блокувати небезпечний трафік.

Антивірусне та антишпигунське програмне забезпечення призначене для виявлення, блокування та видалення шкідливого програмного забезпечення (malware): вірусів, троянів, руткітів, шпигунських програм тощо. Важливо забезпечити централізоване оновлення антивірусних баз і регулярне сканування критичних вузлів.

Криптографічні методи захисту (шифрування) забезпечує недоступність інформації для несанкціонованих користувачів навіть у разі перехоплення трафіку [4]:

– використовуються алгоритми симетричного (AES) і асиметричного шифрування (RSA);
– протоколи SSL/TLS, IPSec забезпечують захист трафіку;
– цифровий підпис та сертифікати гарантують автентичність джерела інформації.

Сегментація мережі – це метод логічного або фізичного поділу мережі на окремі ізольовані зони (VLAN, підмережі, DMZ), що дозволяє:

– обмежити поширення загроз (наприклад, вірус не переходить із VLAN до VLAN);
– реалізувати політики доступу (хто і до чого має доступ);
– підвищити контроль над трафіком між сегментами.

VPN (virtual private network) створює захищений тунель між двома точками в мережі, що дозволяє передавати дані через публічні або незахищені канали (Інтернет), не ризикуючи витоком інформації:

– найбільш безпечними є IPSec VPN (на мережевому рівні) та SSL VPN (на транспортному/прикладному);
– VPN широко використовується для віддаленого доступу працівників до корпоративних ресурсів.

Системи управління доступом (аутентифікація і контроль доступу) визначають [5], хто і до яких ресурсів має право доступу:

– можуть базуватися на логінах/паролях, багатофакторній автентифікації (MFA), токенах тощо;
– реалізуються за принципом найменших привілеїв (least privilege);
– контролюється доступ до файлів, мереж, сервісів, баз даних.

Постійний моніторинг системи безпеки та журналювання (аудит) подій дозволяє:

– виявляти аномальну активність;
– встановлювати факт атаки постфактум;
– проводити розслідування інцидентів.

1.4 Роль VPN у забезпеченні інформаційної безпеки

Віртуальні приватні мережі (VPN) – це технології, які дозволяють створювати логічно ізольовані мережі поверх загальнодоступної інфраструктури (наприклад, Інтернету). Основне завдання VPN – забезпечення захищеного каналу комунікації між вузлами мережі [6].

Основні переваги використання VPN:

– шифрування трафіку (захист від перехоплення);
– ідентифікація та автентифікація сторін (запобігання підміні);
– захист від атак типу Man-in-the-Middle;

– зменшення ризику витоку даних при роботі через відкриті точки доступу.

Серед різновидів VPN (табл. 1.2) найбільш захищеним вважається IPSec VPN, який працює на мережевому рівні моделі OSI та забезпечує шифрування, автентифікацію і цілісність даних.

Таблиця 1.2 – Основні типи VPN

Тип VPN	**Рівень**	**Протоколи**	**Особливості**
IPSec VPN	Мережевий	AH, ESP, IKE	Підтримка site-to-site і remote access
SSL VPN	Транспортний	SSL/TLS	Робота через браузер, проста інтеграція
L2TP/IPSec	Канальний	L2TP + IPSec	Використовується з IPSec для шифрування
GRE	Тунельний	GRE + IPSec	Інкапсуляція нестандартного трафіку

Таким чином, VPN є критичним елементом захисту корпоративної мережі, особливо за умов віддаленого доступу та роботи з чутливою інформацією.

2 ОПИС ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЇ IPSEC VPN

2.1 Архітектура та принципи роботи IPSec

IPSec (Internet Protocol Security) – це набір протоколів і стандартів, який забезпечує захист інформації на мережевому рівні (третій рівень моделі OSI). IPSec використовується для створення віртуальних приватних мереж (VPN) і захищеного передавання даних у потенційно небезпечних середовищах, таких як Інтернет [7]. Основна мета IPSec – забезпечення конфіденційності, цілісності, автентичності та захисту від повторного відтворення (anti-replay protection) при передаванні IP-пакетів.

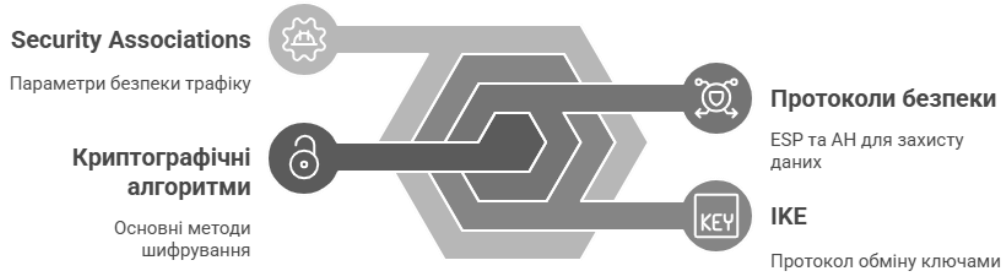

Рисунок 2.1 – Основні компоненти архітектури IPSec

Security Association (SA) – це набір параметрів безпеки, що визначають, як саме буде захищений трафік між двома вузлами. Кожне SA містить:

– метод шифрування (AES, 3DES тощо);
– метод хешування (SHA, MD5);
– обраний протокол (AH або ESP);
– життєвий цикл сесії (lifetime);
– ідентифікатори (SPI – Security Parameter Index).

Для кожного напрямку зв’язку (вхід/вихід) створюється окреме SA.

IKE (Internet Key Exchange) – це протокол для узгодження криптографічних параметрів і обміну ключами між сторонами. Він працює у два етапи (фази):

– фаза 1: встановлення каналу керування безпекою (ISAKMP SA), автентифікація сторін;

– фаза 2: створення IPSec SA для шифрування основного трафіку.

Існує дві версії: IKEv1 (старіша, менш гнучка) та IKEv2 (більш ефективна, з підтримкою NAT і мобільності).

Протокол захисту ESP (Encapsulating Security Payload) забезпечує шифрування даних, цілісність і автентифікацію. Це найчастіше використовуваний протокол IPSec. Протокол захисту AH (Authentication Header) забезпечує лише автентифікацію та цілісність, але не шифрує дані. У практичних VPN-сценаріях AH майже не використовується, оскільки не гарантує конфіденційності.

IPSec підтримує гнучкий набір криптографічних алгоритмів:

– шифрування: AES (128/192/256 біт), DES, 3DES;

– хеш-функції: SHA-1, SHA-2, MD5;

– обмін ключами: алгоритм Диффі-Гелмана (DH Group 1–24).

Режими роботи IPSec визначають, яку частину IP-пакета буде захищено (зашифровано й автентифіковано) під час передавання даних між двома сторонами. Існує два основні режими роботи IPSec (див. табл. 2.1) transport mode (транспортний режим) та tunnel mode (тунельний режим).

У режимі Transport Mode шифрується тільки корисне навантаження (payload) IP-пакета, тобто дані, які йдуть після заголовка. Початковий IP-заголовок залишається незмінним і відкритим.

Основні характеристики режиму Transport Mode:

– використовується для прямого з’єднання між хостами (наприклад, клієнт ↔ сервер);

– підходить для внутрішніх мереж, де не потрібно приховувати IP-адресу;

– менше накладних витрат, ніж у Tunnel Mode.

До недоліку можна віднести те, що IP-адреса відправника та отримувача видима, що не підходить для передачі через незахищене середовище (наприклад, Інтернет).

У режимі Tunnel Mode шифрується весь оригінальний IP-пакет, включаючи заголовок. Потім він інкапсулюється в новий IP-пакет із новим заголовком.

Основні характеристики режиму Tunnel Mode:

– використовується між VPN-шлюзами (наприклад, між двома офісами через Інтернет);
– забезпечує повну конфіденційність – навіть IP-адреса внутрішніх хостів не розкривається;
– створює VPN-тунель, по якому передається трафік між двома мережами.

Таблиця 2.1 – Порівняльна таблиця режимів роботи IPSec

Ознака	**Transport Mode**	**Tunnel Mode**
Що шифрується	Тільки payload	Весь IP-пакет
Новий IP-заголовок	Не додається	Додається
Видимість IP-адрес	Видимі	Приховані
Типове використання	Хост ↔ хост	Шлюз ↔ шлюз (VPN)
Продуктивність	Вища	Трохи нижча (через інкапсуляцію)
Безпека	Менш захищено	Вища безпека

Режим Transport більше підходить для внутрішніх з'єднань у безпечних середовищах, тоді як Tunnel Mode є основним вибором для побудови VPN між географічно розділеними мережами через Інтернет або інші незахищені канали зв’язку.

2.2 Основні протоколи IPSec: AH, ESP, IKEv1/2

Протоколи IPSec виконують різні функції: від шифрування та автентифікації до обміну ключами та управління з’єднаннями [8]. Три основні про-

токоли (див. табл. 2.2), що лежать в основі IPSec, – це AH, ESP та IKE (у двох версіях).

Таблиця 2.2 – Призначення та особливості протоколів IPSec

Протокол	Призначення	Особливості
AH (Authentication Header)	Забезпечення **автентифікації** та **цілісності** IP-пакетів.	Не забезпечує шифрування. Не працює з NAT. Включає IP-заголовок у підпис.
ESP (Encapsulating Security Payload)	**Шифрування**, автентифікація, захист від повторного відтворення.	Підтримує **Tunnel** та **Transport** режим. Найпоширеніший у VPN.
IKEv1	Встановлення **Security Associations (SA)** та обмін ключами.	Працює у 2 фазах. Складніший у налаштуванні. Часто використовується з ACL.
IKEv2	Покращена версія IKE: автоматизує обмін SA.	Швидший, стабільніший, підтримує **NAT-T** (traversal), мобільність, менше трафіку.

2.3 Методи шифрування, автентифікації та управління ключами

Захист інформації в IPSec базується на трьох ключових механізмах [9]: шифрування, автентифікація, та динамічне управління ключами (див. табл. 2.3).

Таблиця 2.3 – Методи шифрування

Алгоритм	Опис
AES	Стандарт сучасного шифрування. Підтримує 128, 192, 256 біт. Висока безпека.
3DES	Старіший алгоритм, використовує потрійне DES-шифрування. Повільніший, але все ще підтримується для сумісності.
DES	Малозахищений, більше не рекомендований до використання.

Методи автентифікації:

– HMAC-SHA1, HMAC-SHA256, HMAC-MD5 – використовуються для хешування і підпису даних. SHA256 має кращу стійкість до колізій, ніж MD5 або SHA1 [10];

– використовуються у поєднанні з ESP або AH.

Управління ключами:

– обмін ключами здійснюється через IKE (Internet Key Exchange);

– IKEv1 має Phase 1 і Phase 2 з ручним або автоматичним SA;
– IKEv2 спрощує обмін ключами, підтримує автентифікацію сертифікатами, PSK (pre-shared key) та EAP.

Алгоритм обміну ключами: Diffie–Hellman (DH) [11]:

– забезпечує безпечний обмін ключами через відкритий канал;
– існують групи DH – від 1 (1024 біт) до 24 (4096+ біт). Чим вища група – тим більше стійкість, але й вища обчислювальна складність.

2.4 Порівняльний аналіз VPN-протоколів

Різні VPN-протоколи забезпечують різний рівень безпеки, продуктивності, простоти налаштування та підтримки пристроями. Нижче (див. табл. 2.4) наведено порівняння найпоширеніших протоколів [12].

Таблиця 2.4 – Порівняння найпоширеніших VPN-протоколів

Характеристика	IPSec VPN	SSL VPN	GRE VPN	L2TP/IPSec
Рівень моделі OSI	Мережевий (рівень 3)	Транспортний / прикладний (4–7)	Мережевий (3)	Канальний + мережевий (2/3)
Шифрування	Так (ESP)	Так (TLS/SSL)	Ні (потрібне поєднання з IPSec)	Так (через IPSec)
Автентифікація	Так (PSK, сертифікати)	Так (через браузер або клієнт)	Ні	Так
Гнучкість	Висока	Дуже висока	Висока у поєднанні з IPSec	Середня
Простота налаштування	Складна (ACL, crypto map)	Відносно проста	Середня	Складна
Мобільність	Частково (IKEv2)	Висока (працює через HTTPS)	Низька	Обмежена
Типове використання	Site-to-Site, Remote	Віддалений доступ (Remote Access)	Інкапсуляція будь-яких протоколів	Доповнення до IPSec (L2TP+IPSec)
Пристрої-клієнти	Роутери, шлюзи	Браузери, ПК, мобільні пристрої	Переважно шлюзи	ОС Windows, мобільні пристрої

Вибір протоколу залежить від цілей [13] – для віддаленого доступу краще використовувати SSL VPN, для захисту трафіку між філіями – IPSec у Tunnel Mode. IPSec VPN ідеально підходить для з'єднання між офісами (Site-to-Site). SSL VPN – кращий вибір для користувацького віддаленого доступу через браузер. GRE VPN не шифрує трафік, але підтримує маршрутизовані протоколи (OSPF, EIGRP). L2TP/IPSec – альтернативний варіант, особливо в системах Windows, але складніший у налаштуванні. Правильна комбінація протоколів, алгоритмів шифрування і методів автентифікації дозволяє побудувати гнучку, безпечну та ефективну VPN-інфраструктуру.

3 ПРОЄКТУВАННЯ, ВПРОВАДЖЕННЯ ТА АНАЛІЗ СИСТЕМИ ЗАХИСТУ НА БАЗІ IPSEC VPN

3.1 Проєктування топології мережі

Проєктована мережева топологія охоплює центральний офіс (HQ) та три філії філії (Branch1, Branch2, Branch3). Всі підрозділи з'єднані через захищені тунелі IPSec VPN, що забезпечує безпечну передачу даних у відкритому середовищі Інтернету. Конфігурація базується на багаторівневій архітектурі з логічною сегментацією VLAN, виділенням DMZ-зони та окремими підмережами для серверів, адміністративного персоналу та користувачів (рис. 3.1).

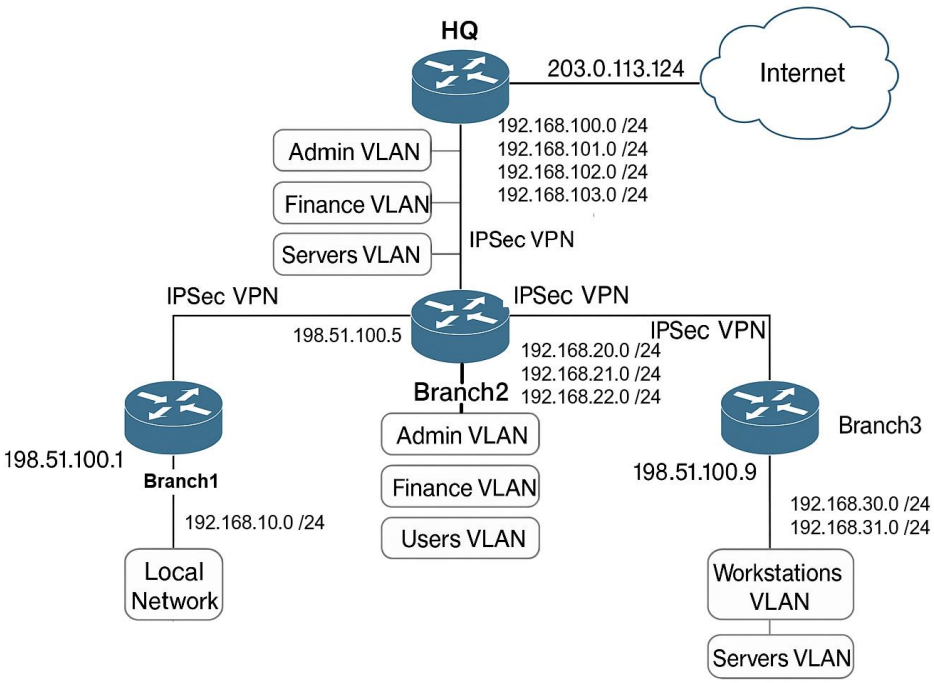

Рисунок 3.1 – Проєктована мережова топологія

WAN-зв'язок забезпечує комунікацію між віддаленими офісами та головним офісом (табл. 3.1) через зовнішню IP-мережу (умовний Інтернет). Кожен офіс має окрему IP-адресу у просторі 10.0.0.0/29, що відповідає масці /30 (255.255.255.252), забезпечуючи двоточкувий тунельний зв'язок.

Таблиця 3.1 – Опис WAN-сегмент

Пристрій	Інтерфейс	IP-адреса	Маска	Призначення
Router1	G0/0	10.0.0.2	255.255.255.248	WAN Branch1
Router2	G0/0	10.0.0.6	255.255.255.248	WAN Branch2
Router4	G0/0	10.0.0.10	255.255.255.248	WAN Branch3
R-HQ	G0/0	203.0.113.1	255.255.255.0	WAN HQ (до Cloud)

Branch1 – це мала філія, яка має просту топологію з одним підмережевим сегментом. Основна мережа надає доступ користувачам через DHCP або статичне IP-призначення (див. табл. 3.2).

Таблиця 3.2 – Опис основних інтерфейсів та пристроїв (обладнання) на філії Branch1

Пристрій	Інтерфейс	IP-адреса	Призначення
Router1	G0/1	192.168.10.1	Gateway для SW1 і ПК
Tunnel1	-	10.0.0.2 /30	Тунель HQ–Branch1
SW1	-	Trunk	До Router1
PC0 – PC4	-	192.168.10.10–14	DHCP або статичні адреси

Branch2 (філія з VLAN-сегментацією) має структуру router-on-a-stick, де кожна VLAN обслуговується через сабінтерфейс маршрутизатора. Це дозволяє забезпечити ізоляцію трафіку між відділами (див. табл. 3.3, 3.4, 3.5).

Таблиця 3.3 – Опис філії Branch2 (сабінтерфейсів маршрутизатора)

Сабінтерфейс	VLAN	IP-адреса	Призначення
G0/1.20	20	192.168.20.1	Admin VLAN
G0/1.21	21	192.168.21.1	Finance VLAN
G0/1.22	22	192.168.22.1	Users VLAN

Таблиця 3.4 – Опис філії Branch2 (розподіл пристроїв по VLAN)

VLAN	Пристрої	IP-адреси
20	PC10, PC11	192.168.20.10 – 192.168.20.11
21	PC5 – PC8	192.168.21.5 – 192.168.21.8
22	PC12 – PC18	192.168.22.12 – 192.168.22.18

Таблиця 3.5 – Опис основних інтерфейсів на філії Branch2

Пристрій	Інтерфейс	IP-адреса	Призначення
Router2	G0/0	198.51.100.5	WAN до Cloud
Tunnel1	-	10.0.0.6 /30	Тунель HQ – Branch2

Branch3 – це офіс, що має складну внутрішню інфраструктуру, яка включає VLAN для користувачів і виділену серверну зону (див. табл. 3.6). Це дозволяє оптимізувати трафік і підвищити рівень безпеки.

Таблиця 3.6 – Опис основних інтерфейсів та пристроїв (обладнання) на філії Branch3

Інтерфейс	IP-адреса	VLAN / Призначення
G0/1.30	192.168.30.1	Workstations VLAN
G0/1.31	192.168.31.1	Servers VLAN
Tunnel1	10.0.0.10 /30	Тунель HQ – Branch3
-	192.168.30.19 – 192.168.30.28	PC19–PC28
Fa0/2	192.168.31.10	Server (локальний)
Fa0/3	192.168.31.11	Server (локальний)

Центральна частина мережі підприємства (Центральний офіс/HQ (див. табл. 3.7)), містить:

– VLAN для адміністрації, бухгалтерії, сервісів;

– серверну частину (AD, File, DB);

– публічну DMZ-зону з Web та FTP-серверами;

– IPSec тунелі до трьох філій.

Таблиця 3.7– Опис основних інтерфейсів та пристроїв (обладнання) в Центральний офіс (HQ)

Інтерфейс	IP-адреса	VLAN / Призначення
G0/0/0	203.0.113.1 /24	WAN
G0/0/1.100	192.168.100.1	Admin VLAN
G0/0/1.101	192.168.101.1	Finance VLAN
G0/0/1.102	192.168.102.1	DMZ (публічні сервери)
G0/0/1.103	192.168.103.1	Server VLAN (внутрішні)
Tunnel1	10.0.0.1 /30	До Branch1
Tunnel2	10.0.0.5 /30	До Branch2
Tunnel3	10.0.0.9 /30	До Branch3
-	192.168.103.4, 192.168.103.5, 192.168.103.6	Server4 (Active Directory), Server5 (File Server), Server6 (Database)
-	192.168.102.2, 192.168.102.3	Server2 (Web Server), Server3 (FTP / DNS)
-	192.168.101.x	PC29 – 35 (бухгалтерія)
-	192.168.100.x	PC36 – 38 (адміністратори)

3.2 Налаштування IPSec VPN

Налаштування IPSec VPN – це процес створення захищеного каналу зв'язку між двома або більше мережевими вузлами (наприклад, офісами, філіями, серверами), [14] який дозволяє передавати дані через незахищене середовище, таке як Інтернет, з дотриманням конфіденційності, цілісності та автентичності. Конфігурація виконувалась за допомогою crypto map-методу. Налаштовані політики шифрування, ACL для дозволених мереж, та map-прив'язки на інтерфейсах.

Основні команди для налаштування на HQ:

```
crypto isakmp policy 10
 encr aes
 hash sha
 authentication pre-share
 group 2
 lifetime 86400
crypto isakmp key cisco address 198.51.100.X
crypto ipsec transform-set MY-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 198.51.100.1
 set transform-set MY-SET
 match address 100
!
interface G0/0/0
 crypto map VPN-MAP
! Access-list для фільтрації трафіку:
access-list 100 permit ip 192.168.100.0 0.0.0.255 192.168.10.0 0.0.0.255
```

Аналогічно конфігуруються Branch1 – Branch3 з відповідними peers та ACL (рис. 3.2).

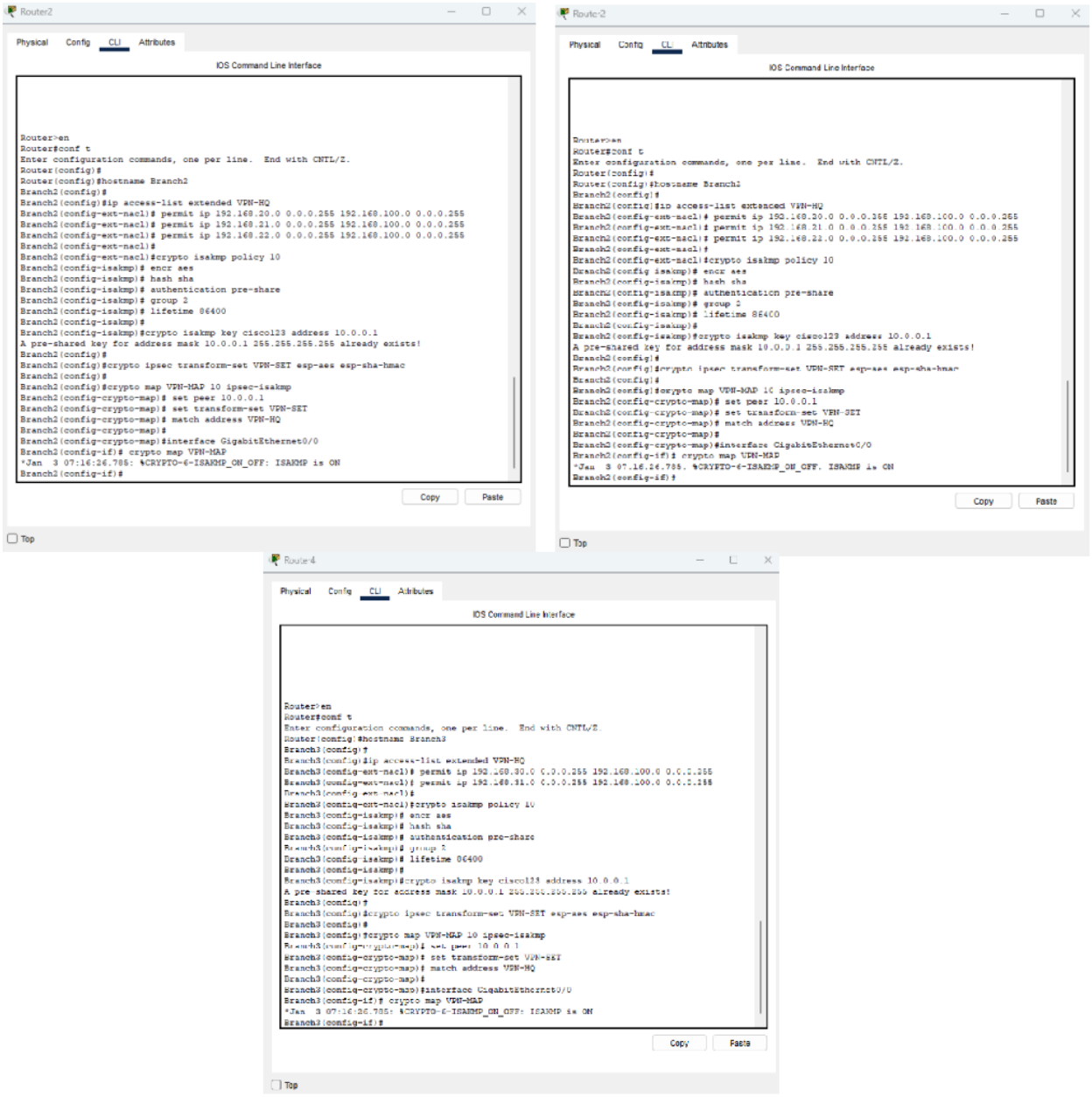

Рисунок 3.2 – Конфігурація Branch1 – Branch3 з відповідними peers та ACL

ACL (Список керування доступом) – це механізм на маршрутизаторах або комутаторах, який дозволяє фільтрувати мережевий трафік на основі визначених правил.

Ці правила можуть дозволяти або забороняти проходження пакетів за такими критеріями:

- IP-адреса джерела або призначення;
- протокол (TCP, UDP, ICMP);

- номер порту (80, 443, 22 тощо);
- напрямок (вхідний або вихідний трафік).

Команда show access-lists виведе всі налаштовані списки ACL на пристрої та лічильники трафіку для кожного правила.

Нижче на рис. 3.3 представлено виведення відповідної інформації після виконання команди show access-lists на HQ, Branch1, Branch2 та Branch3.

```
HQ#show access-lists
Extended IP access list VPN-BRANCH1
    10 permit ip 192.168.100.0 0.0.0.255 192.168.10.0 0.0.0.255
    20 permit ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
Extended IP access list VPN-BRANCH2
    10 permit ip 192.168.100.0 0.0.0.255 192.168.20.0 0.0.0.255
    20 permit ip 192.168.100.0 0.0.0.255 192.168.21.0 0.0.0.255
    30 permit ip 192.168.100.0 0.0.0.255 192.168.22.0 0.0.0.255
    40 permit ip 192.168.20.0 0.0.0.255 192.168.100.0 0.0.0.255
    50 permit ip 192.168.21.0 0.0.0.255 192.168.100.0 0.0.0.255
    60 permit ip 192.168.22.0 0.0.0.255 192.168.100.0 0.0.0.255
Extended IP access list VPN-BRANCH3
    10 permit ip 192.168.100.0 0.0.0.255 192.168.30.0 0.0.0.255
    20 permit ip 192.168.100.0 0.0.0.255 192.168.31.0 0.0.0.255
    30 permit ip 192.168.30.0 0.0.0.255 192.168.100.0 0.0.0.255
    40 permit ip 192.168.31.0 0.0.0.255 192.168.100.0 0.0.0.255
Extended IP access list 101
    10 permit tcp any host 192.168.102.2 eq www
    20 permit tcp any host 192.168.102.3 eq ftp
    30 deny ip any 192.168.102.0 0.0.0.255
    40 permit ip any any
Standard IP access list 1
    10 permit 192.168.0.0 0.0.255.255
Standard IP access list 2
    10 permit 192.168.0.0 0.0.255.255
```

```
Branch1#show access-lists
Extended IP access list VPN-HQ
    10 permit ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
    20 permit ip 192.168.100.0 0.0.0.255 192.168.10.0 0.0.0.255
Extended IP access list NAT-EXCLUDE
    10 deny ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
    20 permit ip 192.168.10.0 0.0.0.255 any
```

```
Branch2#show access-lists
Extended IP access list VPN-HQ
    10 permit ip 192.168.20.0 0.0.0.255 192.168.100.0 0.0.0.255
    20 permit ip 192.168.21.0 0.0.0.255 192.168.100.0 0.0.0.255
    30 permit ip 192.168.22.0 0.0.0.255 192.168.100.0 0.0.0.255
    40 permit ip 192.168.100.0 0.0.0.255 192.168.20.0 0.0.0.255
    50 permit ip 192.168.100.0 0.0.0.255 192.168.21.0 0.0.0.255
    60 permit ip 192.168.100.0 0.0.0.255 192.168.22.0 0.0.0.255
Extended IP access list NAT-EXCLUDE
    10 deny ip 192.168.20.0 0.0.0.255 192.168.100.0 0.0.0.255
    20 deny ip 192.168.21.0 0.0.0.255 192.168.100.0 0.0.0.255
    30 deny ip 192.168.22.0 0.0.0.255 192.168.100.0 0.0.0.255
    40 permit ip 192.168.20.0 0.0.0.255 any
    50 permit ip 192.168.21.0 0.0.0.255 any
    60 permit ip 192.168.22.0 0.0.0.255 any
```

```
Branch3#show access-lists
Extended IP access list VPN-HQ
    10 permit ip 192.168.30.0 0.0.0.255 192.168.100.0 0.0.0.255
    20 permit ip 192.168.31.0 0.0.0.255 192.168.100.0 0.0.0.255
    30 permit ip 192.168.100.0 0.0.0.255 192.168.30.0 0.0.0.255
    40 permit ip 192.168.100.0 0.0.0.255 192.168.31.0 0.0.0.255
Extended IP access list NAT-EXCLUDE
    10 deny ip 192.168.30.0 0.0.0.255 192.168.100.0 0.0.0.255
    20 permit ip 192.168.30.0 0.0.0.255 any
    30 deny ip 192.168.31.0 0.0.0.255 192.168.100.0 0.0.0.255
    40 permit ip 192.168.31.0 0.0.0.255 any
```

Рисунок 3.3 – Виконанн команди show access-lists на HQ, Branch1, Branch2 та Branch3

Також слід звернути увагу на налаштування на основних етапах конфігурації маршрутизаторів Cisco у філіях підприємства, а саме для реалізації:

- інтерфейсного налаштування (IP-адресація);
- NAT (перетворення адрес);
- VLAN (для сабінтерфейсів);
- тунельного інтерфейсу (IPSec GRE VPN).

Для початку варто налаштувати WAN-інтерфейсу (у режим глобального конфігурування), що з’єднується з Інтернетом на Branch1. ip nat outside вказує, що це зовнішній інтерфейс для NAT.

```
interface G0/0
```

```
ip address 198.51.100.1 255.255.255.0
ip nat outside
no shutdown
```

Дал слід налаштуватия LAN-інтерфейс, шлюз для локальної мережі.ip nat inside – внутрішня зона NAT.

```
interface G0/1
ip address 192.168.10.1 255.255.255.0
ip nat inside
no shutdown
```

Налаштування NAT PAT (перевантаження) – дозволяє локальним пристроям виходити в Інтернет через єдину публічну адресу.

```
access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface G0/0 overload
```

Налаштування GRE-тунелю до головного офісу (HQ). Працює поверх IPSec. Використовується IP-адреса WAN HQ як пункт призначення.

```
interface Tunnel1
ip address 10.0.0.2 255.255.255.252
tunnel source G0/0
tunnel destination 203.0.113.1
```

Налаштування WAN-інтерфейс для NAT-з’єднання на Branch2 (філія з VLAN).

```
interface G0/0
ip address 198.51.100.5 255.255.255.0
ip nat outside
```

Конфігурація сабінтерфейс для VLAN 20 (Admin).

```
interface G0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
ip nat inside
```

Аналогічно налаштовуються G0/1.21 – VLAN 21 (Finance) та G0/1.22 – VLAN 22 (Users).

Налаштування дозволу NAT для всіх VLAN-сегментів. Це в свою чергу дозволяє пристроям у VLAN виходити в Інтернет через G0/0.

```
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.22.0 0.0.0.255
```

```
ip nat inside source list 1 interface G0/0 overload
```

Налаштування тунелю до HQ (як у Branch1).

```
interface Tunnel1
ip address 10.0.0.6 255.255.255.252
tunnel source G0/0
tunnel destination 203.0.113.1
```

Конфігурація WAN-з’єднання (зовнішній інтерфейс NAT) у Branch3 (філія з серверами).

```
interface G0/0
ip address 198.51.100.9 255.255.255.0
ip nat outside
```

Налаштування сабінтерфейсів для VLAN 30 (Workstations) і VLAN 31 (Servers).

```
interface G0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
ip nat inside

interface G0/1.31
encapsulation dot1Q 31
ip address 192.168.31.1 255.255.255.0
ip nat inside
```

Налаштування NAT для обох VLAN.

```
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.31.0 0.0.0.255
ip nat inside source list 1 interface G0/0 overload
```

Конфігурація тунелю до HQ (Tunnel3).

```
interface Tunnel1
ip address 10.0.0.10 255.255.255.252
tunnel source G0/0
tunnel destination 203.0.113.1
```

3.3 Налаштування статичної маршрутизації

Статична маршрутизація – це метод керування мережевим трафіком, за якого маршрути до інших мереж або підмереж встановлюються вручну адмі-

ністратором і залишаються незмінними, доки не будуть змінені або видалені вручну [15].

Іншими словами, у статичній маршрутизації всі маршрути "прописуються вручну" у конфігурації маршрутизатора.

```
ip route 192.168.20.0 255.255.255.0 10.0.0.6    ! Для трафіку від Branch1 до Branch2 через тунель
ip route 192.168.30.0 255.255.255.0 10.0.0.10   ! Для трафіку від Branch1 до Branch3 через тунель
ip route 192.168.100.0 255.255.255.0 10.0.0.1   ! Для трафіку від Branch1 до HQ через тунель
ip route 192.168.10.0 255.255.255.0 10.0.0.2    ! Для трафіку від Branch2 до Branch1 через тунель
ip route 192.168.30.0 255.255.255.0 10.0.0.10   ! Для трафіку від Branch2 до Branch3 через тунель
ip route 192.168.100.0 255.255.255.0 10.0.0.1   ! Для трафіку від Branch2 до HQ через тунель
ip route 192.168.10.0 255.255.255.0 10.0.0.2    ! Для трафіку від Branch3 до Branch1 через тунель
ip route 192.168.20.0 255.255.255.0 10.0.0.6    ! Для трафіку від Branch3 до Branch2 через тунель
ip route 192.168.100.0 255.255.255.0 10.0.0.1   ! Для трафіку від Branch3 до HQ через тунель
ip route 192.168.10.0 255.255.255.0 10.0.0.2     ! Для трафіку від HQ до Branch1 через тунель
ip route 192.168.20.0 255.255.255.0 10.0.0.6     ! Для трафіку від HQ  до Branch2 через тунель
ip route 192.168.30.0 255.255.255.0 10.0.0.10    ! Для трафіку від HQ  до Branch3 через тунель
```

3.4 Сегментація мережі

У рамках проєктування захищеної інформаційної мережі підприємства було реалізовано логічну сегментацію за допомогою VLAN (Virtual LAN) на базі маршрутизаторів із підтримкою сабінтерфейсів (router-on-a-stick), що дозволило розподілити мережу на ізольовані сегменти відповідно до функціональних підрозділів компанії [16].

Мета сегментації [17]:

- забезпечити логічне розділення трафіку між різними відділами та службами;
- обмежити розповсюдження потенційних загроз у разі компрометації окремого сегмента;
- реалізувати правила доступу між сегментами (через ACL або firewall);
- оптимізувати трафік і підвищити загальну керованість інфраструктури.

У центральному офісі (HQ) було створено чотири окремі підмережі, кожна з яких обслуговує визначену функціональну зону:

- VLAN 100 (192.168.100.0 /24) – для IT-персоналу та адміністраторів;
- VLAN 101 (192.168.101.0 /24) – для бухгалтерії та фінансів;
- VLAN 102 (192.168.102.0 /24) – зона DMZ, у якій розміщені публічні сервіси (Web/FTP/DNS);
- VLAN 103 (192.168.103.0 /24) – внутрішня серверна мережа (AD, File Server, Database).

Це дозволяє ізолювати адміністративні, користувацькі та серверні ресурси, обмежуючи їхній доступ лише необхідними маршрутами.

У другій філії (Branch2/філія з VLAN), де працює кілька підрозділів, реалізовано наступні VLAN:

- VLAN 20 (192.168.20.0 /24) – адміністрація філії;
- VLAN 21 (192.168.21.0 /24) – фінансовий відділ;
- VLAN 22 (192.168.22.0 /24) – звичайні користувачі.

Кожна VLAN під’єднана до сабінтерфейсу маршрутизатора (G0/1.x), що дозволяє здійснювати міжмережеву маршрутизацію всередині філії та контролювати доступ за допомогою NAT і VPN.

У третій філії (Branch3) була впроваджена сегментація:

- VLAN 30 (192.168.30.0 /24) – користувацькі пристрої (робочі станції);

- VLAN 31 (192.168.31.0 /24) – серверна зона філії (локальні служби, локальні БД).

Цей поділ дозволяє ізолювати критичні сервери від звичайних користувачів навіть у межах одного офісу, що відповідає політиці "zero trust".

Безпекові переваги впровадженої сегментації мережі полягають у підвищенні рівня контролю над передаванням даних між різними функціональними зонами та зменшенні потенційних ризиків кіберзагроз. По-перше, ізоляція трафіку між VLAN'ами унеможливлює пряму взаємодію між сегментами без участі маршрутизатора, що дозволяє повністю виключити неконтрольований обмін даними між відділами чи зонами з різними рівнями довіри.

По-друге, сегментація забезпечує надійний захист серверів і внутрішніх даних від прямого доступу з демілітаризованої зони (DMZ) або з користувацьких мереж, що критично важливо для збереження цілісності і конфіденційності чутливої інформації.

Крім того, можливість використання списків контролю доступу (ACL) або фаєрволів між VLAN дозволяє реалізувати принцип найменших привілеїв (Least Privilege), при якому кожен сегмент має лише той доступ, що є необхідним для виконання його функцій.

Така архітектура істотно зменшує зону ураження в разі проникнення шкідливого коду або внутрішньої компрометації, оскільки обмежує поширення загрози в межах ізольованого сегмента, не даючи їй охопити всю мережу.

3.5 Опис команд визначених для методики тестування

По-перше слід перевірити, чи працює тунель і чи маршрутизується трафік через IPSec з одного сегмента до іншого. Успішна відповідь = тунель активний, маршрути налаштовані правильно. Перевірка доступності через VPN-тунель. Під час цієї перевірки надсилаються ICMP-пакети на ПК з Branch1 з HQ або з іншої філії.

```
ping 192.168.10.10
```

По-друге, варто протестувати трасування маршруту (маршрут трафіку). Це даст змогу переконатися, що трафік йде через GRE/IPSec тунель, а не напряму в Інтернет або обхідними маршрутами. Дана команда для перевірки показує шлях, яким трафік рухається до ПК у Branch3.

```
traceroute 192.168.30.19
```

По-третє, слід виконати перевірку маршрутизації (на маршрутизаторі). Дана перевірка дозволить перешлянути чи існують статичні маршрути до віддалених підмереж (наприклад, 192.168.20.0/24, 192.168.103.0/24 через Tunnel1/2/3). У результаті виконання команди повинно відобразитися таблиця маршрутів пристрою.

```
show ip route
```

Також, під час тестування необхідно виконати перевірку встановленого тунелю GRE/IPSec. Під час цієї перевірки визначається стан тунельного інтерфейсу: чи активний він (up/up). Це дозволить переконатися, що GRE-тунель працює фізично й логічно.

```
show interface Tunnel1
```

Ще одним методом є перевірка IPSec SA (Security Associations). Дана перевірка показує статистику IPSec – кількість зашифрованих/розшифрованих пакетів, встановлені тунелі. Слід зазначити, що це одна з головних команд для перевірки того, чи реально відбувається шифрування трафіку між філіями.

```
show crypto ipsec sa
```

Перевірити стану IKE (Phase 1/2) обміну ключами можна за допомогою команди:

```
show crypto isakmp sa
```

Перевірка, дозволить переглянути чи успішно пройшло узгодження криптографічних параметрів і чи встановлено захищений канал.

Варто приділити увагу перевірці зовнішнішнього трафіку. У результаті виконання команди повинна відобразитися таблиця NAT-трансляцій (локальна IP ↔ публічна IP). Це дозволить переконатися, що пристрої з внутрішньої мережі правильно транслюються в Інтернет.

```
show ip nat translations
```

Необхідно під час тестування переконатися, що трафік потрапляє під потрібне правило ACL (наприклад, NAT), і воно працює. Перевірити, скільки разів кожне правило списку доступу було застосоване можна за допомогою виконання команди:

```
show access-lists
```

Також слід виконати тестування з пристроїв-клієнтів. Це дозволить перевірити доступність Active Directory у серверному сегменті HQ задля валідація між VLAN’ами, маршрутизації, тунелю і правил доступу. Команда (на ПК у Cisco Packet Tracer):

```
ping 192.168.103.4
```

У рамках практичної частини роботи було розроблено, змодельовано та реалізовано повнофункціональну топологію захищеної корпоративної мережі в середовищі Cisco Packet Tracer, яка відображає типову інфраструктуру середнього підприємства з центральним офісом та трьома філіями (рис. 3.4).

Мережева структура була побудована відповідно до принципів багаторівневої інформаційної безпеки, з використанням логічної сегментації, шифрування трафіку, NAT, VPN та маршрутизації.

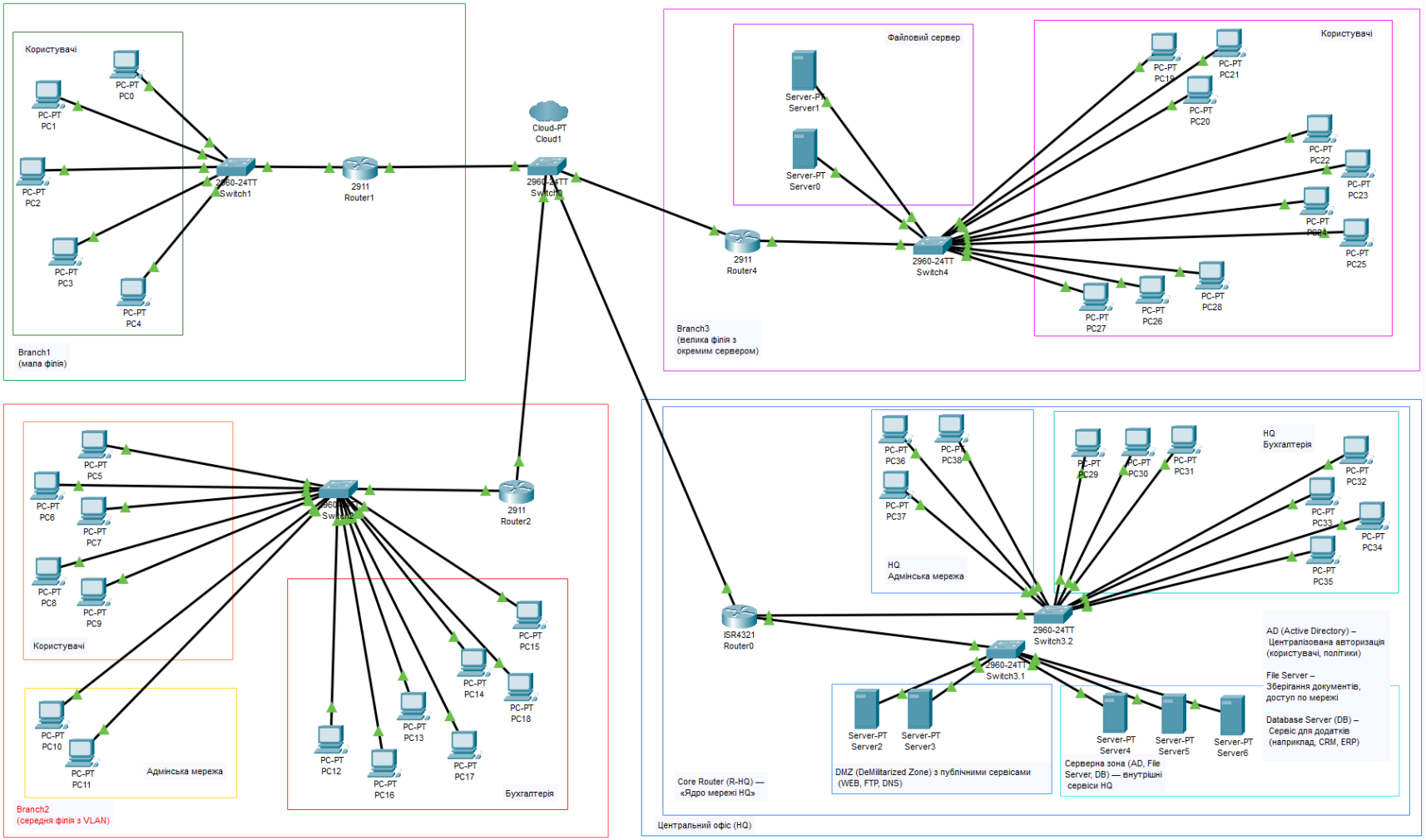

Рисунок 3.4 – Топологія захищеної корпоративної мережі в середовищі Cisco Packet Tracer

Відповідно до реалізованої топологія захищеної корпоративної мережі в середовищі Cisco Packet Tracer, можна визначити основні її (топології) компоненти:

a) Головний офіс (HQ) – центр управління мережею, де зосереджено:
   1) адміністративний сегмент (VLAN 100);
   2) бухгалтерія (VLAN 101);
   3) DMZ (VLAN 102 – публічні сервіси);
   4) серверна частина (VLAN 103 – внутрішні служби);
   5) три VPN-тунелі до філій;
b) Branch1 – проста філія з одною локальною підмережею (192.168.10.0 /24), яка забезпечує базову роботу користувачів і має VPN-з’єднання до HQ;
c) Branch2 – філія з логічною сегментацією (router-on-a-stick) і трьома VLAN:
   1) адміністрація;
   2) фінансовий відділ;
   3) користувачі;
d) Branch3 – велика філія з окремими сегментами для робочих станцій і серверів, які працюють незалежно від HQ.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи була досягнута поставлена мета – спроєктовано, реалізовано та протестовано функціональну систему захисту інформаційної мережі підприємства на базі технології IPSec VPN. Отримані результати підтверджують ефективність комплексного підходу до забезпечення інформаційної безпеки в умовах відкритого мережевого середовища.

Аналіз сучасного стану кіберзагроз, розвитку інформаційних технологій, активного впровадження віддаленої роботи та хмарних сервісів підтвердив об’єктивну необхідність створення надійної системи захисту передавання даних. У таких умовах впровадження IPSec VPN виявилось доцільним і науково обґрунтованим вибором, що узгоджується з сучасними світовими стандартами у сфері мережевої безпеки.

У роботі було проаналізовано поняття інформаційної безпеки, класифікацію типових загроз (внутрішніх та зовнішніх), а також засоби та методи захисту інформації в комп’ютерних мережах. Особливу увагу приділено архітектурі протоколу IPSec, включаючи режими роботи (Tunnel / Transport), протоколи (AH, ESP, IKEv1/2), алгоритми шифрування та автентифікації, і порівнянню IPSec з іншими VPN-рішеннями (SSL VPN, GRE, L2TP/IPSec).

У середовищі Cisco Packet Tracer була побудована мережева топологія корпоративного підприємства, що включає центральний офіс і три географічно розподілені філії. Мережа реалізована з дотриманням принципів:

- багаторівневої логічної сегментації (через VLAN),
- ізоляції критичних ресурсів (сервери, DMZ),
- застосування NAT, статичної маршрутизації та GRE/IPSec тунелів.

Було налаштовано IPSec-тунелі між філіями та головним офісом, реалізовано NAT для виходу в Інтернет, і побудовано сабінтерфейси для VLAN. Структура забезпечила не лише захищений обмін даними, а й логічний розподіл доступу між підрозділами.

Завдяки впровадженню VLAN та ізоляції DMZ-сервісів, вдалось досягти високого ступеня контролю над трафіком і мінімізації зони ураження. Роль IPSec VPN – у забезпеченні шифрування, цілісності та автентичності даних при їх передаванні між офісами через загальнодоступну мережу. Сегментація і застосування ACL дозволили впровадити політику найменших привілеїв, що відповідає сучасним підходам до кіберзахисту.

Робота має практичне значення для IT-інфраструктур навчальних закладів, підприємств малого та середнього бізнесу, які потребують захищеного віддаленого обміну даними. Представлена модель може бути використана як навчальний стенд для вивчення принципів VPN, маршрутизації, NAT, VLAN та мережевої безпеки.

Усі поставлені в роботі завдання – від аналізу загроз до конфігурації VPN-тунелів – були успішно реалізовані. Розроблену модель протестовано, перевірено на працездатність, її ефективність обґрунтовано як з точки зору продуктивності, так і з точки зору безпеки.

ПЕРЕЛІК ВИКОРИСТАННИХ ДЖЕРЕЛ

Web-сторінки:

1. CIA triad (confidentiality, integrity and availability) [Електронний ресурс] // TechTarget. – Режим доступу: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.
2. What is a Firewall? [Електронний ресурс] // Cisco. – Режим доступу: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.
3. IDS vs IPS: What's the Difference? [Електронний ресурс] // Fortinet. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-prevention-system.
4. TLS and SSL Protocols [Електронний ресурс] // Cloudflare. – Режим доступу: https://www.cloudflare.com/learning/ssl/what-is-ssl/.
5. Multi-Factor Authentication (MFA) [Електронний ресурс] // Microsoft Learn. – Режим доступу: https://learn.microsoft.com/en-us/security/compass/identity-access-concepts.
6. Zero Trust Architecture (SP 800-207) [Електронний ресурс] // NIST. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-207/final.
7. RFC 4301 – Security Architecture for the Internet Protocol [Електронний ресурс] // IETF. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc4301.
8. RFC 2409 – The Internet Key Exchange (IKE) [Електронний ресурс] // IETF. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2409.
9. Symmetric vs Asymmetric Encryption [Електронний ресурс] // IBM Security. – Режим доступу: https://www.ibm.com/docs/en/sva/10.0.5?topic=overview-encryption-types.
10. What is HMAC? [Електронний ресурс] // TechTarget. – Режим доступу: https://www.techtarget.com/searchsecurity/definition/HMAC.

11. Diffie-Hellman Key Exchange [Електронний ресурс] // Cloudflare. – Режим доступу: https://www.cloudflare.com/learning/ssl/what-is-diffie-hellman.
12. VPN Protocols Explained [Електронний ресурс] // Comparitech. – Режим доступу: https://www.comparitech.com/blog/vpn-privacy/vpn-protocols.
13. SSL VPN vs. IPSec: What Are the Differences? [Електронний ресурс] // Palo Alto Networks. – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/ipsec-vs-ssl-vpn.
14. IPSec Configuration Guide [Електронний ресурс] // Cisco. – Режим доступу: https://www.cisco.com/c/en/us/tech/ip/ip-security-ipsec/index.html.
15. NAT Configuration Examples [Електронний ресурс] // Cisco. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-nat-config.html.
16. Cisco GRE over IPSec Design Guide [Електронний ресурс] // Cisco. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/24865-gre-over-ipsec.html.
17. Network Segmentation Best Practices [Електронний ресурс] // Fortinet. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/network-segmentation.