

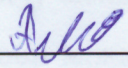
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

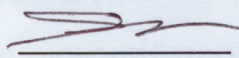
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної корпоративної мережі з
централізованим управлінням Active Directory, контро-
лем доступу на рівні портів та безпечним VPN-шлю-
зом»

Виконав: студент 4-го курсу групи КІ-22-1

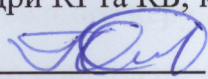
спеціальності 123 «Комп'ютерна інженерія»

 Артем РЕДЧИЦЬ

Керівник: Доцент кафедри КІ та КБ, к.т.н., доцент,

 Юрій РОССІНСЬКИЙ

Рецензент: Доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

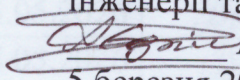
Житомир – 2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
5 березня 2026 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Редчиць Артем Олегович

Тема роботи: «Проект захищеної корпоративної мережі з централізованим управлінням Active Directory, контролем доступу на рівні портів та безпечним VPN-шлюзом»

затверджена Наказом університету від 5 березня 2026 р. № 97/с

Термін здачі студентом закінченої роботи 18 червня 2026 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Предметом дослідження є технології логічної сегментації мереж (VLAN), механізми забезпечення відмовостійкості зовнішніх каналів зв'язку (IP SLA та Object Tracking), служби каталогів Active Directory, механізми автентифікації LDAP, а також програмно-апаратні засоби побудови міжмережевих екранів та шлюзів безпечного віддаленого доступу (SSL/DTLS VPN);

Об'єктом дослідження є безпека та відмовостійкість корпоративної мережевої інфраструктури, зокрема процес централізованого керування доступом співробітників (як локальних, так і віддалених) до конфіденційних інформаційних ресурсів підприємства;

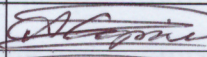
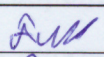
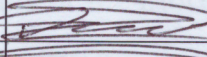
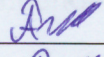
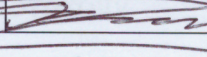
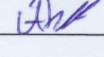
Обладнання та програмне забезпечення:

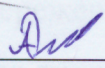
1. GNS3
2. QEMU
3. Cisco ASA
4. Windows Server 2025, Windows 11

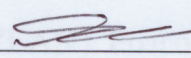
5. Cisco AnyConnect

6. Microsoft: Active Directory Domain Services, оболонка PowerShell

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

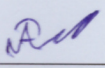
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 05.05.2026	 05.05.2026
2	Єфіменко А.А.	 05.05.2026	 05.05.2026
3	Єфіменко А.А.	 05.05.2026	 05.05.2026

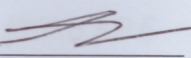
Студент  Артем РЕДЧИЦЬ

Керівник  Юрій РОССІНСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.03.2026	
2	Аналіз отриманого завдання	05.03.2026	
3	Аналіз літературних джерел	10.03.2026 – 20.03.2026	
4	Постановка задачі дослідження	23.03.2026 – 30.03.2026	
5	Вибір засобів реалізації	01.04.2026 – 12.04.2026	
6	Проектування мережі	13.04.2026 – 30.04.2026	
7	Налаштування і відлагодження проєкту	01.05.2026 – 22.05.2026	
8	Комплексне тестування працездатності мережі	23.05.2026 – 29.05.2026	
9	Написання та остаточне оформлення пояснювальної записки	30.05.2026 – 09.06.2026	
10	Захист випускної кваліфікаційної роботи	18.06.2026	

Студент  Артем РЕДЧИЦЬ

Керівник  Юрій РОССІНСЬКИЙ

АНОТАЦІЯ

У кваліфікаційній роботі розглянуто проєкт створення захищеної корпоративної мережі підприємства з централізованим управлінням Active Directory, логічною сегментацією та безпечним VPN-шлюзом. Метою роботи було забезпечення надійної ізоляції внутрішніх інформаційних потоків та створення стійкого до загроз зовнішнього периметра для безпечного віддаленого підключення співробітників з використанням LDAP-протоколу.

У процесі реалізації було спроектовано мережеву топологію зі згорнутим ядром на базі міжмережевого екрана Cisco ASA та впроваджено логічну ізоляцію за допомогою віртуальних локальних мереж (VLAN). Розгорнуто доменну інфраструктуру на базі Windows Server для реалізації управління доступом на основі ролей (RBAC). Налаштовано підсистему захищеного віддаленого доступу Cisco AnyConnect SSL/DTLS VPN, інтегровану з Active Directory. Реалізовано механізм розмежування доступу до ресурсів мережі та спільної файлової системи: гостей пристрої надійно ізолювані від корпоративного сегмента, віддалені користувачі авторизуються виключно через доменні глобальні групи безпеки, а технологія IP SLA та Object Tracking забезпечує автоматичну відмовостійкість зовнішніх інтернет-каналів.

Пояснювальна записка містить 85 сторінок, включає 35 рисунків, 13 таблиць та 8 лістингів. Список використаних джерел налічує 25 найменувань.

Ключові слова: ACTIVE DIRECTORY, LDAP, CISCO ASA, ANYCONNECT VPN, VLAN, IP SLA, OBJECT TRACKING, КІБЕРБЕЗПЕКА, ZERO TRUST.

					ККІКБ.КР.Б - 123 - 12 - ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Редчиць А.О.		22.06.26	Проект захищеної корпоративної мережі з централізованим управлінням Active Directory, контролем доступу на рівні портів та безпечним VPN-шлюзом	Літ.	Арк.
Керівник		Росінський Ю.М.		22.06.26			4
Реценз.		Головня О.С.		22.06.26			85
Н. контр.		Росінський Ю.М.		22.06.26		ФІКТ, Гр. КІ-22-1	
Затверд.		Сфіменко А.А.		22.06.26			

ANNOTATION

This thesis examines a project to create a secure corporate network for an enterprise featuring centralized Active Directory management, logical segmentation, and a secure VPN gateway. The goal of the project was to ensure reliable isolation of internal information flows and to create a threat-resistant external perimeter for secure remote access by employees using the LDAP protocol.

During implementation, a network topology with a converged core based on a Cisco ASA firewall was designed, and logical isolation was implemented using virtual local area networks (VLANs). A Windows Server-based domain infrastructure was deployed to implement role-based access control (RBAC). The Cisco AnyConnect SSL/DTLS VPN secure remote access subsystem, integrated with Active Directory, was configured. A mechanism for separating access to network resources and the shared file system has been implemented: guest devices are securely isolated from the corporate segment, remote users are authenticated exclusively through domain-level global security groups, and IP SLA and Object Tracking technologies ensure automatic fault tolerance for external Internet links.

The explanatory note consists of 85 pages and includes 35 figures, 13 tables, and 8 code listings. The list of references contains 25 titles.

Keywords: ACTIVE DIRECTORY, LDAP, CISCO ASA, ANYCONNECT VPN, VLAN, IP SLA, OBJECT TRACKING, CYBERSECURITY, ZERO TRUST.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП.....	9
РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ТА ЗАХИСТУ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ.....	11
1.1 Архітектура захищених мереж та концепція Zero Trust	11
1.2 Технологія централізованого управління інфраструктурою Microsoft Active Directory	13
1.3 Технологія захищеного віддаленого доступу Cisco AnyConnect.....	16
1.4 Технології забезпечення відмовостійкості мережі	20
Висновок до першого розділу	23
РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ	25
2.1 Вимоги до апаратного середовища та моделі загроз	25
2.2 Проєктування топології, IP-адресації та VLAN.....	27
2.3 Проєктування системи відмовостійкості зовнішніх каналів зв'язку на базі IP SLA Tracking	32
2.4 Проєктування логічної структури Active Directory та моделі RBAC	36
2.5 Проєктування підсистеми AnyConnect SSL VPN	39
Висновок до другого розділу	43
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ	44
3.1 Конфігурація мережевої інфраструктури на міжмережевому екрані Cisco ASA	44
3.2 Розгортання та конфігурація Active Directory.....	46
3.3 Конфігурація VPN-шлюзу та інтеграція з Active Directory	51
3.4 Комплексне тестування працездатності та безпеки мережі	56
Висновок третього розділу	64
ВИСНОВКИ	65
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	67
ДОДАТКИ.....	70

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA (Authentication, Authorization, Accounting) – Аутентифікація, авторизація та адміністрування (облік)

ACL (Access Control List) – Список контролю доступу

AD DS (Active Directory Domain Services) – Служби доменів Active Directory

ASA (Adaptive Security Appliance) – Адаптивний міжмережевий екран компанії Cisco

ASBR (Autonomous System Boundary Router) – Межовий маршрутизатор автономної системи

CPU (Central Processing Unit) – Центральний процесор

DHCP (Dynamic Host Configuration Protocol) – Протокол динамічної конфігурації мережевого вузла

DNS (Domain Name System) – Система доменних імен

DTLS (Datagram Transport Layer Security) – Протокол безпеки транспортного рівня для дейтаграм

ESP (Encapsulating Security Payload) – Протокол інкапсуляції зашифрованого корисного навантаження

GPO (Group Policy Object) – Об'єкт групової політики

GUI (Graphical User Interface) – Графічний інтерфейс користувача

HTTPS (HyperText Transfer Protocol Secure) – Захищений протокол передачі гіпертексту

ICMP (Internet Control Message Protocol) – Протокол керуючих повідомлень Інтернету

IP (Internet Protocol) – Міжмережевий протокол

IPsec (Internet Protocol Security) – Набір протоколів для забезпечення захисту IP-трафіку

IP SLA (Service Level Agreements) - Технологія від Cisco, яка безперервно вимірює ключові параметри мережі в реальному часі

ISP (Internet Service Provider) – Інтернет-провайдер

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Россінський Ю.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

L2TP (Layer 2 Tunneling Protocol) – Протокол тунелювання другого рівня
LDAP (Lightweight Directory Access Protocol) – Полегшений протокол доступу до каталогів

NAT (Network Address Translation) – Трансляція мережевих адрес

NTFS (New Technology File System) – Файлова система нової технології

OSI (Open Systems Interconnection) – Еталонна модель взаємодії відкритих систем

OU (Organizational Unit) – Організаційна одиниця

PAT (Port Address Translation) – Трансляція мережевих портів

RBAC (Role-Based Access Control) – Управління доступом на основі ролей

RSA (Rivest–Shamir–Adleman) – Криптографічний алгоритм із відкритим ключем

SG (Security Group) – Група безпеки

SID (Security Identifier) – Ідентифікатор безпеки

SMB (Server Message Block) – Мережевий протокол прикладного рівня для доступу до файлів

SPF (Shortest Path First) – Алгоритм найкоротшого шляху (алгоритм Дейкстри)

SSL (Secure Sockets Layer) – Рівень захищених сокетів

TCP (Transmission Control Protocol) – Протокол управління передачею

TLS (Transport Layer Security) – Протокол захисту транспортного рівня

UDP (User Datagram Protocol) – Протокол користувацьких дейтаграм

VLAN (Virtual Local Area Network) – Віртуальна локальна мережа

VPN (Virtual Private Network) – Віртуальна приватна мережа

WAN (Wide Area Network) – Глобальна комп'ютерна мережа

KIM – Корпоративна інформаційна мережа

ЛОМ – Локальна обчислювальна мережа

ПЗ – Програмне забезпечення

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Россінський Ю.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасних умовах стрімкої цифровізації бізнес-процесів та масового переходу підприємств на гібридні або віддалені формати роботи, питання забезпечення безперебійного та безпечного функціонування корпоративних інформаційних систем набуває критичного значення. Традиційні підходи до побудови мереж, що базуються на концепції довіреного внутрішнього периметра («плоскі мережі»), сьогодні є системно вразливими до внутрішніх загроз та горизонтального поширення кібератак (Lateral Movement) [1]. Крім того, децентралізоване управління правами користувачів ускладнює аудит безпеки та порушує принцип найменших привілеїв [16], а використання застарілих протоколів тунелювання для віддаленого доступу часто призводить до конфліктів із системами трансляції адрес (NAT/PAT) інтернет-провайдерів [2, 10].

Усе це зумовлює гостру необхідність розробки комплексних архітектурних рішень, які поєднують логічну сегментацію на каналному рівні [4], централізоване управління ідентифікацією [12] та надійні криптографічні шлюзи. Саме тому тема дипломного проєкту, присвячена розробці захищеної мережі з інтеграцією служби каталогів Active Directory та сучасного VPN-шлюзу на базі міжмережевого екрана, є вкрай актуальною та має високе практичне значення [3, 19].

Мета дипломного проєкту полягає у проєктуванні, конфігурації та тестуванні комплексної архітектури захищеної корпоративної мережі, що забезпечує логічну ізоляцію інформаційних потоків, централізоване управління доступом на основі ролей (RBAC) [15] та безпечне підключення віддалених користувачів.

Для досягнення поставленої мети було сформульовано та вирішено такі основні завдання:

1. Провести аналіз сучасних технологій та протоколів побудови захищених корпоративних мереж, методів сегментації та тунелювання трафіку.
2. Спроектувати логічну та фізичну топологію мережі на основі архітектури зі згорнутим ядром (Firewall-centric), розробити модель IP-адресації.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Россінський Ю.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

3. Реалізувати логічне розділення трафіку за допомогою віртуальних локальних мереж (VLAN) з налаштуванням міжмережевої маршрутизації та списків контролю доступу (ACL) за принципом нульової довіри (Zero Trust).
4. Розгорнути та налаштувати службу каталогів Active Directory для централізованого управління об'єктами мережі та розмежування прав доступу до корпоративних ресурсів.
5. Налаштувати граничний міжмережевий екран Cisco ASA для забезпечення відмовостійкості зовнішніх каналів зв'язку на базі IP SLA та Object Tracking та обробки трансляції адрес (NAT/PAT).
6. Впровадити підсистему захищеного віддаленого доступу на базі Cisco AnyConnect SSL/DTLS VPN з делегуванням авторизації користувачів до Active Directory через протокол LDAP.
7. Провести комплексне тестування розгорнутої інфраструктури в середовищі емуляції для підтвердження її працездатності та стійкості до мережевих загроз.

Об'єкт дослідження – процес побудови та функціонування захищених корпоративних інформаційних мереж.

Предмет дослідження – методи, протоколи та програмно-апаратні засоби (IP SLA та Object Tracking, VLAN, Active Directory, Cisco AnyConnect VPN), що забезпечують захист, сегментацію, відмовостійкість та управління доступом у корпоративній мережі.

Практичне значення одержаних результатів. Розроблена та протестована мережева архітектура являє собою готове, масштабоване інженерне рішення. Запропонована модель налаштування списків доступу, інтеграції Active Directory з міжмережевим екраном [9, 12] та організація двоканального SSL/DTLS тунелю [7, 8] може бути безпосередньо впроваджена в ІТ-інфраструктуру реального підприємства для підвищення загального рівня кібербезпеки та забезпечення безпечної віддаленої роботи співробітників компанії.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ТА ЗАХИСТУ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Архітектура захищених мереж та концепція Zero Trust

Сучасна корпоративна інформаційна мережа (KIM) являє собою складну, багаторівневу екосистему, яка об'єднує різноманітні класи пристроїв, сервісів та типів користувачів. Традиційний підхід до побудови мереж у вигляді єдиного «плоского» (flat) простору, де всі вузли знаходяться в одному широкомовному домені, сьогодні вважається критично небезпечним та архітектурно застарілим. У такій топології компрометація хоча б однієї робочої станції автоматично відкриває зловмишнику прямий шлях до критично важливих серверів та баз даних шляхом горизонтального переміщення мережею (Lateral Movement). Крім того, неконтрольоване розростання широкомовного трафіку (ARP-запити, DHCP-повідомлення тощо) призводить до суттєвого зниження загальної пропускної здатності каналів зв'язку.

Сьогодні еталонним стандартом індустрії кібербезпеки є відмова від застарілої моделі «замку і рову» (периметрового захисту) на користь архітектури Zero Trust (Нульової довіри), яка детально описана в стандартах Національного інституту стандартів і технологій США (NIST) [1]. Головний постулат цієї концепції: «ніколи не довіряй, завжди перевіряй». Мережа розглядається як апріорі вороже середовище, тому довіра не повинна надаватися жодному пристрою чи користувачу лише на основі того, що вони фізично знаходяться всередині корпоративної будівлі [1].

Для наочного розуміння еволюції підходів до кібербезпеки, у таблиці 1.1 наведено порівняльний аналіз традиційної периметрової моделі та архітектури Zero Trust.

Таблиця 1.1

Порівняльна характеристика мережевих архітектур

Критерій оцінки	Традиційна модель («Замок і рів»)	Архітектура Zero Trust (Нульова довіра)
Базовий рівень довіри	Високий для всіх пристроїв усередині мережі.	Відсутній. Довіра встановлюється динамічно після верифікації.

Управління доступом	Одноразова перевірка на вході в мережу (VPN/Шлюз).	Безперервна автентифікація для кожної сесії та ресурсу.
Поширення загроз	Високий ризик горизонтального переміщення (Lateral Movement).	Мінімальний завдяки жорсткій мікросегментації інфраструктури.
Фокус захисту	Захист зовнішнього периметра мережі від Інтернету.	Захист безпосередньо даних, застосунків та ідентичностей.

Фундаментом для реалізації Zero Trust на базовому мережевому рівні є мікросегментація інфраструктури за допомогою технології віртуальних локальних мереж (VLAN), що регламентується стандартом IEEE 802.1Q [4]. Концептуальну модель мікросегментації та переходу до архітектури нульової довіри проілюстровано на рисунку 1.1.

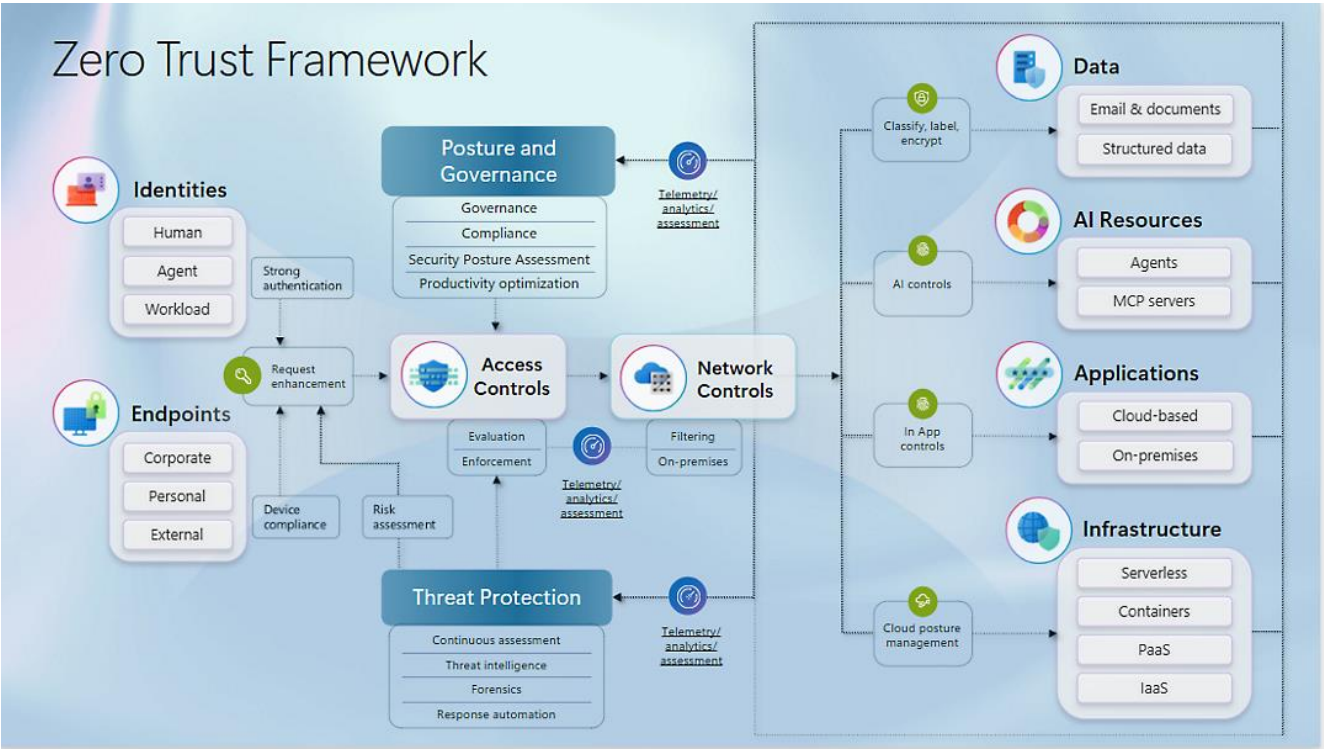


Рисунок 1.1 – Концептуальна модель логічної мікросегментації та ізоляції в архітектурі Zero Trust

Логічна сегментація дозволяє на базі єдиної фізичної інфраструктури комутаторів створити безліч ізольованих логічних підмереж (окремі зони для серверів, штатних працівників та гостей пристроїв). Кожен VLAN формує власний закритий широкомовний домен, вийти за межі якого трафік може виключно через пристрої мережевого рівня (L3-комутатори або міжмережеві екрани). Це створює іде-

альну точку контролю (Choke Point) для застосування суворих списків контролю доступу (ACL) на апаратних шлюзах безпеки [19].

Реалізація такої моделі мікросегментації кардинально звужує поверхню атаки підприємства. Навіть якщо пристрій у недовіреному гостьовому сегменті або на робочому місці співробітника буде інфіковано шкідливим програмним забезпеченням чи вірусом-шифрувальником (Ransomware), жорсткі правила маршрутизації та апаратний міжмережевий екран не дозволять загрозі розповсюдитися та паралізувати роботу критичних баз даних у сегменті серверів.

Таким чином, логічне розділення трафіку за допомогою стандарту 802.1Q є фундаментальним рівнем безпеки. Однак, розмежування мереж виключно на мережевому рівні (L2/L3) забезпечує лише логічну ізоляцію потоків даних. Для повноцінного впровадження моделі Zero Trust, де враховується не лише IP-адреса, але й особа самого користувача, мережева інфраструктура потребує розгортання служби каталогів верхнього рівня та впровадження рольової моделі управління доступом.

1.2 Технологія централізованого управління інфраструктурою Microsoft Active Directory

Масштабування корпоративної мережі та впровадження логічної сегментації розв'язують проблеми маршрутизації та базової ізоляції трафіку. Проте на рівні управління кінцевими вузлами та доступом користувачів децентралізована модель (робочі групи, Workgroups) швидко стає некерованою. У такій моделі облікові записи та політики безпеки зберігаються локально (в базах SAM) на кожному окремому комп'ютері. Це унеможливорює швидке блокування скомпрометованих облікових записів, аудит доступу до спільних ресурсів та впровадження єдиних стандартів парольного захисту [12].

Для забезпечення монолітної системи ідентифікації, автентифікації та авторизації (AAA) сучасні корпоративні мережі будуються навколо спеціалізованих служб каталогів. Де-факто галузевим стандартом у цій сфері є технологія Active Directory Domain Services (AD DS) від корпорації Microsoft [12]. Ця служба інтегрує мережеві протоколи LDAP (Lightweight Directory Access Protocol) для пошуку та

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

модифікації об'єктів [9], DNS для маршрутизації запитів доступу та протокол мережевої автентифікації Kerberos, що забезпечує надійне підтвердження особи користувача без передачі відкритих паролів по мережі.

Основою ефективного управління інфраструктурою в Active Directory є правильне проєктування її логічної топології, яка складається з доменів, дерев та лісів, а на мікрорівні — з організаційних одиниць (Organizational Units, OU). Ієрархічну модель взаємодії компонентів служби каталогів представлено на рисунку 1.2.

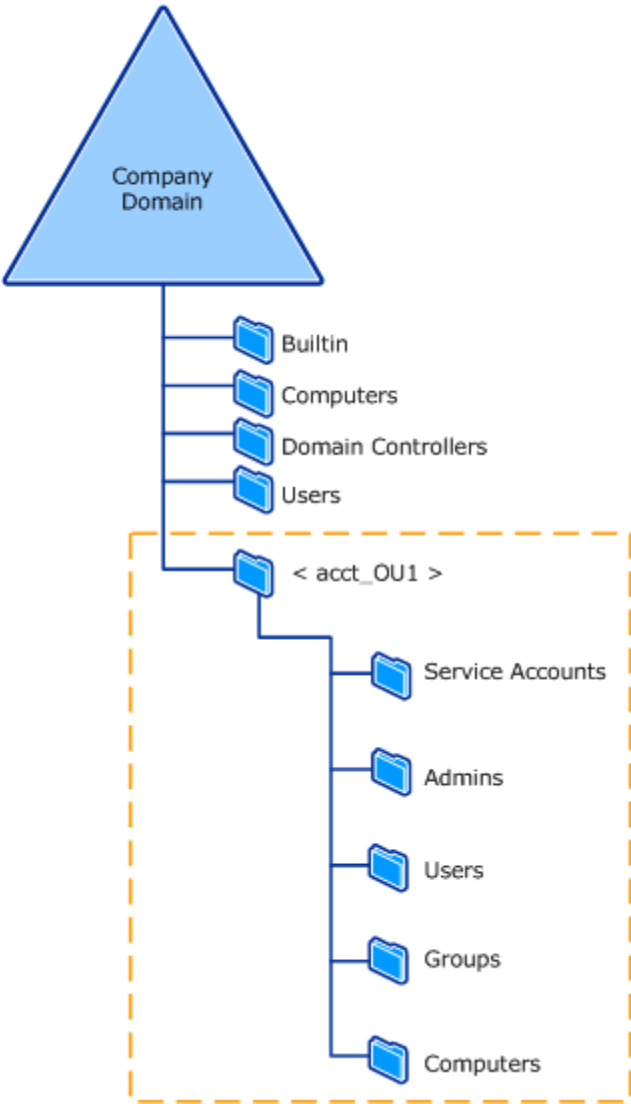


Рисунок 1.2 – Логічна ієрархія базових об'єктів та контейнерів у середовищі Active Directory

Організаційні одиниці діють як логічні контейнери, що дозволяють відтворити реальну адміністративну структуру підприємства, згрупувати об'єкти (користувачів, сервери, робочі станції) та точково застосовувати до них об'єкти групових

політик (GPO) [14] або делегувати адміністративні повноваження згідно з принципом найменших привілеїв [16].

Проте самої лише приналежності користувача до певної організаційної одиниці недостатньо для надання йому доступу до мережевих ресурсів. Відповідно до концепції управління доступом на основі ролей (Role-Based Access Control, RBAC) [15], дозволи ніколи не призначаються безпосередньо обліковим записам користувачів. Натомість використовуються глобальні групи безпеки (Global Security Groups) [13]. Аналіз впливу ключових компонентів AD на безпеку інфраструктури наведено у таблиці 1.2.

Таблиця 1.2

Аналіз впливу компонентів Active Directory на кібербезпеку мережі

Технологічний компонент AD DS	Функціональне призначення	Роль у системі кібербезпеки
Організаційна одиниця (OU)	Логічне групування об'єктів (користувачів, ПК).	Ізоляція політик безпеки для різних відділів; делегування прав адміністраторам.
Група безпеки (Security Group)	Об'єднання користувачів за посадовими ролями.	Реалізація моделі RBAC; призначення прав доступу до файлових систем (NTFS) [17].
Групова політика (GPO)	Централізоване налаштування параметрів ОС.	Примусове застосування складності паролів, налаштування брандмауерів [14].
Інтеграція по LDAP/RADIUS	Взаємодія AD із зовнішнім мережевим обладнанням.	Єдина точка автентифікації для віддалених підключень (VPN) [9, 11].

Важливим архітектурним рішенням на стику системного адміністрування та мережевої безпеки є саме інтеграція служби каталогів із зовнішніми шлюзами. Замість створення локальних користувачів безпосередньо в пам'яті міжмережевих екранів, шлюзи безпеки налаштовуються на взаємодію з Active Directory через стандартизовані протоколи LDAP або RADIUS.

Коли віддалений користувач намагається встановити VPN-сесію, міжмережевий екран пересилає його облікові дані на перевірку до контролера домену. Якщо пароль вірний, але користувач не є членом відповідної цільової групи безпеки для віддаленого доступу, з'єднання буде відхилено на етапі авторизації. Це дозволяє ІТ-відділу централізовано керувати доступом (наприклад, миттєво відк-

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

ливати права при звільненні співробітника), вилучаючи його з глобальної групи в Active Directory [13], не торкаючись конфігурації самого мережевого екрана.

Таким чином, розгортання служби каталогів Active Directory з чітко спроектованою ієрархією OU та груп безпеки перетворює розрізнені сегменти мережі на єдиний, легко керований корпоративний простір. Централізація автентифікації не лише спрощує аудит інформаційної безпеки, але й створює надійний фундамент для впровадження складних протоколів віддаленого доступу, які вимагають суворої верифікації особи на кордоні периметра.

1.3 Технологія захищеного віддаленого доступу Cisco AnyConnect

Побудова сегментованої мережевої інфраструктури та впровадження служби каталогів Active Directory формують надійний внутрішній периметр безпеки. Однак, із переходом до гібридних моделей роботи виникає критична потреба у забезпеченні доступу до корпоративних ресурсів для віддалених співробітників. Відкриття прямих мережевих портів до внутрішніх серверів через трансляцію адрес (Port Forwarding) є неприпустимим з точки зору кібербезпеки, оскільки це піддає інфраструктуру постійним атакам типу Brute-force та експлуатації вразливостей нульового дня (Zero-day). Єдиним архітектурно правильним рішенням є розгортання віртуальної приватної мережі віддаленого доступу (Remote Access VPN). Для обґрунтування вибору оптимальної технології побудови захищеного тунелю був проведений порівняльний аналіз трьох найпопулярніших корпоративних VPN-протоколів: IPsec (IKEv2), OpenVPN та SSL/DTLS. Результати порівняння наведено у таблиці 1.3.

Таблиця 1.3

Характеристика	IPsec (IKEv2)	OpenVPN	SSL/DTLS (напр., AnyConnect)
Транспортний протокол / Порти	ESP (L3), UDP 500 / 4500	UDP 1194 або TCP 1194	TCP 443 (TLS) + UDP 443 (DTLS)
Пройдення крізь NAT / Фільтри	Ускладнене (потребує NAT-T), часто блокується провайдерами	Добре, але порт 1194 легко ідентифікується системами DPI	Відмінне, імітує стандартний HTTPS-трафік

Стійкість до "TCP Meltdown"	Не схильний (працює на мережевому рівні)	Схильний при використанні TCP-транспорту	Вирішено архітектурно (динамічний перехід на DTLS)
Інтеграція з AD та AAA	Складна в налаштуванні	Потребує сторонніх RADIUS-конекторів	Нативна глибока інтеграція з корпоративними шлюзами

Традиційно для вирішення завдань віддаленого доступу використовувалися протоколи сімейства IPsec [2]. Вони забезпечують високий рівень криптографічної стійкості, проте мають фундаментальний недолік при роботі в сучасних гетерогенних мережах — проблему проходження через пристрої динамічної трансляції мережевих адрес (NAT/PAT). Протокол інкапсуляції ESP (Encapsulating Security Payload), що є ядром IPsec, функціонує безпосередньо поверх мережевого рівня (IP) і не має концепції портів транспортного рівня (TCP/UDP).

Коли віддалений співробітник намагається підключитися до корпоративного шлюзу з домашньої мережі або публічної точки доступу Wi-Fi (в готелі чи аеропорту), локальний маршрутизатор не може коректно обробити вихідний ESP-трафік через технологію PAT. Для обходу цього обмеження застосовується механізм NAT Traversal (NAT-T), який регламентується стандартом RFC 3948 [10] і примусово інкапсулює ESP-пакети в додатковий заголовок UDP з портом 4500. Проте адміністратори публічних мереж та інтернет-провайдери часто блокують нестандартні порти з метою економії пропускної здатності або з міркувань безпеки, що робить підключення класичних IPsec-клієнтів неможливим.

Для усунення транспортних обмежень та забезпечення гарантованого доступу з будь-якої точки світу найбільш доцільним та сучасним підходом є розгортання архітектури SSL VPN (наприклад, на базі технології Cisco AnyConnect) [3, 20].

Сучасні реалізації SSL VPN кардинально відрізняються від класичних IPsec-рішень своєю двоканальною архітектурою (Dual-Tunnel). Первинна ініціалізація тунелю, автентифікація користувача в службі каталогів та обмін криптографічними сертифікатами здійснюються через контрольний канал керування. Для цього вико-

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Россінський Ю.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

ристовується протокол TLS (Transport Layer Security) [7] поверх стандартного TCP-порту 443 (HTTPS). Архітектура цього процесу представлена на рисунку 1.3.

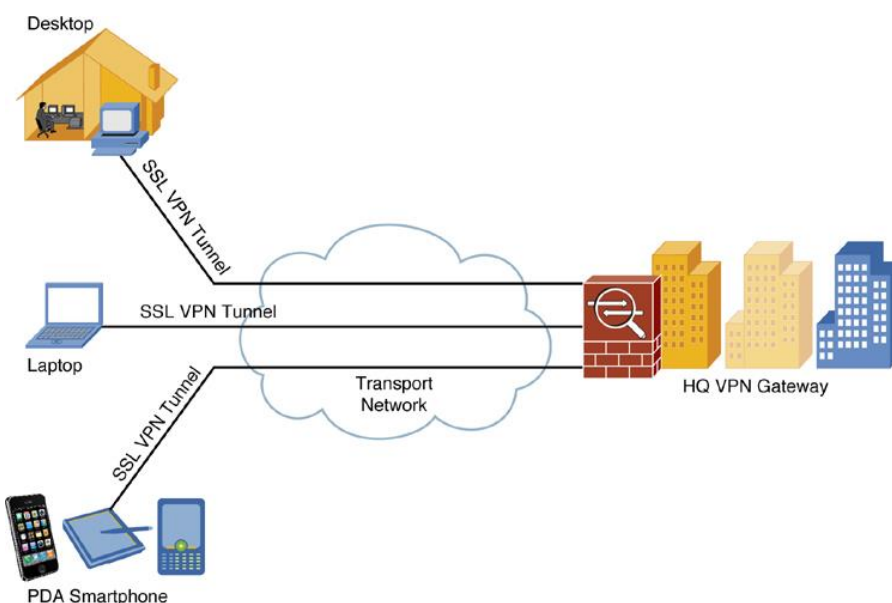


Рисунок 1.3 – Архітектура двоканального тунелювання SSL та DTLS у корпоративних VPN-клієнтах

Використання TCP 443 є стратегічною перевагою технології [3]. Для будь-якого транзитного міжмережевого екрана або системи глибокого аналізу пакетів (DPI) провайдера трафік виглядає як звичайний безпечний вебсерфінг або підключення до систем інтернет-банкінгу. Заблокувати цей порт неможливо без порушення роботи всієї глобальної мережі, що гарантує віддаленому співробітнику безперешкодний доступ до корпоративного шлюзу.

Проте інкапсуляція мережевого трафіку всередині TCP-тунелю створює відому інженерну проблему — TCP Meltdown (TCP-колапс). Якщо корисне навантаження (наприклад, файлова передача) обертається в зовнішній TCP-тунель, при найменшій затримці або втраті пакетів у публічній мережі таймери повторної відправки обох рівнів починають конфліктувати. Це призводить до експоненціального зростання затримок та лавиноподібного падіння пропускної здатності.

Для усунення ефекту TCP Meltdown VPN-клієнт відразу після успішної авторизації по TLS намагається встановити паралельний канал даних з використанням протоколу DTLS (Datagram Transport Layer Security) [8] поверх UDP-порту 443. Протокол DTLS забезпечує аналогічний TLS рівень шифрування, але завдяки використанню дейтаграм не має вбудованих механізмів підтвердження доставки на

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

транспортному рівні. Втрачені пакети обробляються безпосередньо кінцевими додатками, що дозволяє VPN-тунелю працювати на максимальній фізичній швидкості каналу.

Системна інтеграція VPN в корпоративну інфраструктуру відбувається на рівні граничного міжмережевого екрана. Оскільки сучасні корпоративні міжмережеві екрани функціонують за концепцією Stateful Inspection [19], вони не просто приймають тунель, а термінують його на зовнішньому інтерфейсі. Після розшифрування пакетів трафік віддаленого користувача піддається суворій перевірці списками доступу (ACL), перш ніж потрапити у внутрішні захищені сегменти.

Критично важливим етапом налаштування мережевого шлюзу є реалізація правила обходу трансляції адрес — NAT Exemption (NAT Bypass). За замовчуванням шлюзи використовують NAT для приховування внутрішніх адрес мережі. Проте для коректної маршрутизації VPN-трафіку застосовується механізм Identity NAT [25]: якщо трафік прямує з локальних мереж до пулу віддалених VPN-клієнтів, пристрій зобов'язаний залишити оригінальні IP-адреси без змін. Це дозволяє віддаленим станціям та серверам взаємодіяти безпосередньо. Логіка цього процесу відображена на рисунку 1.4.

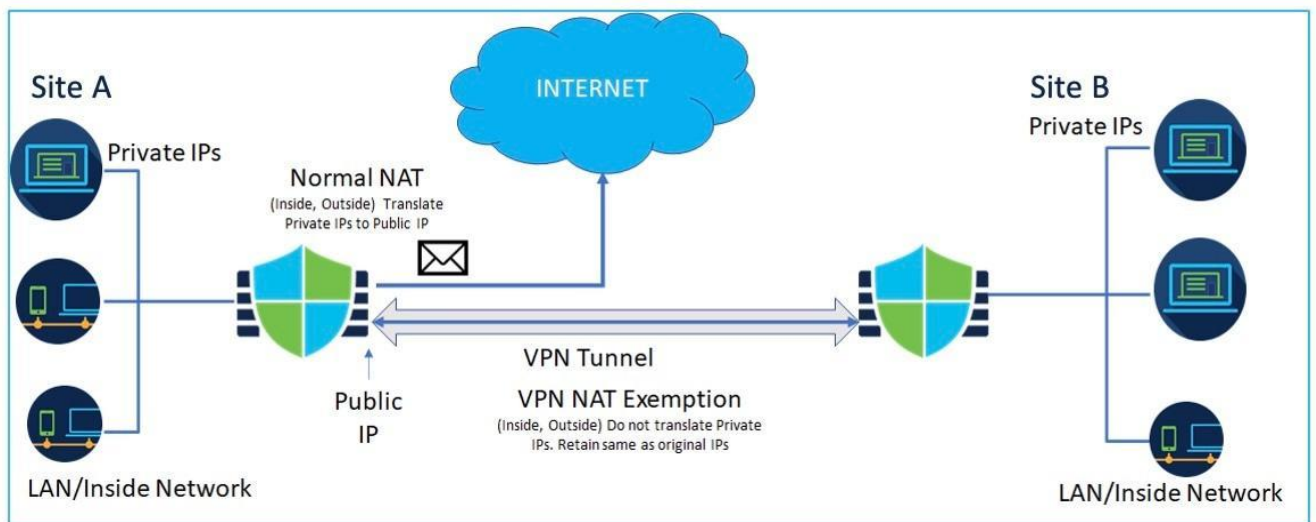


Рисунок 1.4 – Логіка маршрутизації VPN-трафіку в умовах обходу динамічної трансляції (NAT Exemption)

Керування доступом реалізується за принципом AAA (Authentication, Authorization, Accounting) з жорсткою прив'язкою до корпоративної служби ката-

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

логів. Замість створення вразливих локальних облікових записів безпосередньо на міжмережевих екранах, шлюз безпеки пересилає запити на авторизацію до контролера домену через стандартизовані протоколи, такі як LDAP [9]. Завдяки політикам безпеки, ініціювати тунель може лише той користувач, який попередньо доданий ІТ-адміністратором до спеціалізованої глобальної групи безпеки в Active Directory [13]. Це забезпечує єдину точку управління життєвим циклом облікових записів та повністю відповідає концепції централізованої безпеки корпоративного рівня.

1.4 Технології забезпечення відмовостійкості мережі

У сучасних умовах безперервність доступу до корпоративних інформаційних ресурсів та стабільність віддалених підключень є критично важливими вимогами для життєдіяльності будь-якого підприємства. Оскільки збої на стороні інтернет-провайдерів (ISP) можуть призвести до повної зупинки бізнес-процесів, архітектура граничного периметра мережі обов'язково повинна передбачати наявність резервних каналів зв'язку (концепція Dual-WAN) та механізмів автоматичного перемикавання трафіку (Failover).

Традиційно для забезпечення відмовостійкості та резервування на стику з глобальною мережею розглядається використання протоколів динамічної маршрутизації, таких як OSPF або BGP. Проте в реальних умовах корпоративного сектора інтернет-провайдери зазвичай не підтримують встановлення сусідства за цими протоколами з клієнтським обладнанням на стандартних тарифах для бізнесу. Перехід на виділені BGP-канали вимагає значних фінансових витрат, отримання власної автономної системи (AS) та виділення пулу незалежних провайдерських адрес, що часто є економічно недоцільним для середнього бізнесу або філій компаній.

З огляду на це, найбільш оптимальним, гнучким та архітектурно правильним інженерним підходом є використання статичної маршрутизації у поєднанні з технологіями активного моніторингу стану каналів зв'язку. Еталонним стандартом у цьому напрямку є технологія IP SLA (Service Level Agreement) від компанії Cisco, яка функціонує в синергії з механізмом об'єктного відстеження Object Tracking.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Россінський Ю.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Для обґрунтування вибору технології автоматичного перемикавання зовнішніх каналів зв'язку у таблиці 1.4 наведено порівняльний аналіз динамічної маршрутизації та статичної маршрутизації з підтримкою IP SLA Tracking.

Таблиця 1.4

Порівняльний аналіз методів резервування зовнішніх WAN-каналів

Критерій порівняння	Динамічна маршрутизація (BGP/OSPF)	Статична маршрутизація з IP SLA Tracking
Складність налаштування	Висока (потребує узгодження параметрів автономних систем та стикування)	Середня (реалізується автономно на граничному міжмережевому екрані)
Вимоги до ISP	Обов'язкова підтримка протоколу динамічної маршрутизації з боку провайдера	Відсутні (провайдер надає стандартний статичний або динамічний шлюз)
Фінансові витрати	Високі (оплата дороговартісних виділених ліній, купівля AS та IP-пулів)	Мінімальні (використовуються стандартні бізнес-тарифи будь-яких двох ISP)
Швидкість збіжності	Від кількох секунд (BGP) до десятків секунд залежно від таймерів	Регулюється адміністратором (зазвичай 5–10 секунд)
Обробка VPN-трафіку	Потребує складного перерозподілу маршрутів та моніторингу peer-to-peer	Забезпечує стабільну безшовну міграцію тунелів завдяки стійкості DTLS

Принцип роботи зв'язки технологій IP SLA та Object Tracking базується на генерації безперервного діагностичного трафіку для перевірки доступності конкретного вузла. Граничний пристрій (міжмережевий екран) через заданий інтервал часу (Frequency) надсилає тестові ICMP Echo-запити через основний WAN-інтерфейс у бік шлюзу першого провайдера або публічного DNS-сервера.

Логічний алгоритм функціонування даної системи складається з трьох рівнів:

1. Процес IP SLA: Безперервно вимірює параметри затримки та доступності вузла. Якщо протягом встановленого таймауту (Timeout) відповідь на ICMP-запит не надходить, транзакція вважається невдалою.
2. Об'єкт відстеження (Track): Аналізує результати роботи процесу IP SLA та динамічно змінює свій стан. У разі успішних відповідей об'єкт перебуває у стані «Up», а при втраті пакетів — переходить у стан «Down».
3. Таблиця маршрутизації: Основний маршрут за замовчуванням (з мінімальною метрикою) жорстко прив'язується до стану об'єкта Track. Щойно

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

об'єкт переходить у стан «Down», міжмережевий екран миттєво видаляє цей маршрут із таблиці маршрутизації.

Після видалення основного маршруту активується так званий плаваючий статичний маршрут (Floating Static Route), який має вищу адміністративну відстань (метрику) і веде через інтерфейс резервного провайдера. Увесь корпоративний та VPN-трафік автоматично перенаправляється на другий канал зв'язку. Коли працездатність основного провайдера відновлюється, IP SLA фіксує успішні ICMP-відповіді, об'єкт Track повертається у стан «Up», основний маршрут автоматично інсталюється назад у таблицю, а плаваючий маршрут знову стає неактивним.

Таким чином, впровадження технології IP SLA у поєднанні з Object Tracking дозволяє створити повністю автоматизований, економічно доцільний та стійкий до відмов зовнішній периметр безпеки, що гарантує безперебійну роботу локальних користувачів та віддалених VPN-клієнтів підприємства.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Висновок до першого розділу

У першому розділі дипломного проєкту було проведено комплексний аналіз сучасних технологій, протоколів та архітектурних підходів до побудови безпечної корпоративної інформаційної мережі. Доведено, що використання традиційних не-сегментованих топологій є вразливим до сучасних кіберзагроз, що обумовлює необхідність впровадження концепції Zero Trust (нульової довіри) [1]. Обґрунтовано доцільність логічної мікросегментації інфраструктури на базі стандарту IEEE 802.1Q (VLAN) [4], що дозволяє звужити поверхню атаки та унеможливити горизонтальне розповсюдження загроз між ізольованими серверними, робочими та гостьовими сегментами мережі.

Дослідження технологій централізованого управління інфраструктурою підтвердило фундаментальну роль служби каталогів Active Directory (AD DS) [12] у забезпеченні корпоративної безпеки. Встановлено, що розгортання єдиного керованого домену є оптимальним рішенням для реалізації політики безпеки та забезпечення керування доступом на основі ролей (RBAC) [15]. Це дозволяє ефективно адмініструвати права користувачів на рівні файлової системи та уникати вразливостей, притаманних децентралізованим локальним обліковим записам.

Завершальним етапом аналізу стало дослідження технологій віддаленого доступу та обґрунтування вибору архітектури SSL/DTLS VPN на базі Cisco AnyConnect [3, 20]. Здійснений порівняльний аналіз довів, що дане рішення ефективно долає проблеми блокування трафіку пристроями динамічної трансляції адрес (NAT/PAT) [10] та усуває затримки передачі даних (TCP Meltown) завдяки паралельному використанню протоколу DTLS [8]. Сформовано концептуальний підхід до захисту периметра, що базується на інтеграції міжмережевого екрана Cisco ASA [19] із сервером автентифікації Active Directory за протоколом LDAP [9] та використанні механізмів обходу трансляції Identity NAT [25] для створення безпечного середовища віддаленої роботи.

Додатково досліджено методи моніторингу граничного периметра та обґрунтовано використання технології IP SLA і механізму Object Tracking [6, 21] замість складних протоколів динамічної маршрутизації. Це дозволяє надійно та економі-

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

чно доцільно забезпечити автоматичну відмовостійкість зовнішніх каналів зв'язку (Dual-WAN), що детально розглянуто у підпункті 1.4.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Вимоги до апаратного середовища та моделі загроз

Для практичної реалізації та тестування спроектованої корпоративної мережі без ризику впливу на реальні бізнес-процеси підприємства було обрано метод програмно-апаратної емуляції. Основним інструментом розгортання топології виступає графічний симулятор мережі GNS3 (Graphical Network Simulator-3) [23], який дозволяє запускати віртуальні образи реального мережевого обладнання Cisco за допомогою гіпервізора QEMU [24], а також інтегрувати в загальну топологію повноцінні віртуальні машини на базі клієнтських та серверних ОС Windows.

Зважаючи на високу ресурсомісткість одночасного запуску апаратного міжмережевого екрана зі Stateful-фільтрацією, контролера домену Active Directory та декількох клієнтських операційних систем, було сформовано базові вимоги до апаратного та програмного забезпечення хостової станції. Конфігурацію тестового стенда наведено в таблиці 2.1.

Таблиця 2.1

Вимоги до апаратного та програмного забезпечення середовища емуляції

Компонент інфраструктури	Програмне забезпечення / Версія ОС	Мінімальні виділені ресурси
VPN PC	Windows 11 Pro (64-bit) Cisco AnyConnect Secure Mobility Client 4.10	2 vCPU, 4 ГБ vRAM
Мережевий симулятор	GNS3 версії 2.2.55	2 vCPU, 4 ГБ vRAM
Міжмережевий екран	Образ Cisco ASAv 9.8.1	1 vCPU, 2 ГБ vRAM емуляція QEMU
Серверний сегмент (VLAN 10)	Windows Server 2025 (Active Directory, DNS)	2 vCPU, 4 ГБ vRAM
Робоча станція (VLAN 20)	Windows 11 Pro	2 vCPU, 4 ГБ vRAM

Наступним критичним кроком проєктування є розробка моделі загроз інформаційній безпеці (Threat Model). Цей процес дозволяє ідентифікувати потенційні вектори атак на корпоративну інфраструктуру та сформувавши перелік превентивних архітектурних заходів, які мають бути практично реалізовані в межах даного дипломного проєкту.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Система захисту мережі проєктується з урахуванням концепції Zero Trust [1], де загроза може виходити як із зовнішнього середовища (Інтернет), так і зсередини корпоративного периметра. Основні ідентифіковані вектори атак та інженерні методи їх нейтралізації за допомогою обраного апаратного та програмного забезпечення наведено в таблиці 2.2.

Таблиця 2.2

Модель загроз інформаційної безпеки корпоративної мережі

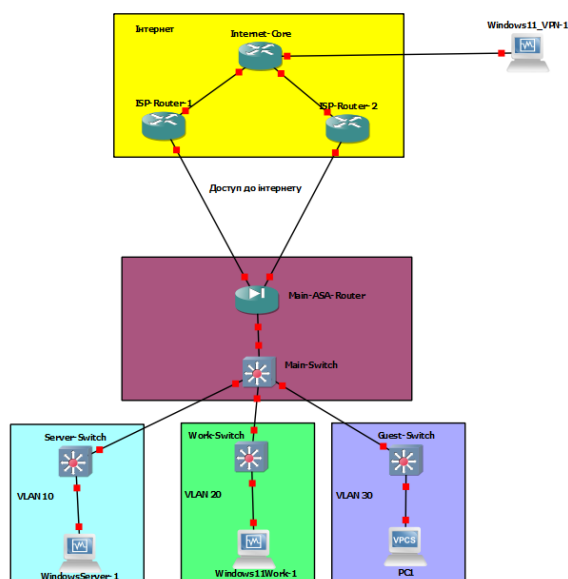
Ідентифікована загроза	Вектор та наслідки атаки	Архітектурне рішення для нейтралізації
Несанкціонований доступ із гостьової мережі	Підключення злоумисника до відкритого гостьового Wi-Fi (VLAN 30) з метою сканування внутрішніх ресурсів або викрадення даних із серверів.	Логічна ізоляція за допомогою IEEE 802.1Q. Застосування списків контролю доступу (ACL) на рівні Cisco ASA (Deny Any для напрямків VLAN 30 → VLAN 10/20).
Горизонтальне переміщення загроз (Lateral Movement)	Інфікування робочого комп'ютера співробітника (VLAN 20) програмою-вимагачем (Ransomware) та спроба її поширення на контролер домену.	Сегментація трафіку за рівнями безпеки (Security Levels). Суворе обмеження дозволених портів між VLAN 20 та VLAN 10 (тільки LDAP, DNS, SMB).
Компрометація віддаленого VPN-з'єднання	Атака типу Man-in-the-Middle (MitM) або перехоплення паролів при підключенні співробітника через публічну мережу Інтернет.	Використання криптографічно стійких тунелів SSL/DTLS (Cisco AnyConnect). Перевірка валідності підключення за допомогою локальних сертифікатів RSA (Trustpoint).
Несанкціонований доступ до конфіденційних даних	Спроба рядового співробітника або VPN-користувача відкрити директорії відділу кадрів чи бухгалтерії.	Впровадження служби Active Directory. Керування доступом на основі ролей (RBAC) за допомогою глобальних груп безпеки (Security Groups).
Відмова в обслуговуванні через збій провайдера	Фізичне пошкодження каналу зв'язку основного інтернет-провайдера (ISP 1), що призводить до зупинки бізнес-процесів.	Підключення резервного каналу (ISP 2) та використання технології IP SLA з відстеженням об'єктів (Object Tracking) для автоматичного перемикання трафіку (Failover).

Сформована модель загроз та визначені апаратні вимоги слугують технічним фундаментом для подальшої розробки логічної топології мережі, розподілу адресного простору та конфігурації політик маршрутизації, що детально розглядаються у наступних підрозділах.

2.2 Проєктування топології, IP-адресації та VLAN

Проєктування надійної корпоративної мережі розпочинається зі створення логічної та фізичної топології, яка б відповідала вимогам відмовостійкості, масштабованості та безпеки. Для реалізації завдань даного дипломного проєкту було обрано архітектурну модель зі згорнутим ядром (Collapsed Core) та централізованим міжмережевим екраном (Firewall-centric architecture) [19]. У такій моделі пристрій Cisco ASA виступає не лише як граничний шлюз доступу до мережі Інтернет, але й як центральний маршрутизатор (Core Router) для всіх внутрішніх локальних мереж, що дозволяє застосовувати політики глибокої інспекції трафіку безпосередньо між відділами підприємства.

На фізичному рівні інфраструктура складається з граничного шлюзу безпеки (Cisco ASA), який підключено до інтернет-провайдерів (ISP) через зовнішні інтерфейси, та керованих комутаторів рівня доступу, до яких фізично підключаються кінцеві вузли: сервери, робочі станції співробітників та гостьові пристрої. Фізична топологія мережі наведена на рисунку 2.1.



		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Рисунок 2.1 – Фізична топологія корпоративної мережі, реалізована в середовищі емуляції GNS3

З точки зору логічної топології, мережа проєктується на основі поділу на ізольовані зони безпеки за допомогою технології віртуальних локальних мереж (VLAN) стандарту IEEE 802.1Q [4]. Кожен комутатор налаштовується на передачу маркованого трафіку (Trunk) до центрального інтерфейсу Cisco ASA. На самій ASA створюються логічні субінтерфейси (Sub-interfaces), кожен з яких виступає шлюзом за замовчуванням (Default Gateway) для відповідного VLAN. Така маршрутизація відома як концепція «Router-on-a-Stick».

Для побудови внутрішньої інфраструктури використовується приватний адресний простір, регламентований стандартом RFC 1918 [5]. Базовою мережею обрано діапазон 192.168.0.0/16, який логічно поділено на підмережі з маскою /24 (255.255.255.0). Це забезпечує оптимальний розмір широкомовного домену (до 254 хостів), який запобігає перевантаженню каналів зв'язку паразитним трафіком. Зведена модель розподілу IP-адрес наведена у таблиці 2.3.

Таблиця 2.3

Модель IP-адресації корпоративної мережі

Назва сегмента (Зона)	VLAN / Інтерфейс	Адреса підмережі (Маска)	IP-адреса шлюзу (ASA)	Призначення та пули адрес
Servers (Inside)	VLAN 10 (inside10)	192.168.10.0 /24	192.168.10.1	Серверна інфраструктура. Статична IP 192.168.10.10 для AD/DNS/DHCP.
Work (Corporate)	VLAN 20 (inside20)	192.168.20.0 /24	192.168.20.1	Робочі станції. Динамічна видача DHCP: пули 192.168.20.100-200.
Guest (Untrusted)	VLAN 30 (inside30)	192.168.30.0 /24	192.168.30.1	Гостьова мережа. Динамічна видача DHCP для ізольованого доступу до Інтернету.
VPN Clients	Віртуальний пул	192.168.250.0 /24	Маршрутизується ASA	Виділений пул адрес (192.168.250.10+) для клієнтів AnyConnect.
Primary ISP	outside1	100.70.1.0 /30	100.70.1.2 (на ASA)	Основний зовнішній стик. Шлюз провайдера: 100.70.1.1.

Backup ISP	outside2	100.70.1.4 /30	100.70.1.6 (на ASA)	Резервний лінк. Шлюз провайдера: 100.70.1.5.
-------------------	----------	-------------------	------------------------	---

У межах проєкту інфраструктура підприємства логічно поділяється на три ключові сегменти:

1. VLAN 10 (Servers) – Серверна зона, де розгорнуто корпоративні служби Active Directory, DNS та захищені файлові сховища.
2. VLAN 20 (Workstations) – Робоча зона, призначена для ПК штатних співробітників компанії.
3. VLAN 30 (Guest) – Гостьова зона, виділена виключно для ізольованого підключення особистих мобільних пристроїв.

Фундаментальною архітектурною особливістю даного проєкту є підхід до призначення рівнів довіри (Security Levels) на міжмережевому екрані. Для забезпечення максимальної відповідності парадигмі Zero Trust (нульової довіри) [1], у цій роботі відкинуто класичну ієрархічну модель довіри. Усім внутрішнім логічним інтерфейсам (inside10, inside20, inside30) призначено однаковий максимальний рівень безпеки – security-level 100.

За замовчуванням операційна система Cisco ASA повністю блокує будь-яку взаємодію між інтерфейсами з однаковим рівнем безпеки. Для подолання цього обмеження на глобальному рівні застосовано команду «same-security-traffic permit inter-interface» [19]. Такий інженерний метод повністю нівелює будь-які неявні (implicit) дозволи. Відтепер міжмережевий екран покладається виключно на явно задані списки контролю доступу (ACL). Ізоляція сегментів базується на правилах, де дозволено лише необхідний для бізнесу трафік, а все інше блокується політикою «Deny Any». Для наочного відображення логіки взаємодії між сегментами сформовано матрицю мережевого доступу (Таблиця 2.4).

Таблиця 2.4

Матриця логічної взаємодії та маршрутизації між сегментами (VLAN)

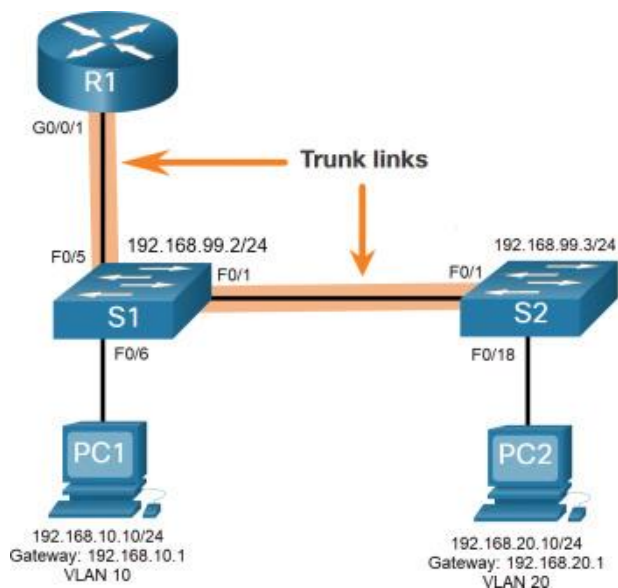
Джерело трафіку	VLAN 10 (Servers)	VLAN 20 (Workstations)	VLAN 30 (Guest)	Рівень безпеки (Security Level)
VLAN 10	Локальний трафік	Дозволено (Повний доступ)	Дозволено (Керування/Моніторинг)	Високий (High)

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Россінський Ю.М.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

VLAN 20	Дозволено (Доступ до сервісів)	Локальний трафік	Заборонено (Ізоляція)	Середній (Medium)
VLAN 30	Заборонено (Окрім DHCP)	Заборонено (Ізоляція)	Локальний трафік	Низький (Low)

Особливої інженерної уваги потребує реалізація механізму динамічної видачі IP-адрес (DHCP) для ізольованого гостьового сегмента (VLAN 30). Оскільки прямий доступ із VLAN 30 до сервера Active Directory заборонений, стандартні широкомовні запити від гостьових клієнтів будуть відкинуті. Для вирішення цієї колізії використовується технологія DHCP Relay (RFC 3046) [22]. Cisco ASA перехоплює широкомовні UDP-пакети на інтерфейсі inside30, інкапсулює їх в одноадресні пакети та від свого імені перенаправляє на авторизований сервер (192.168.10.10) в обхід стандартних списків ACL. Це дозволяє гостьовим клієнтам отримувати мережеві налаштування, залишаючись повністю ізольованими від прямого контакту з серверами.

Окремим архітектурним рішенням є виділення логічного пулу для віддалених користувачів VPN (192.168.250.0/24). Адреси VPN-клієнтів не перетинаються з існуючими локальними підмережами. Це дозволяє маршрутизувати зворотний трафік від серверів на шлюз ASA, створювати гранулярні списки доступу спеціально для віддалених працівників та налаштувати механізм Identity NAT (щоб трафік між серверами та VPN-клієнтами не піддавався підміні адрес). Логічна схема маршрутизації між VLAN та підключення VPN-пулу детально наведена на рисунку 2.2.



		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 2.2 – Логічна схема маршрутизації між VLAN (Router-on-a-Stick) та підключення VPN-пулу

Для забезпечення повної ізоляції гостьового сегмента та регламентованого доступу робочих станцій до серверів застосовуються строгі правила фільтрації трафіку. Схема застосування цих списків контролю доступу (ACL) на відповідних субінтерфейсах Cisco ASA проілюстрована на рисунку 2.3.

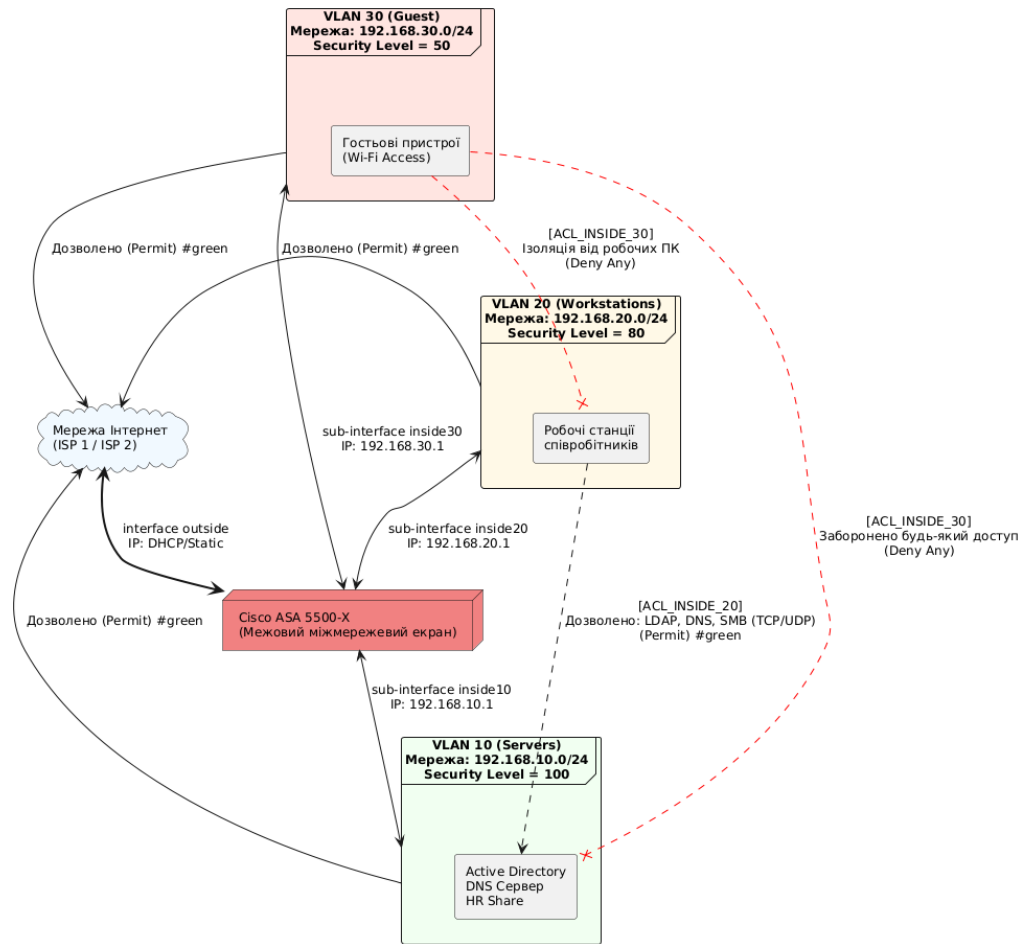


Рисунок 2.3 – Схема маршрутизації та застосування списків контролю доступу (ACL) між VLAN на інтерфейсах Cisco ASA

Логіка налаштування списків ACL, яка реалізує концепцію нульової довіри для внутрішніх сегментів мережі, систематизована в таблиці 2.5.

Таблиця 2.5

Правила списків контролю доступу (ACL) для внутрішніх сегментів мережі

Прив'язка ACL до інтерфейсу	Напрямок (Direction)	Джерело (Source)	Призначення (Destination)	Протокол / Порт	Дія (Action)
-----------------------------	----------------------	------------------	---------------------------	-----------------	--------------

ACL_INSIDE_20 (VLAN 20)	IN	192.168.20.0 /24	192.168.10.0/24	IP / Any	Permit (Доступ до сер- верів)
ACL_INSIDE_20 (VLAN 20)	IN	192.168.20.0 /24	192.168.30.0/24	IP / Any	Deny (Ізо- ляція від гос- тей)
ACL_INSIDE_20 (VLAN 20)	IN	192.168.20.0 /24	0.0.0.0/0 (Internet)	IP / Any	Permit (Доступ у ме- режу)
ACL_INSIDE_30 (VLAN 30)	IN	192.168.30.0 /24	192.168.10.0/24	IP / Any	Deny (Захист сер- верів)
ACL_INSIDE_30 (VLAN 30)	IN	192.168.30.0 /24	192.168.20.0/24	IP / Any	Deny (Захист рабо- чих станцій)
ACL_INSIDE_30 (VLAN 30)	IN	192.168.30.0 /24	0.0.0.0/0 (Internet)	IP / Any	Permit (Доступ у ме- режу)

Спроектовані правила взаємодії між віртуальними локальними мережами забезпечують надійний захист корпоративного периметра. Інтеграція L3-маршрутизації зі списками контролю доступу (ACL) та технологією DHCP Relay на базі Cisco ASA дозволяє створити гнучке, але суворо контрольоване середовище, в якому бізнес-процеси штатних співробітників та робота зовнішніх користувачів протікають у повністю незалежних площинах мережевої безпеки.

2.3 Проектування системи відмовостійкості зовнішніх каналів зв'язку на базі IP SLA Tracking

Забезпечення безперервної доступності корпоративних сервісів та надійного зв'язку з віддаленими клієнтами вимагає створення відмовостійкої архітектури маршрутизації. Використання базової статичної маршрутизації (Static Routing) у корпоративних мережах з кількома каналами зв'язку (Dual-WAN) є неефективним під-

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

ходом, оскільки вона не здатна автоматично адаптуватися до змін топології, обривів фізичних лінків або деградації каналів на боці інтернет-провайдерів.

Для вирішення завдання автоматичного управління шляхами передачі даних у даному дипломному проєкті впроваджено технологію моніторингу стану мережі IP SLA (Service Level Agreement) у поєднанні з механізмом Object Tracking. На відміну від протоколів динамічної маршрутизації (таких як OSPF або BGP), які вимагають підтримки та складних налаштувань з боку інтернет-провайдерів на стандартних бізнес-тарифах, IP SLA дозволяє міжмережевому екрану самостійно оцінювати доступність каналу та миттєво приймати рішення про перемикання трафіку.

У спроектованій топології міжмережевий екран Cisco ASA виконує роль межового шлюзу, який підключено до двох незалежних інтернет-провайдерів: основного (Primary ISP) через інтерфейс outside1 та резервного (Backup ISP) через інтерфейс outside2. Топологія механізму моніторингу та маршрутизації наведена на рисунку 2.4.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

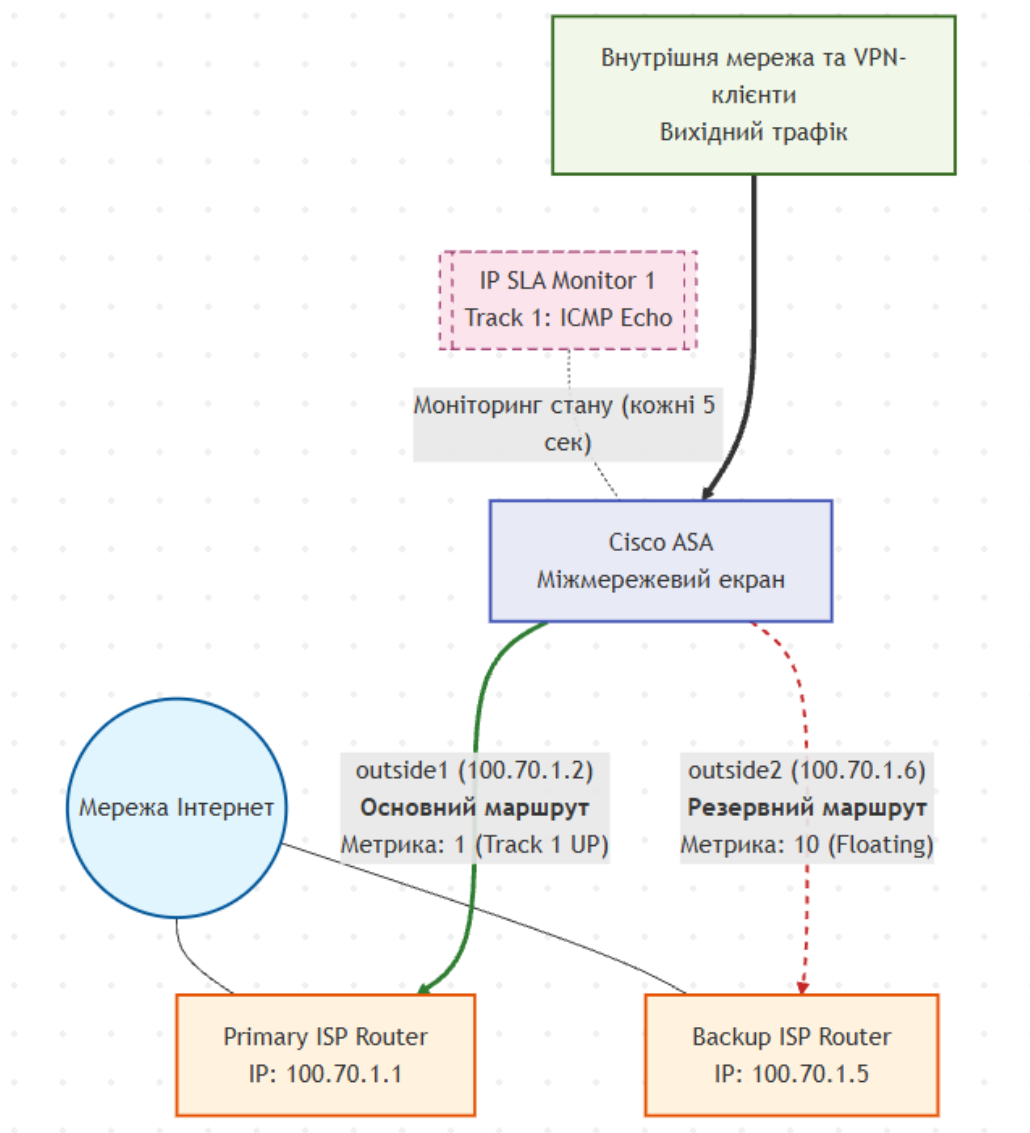


Рисунок 2.4 – Логічна схема організації відмовостійкості зовнішніх каналів зв'язку на базі IP SLA та Object Tracking)

Логіка роботи системи відмовостійкості базується на безперервному активному моніторингу. Процес IP SLA налаштовується на регулярне відправлення діагностичних ICMP-запитів (Echo Request) через основний інтерфейс outside1 до шлюзу провайдера (або до надійного зовнішнього вузла в мережі Інтернет). Стан цього процесу моніторингу логічно прив'язується до об'єкта відстеження — Track 1.

Маршрутизація трафіку реалізується за допомогою механізму плаваючих статичних маршрутів (Floating Static Routes). Основному маршруту за замовчуванням (Default Route), який спрямовує весь вихідний трафік через інтерфейс outside1, призначається стандартна адміністративна відстань (метрика 1). Цей статичний марш-

рут жорстко прив'язується до стану об'єкта Track 1. Резервному маршруту, що веде через інтерфейс outside2, призначається вища метрика (Cost = 10). Через більшу метрику резервний маршрут залишається неактивним (прихованим) у таблиці маршрутизації за нормальних умов роботи мережі.

Особливу увагу при проектуванні було приділено питанням мережевої безпеки та коректної обробки VPN-трафіку. Оскільки технологія AnyConnect SSL VPN налаштована з використанням правила NAT Exemption (виключення з динамічної трансляції адрес) для пулу 192.168.250.0/24, для забезпечення коректного зворотного зв'язку на маршрутизаторах провайдерів передбачаються відповідні зворотні статичні маршрути, спрямовані на зовнішні інтерфейси Cisco ASA. Завдяки механізму IP SLA, при перемиканні каналів ASA автоматично починає маршрутизувати тунельований трафік через резервний інтерфейс, зберігаючи цілісність підключень завдяки стійкості протоколу DTLS до короточасних обривів.

Логіка налаштування процесу моніторингу та маршрутизації на центральному шлюзі систематизована в таблиці 2.6.

Таблиця 2.6

Параметри конфігурації процесу IP SLA на міжмережевому екрані Cisco ASA

Параметр протоколу	Значення в проєкті	Інженерне обґрунтування налаштування
SLA Monitor ID	1	Локальний ідентифікатор процесу моніторингу мережі на Cisco ASA.
ICMP Echo Target	100.70.1.1 (шлюз Primary ISP)	IP-адреса, до якої постійно надсилаються запити для перевірки працездатності основного каналу.
Frequency / Timeout	5 секунд / 1 секунда	Інтервал відправки ICMP-запитів та час очікування відповіді, що гарантує швидке виявлення аварії.
Track ID	1	Логічний об'єкт відстеження, який змінює свій стан (Up/Down) на основі успішності ICMP-відповідей від SLA Monitor.
Primary Route Metric	1 (прив'язка до Track 1)	Основний маршрут через outside1. Працює виключно тоді, коли Track 1 знаходиться у стані Up.
Backup Route Metric	10 (Floating Route)	Резервний маршрут через outside2. Автоматично додається до таблиці маршрутизації, якщо основний маршрут зникає.

Критично важливим аспектом налаштування є автоматична реакція системи на інциденти. У штатному режимі, поки ICMP-відповіді успішно надходять через outside1, об'єкт Track 1 перебуває у стані «Up», і весь корпоративний трафік маршрутизується через основного провайдера.

У разі фізичного обриву кабелю, проблем на обладнанні провайдера або втрати ICMP-пакетів, об'єкт Track 1 миттєво переходить у стан «Down». Унаслідок цього міжмережевий екран автоматично видаляє основний статичний маршрут (із метрикою 1) з таблиці маршрутизації. Відразу після цього активується плаваючий резервний маршрут із метрикою 10, і весь потік даних перенаправляється через канал outside2 (Backup ISP). Цей процес займає лічені секунди, забезпечуючи надійну та безшовну відмовостійкість (Failover) інфраструктури без необхідності використання складних протоколів динамічної маршрутизації.

2.4 Проектування логічної структури Active Directory та моделі RBAC

Основою централізованого управління корпоративною інфраструктурою підприємства є служба каталогів Active Directory Domain Services (AD DS) [12]. Для реалізації проєкту було обрано архітектуру з одним лісом та одним кореневим доменом, якому призначено внутрішнє ім'я corp.local. Контролер домену логічно розташовується в максимально захищеному серверному сегменті (VLAN 10) з виділеною статичною IP-адресою 192.168.10.10.

Відповідно до вимог політики безпеки підприємства та для забезпечення ефективного керування доступом на основі ролей (Role-Based Access Control, RBAC) [15], першочерговим завданням є проектування чіткої ієрархічної структури організаційних одиниць (Organizational Units, OU). Замість використання стандартних вбудованих контейнерів Windows (таких як CN=Users або CN=Computers), розроблена модель передбачає створення повністю ізольованої кастомної структури. Це дозволяє безпечно делегувати права адміністрування та точково застосовувати об'єкти групових політик (GPO) виключно до корпоративних ресурсів.

Розроблена логічна ієрархія каталогів Active Directory на рисунку 2.5

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

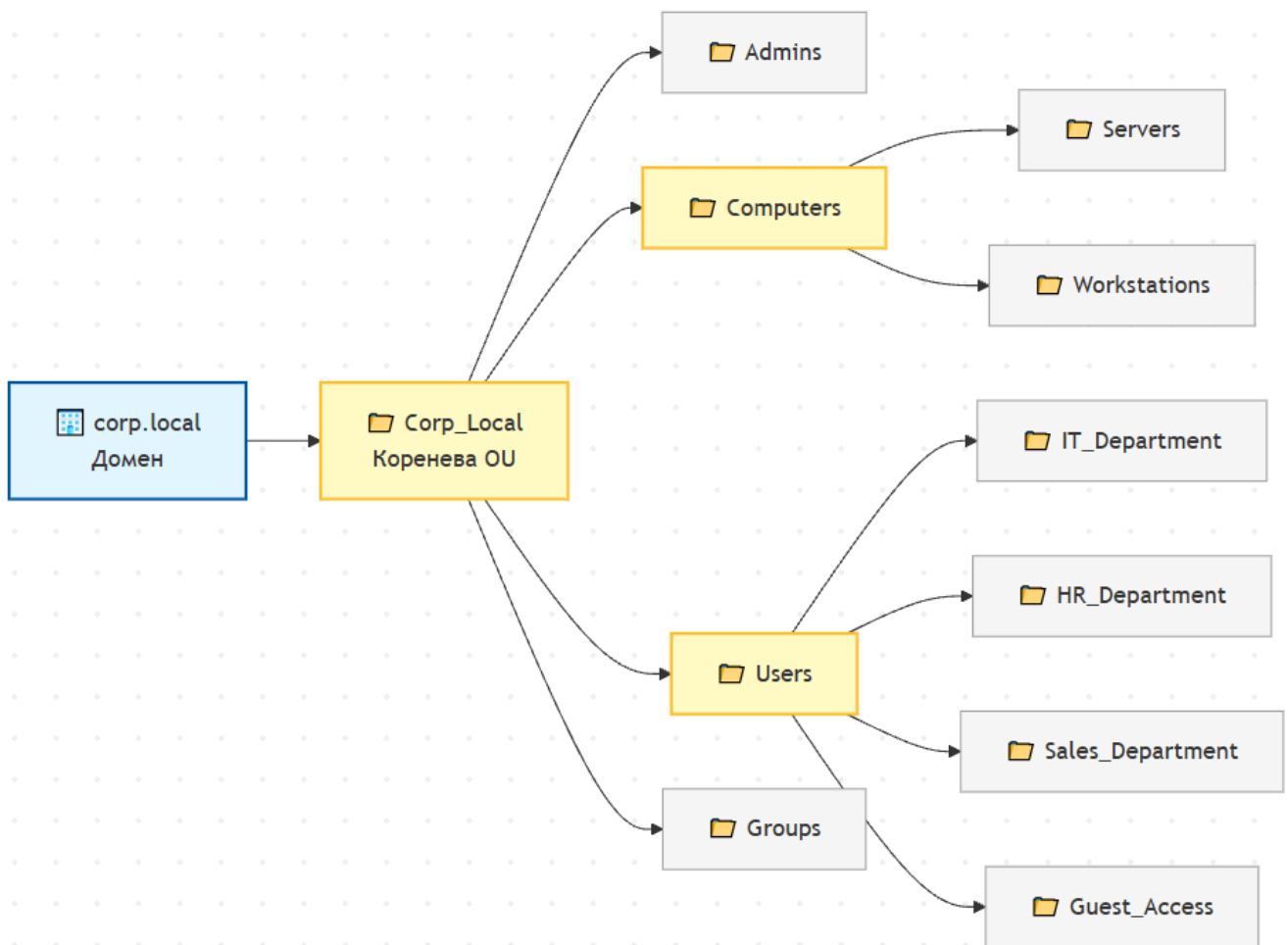


Рисунок 2.5 – Логічна ієрархія Active Directory

Після формування логічного каркаса інфраструктури проектується модель розмежування прав. В архітектурі Active Directory призначення прав безпосередньо окремим користувачам вважається грубим порушенням безпеки. Згідно з концепцією RBAC, усі дозволи призначаються виключно через глобальні групи безпеки (Global Security Groups) [13], які відповідають структурним підрозділам або посадовим обов'язкам.

Для забезпечення життєдіяльності підприємства та інтеграції з мережевим обладнанням було спроектовано наступні ключові групи безпеки (Таблиця 2.7).

Таблиця 2.7

Модель глобальних груп безпеки підприємства

Назва групи (Security Group)	Область дії	Призначення та логіка членства
SG_HR_Staff	Global	Група для співробітників кадрової служби (HR_Department). Надає доступ до конфіденційної інформації персоналу.

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

SG_IT_Staff	Global	Група для системних адміністраторів та інженерів мережі. Надає розширені права на управління інфраструктурою.
SG_VPN_Access	Global	Інфраструктурна група для інтеграції з Cisco ASA. Учасники цієї групи мають легітимне право ініціювати віддалене підключення AnyConnect VPN.

Особливої інженерної уваги під час проєктування RBAC заслуговує логіка налаштування вкладеності груп (Group Nesting) [13]. Замість ручного додавання кожного системного адміністратора до групи VPN, до складу інфраструктурної групи SG_VPN_Access вкладається ціла група SG_IT_Staff. Така архітектура дозволяє реалізувати ієрархічне успадкування прав: усі поточні та майбутні співробітники IT-відділу за замовчуванням отримують право на зовнішнє підключення. Це значно спрощує адміністрування та усуває ризик людської помилки [16].

Наступним кроком проєктування є розробка матриці доступу до корпоративних файлових ресурсів на прикладі спільної директорії кадрової служби (HR_Share), яка розгортається з використанням протоколу SMB [17].

Стандартні налаштування операційної системи Windows автоматично додають вбудовану групу «Everyone» (Bci) або «Authenticated Users» (Авторизовані користувачі) до списків контролю доступу (ACL) нових файлових ресурсів. З точки зору кібербезпеки це є неприпустимим, оскільки створює ризик несанкціонованого доступу до конфіденційних даних у разі компрометації будь-якого рядового облікового запису.

Для забезпечення конфіденційності даних розроблена жорстка матриця доступу, логіка якої наведена у таблиці 2.6.

Таблиця 2.8

Матриця доступу (NTFS Permissions) для захищеної директорії HR_Share

Суб'єкт доступу (Користувач або Група)	Рівень прав доступу (NTFS)	Обґрунтування застосованої політики
Everyone / Authenticated Users	<i>Видалено повністю</i>	Запобігання доступу неавторизованого персоналу.
Domain Admins	Full Control (Повний контроль)	Необхідно для системного резервного

		копіювання та управління.
SG_HR_Staff	Modify (Зміна), Read & Execute (Читання)	Виключне право кадрової служби на створення, редагування та читання робочих документів у своїй директорії.
Інші групи (SG_IT_Staff, SG_Sales)	Доступ заборонено (Access Denied)	Неявна заборона за відсутності прямого дозволу у списку ACL.

Таким чином, спроектована логічна структура Active Directory та розроблена матриця доступу RBAC формують надійний системний фундамент корпоративної мережі. Жорстка прив'язка дозволів виключно до спеціалізованих глобальних груп безпеки гарантує дотримання принципу найменших привілеїв (Principle of Least Privilege) та готує інфраструктуру до безпечної інтеграції зі шлюзом віддаленого доступу VPN.

2.5 Проектування підсистеми AnyConnect SSL VPN

Після розробки логіки внутрішньої маршрутизації та політик доступу Active Directory, наступним етапом проектування є архітектурне планування зовнішнього периметра безпеки. Головним завданням є забезпечення безпечного віддаленого доступу співробітників до корпоративних ресурсів підприємства за допомогою технології Cisco AnyConnect SSL/DTLS VPN.

Оскільки первинне встановлення сесії AnyConnect відбувається через контрольний канал HTTPS, інфраструктура потребує надійного механізму криптографічної ідентифікації. Для цього проектом передбачено створення локального центру сертифікації (Trustpoint) безпосередньо на міжмережевому екрані Cisco ASA. Цей центр генеруватиме пару ключів RSA (2048 біт) та випускатиме сертифікат для зовнішнього інтерфейсу outside1. Це гарантує клієнтському додатку, що підключення здійснюється до легітимного корпоративного шлюзу, а не до підробленого вузла злоумисників.

Наступним концептуальним кроком є проектування мережевих параметрів для майбутніх тунелів. Відповідно до загальної моделі IP-адресації підприємства,

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Россінський Ю.М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

для віддалених підключень виділяється спеціалізований логічний пул адрес (VPN_POOL) у діапазоні 192.168.250.0/24.

Для оптимізації маршрутизації та економії пропускну здатності корпоративного інтернет-каналу проєктом передбачено обов'язкове використання технології Split Tunneling (Роздільне тунелювання). Замість того, щоб направляти весь мережевий трафік віддаленого комп'ютера (включаючи перегляд новин чи потокове відео) на корпоративний шлюз, Split Tunneling дозволяє створити цільовий список контролю доступу (ACL). Згідно з цим списком, через зашифрований тунель маршрутизується виключно той трафік, який прямує до внутрішніх мереж підприємства: серверного сегмента (VLAN 10 — 192.168.10.0/24) та робочого сегмента (VLAN 20 — 192.168.20.0/24). Увесь інший повсякденний інтернет-трафік віддаленого користувача відправляється через його домашнього провайдера у відкритому вигляді.

Найбільш критичним інженерним аспектом проєктування VPN-шлюзу є логіка трансляції мережевих адрес. За замовчуванням корпоративний міжмережевий екран налаштовується на виконання динамічної трансляції портів та адрес (PAT) для всього вихідного трафіку: внутрішні IP-адреси (192.168.x.x) приховуються за єдиною публічною адресою зовнішнього інтерфейсу.

Однак застосування класичного PAT до VPN-трафіку є архітектурною помилкою. Щоб сервери (VLAN 10) та віддалені клієнти (192.168.250.0/24) могли встановлювати двосторонні з'єднання (наприклад, сервер AD міг оновлювати групові політики на віддаленому ПК), вони повинні "бачити" справжні IP-адреси один одного. Для вирішення цієї колізії в проєкті застосовується правило обходу трансляції — NAT Exemption (також відоме як Identity NAT). Ця політика інструктує мікроядро Cisco ASA не піддавати трансляції трафік, у якому джерелом є підмережа 192.168.10.0/24, а призначенням — підмережа 192.168.250.0/24 (і навпаки). Це дозволяє пакетам безперешкодно маршрутизуватися між фізичною та віртуальною мережами зі збереженням оригінальних заголовків L3. Логіка маршрутизації корпоративного та особистого трафіку клієнта, а також застосування правила NAT Exemption наведено на рисунку 2.5

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

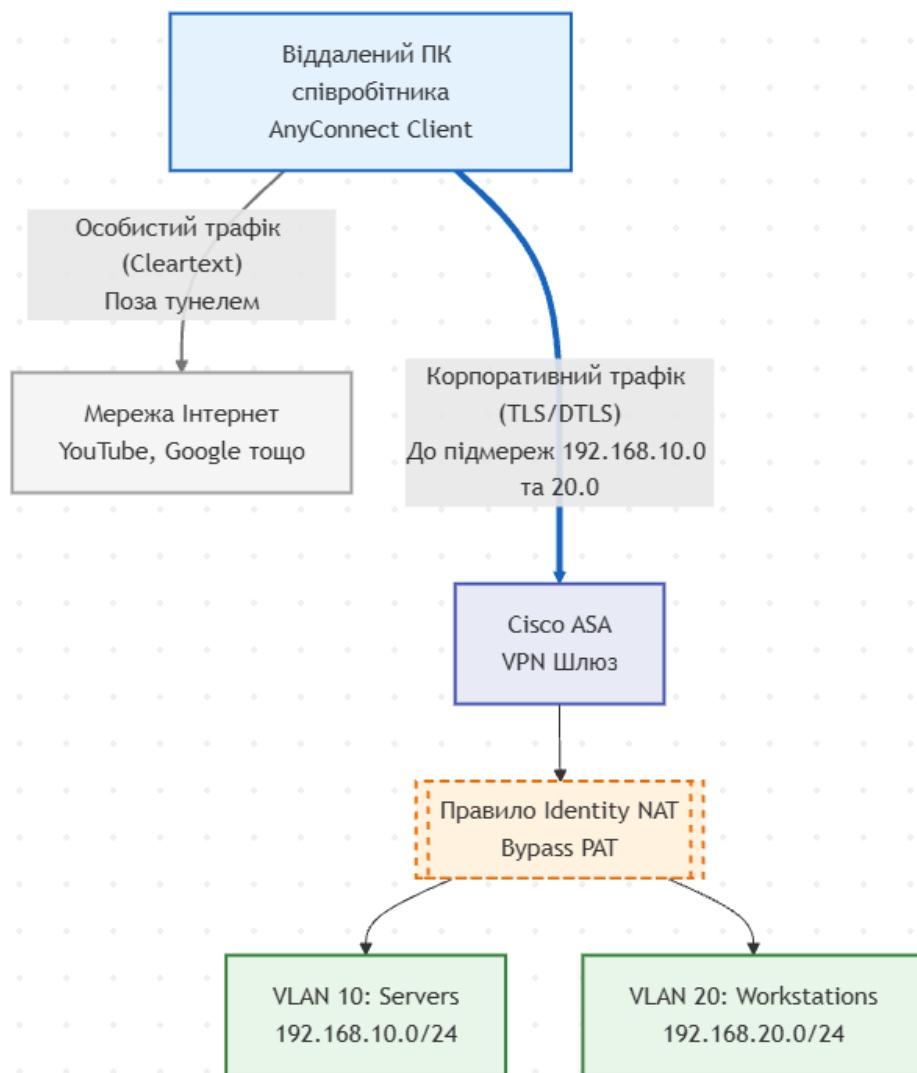


Рисунок 2.6 – Схема роздільного тунелювання та NAT Exemption

Завершальним, але концептуально найважливішим етапом проєктування підсистеми VPN є вибір механізму автентифікації. Оскільки підприємство використовує єдиний простір управління доступом на базі ролей (RBAC) у домені corp.local, створення локальних облікових записів безпосередньо на міжмережевому екрані є недоцільним і знижує загальний рівень безпеки.

Замість цього розроблена архітектура передбачає делегування процесу авторизації до контролера домену (192.168.10.10). Cisco ASA виступатиме як клієнт AAA (Authentication, Authorization, and Accounting) і використовуватиме протокол LDAP для передачі облікових даних зовнішніх користувачів на перевірку до Active Directory.

Для забезпечення максимальної безпеки простого введення правильного логіна та пароля буде недостатньо. За допомогою перевірки LDAP-атрибутів (зокрема атрибута memberOf), шлюз дозволить ініціалізацію тунелю виключно тим співробітникам, які явно включені до глобальної доменної групи безпеки SG_VPN_Access. Таким чином, адміністратор IT-відділу (через успадкування групи SG_IT_Staff) або спеціально авторизований віддалений працівник успішно підключаться до мережі, тоді як рядовий співробітник відділу продажів отримає відмову в доступі ще на етапі перевірки сертифіката, повністю відповідаючи вимогам концепції Zero Trust. Послідовність процесу безпечної авторизації віддаленого користувача за допомогою протоколу LDAP схематично зображена на рисунку 2.7

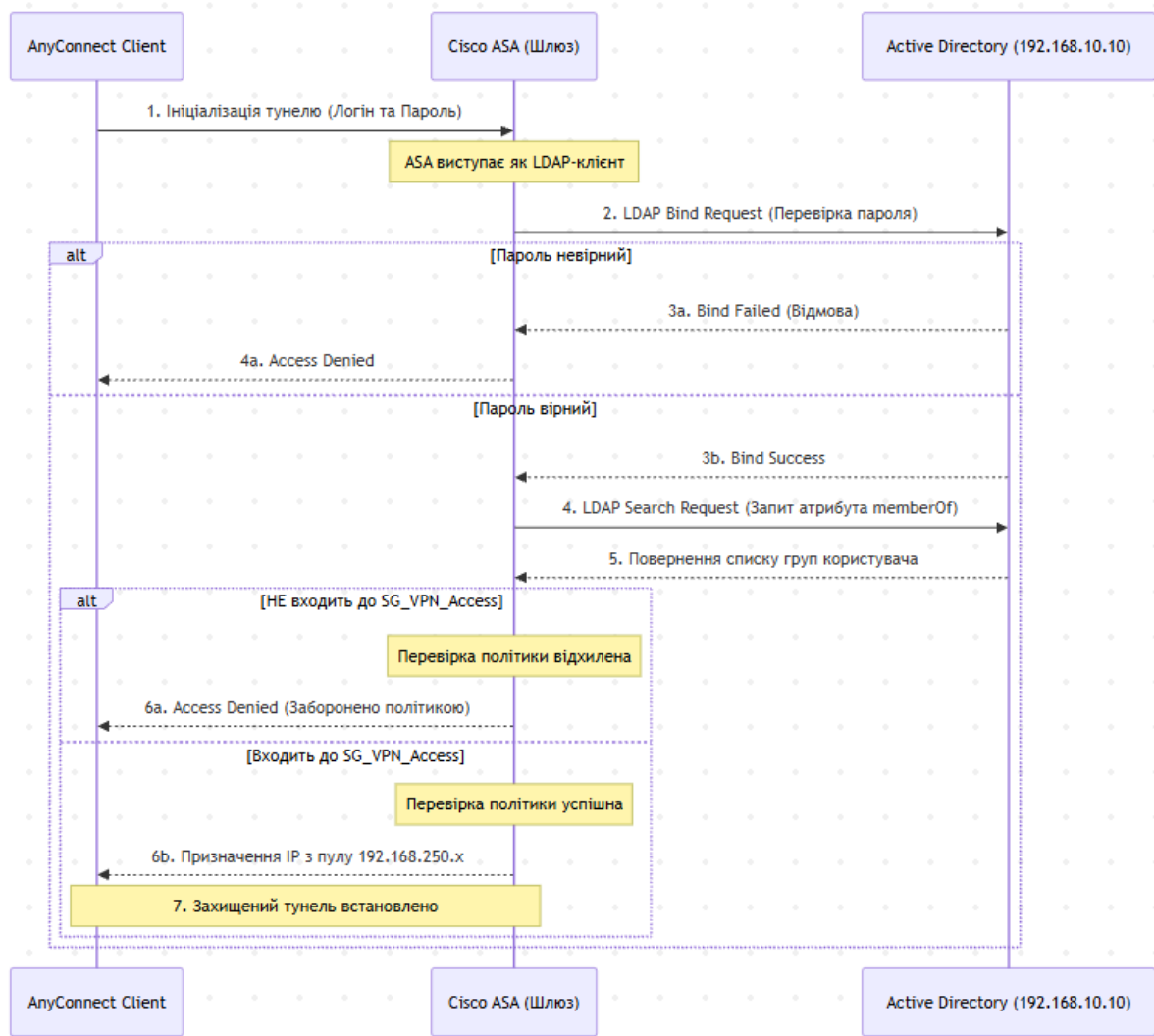


Рисунок 2.7 – Алгоритм LDAP-авторизації

Висновок до другого розділу

У другому розділі було визначено вимоги до апаратного та програмного забезпечення середовища емуляції на базі GNS3 [23, 24], що дозволило підготувати платформу для безпечної практичної реалізації проєкту. Сформована на початковому етапі модель загроз інформаційній безпеці дозволила ідентифікувати потенційні вектори атак (від несанкціонованого доступу до компрометації VPN-з'єднань [3]) та обґрунтувати архітектурні рішення для їх ефективної нейтралізації згідно з принципами Zero Trust [1].

На етапі проєктування мережевої інфраструктури було розроблено комплексну логічну топологію, що базується на архітектурі зі згорнутим ядром (Firewall-centric). Розробка системи IP-адресації з використанням приватного адресного простору [5] дозволила чітко структурувати мережу та виділити незалежні сегменти для серверного обладнання (VLAN 10), робочих станцій (VLAN 20) і гостей пристроїв (VLAN 30) на базі стандарту IEEE 802.1Q [4], а також зарезервувати окремий пул адрес для підсистеми AnyConnect VPN (192.168.250.0/24) [20].

Проєктування міжмережевої взаємодії довело ефективність інтеграції L3-маршрутизації (Router-on-a-Stick) безпосередньо на граничному шлюзі Cisco ASA [19]. Застосування суворих списків контролю доступу (ACL) дозволило на практиці реалізувати модель нульової довіри [1], за якої критичні корпоративні ресурси надійно ізольовані від недовіrenих сегментів. Проблему динамічної адресації в ізольованій гостьовій мережі було успішно вирішено механізмом DHCP Relay [22]. Завершальним етапом проєктування стало впровадження технології моніторингу IP SLA у поєднанні з Object Tracking [6, 21]. Це рішення забезпечило автоматичне резервування зовнішніх каналів провайдерів (Dual-WAN Failover) без необхідності використання складних протоколів динамічної маршрутизації. Розроблена комплексна модель є повністю готовою до конфігурації у середовищі емуляції.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Конфігурація мережевої інфраструктури на міжмережевому екрані Cisco ASA

Для реалізації спроектованої топології (п. 2.2) на міжмережевому екрані Cisco ASA було налаштовано логічні субінтерфейси, які виконують роль шлюзів за замовчуванням для відповідних віртуальних локальних мереж (VLAN). Базове налаштування здійснювалося через інтерфейс командного рядка (CLI) в привілейованому режимі конфігурації.

Відповідно до розробленої політики Zero Trust, усім внутрішнім інтерфейсам було примусово призначено однаковий максимальний рівень безпеки (security-level 100). Процес створення субінтерфейсів на базі фізичного порту GigabitEthernet0/2 та застосування глобальної політики дозволу маршрутизації між інтерфейсами з однаковим рівнем довіри наведено у лістингу 3.1.

Лістинг 3.1 – Налаштування логічних субінтерфейсів та політик безпеки VLAN

```
ciscoasa(config)# same-security-traffic permit inter-interface

ciscoasa(config)# interface GigabitEthernet0/2.10
ciscoasa(config-subif)# vlan 10
ciscoasa(config-subif)# nameif inside10
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip address 192.168.10.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2.20
ciscoasa(config-subif)# vlan 20
ciscoasa(config-subif)# nameif inside20
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip address 192.168.20.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2.30
ciscoasa(config-subif)# vlan 30
ciscoasa(config-subif)# nameif inside30
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip address 192.168.30.1 255.255.255.0
```

Після базової ініціалізації інтерфейсів було розв'язано проблему динамічної видачі IP-адрес для ізольованого гостьового сегмента. Оскільки прямий доступ до сервера Active Directory заборонений, на Cisco ASA було активовано та налашто-

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Россінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

вано службу DHCP Relay. Наступні команди вказують міжмережевому екрану перехоплювати запити на інтерфейсі inside30 та перенаправляти їх на IP-адресу корпоративного сервера 192.168.10.10 через інтерфейс inside10:

```
ciscoasa(config)# dhcprelay server 192.168.10.10 inside10
ciscoasa(config)# dhcprelay enable inside30
```

Оскільки маршрутизація між інтерфейсами з однаковим рівнем безпеки тепер дозволена глобально, наступним критичним кроком стало застосування розширених списків контролю доступу (Extended ACL) для жорсткої фільтрації трафіку. Для гостьового сегмента (VLAN 30) було створено список VLAN30_IN, який суворо забороняє доступ до серверної (192.168.10.0/24) та робочої (192.168.20.0/24) підмереж, але дозволяє вихід у мережу Інтернет. Для робочих станцій (VLAN 20) список VLAN20_IN дозволяє доступ до серверів, забороняє зв'язок з гостями і дозволяє інтернет-трафік. Налаштування цих списків та їх прив'язка до інтерфейсів виглядає наступним чином:

```
ciscoasa(config)# access-list VLAN30_IN extended deny ip any 192.168.10.0
255.255.255.0
ciscoasa(config)# access-list VLAN30_IN extended deny ip any 192.168.20.0
255.255.255.0
ciscoasa(config)# access-list VLAN30_IN extended permit ip any any

ciscoasa(config)# access-list VLAN20_IN extended permit ip any 192.168.10.0
255.255.255.0
ciscoasa(config)# access-list VLAN20_IN extended deny ip any 192.168.30.0
255.255.255.0
ciscoasa(config)# access-list VLAN20_IN extended permit ip any any

ciscoasa(config)# access-group VLAN30_IN in interface inside30
ciscoasa(config)# access-group VLAN20_IN in interface inside20
```

Завершальним етапом базового налаштування мережевої інфраструктури стала реалізація відмовостійкості зовнішніх каналів зв'язку (Dual-WAN), спроектованої у підрозділі 2.3. Для автоматичного перемикавання трафіку у разі падіння основного провайдера було впроваджено процес IP SLA.

Процес налаштовано на відправку ICMP-запитів (Echo) кожні 5 секунд до шлюзу основного провайдера (100.70.1.1) через інтерфейс outside1. Стан цього моніторингу прив'язано до об'єкта відстеження (Track 1). Основному статичному маршруту (через outside1) призначено метрику 1 із жорсткою прив'язкою до Track 1. Резервному маршруту (через outside2) призначено метрику 10, що робить його

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

"плаваючим" (Floating Route) — він активується лише тоді, коли об'єкт Track 1 переходить у стан "Down". Конфігурацію процесу моніторингу та маршрутизації наведено у лістингу 3.2.

Лістинг 3.2 – Налаштування системи відмовостійкості на базі IP SLA та Object Tracking

```
ciscoasa(config)# sla monitor 1
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 100.70.1.1
interface outside1
ciscoasa(config-sla-monitor-echo)# frequency 5
ciscoasa(config-sla-monitor-echo)# exit
ciscoasa(config)# sla monitor schedule 1 life forever start-time now

ciscoasa(config)# track 1 rtr 1 reachability

ciscoasa(config)# route outside1 0.0.0.0 0.0.0.0 100.70.1.1 1 track 1
ciscoasa(config)# route outside2 0.0.0.0 0.0.0.0 100.70.1.5 10
```

Впроваджені конфігурації повністю реалізують спроектовану архітектуру маршрутизації, забезпечуючи ізоляцію внутрішніх сегментів, керовану трансляцію широкомовних DHCP-запитів та високонадійний, автоматизований зовнішній периметр безпеки.

3.2 Розгортання та конфігурація Active Directory

Для практичної реалізації централізованої системи управління інфраструктурою було розгорнуто віртуальну машину під управлінням серверної операційної системи Windows Server. У серверному сегменті (VLAN 10) мережевому інтерфейсу сервера було призначено статичну IP-адресу 192.168.10.10, яка одночасно виступає як адреса корпоративного DNS-сервера. Після базового налаштування операційної системи було інстальовано рольові служби Active Directory Domain Services (AD DS) та виконано підвищення сервера до рівня кореневого контролера домену (Root Domain Controller) з ім'ям лісу corp.local.

Відповідно до розробленої логічної структури та вимог політики RBAC, процес формування ієрархії організаційних одиниць (OU) було повністю автоматизовано за допомогою об'єктно-орієнтованої командної оболонки PowerShell. Це гарантує точність застосування політик та унеможливорює помилки ручного введення

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

через графічний інтерфейс. У лістингу 3.3 наведено фрагмент розробленого сценарію, який формує базові контейнери для комп'ютерів, користувачів та відділів.

Лістинг 3.3 – Сценарій ініціалізації ієрархії організаційних одиниць (OU)

```
# Створення кореневої організаційної одиниці підприємства
New-ADOrganizationalUnit -Name "Corp_Local" -Path "DC=corp,DC=local"

# Створення базових контейнерів першого рівня
New-ADOrganizationalUnit -Name "Admins" -Path "OU=Corp_Local,DC=corp,DC=local"
New-ADOrganizationalUnit -Name "Users" -Path "OU=Corp_Local,DC=corp,DC=local"
New-ADOrganizationalUnit -Name "Computers" -Path "OU=Corp_Local,DC=corp,DC=local"
New-ADOrganizationalUnit -Name "Groups" -Path "OU=Corp_Local,DC=corp,DC=local"

# Деталізація ієрархії обчислювальної техніки
New-ADOrganizationalUnit -Name "Servers" -Path "OU=Computers,OU=Corp_Local,DC=corp,DC=local"
New-ADOrganizationalUnit -Name "Workstations" -Path "OU=Computers,OU=Corp_Local,DC=corp,DC=local"

# Деталізація підрозділів усередині контейнера Users
New-ADOrganizationalUnit -Name "IT_Department" -Path "OU=Users,OU=Corp_Local,DC=corp,DC=local"
New-ADOrganizationalUnit -Name "HR_Department" -Path "OU=Users,OU=Corp_Local,DC=corp,DC=local"
New-ADOrganizationalUnit -Name "Sales_Department" -Path "OU=Users,OU=Corp_Local,DC=corp,DC=local"
New-ADOrganizationalUnit -Name "Guest_Access" -Path "OU=Users,OU=Corp_Local,DC=corp,DC=local"
```

Результат автоматизованого розгортання логічної структури організаційних одиниць в інструменті керування доменом представлено на рисунку 3.1.

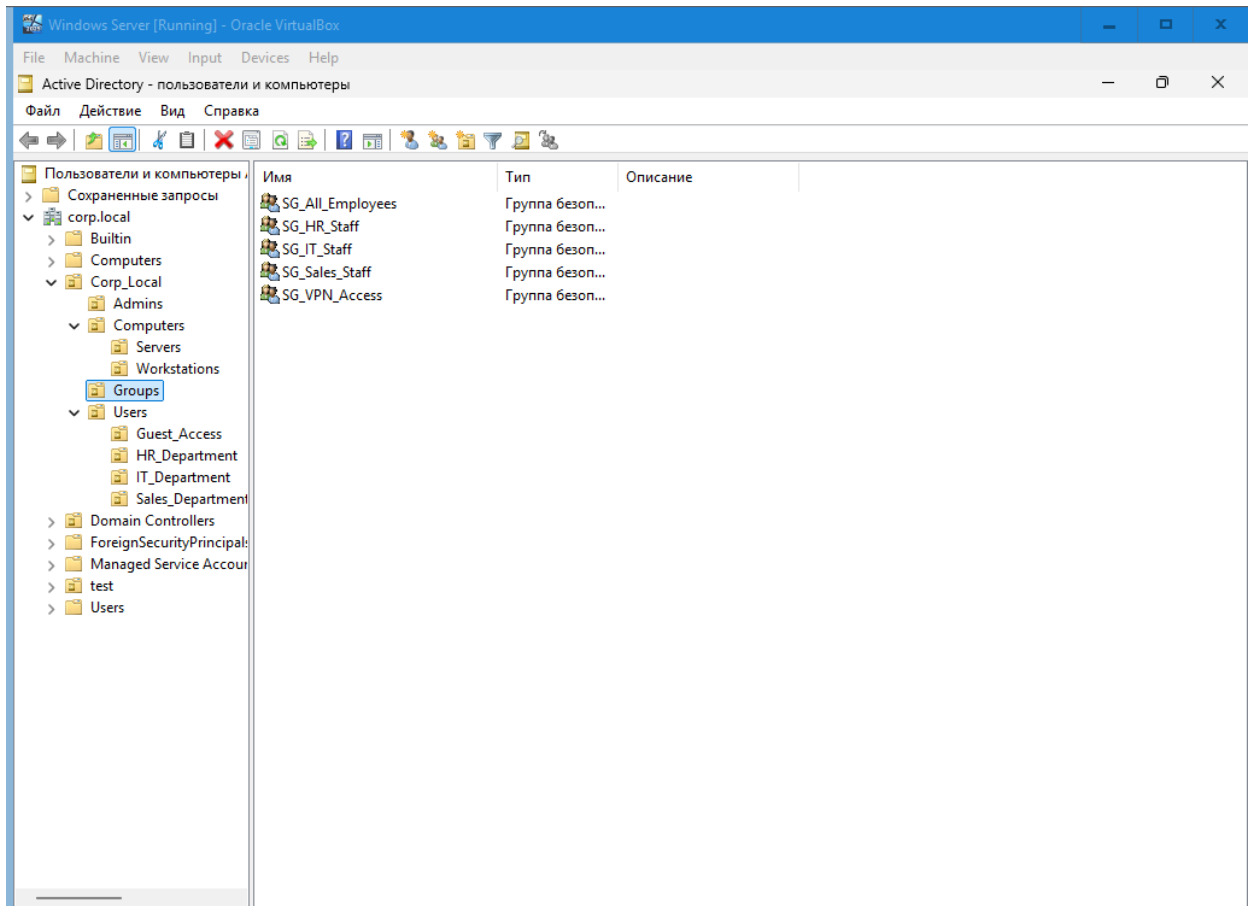


Рисунок 3.1 – Відображення згенерованої структури організаційних одиниць в оснащенні Active Directory Users and Computers

Після побудови логічного каркаса інфраструктури було згенеровано глобальні групи безпеки (Security Groups) для реалізації моделі управління доступом. Окрім груп для стандартних відділів, було згенеровано критично важливу інфраструктурну групу SG_VPN_Access, яка використовуватиметься граничним міжмережним екраном для авторизації підключень.

Далі базу даних Active Directory було наповнено обліковими записами тестових користувачів. Для гарантування безпеки конфіденційних даних під час виконання сценаріїв, відкриті паролі конвертувалися у захищені криптографічні рядки за допомогою командлету ConvertTo-SecureString. Процес створення груп, генерації користувачів та налаштування їхньої вкладеності (Group Nesting) наведено у лістингу 3.4.

Лістинг 3.4 – Генерація облікових записів та формування складу груп безпеки

```
# Створення глобальних груп безпеки
New-ADGroup -Name "SG_HR_Staff" -GroupScope Global -Path "OU=Groups,OU=Corp_Local,DC=corp,DC=local"
```

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

```

New-ADGroup -Name "SG_IT_Staff" -GroupScope Global -Path
"OU=Groups,OU=Corp_Local,DC=corp,DC=local"
New-ADGroup -Name "SG_VPN_Access" -GroupScope Global -Path
"OU=Groups,OU=Corp_Local,DC=corp,DC=local"

# Створення користувачів у відповідних підрозділах
New-ADUser -Name "Olena Petrenko" -SamAccountName "o.petrenko" -Path
"OU=HR_Department,OU=Users,OU=Corp_Local,DC=corp,DC=local" -
AccountPassword (ConvertTo-SecureString "TopSecret2026!" -AsPlainText -
Force) -Enabled $true
New-ADUser -Name "VPN Remote User" -SamAccountName "vpnuser" -Path
"OU=Guest_Access,OU=Users,OU=Corp_Local,DC=corp,DC=local" -
AccountPassword (ConvertTo-SecureString "TopSecret2026!" -AsPlainText -
Force) -Enabled $true

# Додавання користувачів у профільні групи
Add-ADGroupMember -Identity "SG_HR_Staff" -Members "o.petrenko"

# Налаштування вкладеності (Nesting) для автоматизації доступу через VPN
Add-ADGroupMember -Identity "SG_VPN_Access" -Members "SG_IT_Staff",
"vpnuser"

```

Завершальним кроком конфігурації стала практична імплементація політик доступу до корпоративних ресурсів на рівні файлової системи. На файловому сервері було розгорнуто спільну мережеву директорію для кадрової служби під назвою HR_Share.

Відповідно до спроектованої матриці доступу, у властивостях безпеки цієї папки (NTFS Permissions) було примусово скасовано успадкування прав та повністю видалено вбудовану системну групу «Everyone» (Bci), яка за замовчуванням надає доступ усім автентифікованим суб'єктам домену. Замість неї до списку контролю доступу (ACL) папки було явно додано виключно глобальну доменну групу SG_HR_Staff із делегованими повноваженнями на зміну та читання даних (Modify, Read & Execute). Процес конфігурації та фінальної перевірки дозволів представлено відповідно на рисунках 3.2 та 3.3.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

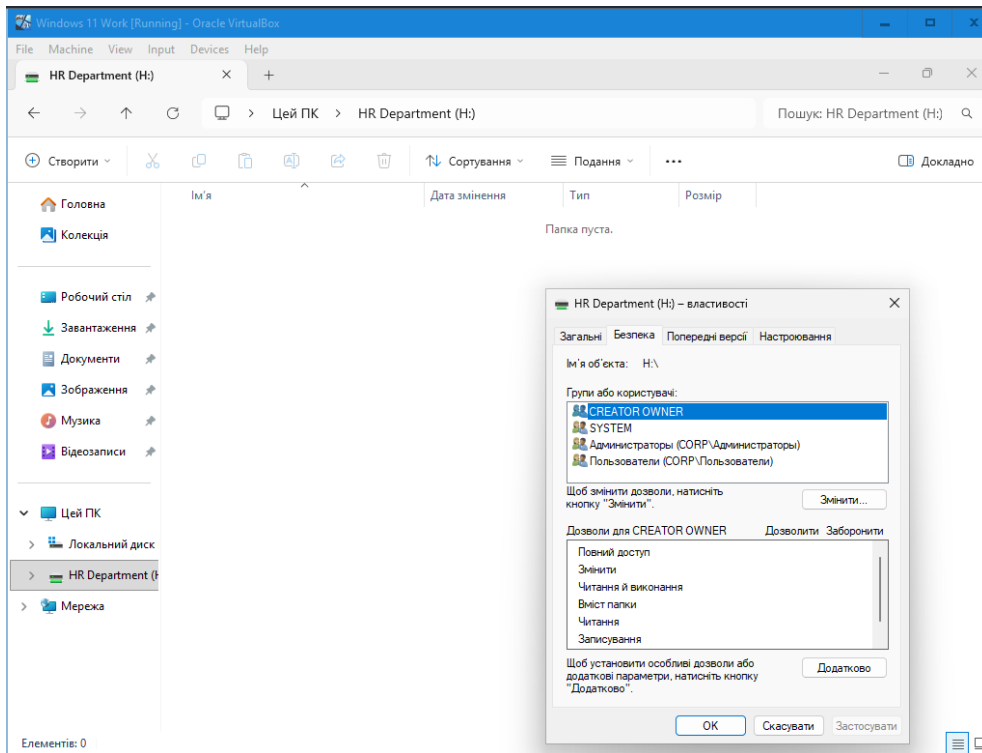


Рисунок 3.2 – Налаштування розмежування прав доступу NTFS на основі глобальної групи безпеки Active Directory

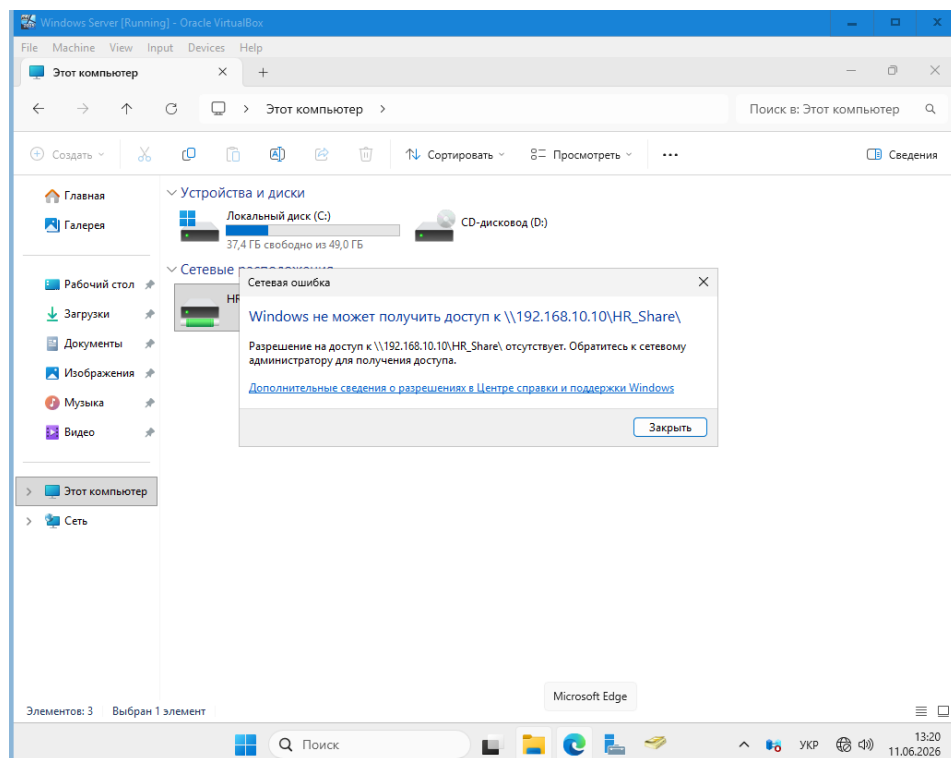


Рисунок 3.3 – Перевірка результуючих прав доступу NTFS для захищеної папки

У результаті, при спробі користувача з IT-відділу чи відділу продажу відкрити директорію HR, контролер домену перевіряє їхній квиток Kerberos (TGT/TGS), не знаходить там ідентифікатора групи (SID) SG_HR_Staff і миттєво

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росінський Ю.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

відхиляє запит із помилкою "Access Denied". Це підтверджує, що логічна ізоляція ресурсів на рівні домену налаштована коректно, і інфраструктура повністю готова до інтеграції з підсистемою віддаленого доступу VPN.

3.3 Конфігурація VPN-шлюзу та інтеграція з Active Directory

Після успішного розгортання служби каталогів Active Directory та налаштування внутрішньої маршрутизації наступним етапом практичної реалізації є конфігурація зовнішнього периметра безпеки. Головним завданням є налаштування міжмережевого екрана Cisco ASA для прийому вхідних підключень віддалених співробітників за допомогою технології AnyConnect SSL/DTLS VPN.

Оскільки первинне встановлення сесії AnyConnect відбувається через контрольний канал HTTPS, міжмережевий екран повинен мати можливість криптографічно підтвердити свою ідентичність клієнтському додатку. Для цього на базі Cisco ASA було згенеровано пару криптографічних ключів RSA із довжиною 2048 біт та створено локальний центр сертифікації (Trustpoint), який випускає самопідписаний сертифікат (Self-Signed Certificate) для зовнішнього інтерфейсу outside1. Процес ініціалізації криптографічного рушія та увімкнення служби WebVPN наведено у лістингу 3.5.

Лістинг 3.5 – Генерація сертифіката Trustpoint та активація WebVPN

```
ciscoasa(config)# crypto key generate rsa label ANYCONNECT_KEY modulus 2048
ciscoasa(config)# crypto ca trustpoint LOCAL_TRUST
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# keypair ANYCONNECT_KEY
ciscoasa(config)# crypto ca enroll LOCAL_TRUST noconfirm

ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable outside1
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-4.10.x.pkg
1
ciscoasa(config-webvpn)# anyconnect enable
```

Згенерований сертифікат та підтвердження його успішної прив'язки до зовнішнього інтерфейсу продемонстровано на рисунках 3.4 та 3.5.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

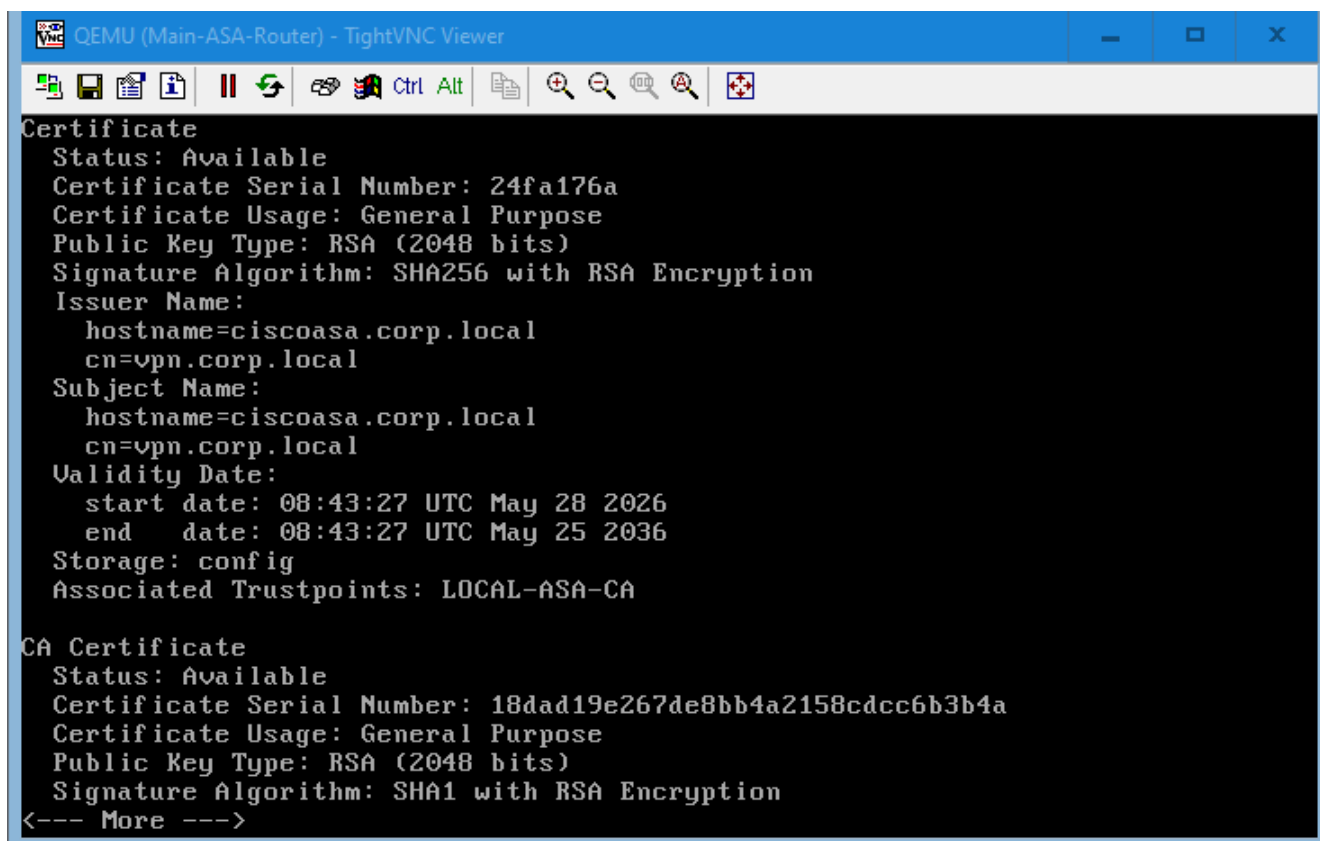


Рисунок 3.4 – Вікно генерації та налаштування параметрів SSL-сертифіката (Trustpoint)

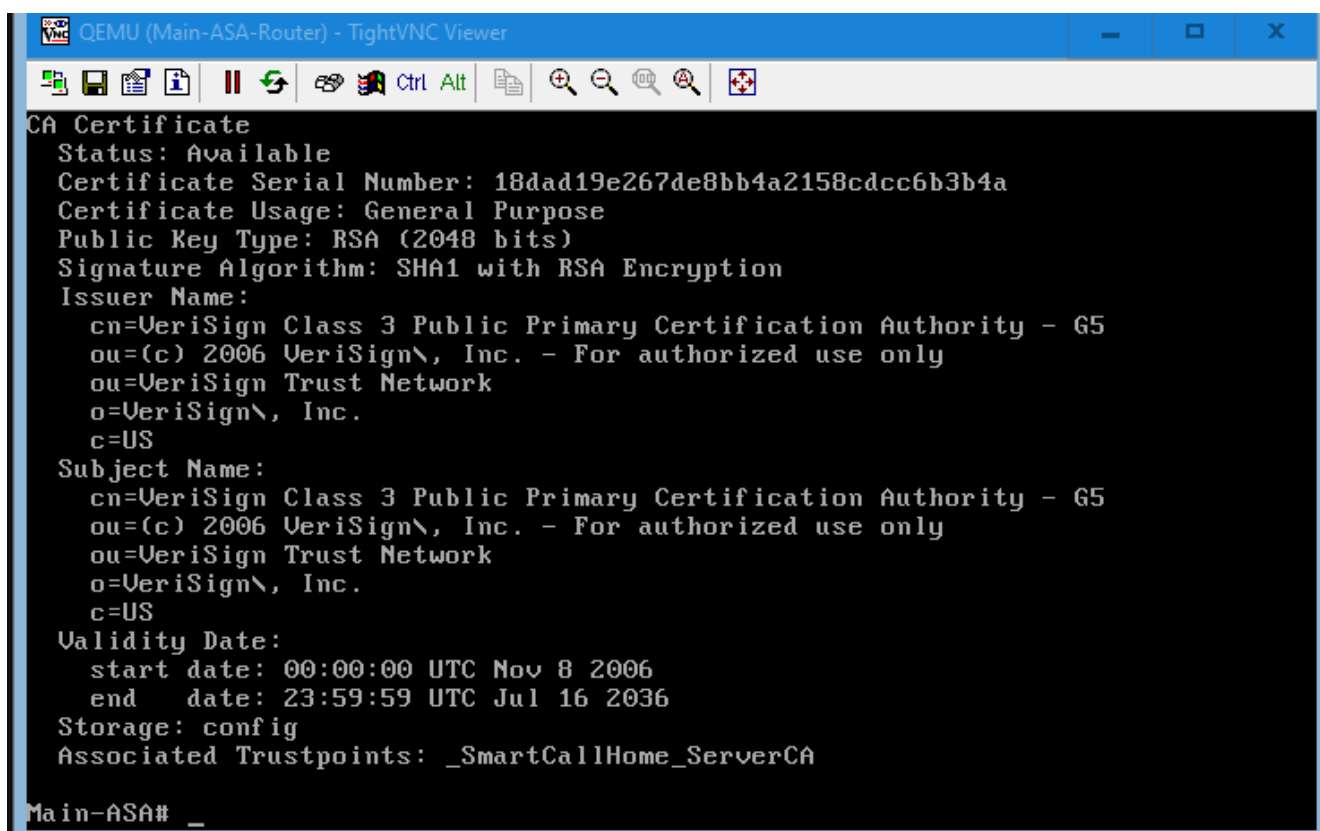


Рисунок 3.5 – Підтвердження успішної прив'язки сертифіката до зовнішнього інтерфейсу

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Після активації базового сервісу було налаштовано параметри мережевого рівня для клієнтів. Відповідно до розробленої архітектури, для VPN-з'єднань було виділено спеціалізований пул IP-адрес 192.168.250.0/24.

З метою економії пропускної здатності корпоративного інтернет-каналу було впроваджено технологію роздільного тунелювання (Split Tunneling). За допомогою стандартного списку доступу шлюз було сконфігуровано так, щоб маршрутизувати через зашифрований тунель лише той трафік, який прямує до серверного сегмента (VLAN 10) та сегмента робочих станцій (VLAN 20). Увесь інший повсякденний інтернет-трафік віддаленого користувача відправляється через його локального провайдера у відкритому вигляді. Ці налаштування відображені в лістингу 3.6.

Лістинг 3.6 – Налаштування IP-пулу та політики Split Tunneling

```
ciscoasa(config)# ip local pool VPN_POOL 192.168.250.10-192.168.250.254
mask 255.255.255.0
ciscoasa(config)# access-list SPLIT_TUNNEL standard permit 192.168.10.0
255.255.255.0
ciscoasa(config)# access-list SPLIT_TUNNEL standard permit 192.168.20.0
255.255.255.0
```

Найбільш критичним інженерним кроком налаштування шлюзу є конфігурація політик трансляції мережевих адрес (NAT). За замовчуванням Cisco ASA здійснює динамічну підміну адрес (PAT) для всього вихідного трафіку. Однак, щоб сервери з VLAN 10 могли відповідати VPN-клієнтам напрямку, необхідно виключити цей специфічний трафік із процесу трансляції. Для цього було впроваджено правило обходу трансляції NAT Exemption (Identity NAT). Це правило інструктує ядро маршрутизатора не змінювати IP-адреси при обміні даними між локальними підмережами та пулом AnyConnect.

Лістинг 3.7 – Налаштування виключення з трансляції адрес (Identity NAT)

```
ciscoasa(config)# object network OBJ_INSIDE10
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config)# object network OBJ_VPN_POOL
ciscoasa(config-network-object)# subnet 192.168.250.0 255.255.255.0
ciscoasa(config)# nat (inside10,outside1) source static OBJ_INSIDE10
OBJ_INSIDE10 destination static OBJ_VPN_POOL OBJ_VPN_POOL no-proxy-arp
route-lookup
```

Етапи верифікації налаштувань обходу трансляції в загальній таблиці маршрутизатора наведені на рисунках 3.6 – 3.9.

```

QEMU (Main-ASA-Router) - TightVNC Viewer
1 (inside10) to (outside1) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static VPN_POOL_SUBNET VPN_POOL_SUBNET no-proxy-arp route-lookup
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination - Origin: 192.168.250.0/24, Translated: 192.168.250.0/24
2 (inside20) to (outside1) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static VPN_POOL_SUBNET VPN_POOL_SUBNET no-proxy-arp route-lookup
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination - Origin: 192.168.250.0/24, Translated: 192.168.250.0/24
3 (inside30) to (outside1) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static VPN_POOL_SUBNET VPN_POOL_SUBNET no-proxy-arp route-lookup
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination - Origin: 192.168.250.0/24, Translated: 192.168.250.0/24
4 (inside10) to (inside20) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-lookup
  translate_hits = 457, untranslate_hits = 589
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination -

```

Рисунок 3.6 – Перевірка конфігурації політик NAT у загальній таблиці маршрутизатора. Частина 1.

```

ed: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination - Origin: 192.168.250.0/24, Translated: 192.168.250.0/24
4 (inside10) to (inside20) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-lookup
  translate_hits = 457, untranslate_hits = 589
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
5 (inside20) to (inside10) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-lookup
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
6 (inside10) to (inside30) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-lookup
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
<--- More --->_

```

Рисунок 3.7 – Перевірка конфігурації політик NAT у загальній таблиці маршрутизатора. Частина 2.

```

translated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
7 (inside30) to (inside10) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-
  lookup
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translat
ed: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
    Destination - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Tra
nslated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
8 (inside30) to (inside20) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-
  lookup
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translat
ed: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
    Destination - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Tra
nslated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
9 (inside20) to (inside30) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-
  lookup
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translat
ed: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
    Destination - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Tra
nslat

```

Рисунок 3.8 – Перевірка конфігурації політик NAT у загальній таблиці маршрутизатора. Частина 3.

```

lookup
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translat
ed: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
  Destination - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Tra
nslated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
9 (inside20) to (inside30) source static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS
  destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-proxy-arp route-
  lookup
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translat
ed: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24
    Destination - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Tra
nslated: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24

Manual NAT Policies (Section 3)
1 (any) to (outside1) source dynamic LOCAL_INTERNAL_NETS interface
  translate_hits = 35, untranslate_hits = 36
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translat
ed: 100.70.1.2/30
2 (any) to (outside2) source dynamic LOCAL_INTERNAL_NETS interface
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, Translat
ed: 100.70.1.6/30
Main-ASA#

```

Рисунок 3.9 – Перевірка конфігурації політик NAT у загальній таблиці маршрутизатора. Частина 4.

Завершальним, але концептуально найважливішим етапом стала інтеграція Cisco ASA з контролером домену Active Directory (192.168.10.10) для забезпечення єдиного простору автентифікації на базі ролей (RBAC). Створення локальних користувачів на міжмережевому екрані було відхилено з міркувань безпеки. Натомість на Cisco ASA було налаштовано AAA-сервер, який використовує протокол LDAP для передачі облікових даних зовнішніх клієнтів на перевірку безпосередньо до бази AD.

Для забезпечення максимального захисту за допомогою параметрів LDAP атрибутів (зокрема атрибута `memberOf`), міжмережевий екран був сконфігурований таким чином, щоб успішну авторизацію проходили виключно ті користувачі, які явно належать до глобальної групи безпеки `SG_VPN_Access` у домені `corp.local`. Це означає, що віддалений співробітник з логіном `vpuser` або системний адміністратор (через успадковану групу `SG_IT_Staff`) успішно встановлять тунель, тоді як співробітник відділу продажів чи гостьовий користувач отримають відмову в доступі ще на етапі перевірки облікових даних, навіть якщо їхній введений пароль є абсолютно правильним.

Усі ці налаштування (пул адрес, списки роздільного тунелювання та LDAP-автентифікація) було об'єднано у єдину групову політику (Group Policy) та профіль підключення (Tunnel Group). Вони примусово застосовуються до кожного вхідного клієнта AnyConnect, повністю ізолюючи його сесію та інтегруючи її в загальну корпоративну архітектуру нульової довіри.

3.4 Комплексне тестування працездатності та безпеки мережі

Завершальним етапом практичної реалізації проєкту є комплексне емпіричне тестування розгорнутої інформаційної інфраструктури. Основною метою випробувань є практичне підтвердження коректності роботи механізмів логічної мікросегментації та ізоляції (VLAN та ACL) [4, 19], системи автоматичного резервування зовнішніх каналів зв'язку (IP SLA та Object Tracking) [6, 21], а також підсистеми захищеного віддаленого доступу (Cisco AnyConnect SSL/DTLS VPN) [20] з її нативною інтеграцією в службу каталогів Active Directory [12].

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Перший етап верифікації був спрямований на перевірку правил внутрішньої маршрутизації між сегментами та працездатності підсистеми DHCP Relay [22]. На робочій станції, розміщеній у недовіреному гостьовому сегменті (VLAN 30), було ініційовано запит на динамічне отримання мережевих налаштувань. Завдяки налаштованому ретранслятору на базі міжмережевого екрана Cisco ASA, гостьовий комп'ютер успішно отримав IP-адресу з пулу 192.168.30.0/24 від сервера 192.168.10.10, який фізично розташований в ізольованому серверному сегменті.

Після успішного отримання мережевих реквізитів було проведено верифікацію дієвості політик списків контролю доступу (ACL). Спроба надсилення тестових ICMP-запитів (утиліта ping) від гостьової станції (VLAN 30) до контролера домену (192.168.10.10) або до робочих станцій штатного персоналу (VLAN 20) завершилася помилкою «Request Timed Out» (Перевищено таймаут запиту). Водночас системний журнал (Syslog) міжмережевого екрана Cisco ASA зафіксував події примусового відкидання пакетів (Drop) згідно з налаштованим правилом ACL_INSIDE_30, що повністю підтверджує надійну ізоляцію гостьового трафіку. Натомість аналогічний ICMP-запит із робочої станції корпоративного сегмента (VLAN 20) до сервера завершився успішно, оскільки цей напрямок руху даних дозволено політиками безпеки компанії. Результати тестування фільтрації трафіку представлено на рисунках 3.10 та 3.11.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

```

Windows 11 Work [Running] - Oracle VirtualBox
File Machine View Input Devices Help
C:\Users\o.petrenko>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=8ms TTL=128
Reply from 192.168.10.10: bytes=32 time=10ms TTL=128
Reply from 192.168.10.10: bytes=32 time=8ms TTL=128
Reply from 192.168.10.10: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 10ms, Average = 7ms

C:\Users\o.petrenko>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : corp.local
    Link-local IPv6 Address . . . . . : fe80::68a:14b3:6b93:1def%10
    IPv4 Address. . . . . : 192.168.20.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.1

C:\Users\o.petrenko>

```

Рисунок 3.10 – Перевірка роботи списків контролю доступу (ACL) між сегмен-
тами мережі. Частина 1.

```

PC1> show ip

NAME           : PC1[1]
IP/MASK        : 0.0.0.0/0
GATEWAY        : 0.0.0.0
DNS            :
MAC           : 00:50:79:66:68:00
LPORT         : 10010
RHOST:PORT     : 127.0.0.1:10011
MTU           : 1500

PC1> ip dhcp
DORA IP 192.168.30.10/24 GW 192.168.30.1

PC1> show ip

NAME           : PC1[1]
IP/MASK        : 192.168.30.10/24
GATEWAY        : 192.168.30.1
DNS            : 192.168.10.10
DHCP SERVER    : 192.168.10.10
DHCP LEASE     : 691198, 691200/345600/604800
DOMAIN NAME    : corp.local
MAC           : 00:50:79:66:68:00
LPORT         : 10010
RHOST:PORT     : 127.0.0.1:10011
MTU           : 1500

PC1> ping 192.168.10.10
192.168.10.10 icmp_seq=1 timeout
192.168.10.10 icmp_seq=2 timeout
192.168.10.10 icmp_seq=3 timeout
192.168.10.10 icmp_seq=4 timeout

PC1>

```

Рисунок 3.11 – Перевірка роботи списків контролю доступу (ACL) між сегмен-
тами мережі. Частина 2.

Другий етап тестування включав перевірку відмовостійкості зовнішнього периметра на базі технології IP SLA та механізму об'єктного відстеження (Object Tracking). Для цього з внутрішньої робочої станції було запущено безперервний процес відправки ICMP-пакетів до віддаленого хоста в мережі Інтернет. Мережева утиліта traceroute підтвердила, що у штатному режимі весь вихідний трафік підприємства спрямовується через основний шлюз першого інтернет-провайдера (outside1), використовуючи статичний маршрут із метрикою 1.

Далі, в середовищі емуляції GNS3 було штучно імітовано аварію на лінії шляхом програмного відключення основного інтерфейсу outside1. Процес моніторингу IP SLA миттєво зафіксував втрату ICMP-відповідей, внаслідок чого об'єкт

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Track 1 перейшов у стан «Down». Міжмережевий екран автоматично вилучив основний маршрут з таблиці маршрутизації та активував резервний плаваючий маршрут (Floating Route) з метрикою 10. Обмін пакетами зупинився лише на 1-2 секунди, після чого зв'язок повністю відновився. Повторне трасування маршруту показало, що трафік компанії автоматично перенаправлено через резервний канал (outside2). Це емпірично доводить високу надійність та безшовність спроектованої Dual-WAN архітектури.

Третій етап полягав у комплексній верифікації підсистеми віддаленого доступу Cisco AnyConnect. На комп'ютері, розміщеному у зовнішній симульованій мережі Інтернет, було ініційовано запуск клієнтського додатка. Під час встановлення з'єднання на порт TCP 443 клієнт успішно здійснив криптографічну перевірку та валідацію SSL-сертифіката Trustpoint, встановленого на інтерфейсі Cisco ASA [3, 7].

Під час появи вікна автентифікації було введено облікові дані віддаленого користувача (vpuser). Міжмережевий екран перенаправив запит через захищений протокол LDAP до контролера домену 192.168.10.10 [9]. Служба Active Directory підтвердила автентичність користувача та наявність його атрибута memberOf у структурі глобальної групи безпеки SG_VPN_Access [13]. Після успішної авторизації клієнтському додатку було динамічно делеговано IP-адресу з віртуального пулу 192.168.250.0/24. Покроковий процес підключення віддаленого клієнта продемонстровано на рисунках 3.12 – 3.15.

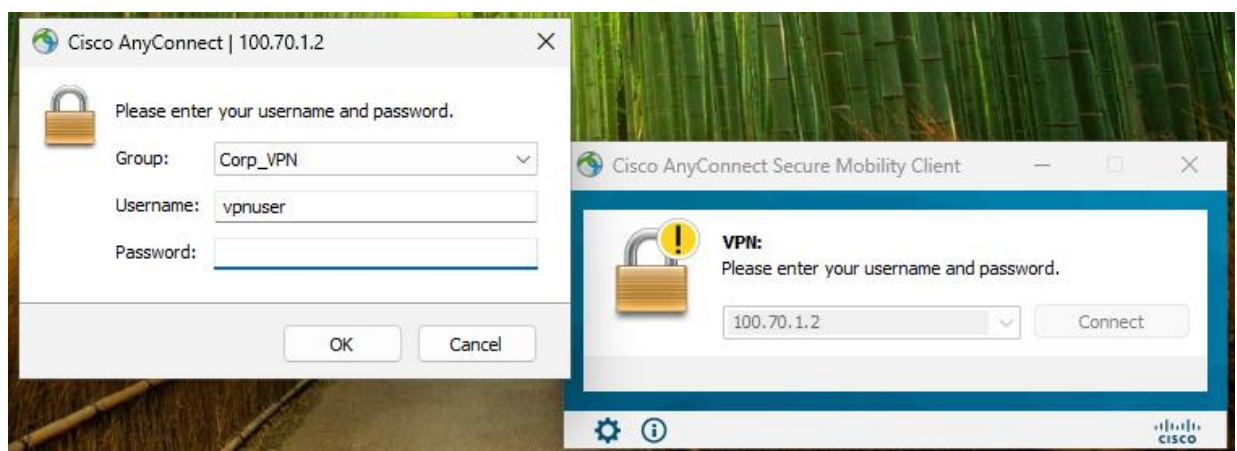


Рисунок 3.12 – Ініціалізація підключення та автентифікація користувача в клієнті Cisco AnyConnect

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росіїнський Ю.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

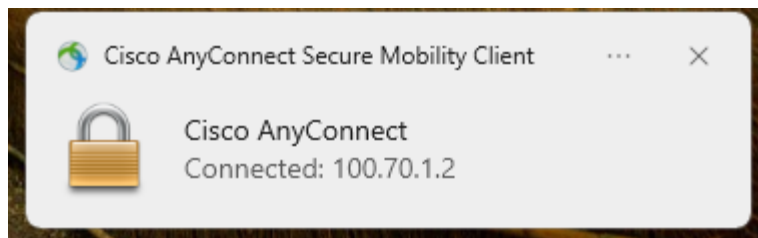


Рисунок 3.13 – Успішне встановлення зашифрованого SSL/DTLS тунелю
AnyConnect VPN

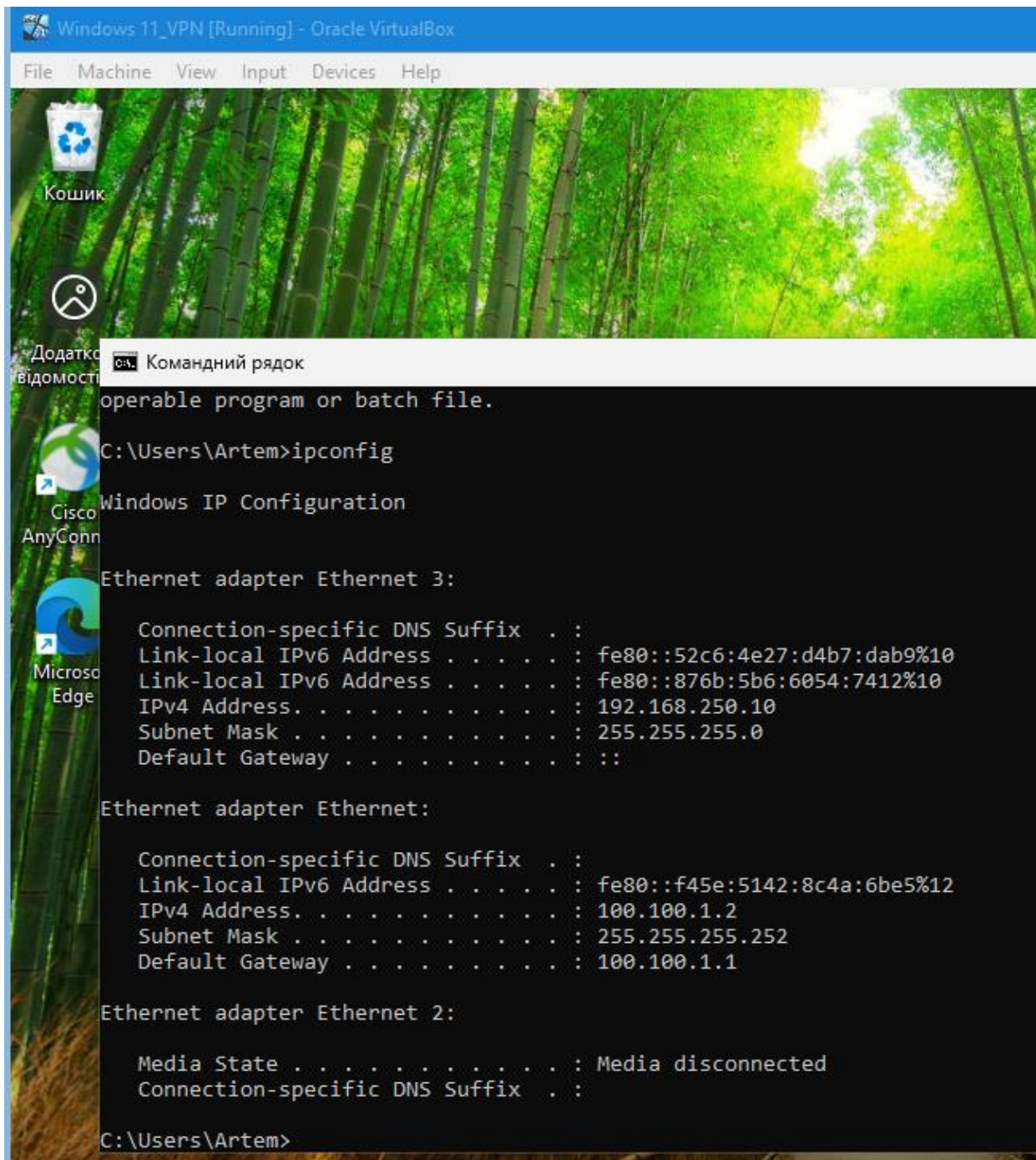


Рисунок 3.14 – Перевірка стану віртуального мережевого адаптера та отриманої
IP-адреси на боці клієнта

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

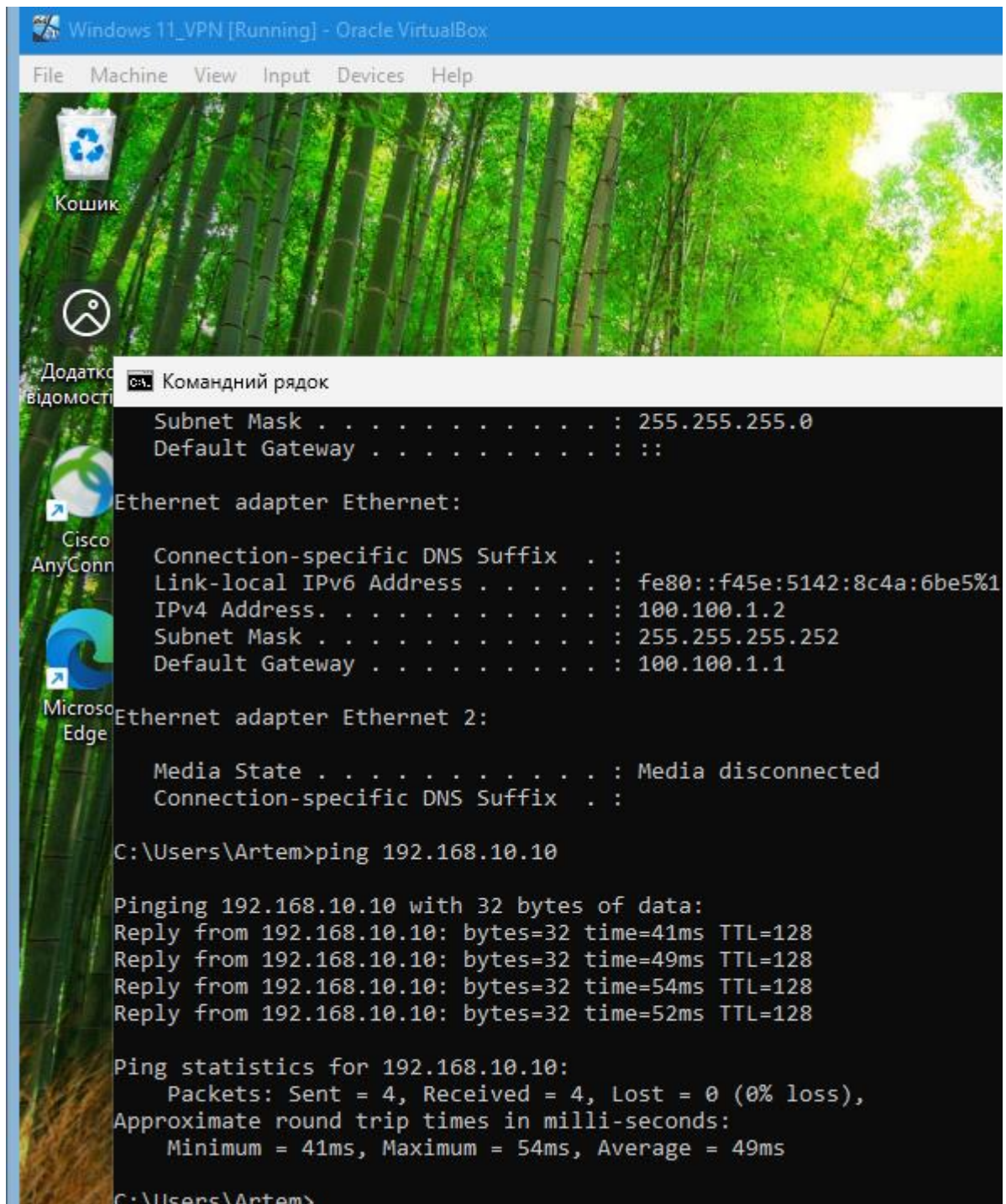


Рисунок 3.15 – Верифікація мережевої доступності внутрішніх ресурсів через VPN за допомогою утиліти ping

Для перевірки роботи механізму роздільного тунелювання (Split Tunneling) та правила обходу трансляції адрес (NAT Exemption), віддалений клієнт здійснив підключення до спільного файлового ресурсу підприємства за протоколом SMB [17]. Оскільки vpnuser отримав IP-адресу з виділеного пулу, трафік не зазнав трансляції на міжмережевому екрані (Identity NAT) [25] і успішно досягнув сервера з оригінальною адресою джерела.

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росінський Ю.М.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Фінальним етапом логічного тестування стала перевірка концепції контролю доступу на основі ролей (RBAC) через VPN [15]. Коли авторизований віддалений користувач спробував відкрити захищену мережеву директорію \\192.168.10.10\HR_Share, файлова система сервера миттєво відхилила запит, оскільки даний обліковий запис не входить до складу глобальної групи безпеки SG_HR_Staff [13]. Це доводить, що розроблена система захисту за принципом Zero Trust працює наскрізно — від граничного шлюзу до конкретного файлового об'єкта на сервері.

Завершальним кроком стало дослідження реальної пропускної здатності та підтвердження активації швидкісного дата-каналу DTLS. За допомогою інструменту глибокого аналізу мережевих протоколів Wireshark було здійснено перехоплення трафіку на зовнішньому інтерфейсі Cisco ASA під час активної VPN-сесії. Аналіз дамів пакетів (PCAP) підтвердив, що після успішного встановлення контрольованого з'єднання по TCP (TLS 1.3) [7], передача основного масиву корпоративних даних автоматично мігрувала на протокол UDP (порт 443), що підтверджує коректність роботи DTLS-тунелю [8, 19].

Для вимірювання реальної пропускної здатності тунелю (Throughput) було використано мережеву утиліту iperf3. Замір швидкості передачі даних між зовнішнім VPN-клієнтом та внутрішнім сервером продемонстрував стабільну утилізацію віртуального каналу без лавиноподібних затримок та втрати пакетів. Це емпірично доводить, що спроектована двоканальна архітектура SSL/DTLS VPN повністю нівелює явище TCP Meltdown та забезпечує максимальну продуктивність для віддалених співробітників підприємства.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Висновок третього розділу

У третьому розділі було успішно здійснено практичну реалізацію та конфігурацію розробленої архітектури в середовищі емуляції мереж. Розгортання служби Active Directory (AD DS) та застосування автоматизованих сценаріїв PowerShell дозволило створити логічно структуровану ієрархію підрозділів підприємства [12]. Використання глобальних груп безпеки (Security Groups) [13] лягло в основу управління правами доступу на рівні файлової системи (NTFS) [15] та забезпечило надійний фундамент для перевірки повноважень віддалених користувачів.

Налаштування міжмережевого екрана Cisco ASA [19] забезпечило практичну реалізацію політик безпеки на мережевому рівні. Успішно сконфігуровано списки контролю доступу (ACL), налаштовано службу ретрансляції DHCP Relay [22] та реалізовано механізм обходу динамічної трансляції адрес (Identity NAT) [25]. Інтеграція підсистеми Cisco AnyConnect [20] довела можливість організації криптографічно захищеного тунелю, який використовує перевірку локальних сертифікатів RSA та нативну авторизацію користувачів безпосередньо в базі Active Directory за протоколом LDAP [9].

Комплексне емпіричне тестування підтвердило повну працездатність спроектованої моделі. Система продемонструвала стовідсоткову відмовостійкість за рахунок механізму активного моніторингу IP SLA та об'єктного відстеження (Object Tracking) для автоматичного перемикавання статичних маршрутів [6, 21], а також підтвердила ефективність налаштованих правил ізоляції трафіку [4, 19]. Додаткові дослідження за допомогою аналізатора пакетів та утиліт тестування пропускну здатності довели успішну активацію швидкісного дата-каналу DTLS [8], що гарантує максимальну продуктивність VPN-тунелю. Усі завдання, поставлені в рамках третього розділу дипломного проєкту, успішно виконані, а створена інфраструктура повністю готова до масштабування та відповідає сучасним галузевим стандартам кібербезпеки [1].

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

ВИСНОВКИ

У результаті виконання дипломного проєкту було успішно вирішено актуальне науково-практичне завдання — розроблено та реалізовано комплексну архітектуру захищеної корпоративної мережі з централізованим управлінням доступом та безпечним зовнішнім периметром. Усі етапи роботи, від теоретичного аналізу до практичного тестування, повністю підтвердили правильність та ефективність обраних інженерних рішень.

Обґрунтовано та спроектовано логічну мікросегментацію інфраструктури на базі стандарту IEEE 802.1Q (VLAN) [4]. Розподіл мережі на серверну (VLAN 10), робочу (VLAN 20) та повністю ізольовану гостьову (VLAN 30) зони дозволив кардинально зменшити поверхню потенційної атаки. Це забезпечило надійний базовий рівень мережевої ізоляції, що повністю відповідає сучасній парадигмі безпеки з нульовою довірою (Zero Trust) [1].

Розгорнуто централізовану службу каталогів Active Directory (AD DS) [12] та побудовано ієрархічну структуру організаційних одиниць (OU). Впровадження моделі управління доступом на основі ролей (RBAC) [15] за допомогою глобальних груп безпеки [13] дозволило об'єднати розрізнені вузли в єдиний керований простір. Налаштування гранулярних політик доступу на рівні файлової системи (NTFS) та мережевого поширення (SMB) [17] гарантувало безкомпромісний захист конфіденційної корпоративної інформації від внутрішніх загроз.

Реалізовано підсистему захищеного віддаленого доступу Cisco AnyConnect SSL/DTLS VPN [3, 20] на базі апаратного міжмережевого екрана Cisco ASA [19]. Двоканальна архітектура тунелю усунула проблему блокування трафіку трансляторами адрес (NAT/PAT) та нівелювала ефект деградації швидкості (TCP Meltdown) завдяки переходу на протокол DTLS [8]. Критично важливим етапом стала інтеграція міжмережевого екрана з Active Directory за стандартизованим протоколом LDAP [9]: це дозволило автоматизувати перевірку повноважень віддалених користувачів через єдину точку автентифікації.

Комплексне емпіричне тестування в середовищі емуляції GNS3 [23] підтвердило стовідсоткову працездатність спроектованої системи. Впровадження техноло-

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

гії активного моніторингу IP SLA та механізму об'єктного відстеження (Object Tracking) забезпечило автоматичне та безшовне резервування каналів зв'язку (Failover) між двома інтернет-провайдерами [6, 21]. Списки контролю доступу (ACL) на рівні L3-шлюзу ефективно блокують нелегітимний трафік, а застосування технології ретрансляції DHCP Relay [22] вирішило завдання динамічної адресації для ізольованих сегментів. Додаткові перевірки підтвердили високу пропускну здатність і стабільність захищених з'єднань при обході трансляції (Identity NAT) [25].

Створена інфраструктура відзначається високою відмовостійкістю, повністю відповідає сучасним галузевим стандартам кібербезпеки, є масштабованою та концептуально готовою до впровадження в реальні бізнес-процеси підприємства.

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Zero Trust Architecture. NIST Special Publication 800-207. [Електронний ресурс] – Режим доступу: <https://csrc.nist.gov/publications/detail/sp/800-207/final>
2. Guide to IPsec Virtual Private Networks. NIST SP 800-77 Rev. 1. [Електронний ресурс] – Режим доступу: <https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final>
3. Guide to SSL Virtual Private Networks. NIST SP 800-113. [Електронний ресурс] – Режим доступу: <https://csrc.nist.gov/publications/detail/sp/800-113/final>
4. IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks (IEEE 802.1Q). IEEE Standards Association. [Електронний ресурс] – Режим доступу: <https://standards.ieee.org/ieee/802.1Q/10323/>
5. RFC 1918: Address Allocation for Private Internets. IETF Datatracker. [Електронний ресурс] – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc1918>
6. Cisco IP SLAs Configuration Guide. Cisco Systems. [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book.html>
7. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. IETF Datatracker. [Електронний ресурс] – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc8446>
8. RFC 9147: The Datagram Transport Layer Security (DTLS) Protocol Version 1.3. IETF Datatracker. [Електронний ресурс] – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc9147>
9. RFC 3377: Lightweight Directory Access Protocol (v3). IETF Datatracker. [Електронний ресурс] – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc3377>
10. RFC 3948: UDP Encapsulation of IPsec ESP Packets (NAT-T). IETF Datatracker. [Електронний ресурс] – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc3948>

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

- 11.RFC 2865: Remote Authentication Dial In User Service (RADIUS). IETF Datatracker. [Електронний ресурс] – Режим доступу: <https://datatracker.ietf.org/doc/html/rfc2865>
- 12.Active Directory Domain Services Overview. Microsoft Learn. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- 13.Active Directory Security Groups. Microsoft Learn. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>
- 14.Group Policy Overview. Microsoft Learn. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview>
- 15.Access Control Overview. Microsoft Learn. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control>
- 16.Implementing Least-Privilege Administrative Models. Microsoft Learn. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>
- 17.Server Message Block (SMB) Overview. Microsoft Learn. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview>
- 18.Windows Defender Firewall with Advanced Security. Microsoft Learn. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/>
- 19.Configuration Guides for Cisco ASA 5500-X Series Firewalls. Cisco Systems. [Електронний ресурс] – Режим доступу:

		Редчиць А.О.			ККІКБ.КР.Б – 123 – 12 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

<https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>

20. Cisco AnyConnect Secure Mobility Client Configuration Guides. Cisco Systems.

[Електронний ресурс] – Режим доступу:

<https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html>

21. Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide:

Static Route Tracking (IP SLA). Cisco Systems. [Електронний ресурс] – Режим доступу:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa919/configuration/general/asa-919-general-config/route-static.html>

22. RFC 3046: DHCP Relay Agent Information Option. IETF Datatracker. [Електронний ресурс]

– Режим доступу: <https://datatracker.ietf.org/doc/html/rfc3046>

23. GNS3 Official Documentation. GNS3 Technologies. [Електронний ресурс] –

Режим доступу: <https://docs.gns3.com/>

24. Cisco ASAv Appliance on GNS3 Marketplace. GNS3 Technologies. [Електронний ресурс]

– Режим доступу: <https://gns3.com/marketplace/appliances/cisco-asav>

25. RFC 3022: Traditional IP Network Address Translator (Traditional NAT). IETF

Datatracker. [Електронний ресурс] – Режим доступу:

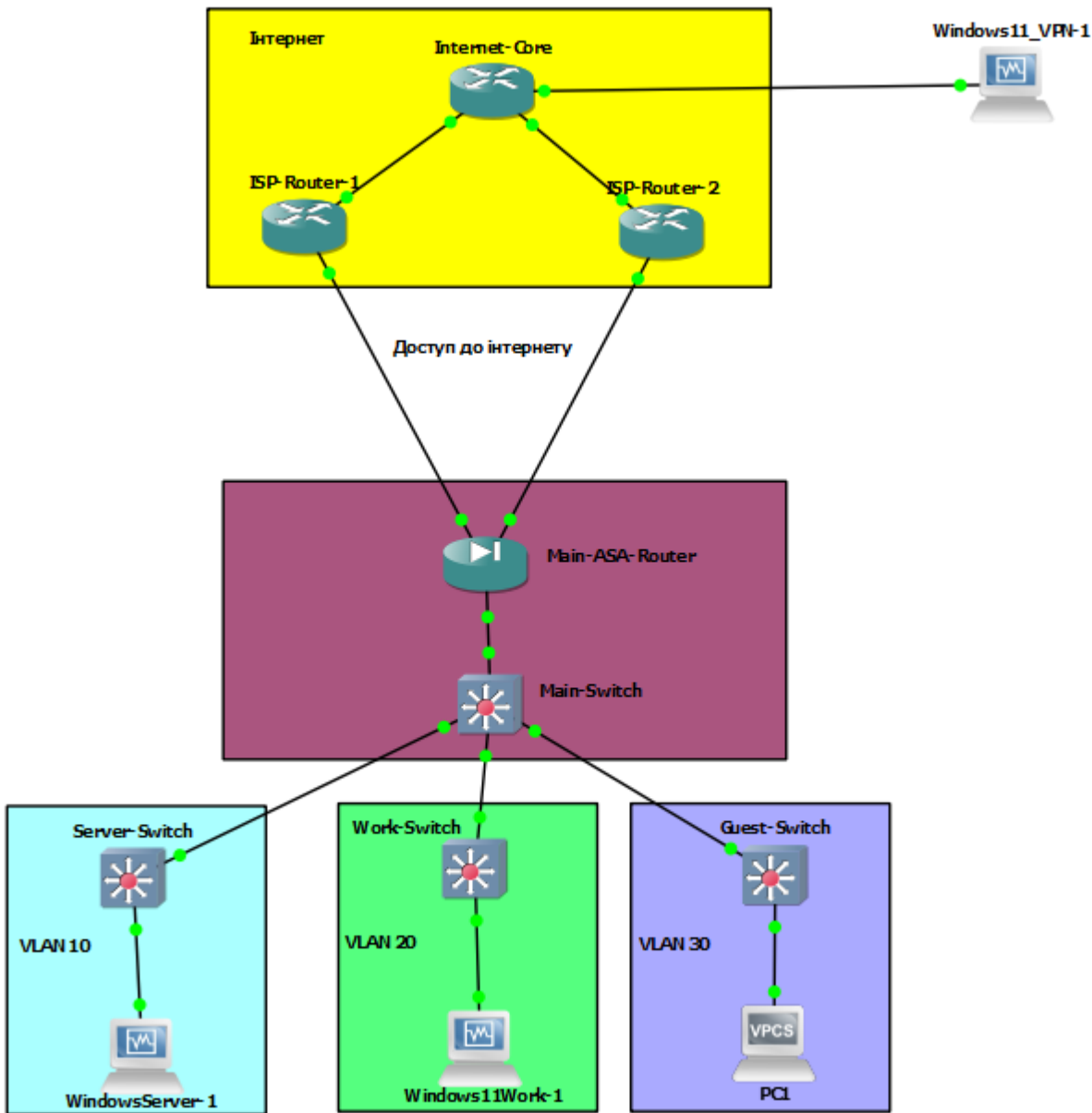
<https://datatracker.ietf.org/doc/html/rfc3022>

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

ДОДАТКИ

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росі́нський Ю.М.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Топологія мережі



Конфігураційний файл Cisco ASA

```

: Saved

:
: Serial Number: 9AGNXAHV2RM
: Hardware:   ASAv, 2048 MB RAM, CPU Unknown Model 3600 MHz
: Written by enable_15 at 11:20:18.679 UTC Thu Jun 11 2026
!
ASA Version 9.8(1)
!
hostname Main-ASA
domain-name corp.local
enable password
$sha512$5000$3HvGFT4N8Pa101/57RTKcg==$eGgSDho2qVpkuaox012uzw== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
ip local pool VPN_POOL 192.168.250.10-192.168.250.50 mask 255.255.255.0

!
interface GigabitEthernet0/0
  description Link_to_ISP1
  nameif outside1
  security-level 0
  ip address 100.70.1.2 255.255.255.252
!
interface GigabitEthernet0/1
  description Link_to_ISP2
  nameif outside2
  security-level 0
  ip address 100.70.1.6 255.255.255.252
!
interface GigabitEthernet0/2
  description Downlink_to_Main_Switch
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/2.10
  vlan 10
  nameif inside10
  security-level 100
  ip address 192.168.10.1 255.255.255.0
!

```

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet0/2.20
vlan 20
nameif inside20
security-level 100
ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/2.30
vlan 30
nameif inside30
security-level 100
ip address 192.168.30.1 255.255.255.0
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
dns server-group DefaultDNS
domain-name corp.local
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network VPN_POOL_OBJ
subnet 192.168.250.0 255.255.255.0
object network INSIDE_10_OBJ
subnet 192.168.10.0 255.255.255.0

```

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```

object network INSIDE_20_OBJ
  subnet 192.168.20.0 255.255.255.0
object network INSIDE_30_OBJ
  subnet 192.168.30.0 255.255.255.0
object network VPN_POOL_SUBNET
  subnet 192.168.250.0 255.255.255.0
object-group network LOCAL_INTERNAL_NETS
  network-object 192.168.10.0 255.255.255.0
  network-object 192.168.20.0 255.255.255.0
  network-object 192.168.30.0 255.255.255.0
access-list LOCAL_INTERNAL_NETS standard permit 192.168.10.0
255.255.255.0
access-list LOCAL_INTERNAL_NETS standard permit 192.168.20.0
255.255.255.0
access-list LOCAL_INTERNAL_NETS standard permit 192.168.30.0
255.255.255.0
access-list VPN_TO_INSIDE extended permit ip 192.168.250.0 255.255.255.0
any
access-list VPN_TO_INSIDE extended permit icmp 192.168.250.0
255.255.255.0 any
access-list ANYCONNECT_ACL extended permit icmp any any
access-list ANYCONNECT_ACL extended permit ip any any
access-list SPLIT_ACL standard permit 192.168.10.0 255.255.255.0
access-list SPLIT_ACL standard permit 192.168.20.0 255.255.255.0
access-list SPLIT_ACL standard permit 192.168.30.0 255.255.255.0
access-list VLAN20_IN extended deny ip any 192.168.30.0 255.255.255.0
access-list VLAN20_IN extended permit ip any any
access-list VLAN30_IN extended permit udp any host 192.168.10.10 eq do-
main
access-list VLAN30_IN extended permit tcp any host 192.168.10.10 eq do-
main
access-list VLAN30_IN extended permit udp any host 192.168.10.10 eq
bootps
access-list VLAN30_IN extended deny ip any 192.168.10.0 255.255.255.0
access-list VLAN30_IN extended deny ip any 192.168.20.0 255.255.255.0
access-list VLAN30_IN extended permit ip any any
pager lines 23
mtu outside1 1500
mtu outside2 1500
mtu inside10 1500
mtu inside20 1500
mtu inside30 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside10
icmp permit any inside20
icmp permit any inside30
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

```

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

```

arp rate-limit 8192
nat (inside10,outside1) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static VPN_POOL_SUBNET VPN_POOL_SUBNET no-proxy-arp
route-lookup
nat (inside20,outside1) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static VPN_POOL_SUBNET VPN_POOL_SUBNET no-proxy-arp
route-lookup
nat (inside30,outside1) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static VPN_POOL_SUBNET VPN_POOL_SUBNET no-proxy-arp
route-lookup
nat (inside10,inside20) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-
proxy-arp route-lookup
nat (inside20,inside10) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-
proxy-arp route-lookup
nat (inside10,inside30) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-
proxy-arp route-lookup
nat (inside30,inside10) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-
proxy-arp route-lookup
nat (inside30,inside20) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-
proxy-arp route-lookup
nat (inside20,inside30) source static LOCAL_INTERNAL_NETS LOCAL_INTER-
NAL_NETS destination static LOCAL_INTERNAL_NETS LOCAL_INTERNAL_NETS no-
proxy-arp route-lookup
!
nat (any,outside1) after-auto source dynamic LOCAL_INTERNAL_NETS inter-
face
nat (any,outside2) after-auto source dynamic LOCAL_INTERNAL_NETS inter-
face
access-group VLAN20_IN in interface inside20
access-group VLAN30_IN in interface inside30
route outside1 0.0.0.0 0.0.0.0 100.70.1.1 1 track 1
route outside2 0.0.0.0 0.0.0.0 100.70.1.5 10
route outside1 100.100.1.0 255.255.255.252 100.70.1.1 1
route outside2 100.100.1.0 255.255.255.252 100.70.1.5 10
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp
0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15

```

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

timeout igp stale-route 0:01:10
aaa-server AD_RADIUS protocol radius
aaa-server AD_RADIUS (inside10) host 192.168.10.10
  key cisco123
user-identity default-domain LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
sla monitor 1
  type echo protocol ipIcmpEcho 100.70.1.1 interface outside1
  num-packets 3
  frequency 5
sla monitor schedule 1 life forever start-time now
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
  no validation-usage
  crl configure
crypto ca trustpoint LOCAL-ASA-CA
  enrollment self
  subject-name CN=vpn.corp.local
  crl configure
crypto ca trustpool policy
  auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
  certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
    308204d3 308203bb a0030201 02021018 dad19e26 7de8bb4a 2158cdcc
6b3b4a30
    0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302
55533117
    30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06
0355040b
    13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038
06035504
    0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d
20466f72
    20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504
03133c56
    65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61
72792043
    65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530
1e170d30
    36313130 38303030 3030305a 170d3336 30373136 32333539 35395a30
81ca310b
    30090603 55040613 02555331 17301506 0355040a 130e5665 72695369
676e2c20
    496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573
74204e65
    74776f72 6b313a30 38060355 040b1331 28632920 32303036 20566572
69536967
    6e2c2049 6e632e20 2d20466f 72206175 74686f72 697a6564 20757365
206f6e6c

```

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

79314530 43060355 0403133c 56657269 5369676e 20436c61 73732033
 20507562
 6c696320 5072696d 61727920 43657274 69666963 6174696f 6e204175
 74686f72
 69747920 2d204735 30820122 300d0609 2a864886 f70d0101 01050003
 82010f00
 3082010a 02820101 00af2408 08297a35 9e600caa e74b3b4e dc7cbc3c
 451cbb2b
 e0fe2902 f95708a3 64851527 f5f1adc8 31895d22 e82aaaa6 42b38ff8
 b955b7b1
 b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4 d8def8e0 c362083d
 5413eb49
 ca595485 26e52b8f 1b9feb5f a191c233 49d84363 6a524bd2 8fe87051
 4dd18969
 7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0 f4a225f2 af1c9267
 18e5f406
 04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb 378becf4 d7acf2f6
 f03dafdd
 75913319 1d1c40cb 74241921 93d914fe ac2a52c7 8fd50449 e48d6347
 883c6983
 cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314 087ee53f 9f73b833
 0acf5d3f
 3487968a ee53e825 15020301 0001a381 b23081af 300f0603 551d1301
 01ff0405
 30030101 ff300e06 03551d0f 0101ff04 04030201 06306d06 082b0601
 05050701
 0c046130 5fa15da0 5b305930 57305516 09696d61 67652f67 69663021
 301f3007
 06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf 806ad448 182c7b19
 2e302516
 23687474 703a2f2f 6c6f676f 2e766572 69736967 6e2e636f 6d2f7673
 6c6f676f
 2e676966 301d0603 551d0e04 1604147f d365a7c2 ddecbbf0 3009f343
 39fa02af
 33313330 0d06092a 864886f7 0d010105 05000382 01010093 244a305f
 62cfd81a
 982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812 ad620e45 7064c5e7
 97662d98
 097e5faf d6cc2865 f201aa08 1a47def9 f97c925a 0869200d d93e6d6e
 3c0d6ed8
 e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415 3881c994 eea28429
 0b136f8e
 db0cdd25 02dba48b 1944d241 7a05694a 584f60ca 7e826a0b 02aa2517
 39b5db7f
 e784652a 958abd86 de5e8116 832d10cc defda882 2a6d281f 0d0bc4e5
 e71a2619
 e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e 85d35bef a57d4540
 728eb70e
 6b0e06fb 33354871 b89d278b c4655f0d 86769c44 7af6955c f65d3208
 33a454b6
 183f685c f2424a85 3854835f d1e82cf2 ac11d6a8 ed636a

		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

quit
crypto ca certificate chain LOCAL-ASA-CA
certificate 24fa176a
  308202f6 308201de a0030201 02020424 fa176a30 0d06092a 864886f7
0d01010b
  0500303d 31173015 06035504 03130e76 706e2e63 6f72702e 6c6f6361
6c312230
  2006092a 864886f7 0d010902 16136369 73636f61 73612e63 6f72702e
6c6f6361
  6c301e17 0d323630 35323830 38343332 375a170d 33363035 32353038
34333237
  5a303d31 17301506 03550403 130e7670 6e2e636f 72702e6c 6f63616c
31223020
  06092a86 4886f70d 01090216 13636973 636f6173 612e636f 72702e6c
6f63616c
  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a
02820101
  00aa0c35 87b7349d ee1fa886 9809e065 96b0539a 229cc94c 96ee3e2a
b0278cf6
  b47ec498 04d4d755 5056d564 648f8635 c845386e 45836d16 34ef57eb
25d7a3a3
  b1c16c9b d3b6d291 859a19c6 77ae0d9d aadf8946 f9495c77 cf8ae615
71342580
  0eb8f9f4 fe2b4004 ed570f16 4a54c0ed ef56f3cf 753b138c f9eb5be6
810e45d3
  bfb4776b 35a92daf b4eb15e3 ea1b2f4e e4aea796 ac653209 b992547f
3a67ddfe
  b6132b01 42c10f9e fe68ab6c 7d93fade f2c7545b d4b1a8c3 0291c335
be2a90c7
  2df8a14f d32eaa81 3bd55bb4 36c9da6b e0a44a61 40052d5d 291bb281
ffc2d88b
  9459224e c47d23a8 52cf157c 1d25f55c 543531d8 94677641 5bb674ba
43fc23f2
  17020301 0001300d 06092a86 4886f70d 01010b05 00038201 01007ade
dc3ec860
  bd55321c 8f4cac87 1b704e78 6ce8bc7c a2ccc503 23a1bf55 f82e82be
257b9d4c
  f508e35b 01102228 a4156e56 cd2a0fdc 9ebefbfe 8ce703da 4293b34e
67092887
  cd5be242 47f10795 33192ecd 4aed154b ac367e64 72438e1e a7e18d3b
a061f241
  e976ee5c 20cc10db d2867f07 7cab412d 1dbae43c 5611a2e3 3aa9ed58
2950ac60
  41c68b48 5d129a66 9aad1f25 9ac50ece eab0e2f6 117705e6 93acf91e
eb26da70
  4a11cd1d 273211d7 47c25a0c 640a5221 66c82816 889fd8e4 d58cf65e
ffe7edbf
  bdaea12f 75527af0 d920c0f9 b371071a 3b8bde65 521b77d6 f99d7cbf
e13747b7
  b03ada01 7ddca172 9cf696cd bcbdfa11 f6915f1b 796fc205 8958
quit

```

		Редчиць А.О.			ККИКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
track 1 rtr 1 reachability
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside10
dhcprelay server 192.168.10.10 inside10
dhcprelay enable inside20
dhcprelay enable inside30
dhcprelay timeout 60
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl trust-point LOCAL-ASA-CA outside1
webvpn
  enable outside1
  anyconnect image disk0:/anyconnect.pkg 1
  anyconnect enable
  tunnel-group-list enable
  cache
    disable
  error-recovery disable
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ssl-client ssl-clientless
group-policy ANYCONNECT_POLICY internal
group-policy ANYCONNECT_POLICY attributes
  vpn-filter value ANYCONNECT_ACL
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT_ACL
dynamic-access-policy-record DfltAccessPolicy
tunnel-group ANYCONNECT_TG type remote-access
tunnel-group ANYCONNECT_TG general-attributes
  address-pool VPN_POOL
  authentication-server-group AD_RADIUS
  default-group-policy ANYCONNECT_POLICY
tunnel-group ANYCONNECT_TG webvpn-attributes
  group-alias Corp_VPN enable
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
  no tcp-inspection
policy-map global_policy
  class inspection_default

```

		Редчиць А.О.			ККИКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росіїнський Ю.М.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

inspect ip-options
inspect netbios
inspect rtsp
inspect sunrpc
inspect tftp
inspect xdmcp
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect esmtp
inspect sqlnet
inspect sip
inspect skinny
inspect icmp
inspect icmp error
policy-map type inspect dns migrated_dns_map_2
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
    no active
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
    destination address email callhome@cisco.com
    destination transport-method http
    subscribe-to-alert-group diagnostic
    subscribe-to-alert-group environment
    subscribe-to-alert-group inventory periodic monthly
    subscribe-to-alert-group configuration periodic monthly
    subscribe-to-alert-group telemetry periodic daily
  profile License
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
    destination transport-method http
Cryptochecksum:3dd67c0fbefe6fb6b45c272491b108b7
: end

```

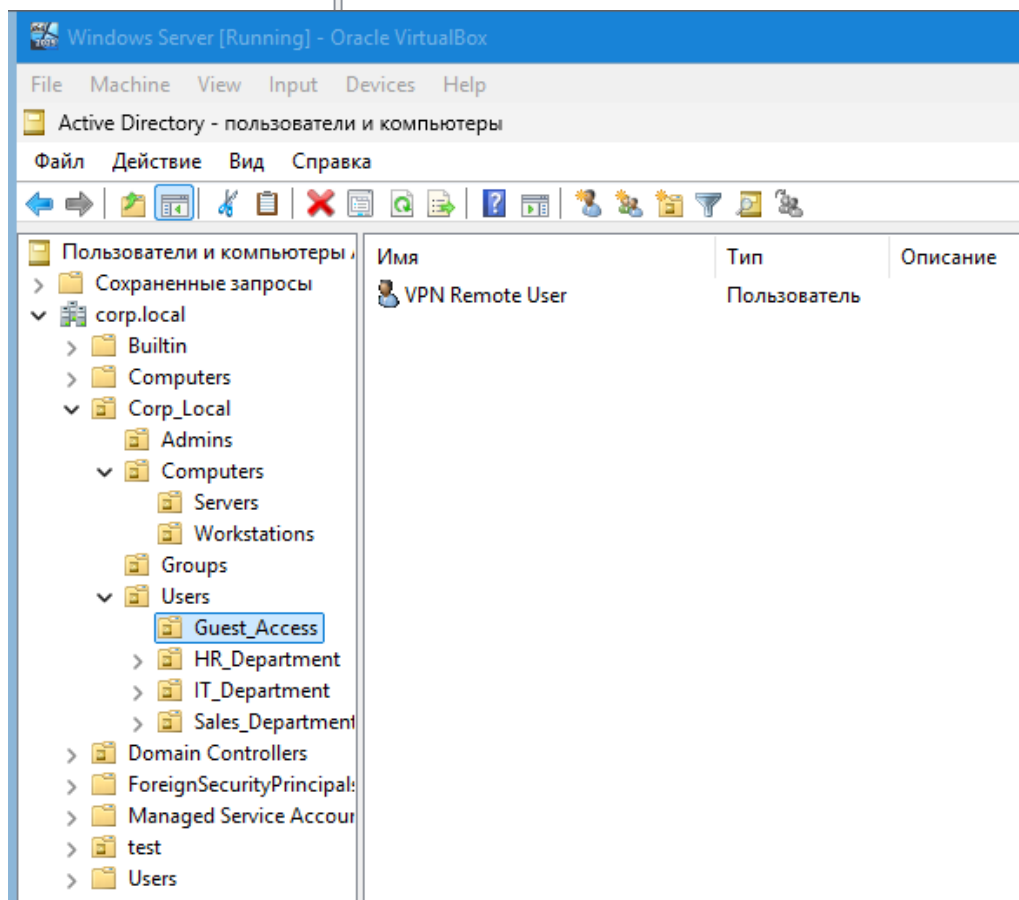
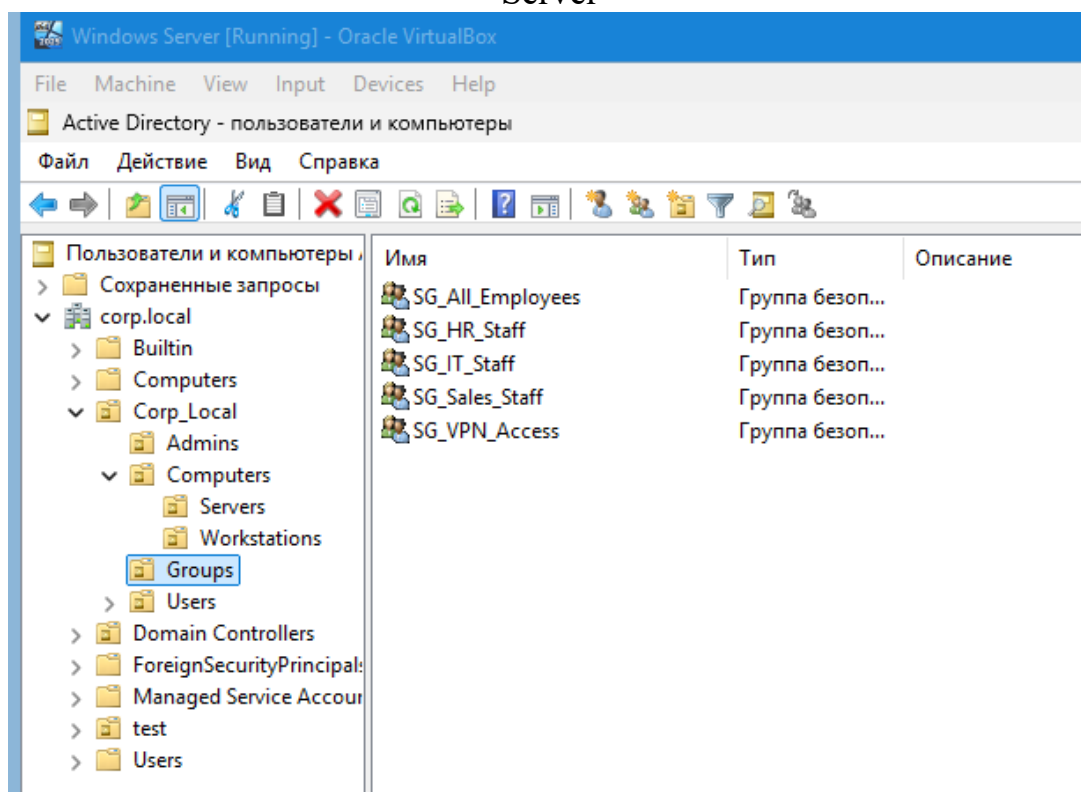
		Редчиць А.О.			ККІКБ.КР.Б - 123 - 12 - ПЗ	Арк.
		Росієнський Ю.М.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

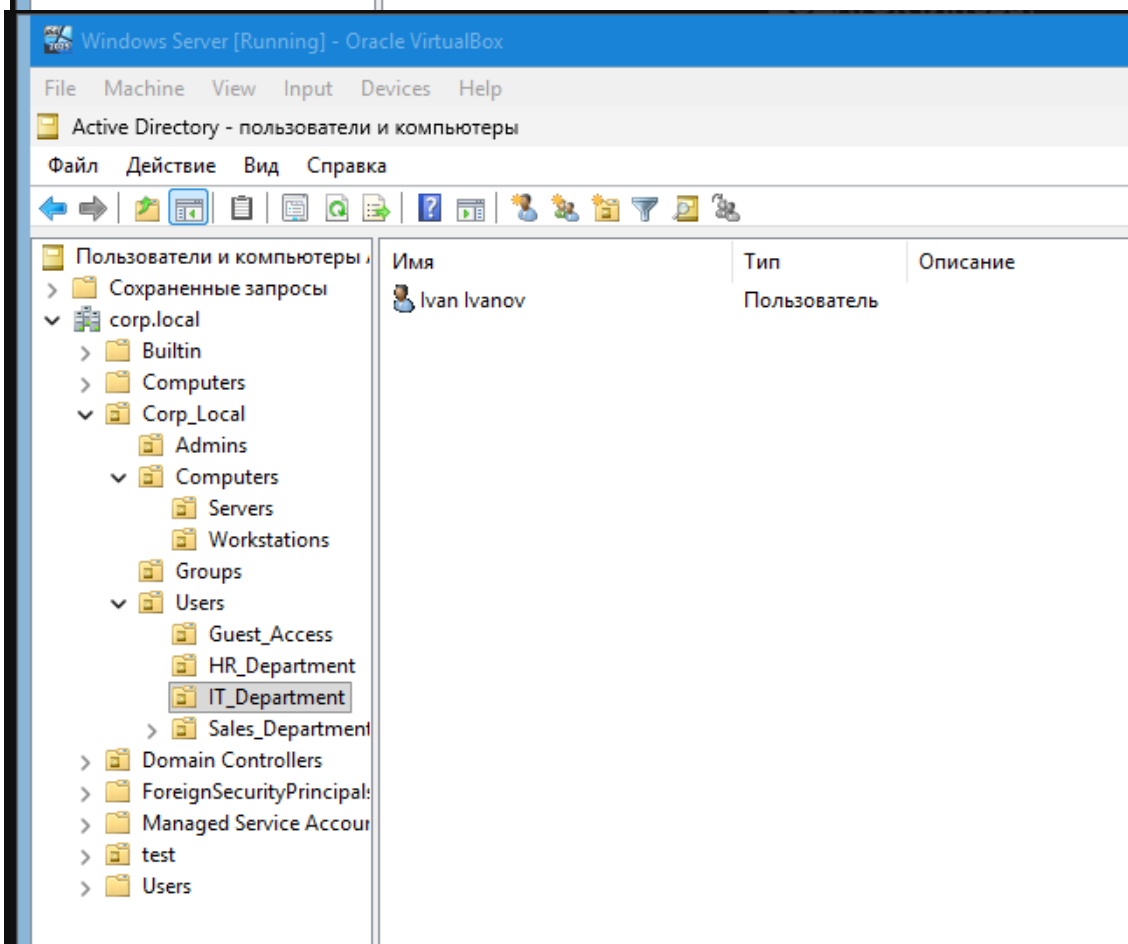
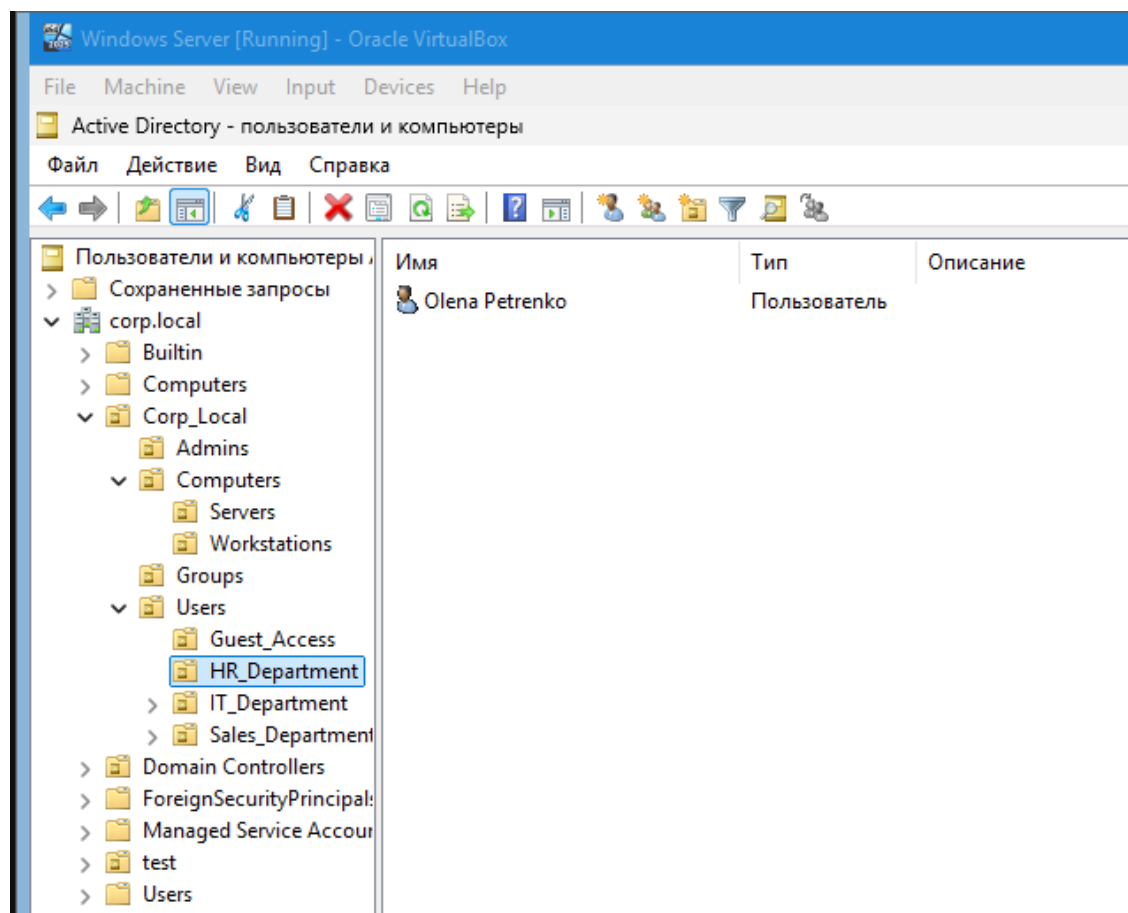
Повна адресація мережі

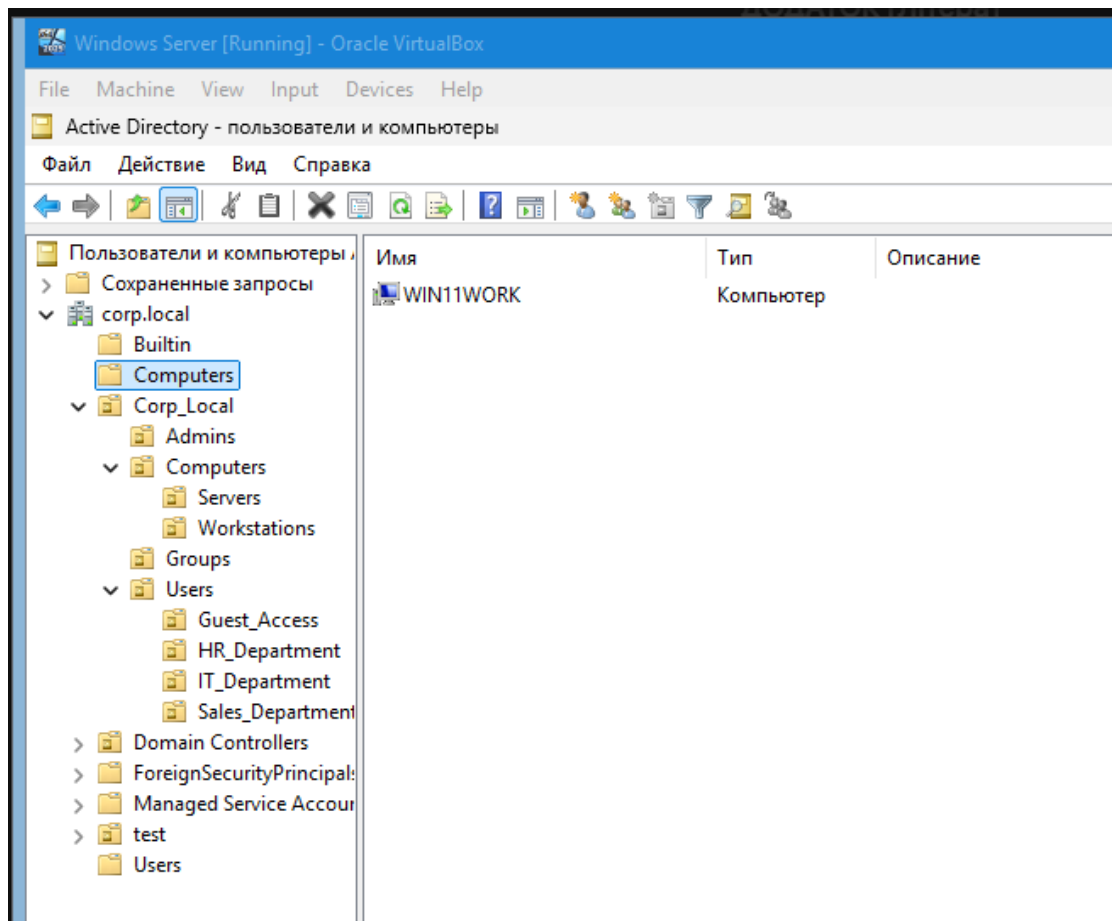
Назва при-строю / Ву-зол	Інтерфейс / Локація	ІР-адреса	Маска підме-режі	Шлюз за замовчу-ванням (Gateway)	Примітка / Роль
Cisco ASA (Шлюз)	GigabitEthernet 0/0 (outside1)	100.70.1.2	255.255.255.252 (/30)	100.70.1.1	Основний ISP (IP SLA Track 1)
	GigabitEthernet 0/1 (outside2)	100.70.1.6		100.70.1.5	Резервний ISP (Floating Route)
	GigabitEthernet 0/2.10 (inside10)	192.168.10.1	255.255.255.0 (/24)	—	Шлюз для VLAN 10 (Servers)
	GigabitEthernet 0/2.20 (inside20)	192.168.20.1			Шлюз для VLAN 20 (Workstations)
	GigabitEthernet 0/2.30 (inside30)	192.168.30.1			Шлюз для VLAN 30 (Guest)
AD / DNS Server	Ethernet0 (VLAN 10)	192.168.10.10	255.255.255.0 (/24)	192.168.10.1	Контролер домену (Статика)
Corp_PC_1	Ethernet0 (VLAN 20)	DHCP			Робоча станція (DHCP/Статика)
Guest_Device	WLAN (VLAN 30)	DHCP			Гостьовий пристрій (DHCP Relay)
AnyConnect VPN	Віртуальний адаптер (VA)	192.168.250.20 - 254	255.255.255.0 (/24)	—	Пул адрес для віддалених клієнтів
ISP 1 Router	GigabitEthernet 0/0	100.70.1.1	255.255.255.252 (/30)	—	Обладнання провайдера 1
ISP 2 Router	GigabitEthernet 0/0	100.70.1.5	255.255.255.252 (/30)	—	Обладнання провайдера 2

Додаток Г

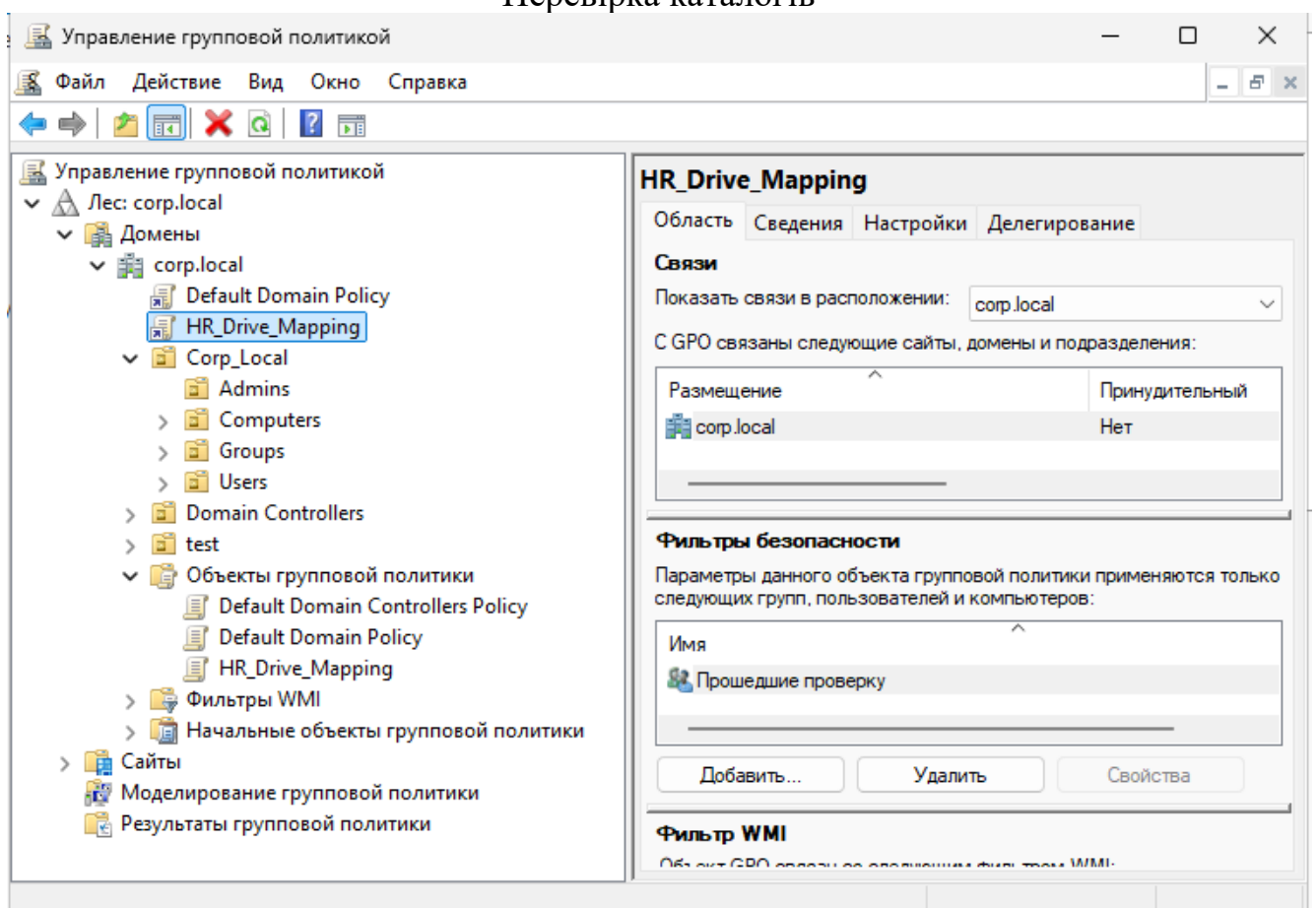
Візуалізація структури каталогів та параметрів керування доступом у Windows Server

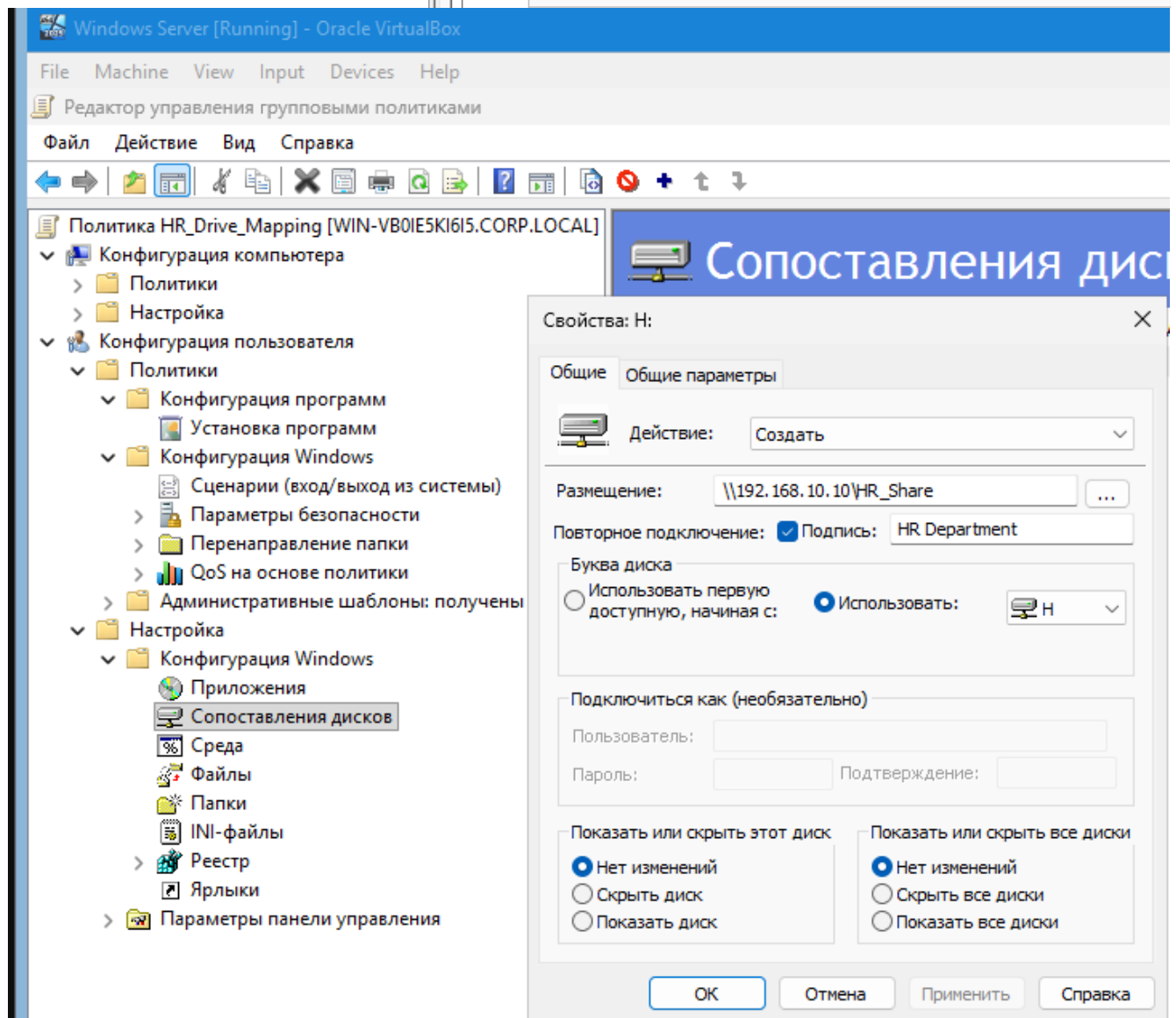
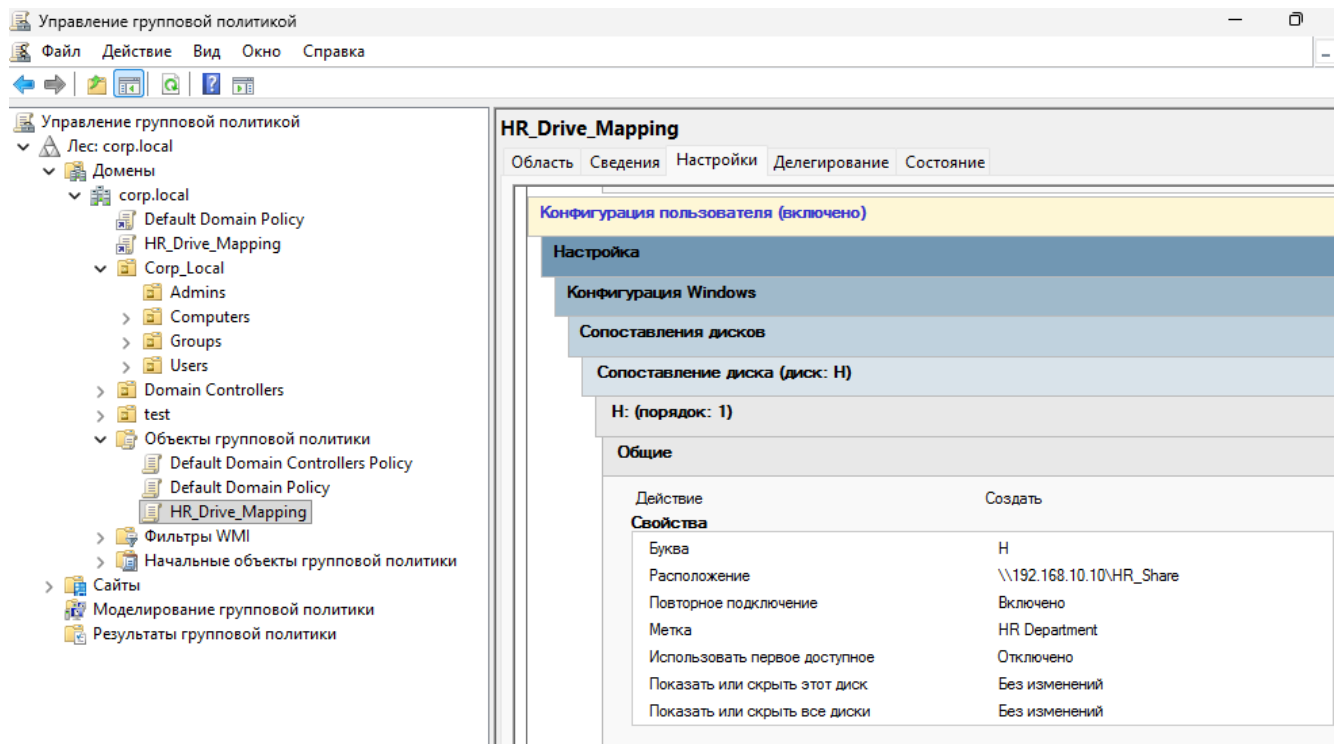






Перевірка каталогів





Перевірка налаштування мережевої папки

		Редчиць А.О.			KKIB.KP.B - 123 - 12 - ПЗ	Арк.
		Росінський Ю.М.				85
Змн.	Арк.	№ докум.	Підпис	Дата		