ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ПІДСИСТЕМА БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ЦЕНТРАЛІЗОВАНОГО КЕРУВАННЯ ДОСТУПОМ ЧЕРЕЗ MICROSOFT ACTIVE DIRECTORY»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Микита ТОКАР*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КСДМ-61
Микита ТОКАР
Ім'я, ПРІЗВИЩЕ

Керівник: Кирило СОКОЛОВ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 Комп'ютерної інженерії
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я, ПРІЗВИЩЕ
«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Токар Микита Денисович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Підсистема безпеки корпоративної мережі на основі централізованого керування доступом через Microsoft Active Directory
керівник кваліфікаційної роботи Кирило СОКОЛОВ,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10 2025р. № 467
2. Строк подання кваліфікаційної роботи «_____» _____ 2025р.
3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, методи системного аналізу для проектування архітектури, методи моделювання мережевих процесів, а також емпіричні методи при налаштуванні та тестуванні програмно-апаратних комплексів.
Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Концептуальні засади побудови безпечного інформаційного середовища підприємства
2. Архітектурне проектування захищеного корпоративного середовища
3. Практична імплементація та верифікація системи захисту інформаційного середовища
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «_____» _____ 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.09-24.10.2025	Виконано
2	Обробка матеріалу	25.10-05.11.2025	Виконано
3	Розробка теоретичної частини	06.11-10.11.2025	Виконано
4	Розробка підсистеми	11.11-15.11.2025	Виконано
5	Висновки за результатами аналізу	15.11-19.11.2025	Виконано
6	Оформлення пояснювальної записки	19.11-21.11.2025	Виконано
7	Розробка презентації	21.11-29.11.2025	Виконано
8	Передзахист	01.12-02.12.2025	Виконано
9	Здача в деканат	15.12-18.12.2025	Виконано

Здобувач вищої освіти _____ Микита ТОКАР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Кирило СОКОЛОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 79 стор., 32 рис., 19 джерел.

Мета дослідження – підвищення захищеності та керованості корпоративної IT-інфраструктури шляхом розробки комплексної архітектури мережі з використанням Active Directory та захищених мережевих протоколів.

Об'єкт дослідження – процеси організації та адміністрування безпечного мережевого середовища підприємства.

Предмет дослідження – архітектурні рішення, програмно-апаратні засоби та політики безпеки для побудови корпоративної мережі на базі технологій Cisco та Microsoft.

Короткий зміст роботи: У кваліфікаційній роботі проведено аналіз сучасних загроз інформаційній безпеці та методів протидії їм. Обґрунтовано вибір апаратного забезпечення Cisco для побудови ієрархічної мережі. Розроблено топологію мережі з використанням протоколу динамічної маршрутизації OSPF та плануванням IP-адресації. Детально описано процес розгортання служби каталогів Active Directory, включаючи налаштування контролерів домену, реплікації та створення організаційних одиниць. Реалізовано практичні заходи захисту: налаштування безпеки мережевого обладнання, впровадження парольних політик та механізмів автентифікації користувачів.

Результати: Спроектовано підсистему захищеної корпоративної мережі, що забезпечує централізоване управління ресурсами, відмовостійкість сервісів та захист від поширених мережевих атак.

КЛЮЧОВІ СЛОВА: IT-ІНФРАСТРУКТУРА, ACTIVE DIRECTORY, КІБЕРБЕЗПЕКА, CISCO, OSPF, МАРШРУТИЗАЦІЯ, АВТЕНТИФІКАЦІЯ, GPO, ТОПОЛОГІЯ МЕРЕЖІ, ЗАХИСТ ІНФОРМАЦІЇ.

ABSTRACT

Textual part of the Master's qualification thesis: 79 pages, 32 figures, 19 references.

Research Objective – to enhance the security and manageability of corporate IT infrastructure by developing a comprehensive network architecture using Active Directory and secure network protocols.

Object of Research – the processes of organizing and administering a secure enterprise network environment.

Subject of Research – architectural solutions, hardware and software tools, and security policies for building a corporate network based on Cisco and Microsoft technologies.

Summary: The thesis conducts an analysis of modern information security threats and countermeasures. The choice of Cisco hardware for building a hierarchical network is justified. A network topology has been developed using the OSPF dynamic routing protocol and IP addressing planning. The process of deploying Active Directory services is described in detail, including the configuration of domain controllers, replication, and the creation of organizational units. Practical security measures have been implemented: network equipment security configuration, implementation of password policies, and user authentication mechanisms.

Results: A secure corporate network subsystem has been designed, ensuring centralized resource management, service fault tolerance, and protection against common network attacks.

KEYWORDS: IT INFRASTRUCTURE, ACTIVE DIRECTORY, CYBERSECURITY, CISCO, OSPF, ROUTING, AUTHENTICATION, GPO, NETWORK TOPOLOGY, INFORMATION PROTECTION.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Токар М. Д. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)
на тему: «Підсистема безпеки корпоративної мережі на основі централізованого керування доступом через Microsoft Active Directory».
Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Токар М. Д. показав відмінну теоретичну підготовку, уміння володіти та розуміння новими комп'ютерними технологіями, користуватися навчальною і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.
Все це дозволяє оцінити кваліфікаційну роботу студента Токара Микити Денисовича на оцінку «відмінно», та присвоїти їй кваліфікацію «магістр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Кирило СОКОЛОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«__» _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Токар М. Д.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Токар Микита Денисович
(прізвище, ім'я, по батькові)
на тему: «Підсистема безпеки корпоративної мережі на основі централізованого керування доступом через Microsoft Active Directory»

Актуальність:

Кваліфікаційна магістерська робота присвячена вирішенню важливого завдання — забезпеченню комплексної безпеки корпоративного інформаційного середовища. В умовах, коли кіберзагрози стають дедалі витонченішими, а атаки на інфраструктуру — частішими, тема побудови захищеної мережі з використанням стандартизованих інструментів управління та надійного комунікаційного обладнання є надзвичайно актуальною. Автор розглядає безпеку не як окремий елемент, а як інтегровану складову архітектури системи.

Позитивні сторони:
1. Робота відзначається глибоким аналізом теоретичної бази: детально розглянуто складові IT-інфраструктури, моделі хмарних обчислень та широкий спектр мережевих загроз.
2. Детально опрацьовано питання впровадження Active Directory. Описано не лише базове встановлення, але й налаштування відмовостійкості, реплікації та структури організаційних одиниць, що свідчить про системний підхід до проектування.
3. Надано чіткі рекомендації щодо безпеки на різних рівнях: від фізичного захисту серверів до конфігурації портів комутаторів та впровадження MFA.

Недоліки:
1. У роботі основну увагу приділено технологіям Microsoft та Cisco, проте менш детально розглянуто питання інтеграції з Linux-системами або альтернативним програмним забезпеченням, що часто зустрічається в гетерогенних мережах.
2. Бажано було б навести детальніші розрахунки вартості впровадження запропонованого апаратного комплексу для оцінки економічної ефективності проекту для середнього бізнесу.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку "відмінно", а здобувач Токар М. Д. заслуговує присвоєння кваліфікації: магістр з комп'ютерної інженерії.*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП.....9
1 КОНЦЕПТУАЛЬНІ ЗАСАДИ ПОБУДОВИ БЕЗПЕЧНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА.....11
1.1 Сутність, структура та складові елементи корпоративної інформаційно-технологічної інфраструктури.....11
1.2 Архітектурні засади організації мережевого середовища на основі Active Directory.....21
1.3 Функціональний інструментарій Active Directory у системі кібербезпеки підприємства.....25
1.4 Аналіз вразливостей мережевих протоколів та векторів атак на інфраструктуру.....30
2 АРХІТЕКТУРНЕ ПРОЕКТУВАННЯ ЗАХИЩЕНОГО КОРПОРАТИВНОГО СЕРЕДОВИЩА.....48
2.1 Обґрунтування вибору апаратного забезпечення для побудови комунікаційної архітектури.....48
2.2 Архітектурне планування та топологічна організація корпоративної мережі.....52
2.3 Організація логічного адресного простору та реалізація протоколів маршрутизації.....54
3 ПРАКТИЧНА ІМПЛЕМЕНТАЦІЯ ТА ВЕРИФІКАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА.....58
3.1 Конфігурація активного мережевого обладнання та базових сервісів.....58
3.2 Розгортання та конфігурація архітектури служб каталогів.....60
3.3 Верифікація функціональності та тестування логічної структури домену69
ВИСНОВКИ.....74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....76
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація).....79

ВСТУП

У сучасному цифровому середовищі стабільність та безпека бізнес-процесів безпосередньо залежать від надійності корпоративної інформаційно-технологічної інфраструктури. Трансформація IT-систем зі допоміжних інструментів у стратегічні активи вимагає нових підходів до їх побудови та захисту. Зростання інтенсивності кібератак, еволюція шкідливого програмного забезпечення та вразливості мережевих протоколів роблять питання забезпечення кіберстійкості пріоритетним завданням для організацій будь-якого масштабу. Типові архітектурні рішення, що не враховують сучасних векторів загроз та необхідності централізованого управління, стають «вузьким місцем» у системі безпеки підприємства.

Це зумовлює необхідність проектування захищеного інформаційного середовища, яке базується на перевірених технологіях управління ідентифікацією, надійному мережевому обладнанні та ешелонованій системі захисту. Використання служби каталогів Active Directory у поєднанні з грамотно спроектованою мережевою топологією дозволяє забезпечити необхідний рівень керованості, масштабованості та конфіденційності даних.

Мета і завдання дослідження. Метою роботи є підвищення рівня інформаційної безпеки та ефективності управління корпоративною мережею шляхом розробки та практичної реалізації захищеної архітектури інформаційного середовища підприємства.

Для досягнення мети поставлені наступні завдання:

1. Проаналізувати концептуальні засади побудови IT-інфраструктури, розглянувши апаратні, програмні складові та моделі розгортання.

2. Дослідити функціональні можливості Active Directory як фундаменту централізованого управління та механізми забезпечення її безпеки.

3. Провести аналіз вразливостей мережевих протоколів та актуальних векторів атак.

4. Обґрунтувати вибір активного мережевого обладнання для рівнів ядра, розподілу та доступу.

5. Розробити ієрархічну топологію мережі та план IP-адресації з використанням протоколу динамічної маршрутизації OSPF.

6. Виконати практичну імплементацію системи: налаштувати мережеве обладнання Cisco, розгорнути контролери домену та верифікувати працездатність політик безпеки.

Об’єкт дослідження – процеси побудови та захисту корпоративних інформаційно-телекомунікаційних мереж.

Предмет дослідження – методи, засоби та технології організації безпечного інформаційного середовища на базі Active Directory та обладнання Cisco.

Методи дослідження. У роботі використано методи системного аналізу для проектування архітектури, методи моделювання мережевих процесів, а також емпіричні методи при налаштуванні та тестуванні програмно-апаратних комплексів.

Практичне значення. Запропоноване архітектурне рішення та алгоритми налаштування дозволяють розгорнути відмовостійку корпоративну мережу з високим рівнем захисту від внутрішніх та зовнішніх загроз, що мінімізує ризики простою бізнесу та витоку конфіденційної інформації.

1 КОНЦЕПТУАЛЬНІ ЗАСАДИ ПОБУДОВИ БЕЗПЕЧНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА

1.1 Сутність, структура та складові елементи корпоративної інформаційно-технологічної інфраструктури

Під поняттям інформаційно-технологічної інфраструктури (IT-інфраструктури) слід розуміти складну, багатокомпонентну архітектуру, яка інтегрує в єдине ціле обчислювальні потужності, програмні комплекси, мережеві сервіси та різноманітні інформаційні системи. Головним призначенням цього комплексу є гарантування стабільної операційної діяльності, забезпечення ефективної комунікації між підрозділами та створення умов для технологічного розвитку інструментарію компанії. До переліку критично важливих інструментів, що функціонують на базі цієї інфраструктури, належать корпоративні веб-ресурси, системи планування ресурсів підприємства (ERP) та управління взаємовідносинами з клієнтами (CRM), бази даних, технології віддаленого доступу до робочих місць, а також сервісні платформи для підтримки користувачів. [3]

У сучасних ринкових умовах ефективне ведення бізнесу стає неможливим без надійного функціонування зазначених інструментів, тому процеси проектування, впровадження та технічної підтримки IT-інфраструктури, рис.1.1, трансформуються з допоміжних функцій у ключові стратегічні пріоритети будь-якої організації. IT-інфраструктура перестає бути лише технічним фундаментом для життєдіяльності підприємства, набуваючи статусу стратегічного активу, який безпосередньо впливає на конкурентоспроможність, стимулює інноваційні процеси та забезпечує масштабування бізнесу. [4]

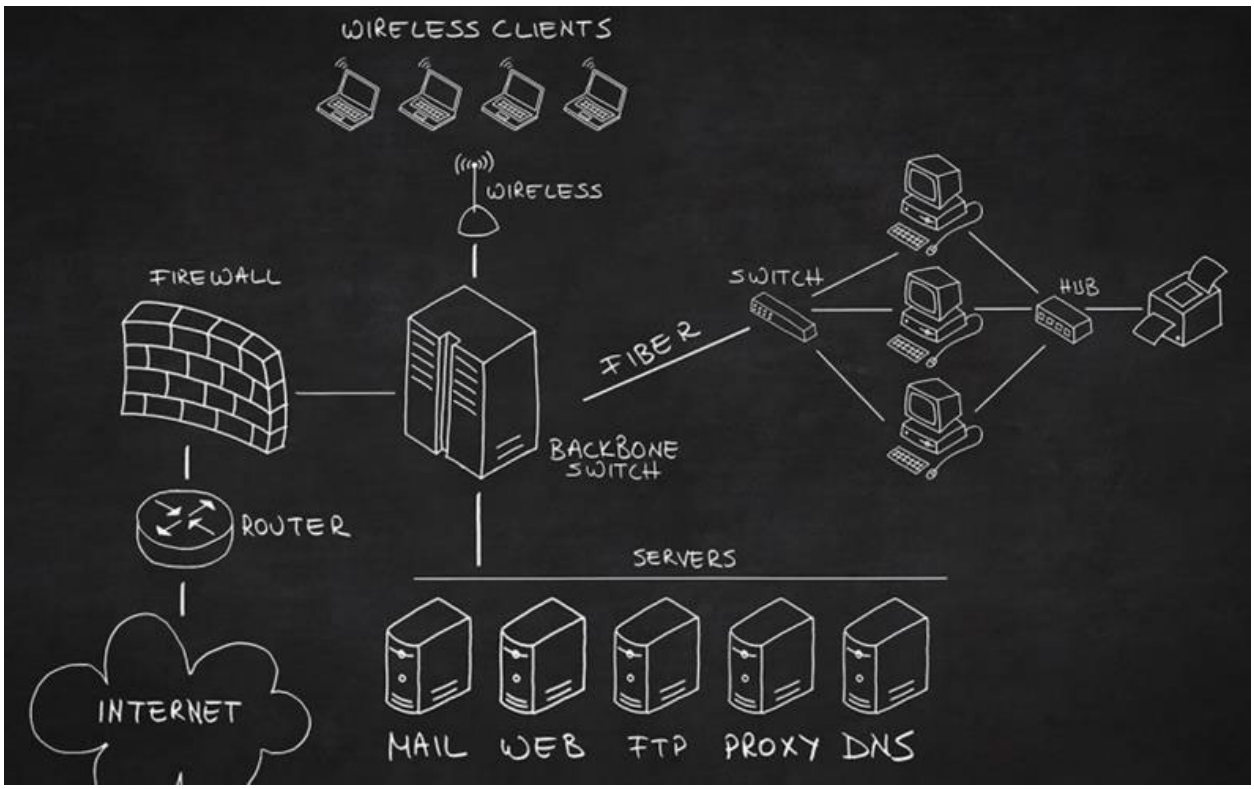


Рисунок 1.1 – Узагальнена архітектурна схема корпоративної IT-інфраструктури

Структурно IT-інфраструктуру доцільно класифікувати за трьома фундаментальними напрямками, кожен з яких відіграє унікальну роль у загальній екосистемі.

Першим базовим компонентом є апаратна складова, яка формує фізичний рівень інфраструктури. Вона представлена сукупністю технічного обладнання, необхідного для розгортання та експлуатації інформаційних систем і сервісів підприємства. Це обладнання виконує функції введення, обробки, передачі та зберігання даних, створюючи матеріальну основу для цифрових процесів. До складу апаратної частини входять персональні обчислювальні пристрої користувачів та потужні сервери, що забезпечують виконання ресурсомістких завдань. Невід'ємним елементом є активне мережеве обладнання, зокрема маршрутизатори, комутатори та апаратні брандмауери, які відповідають за передачу даних та захист периметра мережі. Окрім цього, стабільність роботи забезпечується джерелами безперебійного живлення, а фізична безпека контролюється системами відеоспостереження.

Важливу роль відіграють підсистеми зберігання даних, які включають фізичні сервери, дискові масиви та спеціалізовані апаратні засоби для резервного копіювання інформації. Також до апаратної частини відносять устаткування для підтримки технологій віртуалізації, що дозволяє запускати віртуальні машини та контейнери, а також фізичні ресурси, задіяні в інфраструктурі хмарних технологій, доступ до яких здійснюється через глобальну мережу Інтернет.

Другим ключовим компонентом є програмна складова, що являє собою сукупність програмного забезпечення, яке керує апаратними ресурсами та забезпечує логіку функціонування інформаційних систем. Цей рівень охоплює широкий спектр платформ та додатків, що реалізують конкретні бізнес-завдання. Фундаментом програмної частини виступають операційні системи, поверх яких розгортаються інші рішення. Важливе місце займають системи віртуалізації, що включають гіпервізори та засоби оркестрації контейнерів, дозволяючи оптимізувати використання апаратних ресурсів. Управління даними здійснюється за допомогою систем управління базами даних (СУБД). Критично важливим сегментом є програмні засоби безпеки, до яких належать антивірусні комплекси, антишпигунське ПЗ та програмні фаєрволи. Для автоматизації бізнес-процесів використовуються корпоративні системи класу ERP для планування ресурсів та CRM для менеджменту клієнтських відносин [5], а також спеціалізоване ПЗ для організації віддаленої роботи персоналу. Ефективна робота інфраструктури неможлива без систем моніторингу та управління ресурсами, які дозволяють адміністраторам відстежувати стан мережі та обладнання. Крім того, програмна частина включає офісні пакети, спеціалізовані галузеві додатки, системи ідентифікації та аутентифікації користувачів, а також програмні компоненти хмарної інфраструктури, що забезпечують роботу віртуальних серверів, обчислювальних ресурсів та сервісів хмарного резервного копіювання [6].

Третім інтегруючим компонентом виступає центр обробки даних (ЦОД) або дата-центр. Це спеціалізований інженерно-технічний комплекс,

призначений для централізованого розміщення, обробки та зберігання великих обсягів інформації, а також для забезпечення безперебійної роботи серверного та комунікаційного обладнання. Основною метою функціонування дата-центру є створення максимально надійного та безпечного середовища для експлуатації критично важливих елементів ІТ-інфраструктури.

ЦОД виступає не просто як фізичне приміщення для розміщення апаратури, а як складна екосистема, що гарантує життєздатність техніки. Підприємство може обрати стратегію побудови власного локального дата-центру або скористатися послугами оренди потужностей у професійних провайдерів (колокейшн). Незалежно від форми власності, повноцінний ЦОД повинен бути оснащений рядом інженерних підсистем. Насамперед це системи безперебійного та гарантованого електропостачання, які включають резервні введення, дизель-генератори та альтернативні канали живлення. Обов’язковою є наявність систем диспетчеризації та цілодобового моніторингу параметрів середовища. Фізична безпека об’єкта забезпечується комплексом заходів, що включає автоматичні системи газового або порошкового пожежогасіння, мережу камер відеоспостереження та суворі системи контролю і управління доступом (СКУД). Для запобігання перегріву обладнання використовуються промислові системи прецизійного кондиціонування та клімат-контролю. Комунікаційна складова ЦОД базується на розгалуженій мережевій інфраструктурі та структурованій кабельній системі, а цілісність інформації гарантується спеціалізованими системами захисту даних.

Сучасна практика побудови інформаційних систем виділяє три фундаментальні підходи до організації обчислювального середовища, а саме: серверну, хмарну та гібридну моделі. Розмежування цих категорій базується на відмінностях у принципах архітектурної побудови, методології управління ресурсами та способах доступу до даних. Кожен із цих типів має унікальні технологічні характеристики, які визначають специфіку їх застосування в бізнес-процесах.

Першим класичним типом є серверна інфраструктура, що базується на експлуатації виділених фізичних або віртуалізованих серверів, які забезпечують функціонування внутрішньої корпоративної мережі. У такій моделі обробка обчислювальних запитів відбувається централізовано. Існує поширений стереотип, що серверна інфраструктура обов'язково є локальною (On-premise), тобто фізично розміщеною в офісних приміщеннях компанії, тоді як хмарні рішення асоціюються виключно з віддаленими дата-центрами провайдерів. Проте такий погляд є спрощеним, оскільки серверну архітектуру також можна реалізувати шляхом оренди обладнання у спеціалізованих постачальників послуг (Colocation) та розміщення його у професійних центрах обробки даних [7]. Ключовим тут є не географічне розташування, а принцип виділення ресурсів, що ілюструє рис. 1.2.

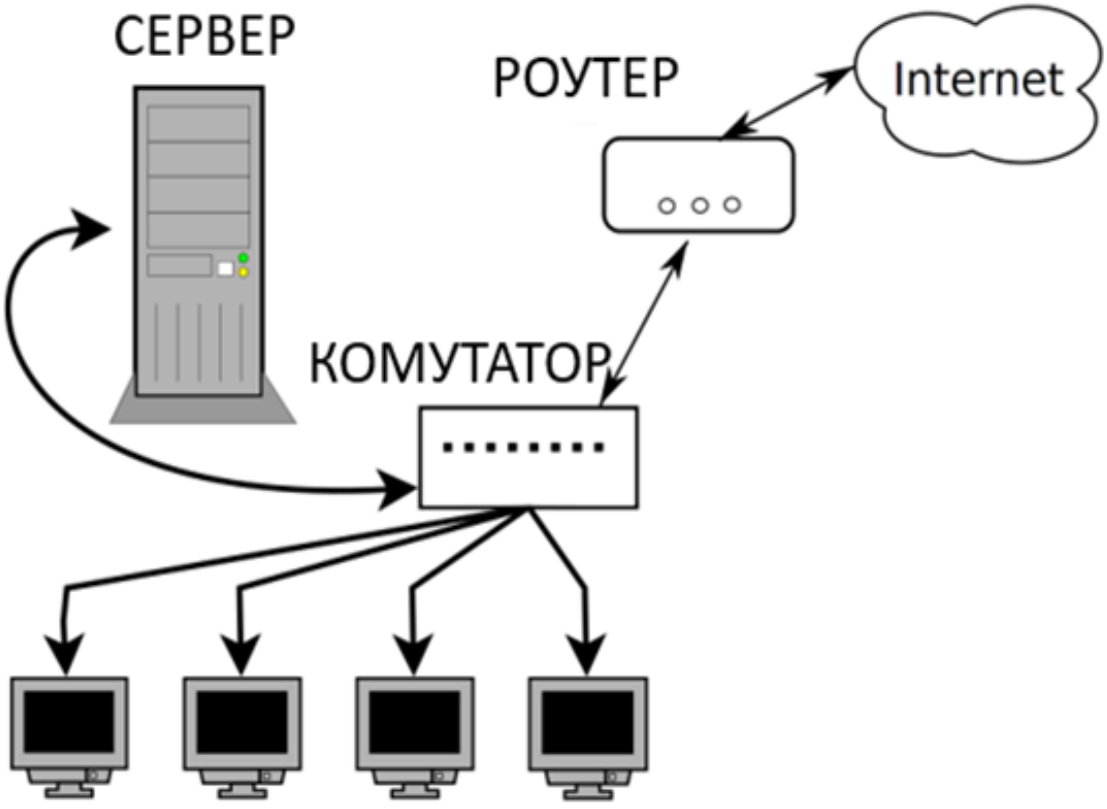


Рисунок 1.2 – Структурна модель традиційної серверної інфраструктури

Характерною рисою традиційної серверної архітектури є робота користувача з чітко визначеними потужностями конкретних машин. У цьому

контексті базовою робочою одиницею часто виступає віртуальний приватний сервер (VPS), який представляє собою ізольований програмний сегмент фізичного сервера. Специфіка VPS полягає у фіксованості виділених ресурсів: кожен такий сервер має жорстко встановлену конфігурацію, що включає певну кількість процесорних ядер, фіксований обсяг оперативної пам'яті та дискового простору. Такий підхід дозволяє ефективно розподіляти наявні фізичні потужності між різними завданнями, однак він має певні обмеження щодо гнучкості масштабування.

Другим типом є хмарна інфраструктура, яка докорінно змінює підхід до споживання IT-послуг, надаючи доступ до ресурсів через глобальну мережу Інтернет. Фундаментальним принципом побудови хмари є абстрагування та об'єднання всіх серверних потужностей у єдиний логічний пул. На відміну від класичної схеми, де ресурси прив'язані до конкретного "заліза", у хмарному середовищі віртуальні сервери, сховища даних та інші сервіси формуються з загального масиву доступних потужностей всієї системи. Ця архітектурна особливість забезпечує високий рівень гнучкості: віртуальна машина у хмарі не залежить від фізичного стану окремого сервера, а її конфігурацію можна динамічно змінювати в будь-який момент часу відповідно до поточних потреб, що відображено на рис. 1.3.

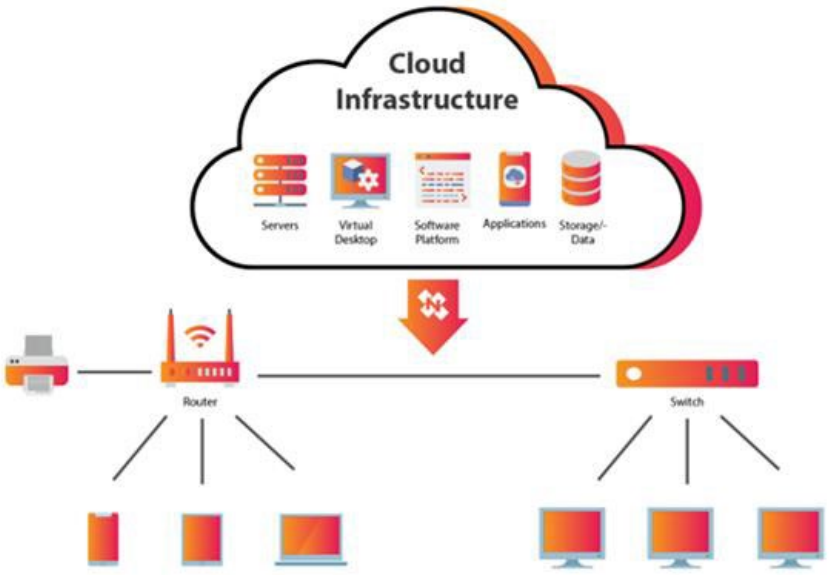


Рисунок 1.3 – Концептуальна схема хмарного середовища обробки даних

Окрім гнучкості виділення ресурсів, критично важливою перевагою хмарної архітектури є високий ступінь автоматизації процесів управління та моніторингу. Завдяки централізованим системам оркестрації, розподіл навантаження, оптимізація роботи віртуальних машин та реагування на пікові запити відбуваються в автоматичному режимі без необхідності ручного втручання адміністраторів. Це дозволяє значно економити часові та людські ресурси, а також гарантує стабільність, надійність та високу швидкість обробки запитів від додатків та користувачів.

Третім, найбільш компромісним варіантом, є гібридна IT-інфраструктура, яка представляє собою конвергентне рішення, що поєднує переваги серверного та хмарного підходів. Логіка побудови такої системи полягає у створенні єдиного інтегрованого середовища, яке дозволяє підприємству гнучко маневрувати між різними типами платформ. Гібридна модель передбачає, що частина критично важливих даних та процесів залишається на локальних серверах або у приватному хмарному сегменті, тоді як інші сервіси виносяться у публічні хмари. Архітектура такої системи може бути реалізована як комбінація публічної та приватної хмар, або як поєднання традиційного серверного обладнання з хмарними сервісами, як показано на рис. 1.4.



Рисунок 1.4 – Архітектура гібридної інформаційної системи

Впровадження гібридної архітектури є стратегічним кроком, що дозволяє бізнесу використовувати сильні сторони обох технологічних підходів

залежно від специфіки конкретних завдань. Наприклад, процеси, що характеризуються стабільним, передбачуваним навантаженням та високими вимогами до безпеки даних, доцільно розміщувати у власній серверній інфраструктурі, що гарантує повний контроль та надійність. Водночас, завдання, які потребують швидкого масштабування, тестування нових продуктів або обробки пікових навантажень, ефективніше переносити у хмарні середовища. Такий розподіл дозволяє оптимізувати операційні витрати та забезпечити максимальну ефективність функціонування IT-ландшафту компанії.

Підсумовуючи вищевикладене, можна стверджувати, що кожна з моделей має свою чітку нішу: серверна інфраструктура фокусується на стабільності та внутрішньому контролі, хмарна — забезпечує безпрецедентну гнучкість та доступність, а гібридна — дозволяє знайти оптимальний баланс, комбінуючи ці характеристики відповідно до унікальних вимог та умов діяльності підприємства.

У реаліях сучасного цифрового простору питання забезпечення кіберстійкості IT-інфраструктури трансформувалося з технічної необхідності у пріоритетну бізнес-стратегію. Це твердження є аксіоматичним для організацій будь-якого масштабу, оскільки зловмисники не обмежують свої цілі лише великими корпораціями. Навпаки, представники малого та середнього бізнесу часто стають об'єктами атак частіше через хибне відчуття безпеки та менші бюджети на захист, що робить їх "легкою здобиччю" для кіберзлочинців. Важливість превентивних заходів стає очевидною, якщо проаналізувати рутинні процеси адміністрування мережі та потенційні руйнівні наслідки інцидентів, описані в спеціалізованій літературі [8].

Надання доступу до цифрових активів є фундаментом ефективності підприємства, проте саме цей процес відкриває двері для широкого спектру ризиків. Аналіз поточної ситуації дозволяє виділити критичні загрози, серед яких домінують: фізичне та моральне старіння апаратної частини, використання неактуальних версій програмного забезпечення та операційних

систем, відсутність належного захисту мережевого периметра, вплив людського фактора через соціальну інженерію, а також ігнорування необхідності постійного моніторингу подій безпеки.

Використання обладнання, термін експлуатації якого вичерпано, створює ланцюгову реакцію негативних наслідків для всієї інфраструктури. Це проявляється не лише у зниженні швидкодії критичних бізнес-додатків, але й у неможливості імплементації сучасних протоколів безпеки, які не підтримуються старим "залізом". Для нівелювання цих ризиків критично важливим є проведення глибокого IT-аудиту, метою якого є інвентаризація активів та виявлення вузьких місць. На основі отриманих даних розробляється план модернізації, що включає заміну фізичних компонентів або, у специфічних випадках, розробку спеціалізованого програмного забезпечення, адаптованого під унікальні потреби компанії та вимоги безпеки. Такий підхід забезпечує підтримання апаратного фундаменту в актуальному стані, що є передумовою стабільності сервісів.

Застарілі програмні комплекси та операційні системи, підтримка яких припинена розробниками, є одним з основних каналів проникнення загроз. Наслідки їх використання варіюються від нестабільності мережевих з'єднань і перевантаження каналів зв'язку до повної нездатності інфраструктури обробляти сучасні типи трафіку.

Ефективною стратегією вирішення цієї проблеми є перехід від локальних рішень до використання хмарних технологій або гібридних моделей. Міграція у хмару дозволяє оптимізувати розподіл навантаження, звільнити фізичний простір в офісі від серверних стійок та автоматично отримати вищий рівень захисту, який забезпечується провайдером хмарних послуг. Крім того, це гарантує доступність корпоративних ресурсів з будь-якої точки світу, що перетворює хмарні технології з модного тренду на необхідний інструмент виживання та розвитку бізнесу.

Ігнорування засобів мережевого захисту неминуче призводить до втрати контролю над трафіком, несанкціонованих вторгнень та витоку

конфіденційних даних. Для побудови надійної оборони необхідна реалізація концепції ешелонованого захисту, де усунення однієї вразливості не повинно залишати відкритими інші вектори атак. Комплексна система безпеки передбачає впровадження ряду взаємопов'язаних заходів.

Насамперед, це розгортання брандмауерів нового покоління та систем виявлення/запобігання вторгненням (IDS/IPS), що дозволяють аналізувати трафік у реальному часі. Паралельно має забезпечуватися безперервне оновлення баз сигнатур антивірусного та антишпигунського ПЗ для блокування шкідливого коду. Критичним елементом є захист каналів передачі даних шляхом наскрізного шифрування та використання термінальних сервісів, що мінімізує ризик перехоплення інформації. Окрему увагу слід приділяти управлінню доступом: впровадження суворих політик та багатофакторної автентифікації (MFA) є обов'язковим стандартом для верифікації користувачів.

Людський фактор залишається найслабшою ланкою в системі інформаційної безпеки. Недбалість або необізнаність персоналу часто використовуються зловмисниками в атаках із застосуванням методів соціальної інженерії. Це може призвести до розголошення облікових даних, помилок в обробці інформації або навіть до фізичного допуску сторонніх осіб у захищені приміщення. Профілактика таких загроз вимагає системного підходу до навчання співробітників. Регулярні тренінги з кібергігієни, симуляції фішингових атак та формування культури безпеки в колективі дозволяють перетворити персонал з потенційної вразливості на першу лінію оборони.

Відсутність інструментів для спостереження за станом IT-середовища робить адміністраторів "сліпими" до подій, що відбуваються в мережі. Це призводить до неможливості своєчасного виявлення аномалій, затримок у реагуванні на інциденти та тривалого відновлення після збоїв. Вирішенням є впровадження професійних систем моніторингу на базі таких платформ, як Zabbix, Microsoft SCOM або Dell Foglight.

Ці системи забезпечують повну візуалізацію процесів, дозволяють аналізувати тренди навантаження та миттєво сповіщати відповідальних осіб про підозрілу активність. В умовах зростання інтенсивності кібератак, наявність розвиненої системи моніторингу є критичною умовою для швидкої локалізації загроз та мінімізації збитків.

Підсумовуючи, слід зазначити, що сукупність факторів — від застарілого обладнання до відсутності моніторингу — формує поле ризиків, яке може паралізувати діяльність підприємства. Забезпечення стабільності бізнесу вимагає постійної модернізації IT-інфраструктури, регулярних аудитів безпеки та інвестицій у сучасні технології захисту.

1.2 Архітектурні засади організації мережевого середовища на основі Active Directory

Фундаментом для побудови керованої та масштабованої корпоративної мережі в екосистемі Microsoft виступає Active Directory (AD). Це не просто служба каталогів, а комплексна розподілена база даних, що забезпечує єдину точку реєстрації та авторизації в системі. Технологія надає системним адміністраторам потужний інструментарій для централізованого менеджменту мережевими ресурсами. Ключовим механізмом управління виступають групові політики (GPO), які дозволяють автоматизувати налаштування робочого середовища користувачів, масово розгортати програмне забезпечення, керувати оновленнями безпеки та конфігурувати параметри операційних систем на всіх підключених пристроях.

Служба каталогів виступає критично важливим елементом IT-інфраструктури, оскільки саме вона зберігає інформацію про облікові записи, комп'ютери та периферійне обладнання, гарантуючи при цьому базовий рівень інформаційної безпеки [9]. Масштабованість системи дозволяє їй ефективно

функціонувати як у невеликих офісах, так і в транснаціональних корпораціях з мільйонами об'єктів.

Архітектура Active Directory базується на суворій ієрархічній моделі, що складається з кількох логічних рівнів: об'єктів, контейнерів, доменів, дерев та лісів. Базовою неподільною одиницею структури є об'єкт (користувач, комп'ютер, принтер). Для ефективного адміністрування ці об'єкти групуються у спеціалізовані контейнери — організаційні одиниці (Organizational Units, OU).

Організаційні одиниці відіграють роль логічних папок, що дозволяють структурувати об'єкти всередині домену відповідно до адміністративних потреб, наприклад, за департаментами або географічним розташуванням. Важливою особливістю OU є можливість вкладеності, що дозволяє створювати багаторівневі ієрархії делегування повноважень. Окрім OU, для управління доступом використовуються групи, які бувають двох основних типів: групи безпеки, що застосовуються для надання дозволів на ресурси, та групи розсилки, призначені виключно для електронної пошти.

На вищому рівні абстракції знаходиться домен — логічний сегмент мережі з унікальним іменем (наприклад, contoso.com) та єдиною базою даних безпеки. Домени можуть об'єднуватися у дерева — структури, що мають спільний простір імен (DNS-суфікс) та ієрархічний зв'язок "батько-нащадок", як-от sales.contoso.com та marketing.contoso.com [10]. Найвищим рівнем організації є ліс, який представляє собою сукупність одного або декількох дерев, що поділяють спільну схему каталогу, глобальний каталог та конфігурацію, навіть якщо вони мають різні простори імен (наприклад, contoso.com та adatum.com). Візуалізацію цієї вкладеної структури наведено на рис. 1.5.

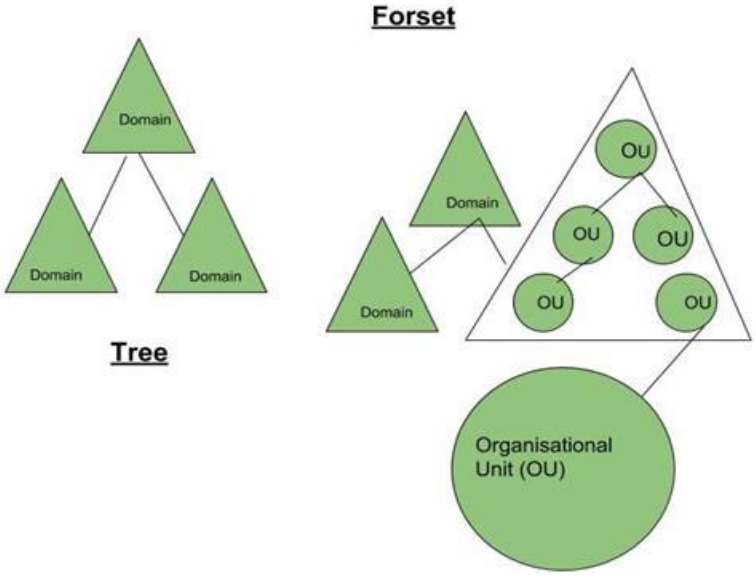


Рисунок 1.5 – Ієрархічна модель організації об’єктів у службі каталогів

Кожна інсталяція Active Directory за замовчуванням створює щонайменше один ліс. Проте залежно від бізнес-вимог, організація може експлуатувати кілька лісів, що часто трапляється внаслідок процесів злиття та поглинання компаній. Вибір архітектури є стратегічним рішенням. Концепція єдиного лісу вважається найбільш економічно вигідною та простою в адмініструванні. Вона забезпечує безшовну взаємодію між користувачами та ресурсами, оскільки всі об'єкти знаходяться в межах одного периметра безпеки і доступні через глобальний каталог.

У той же час, існують сценарії, коли використання декількох лісів є необхідним. Це стосується випадків, коли потрібна сувора ізоляція даних, автономність управління або коли різні частини організації мають несумісні вимоги до схеми каталогу. Однак слід розуміти, що саме по собі збільшення кількості лісів не гарантує вищого рівня безпеки без належного налаштування довірчих відносин та моніторингу. Найкращі практики (Best Practices) рекомендують для кожного лісу створювати окрему команду адміністраторів для уникнення конфлікту інтересів та забезпечення чіткого розмежування відповідальності. Приклад складної структури організації показано на рис. 1.6.

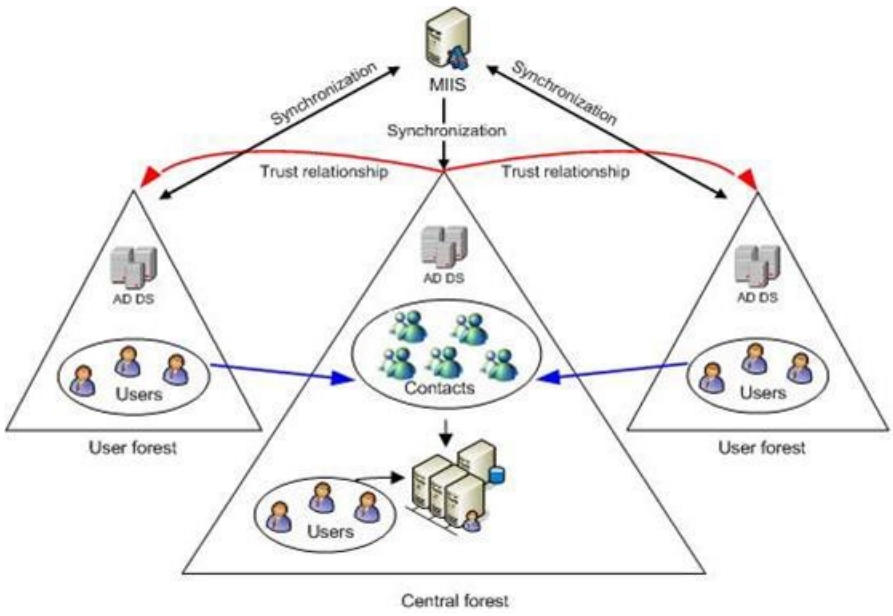


Рисунок 1.6 – Топологія корпоративної мережі з мультилісовою архітектурою

Зазвичай мультилісова архітектура притаманна лише найбільшим корпораціям зі складною структурою власності. Переважна більшість підприємств обмежується одним лісом, всередині якого створюються дочірні домени. Кожен такий домен має власну базу даних, унікальні політики безпеки та набір об'єктів GPO, що дозволяє балансувати між централізацією та локальною автономією.

Впровадження Active Directory надає організації низку критичних переваг. Насамперед це централізоване управління, що дозволяє контролювати всю інфраструктуру з єдиної консолі. По-друге, це високий рівень безпеки, який досягається завдяки надійним протоколам автентифікації (Kerberos) та розмежованій авторизації доступу до ресурсів. По-третє, система забезпечує виняткову масштабованість, адаптуючись до зростання компанії без втрати продуктивності. І, нарешті, гнучкість архітектури дозволяє реалізувати будь-яку топологію мережі, що відповідає унікальним бізнес-процесам підприємства.

1.3 Функціональний інструментарій Active Directory у системі кібербезпеки підприємства

Забезпечення захищеності Active Directory (AD) виходить далеко за межі простого адміністрування облікових записів; це комплексний набір стратегій та технічних заходів, спрямованих на гарантування цілісності всієї IT-екосистеми Microsoft. Оскільки AD виступає центральним вузлом для ідентифікації користувачів та управління ресурсами, її компрометація рівнозначна втраті контролю над усією мережею. Тому захист служби каталогів є фундаментальною умовою для реалізації тріади інформаційної безпеки: конфіденційності, цілісності та доступності даних. Ефективна стратегія захисту AD дозволяє не лише запобігати несанкціонованому доступу, але й забезпечує стійкість бізнес-процесів до зовнішніх та внутрішніх загроз [11].

Наріжним каменем безпеки Active Directory є суворий контроль над адміністративними обліковими записами, які надають необмежені права в системі. Оскільки такі акаунти є пріоритетною ціллю для зловмисників, необхідно мінімізувати їх кількість, надаючи привілеї лише тим співробітникам, чиї посадові обов'язки цього вимагають. Критично важливим є впровадження багатофакторної автентифікації (MFA), яка створює додатковий бар'єр захисту, роблячи викрадення пароля недостатнім для проникнення в систему. Парольна політика для таких облікових записів має вимагати використання складних, унікальних комбінацій, що стійкі до методів повного перебору (brute-force).

Паралельно з захистом адміністраторів, необхідно імплементувати принцип найменших привілеїв для всіх користувачів мережі. Суть цього підходу полягає в тому, що суб'єкт доступу повинен володіти лише тим мінімальним набором прав, який необхідний для виконання поточних завдань. Адміністраторам слід проводити регулярний аудит прав доступу,

переглядаючи та відкликаючи надлишкові дозволи. Це дозволяє значно звузити вектори потенційних атак та знизити ризики, пов'язані зі зловживанням повноваженнями або помилками персоналу [12].

Надійність функціонування IT-інфраструктури неможлива без налагодженої системи резервного копіювання бази даних Active Directory. Наявність актуальних бекапів є гарантією швидкого відновлення працездатності підприємства у випадку критичних збоїв, дії вірусів-шифрувальників або цілеспрямованих атак. Однак саме лише створення копій є недостатнім; процедура відновлення повинна регулярно тестуватися на практиці, щоб підтвердити цілісність даних та ефективність алгоритмів реставрації системи.

Невід'ємною складовою захисту є впровадження глибокого аудиту та безперервного моніторингу подій безпеки. Налаштування детальних журналів подій дозволяє фіксувати всі критичні зміни в конфігурації та спроби доступу до ресурсів. Використання спеціалізованих SIEM-систем для аналізу логів у режимі реального часу надає можливість оперативно виявляти аномальну поведінку, ідентифікувати підозрілі дії та миттєво реагувати на інциденти ще до того, як вони завдадуть значної шкоди організації [12].

Особливу увагу слід приділяти захисту контролерів домену, які є "серцем" Active Directory. Заходи безпеки повинні включати як фізичне обмеження доступу до серверів, так і програмний захист, зокрема використання сучасних антивірусних рішень та регулярне встановлення оновлень безпеки (патчів). Своєчасна інсталяція виправлень для операційної системи та прикладного ПЗ дозволяє усунути відомі вразливості, які можуть бути використані експлойтами.

Комунікація між компонентами мережі також потребує захисту. Для запобігання перехопленню даних та атакам типу «людина посередині» (MitM) необхідно налаштувати шифровані канали зв'язку та відмовитися від застарілих протоколів на користь захищених стандартів, таких як Kerberos. Додатковим рівнем оборони виступає сегментація мережі та використання

міжмережевих екранів (брандмауерів), що дозволяє ізолювати критичні сегменти інфраструктури, контролювати трафік та локалізувати можливі загрози, не даючи їм поширюватися по всій мережі [12].

Сучасний ландшафт загроз вимагає захисту від складних атак на механізми аутентифікації, таких як "Pass-the-Hash" або "Pass-the-Ticket", що дозволяють зловмисникам обходити парольний захист. Для протидії цим методам використовуються такі інструменти, як Credential Guard, білі списки IP-адрес та поведінковий аналіз активності користувачів.

Важливу роль відіграє централізоване управління налаштуваннями через групові політики (GPO). Вони дозволяють автоматично застосовувати стандарти безпеки до всіх кінцевих точок, керувати параметрами паролів, блокуванням облікових записів та обмеженням запуску програм. Крім того, організаційні заходи повинні включати поділ адміністративних обов'язків (Segregation of Duties), що унеможливлює концентрацію критичних повноважень в руках однієї особи. Це, разом із механізмами контролю доступу до конфіденційних даних та регулярними перевірками персоналу, допомагає ефективно протидіяти внутрішнім загрозам та інсайдерським витокам інформації [12].

Автентифікація виступає первинним бар'єром у системі інформаційної безпеки, оскільки саме цей процес відповідає за верифікацію особи користувача або пристрою перед наданням доступу до корпоративних ресурсів. У сучасному цифровому середовищі, де кіберзагрози постійно еволюціонують, покладання виключно на парольний захист є недостатнім. Саме тому стратегічним стандартом стало впровадження багатофакторної аутентифікації (MFA), особливо в середовищах на базі Active Directory, де концентрується критична інформація про інфраструктуру підприємства.

Концепція MFA базується на принципі «глибокого захисту», вимагаючи для підтвердження ідентичності використання мінімум двох незалежних категорій доказів. Найчастіше це комбінація фактора знання (наприклад, пароль) та фактора володіння (апаратний токен, смартфон з додатком-

автентифікатором) або фактора властивості (біометрія). Такий підхід створює додатковий ешелон оборони: навіть у випадку успішного фішингу або підбору пароля зловмисником, доступ до системи залишається заблокованим без другого компонента. Це не лише мінімізує ризики несанкціонованого проникнення, але й забезпечує відповідність суворим регуляторним вимогам щодо захисту персональних даних.

Переваги використання MFA є беззаперечними. По-перше, значно ускладнюється реалізація атак, спрямованих на перехоплення облікових даних, оскільки сам по собі пароль втрачає свою цінність без фізичного доступу до другого фактора. По-друге, система стає стійкішою до компрометації баз даних паролів на сторонніх ресурсах. По-третє, використання різнорідних факторів перевірки створює надійніший механізм довіри. Впровадження MFA перетворилося з рекомендації на категоричну необхідність для будь-якої організації, що прагне захистити свої цифрові активи.

Групові політики (GPO) представляють собою фундаментальний механізм управління в екосистемі Windows, що дозволяє адміністраторам автоматизувати налаштування та забезпечувати дотримання стандартів безпеки в масштабах всього підприємства. GPO — це набір правил, що регулюють поведінку операційної системи, доступ до функцій та параметри безпеки для користувачів і комп'ютерів у домені Active Directory [13].

При ініціалізації нового домену система автоматично генерує два базові об'єкти політик. Перший — це "Default Domain Policy", який визначає глобальні параметри безпеки для всіх учасників домену, зокрема вимоги до складності та зміни паролів, правила блокування облікових записів при невдалих спробах входу та налаштування протоколу Kerberos. Другий — "Default Domain Controllers Policy", що фокусується на специфічних налаштуваннях безпеки та аудиту виключно для контролерів домену, які є найбільш критичними вузлами мережі.

Для того щоб політики почали діяти, вони повинні бути прив'язані (лінковані) до відповідних контейнерів Active Directory: сайтів, доменів або організаційних одиниць (OU). Цей механізм забезпечує високу гнучкість: наприклад, можна заборонити використання USB-накопичувачів лише для відділу бухгалтерії, не обмежуючи при цьому IT-департамент. Важливою характеристикою GPO є принцип успадкування: політики, застосовані до батьківського контейнера, автоматично розповсюджуються на всі вкладені підрозділи та об'єкти, що значно спрощує адміністрування великих структур.

В умовах складної ієрархії політик неминуче виникають конфлікти налаштувань. Система вирішує їх шляхом чітко визначеного пріоритету обробки (LSDOU): спочатку застосовуються локальні політики комп'ютера, потім політики сайту, далі домену і, нарешті, організаційних одиниць. При цьому налаштування, застосовані останніми (на рівні OU), мають найвищий пріоритет і можуть перезаписувати попередні значення.

Адміністратори мають інструменти для модифікації стандартної поведінки успадкування. Зокрема, функція "Enforced" (Примусово) дозволяє надати політиці найвищий пріоритет, ігноруючи будь-які конфлікти на нижчих рівнях, а опція "Block Inheritance" (Блокування успадкування) дозволяє захистити певний контейнер від впливу політик вищого рівня. Також можливе тимчасове відключення зв'язку політики без її видалення, що корисно при діагностиці проблем.

Стабільність роботи Active Directory критично залежить від надійності системи резервного копіювання та відновлення (Disaster Recovery). Для цього використовуються як вбудовані засоби, на кшталт Windows Server Backup, так і спеціалізовані рішення сторонніх розробників. Головною метою цих інструментів є створення узгоджених знімків бази даних каталогу, що включають інформацію про об'єкти, їх атрибути, а також системні файли (SYSVOL).

Наявність актуальних резервних копій дозволяє нівелювати наслідки широкого спектру інцидентів: від випадкового видалення окремого

користувача адміністратором до повного виходу з ладу фізичного сервера або масованої вірусної атаки. Стратегія захисту повинна передбачати регулярне створення бекапів та, що ще важливіше, періодичне тестування процедур відновлення. Це може бути гранулярне відновлення окремих атрибутів або повне відновлення лісу AD (Forest Recovery) у катастрофічних сценаріях. Лише комплексний підхід до бекапування гарантує безперервність бізнес-процесів, які залежать від працездатності служби каталогів [14].

1.4 Аналіз вразливостей мережевих протоколів та векторів атак на інфраструктуру

Процес побудови надійної архітектури корпоративної мережі нерозривно пов'язаний із використанням широкого спектру стандартизованих правил та технологій, які гарантують коректний та захищений обмін інформаційними потоками між вузлами. У загальному розумінні всю сукупність мережевих протоколів доцільно класифікувати за функціональним призначенням на три ключові категорії: протоколи, що забезпечують безпосередній обмін даними (комунікаційні), протоколи, призначені для адміністрування та моніторингу стану мережі, а також спеціалізовані протоколи безпеки, що відповідають за криптографічний захист інформації.

Комунікаційні протоколи виступають фундаментом існування будь-якої комп'ютерної мережі, оскільки саме вони формалізують синтаксис, семантику та синхронізацію передачі даних. Без цих стандартизованих правил взаємодія між різнорідним апаратним та програмним забезпеченням була б неможливою. Вони охоплюють механізми адресації, маршрутизації, виявлення помилок та підтвердження доставки пакетів, забезпечуючи функціонування як глобальних телекомунікаційних систем, так і локальних мереж.

Основним стандартом сучасного цифрового світу є стек протоколів TCP/IP, який визначає логіку передачі інформації в Інтернеті та більшості корпоративних інфраструктур. Протокол керування передачею (TCP) відповідає за розбиття даних на окремі сегменти, встановлення надійної сесії між хостами та гарантовану доставку інформації. У свою чергу, Інтернет-протокол (IP) займається адресацією та маршрутизацією цих пакетів через мережу маршрутизаторів та комутаторів до кінцевого одержувача.

Незважаючи на свою поширеність, стек TCP/IP має вроджені вразливості. Однією з найпоширеніших загроз є атака ARP Spoofing (або ARP Poisoning). Суть цього методу полягає в тому, що зловмисник надсилає в локальну мережу фальсифіковані ARP-повідомлення. Це призводить до підміни запису в таблиці маршрутизації жертви, де IP-адреса шлюзу або іншого хоста починає асоціюватися з MAC-адресою зловмисника. У результаті атакуючий отримує можливість перехоплювати трафік, модифікувати пакети або блокувати передачу даних (атака "людина посередині").

Іншим критично важливим елементом є система доменних імен (DNS), яка виконує роль глобальної телефонної книги, перетворюючи людино-читабельні доменні імена на машинні IP-адреси. Оскільки цей протокол спочатку не мав вбудованих механізмів суворої автентифікації джерела даних, він є вразливим до атак типу DNS Spoofing. Зловмисник може впровадити в кеш DNS-сервера фальшиві записи, що призведе до перенаправлення користувачів на шахрайські веб-ресурси, які візуально імітують легітимні сайти, з метою викрадення облікових даних або конфіденційної інформації.

На прикладному рівні також використовуються різноманітні протоколи. Наприклад, HTTP слугує для передачі гіпертексту, однак через відсутність шифрування він дозволяє перехоплювати дані у відкритому вигляді. Для обміну електронною поштою застосовується протокол SMTP, а для передачі файлів — FTP. Варто зазначити, що для адміністрування віддалених систем стандартом де-факто став протокол SSH, який, на відміну від застарілих

аналогів, створює захищений тунель навіть через ненадійні мережі. Для текстових комунікацій у розподілених системах застосовується протокол IRC.

Протоколи управління мережею є критично необхідними для підтримки стабільності, продуктивності та надійності IT-інфраструктури. Вони надають адміністраторам інструменти для діагностики, виявлення "вузьких місць", аналізу пропускної здатності та оперативного реагування на збої. Завдяки цим протоколам реалізуються політики управління ресурсами, що дозволяє оптимізувати роботу різнотипного обладнання.

Найпоширенішим інструментом у цій сфері є протокол SNMP (Simple Network Management Protocol). Він працює за архітектурою "клієнт-сервер", де на мережевих пристроях (маршрутизаторах, принтерах, серверах) працюють спеціальні програми-агенти, які збирають статистику та передають її на центральну станцію управління. SNMP дозволяє не лише зчитувати параметри, але й змінювати конфігурацію пристроїв віддалено.

Однак ранні версії SNMP (зокрема v1 та v2c) мають серйозну вразливість, пов'язану з використанням так званого "community string" — рядка, що виконує роль пароля і передається відкритим текстом. Атака SNMP Community String Guessing полягає у підборі цього рядка зловмисником. Успішна реалізація такої атаки надає повний доступ до інформації про топологію мережі, а в деяких випадках дозволяє змінювати налаштування обладнання, що може призвести до повного паралічу інфраструктури.

Для базової діагностики мережевого рівня використовується протокол керованих повідомлень ICMP. Він відповідає за відправку сервісних повідомлень про помилки (наприклад, про недоступність вузла) та використовується утилітами ping та traceroute для перевірки зв'язності та якості з'єднання.

Окрему групу становлять протоколи безпеки, головним завданням яких є забезпечення конфіденційності, цілісності та автентичності даних під час їх передачі через публічні або незахищені канали зв'язку. Вони використовують складні математичні алгоритми шифрування, що робить перехоплену

інформацію нечитабельною для третіх осіб без відповідних ключів дешифрування. Незважаючи на високий рівень захисту, сервіси, що працюють на базі цих протоколів, часто стають мішенями для DDoS-атак, спрямованих на вичерпання обчислювальних ресурсів серверів, або складних MITM-атак на етапі узгодження ключів.

Серед найпоширеніших рішень слід виділити протокол SSL (та його наступника TLS), який забезпечує встановлення захищеного з'єднання між клієнтом та сервером. Усі дані, що проходять через такий тунель, шифруються, що гарантує захист від прослуховування.

Логічним розвитком веб-технологій стала поява протоколу HTTPS, який є надбудовою HTTP над шифрованим транспортним рівнем SSL/TLS, що стало обов'язковим стандартом для сучасного Інтернету. Для захищеного обміну файлами замість класичного FTP використовується протокол SFTP, який використовує можливості SSH для шифрування команд та даних, а також для надійної автентифікації користувачів [17].

Active Directory (AD), виконуючи функцію централізованої системи управління ідентифікацією та доступом в екосистемі Windows, є критично важливим вузлом корпоративної мережі. Проте саме ця централізація перетворює AD на пріоритетну ціль для зловмисників: контроль над службою каталогів фактично означає контроль над усією інфраструктурою підприємства. Спектр кібератак на AD є надзвичайно широким і варіюється від спроб підбору паролів до складних маніпуляцій з мережевим трафіком та експлуатації архітектурних особливостей системи.

Типовий ланцюжок атаки часто розпочинається з методів соціальної інженерії, зокрема фішингу, метою якого є отримання первинних облікових даних пересічного користувача. Це стає плацдармом для подальшого горизонтального переміщення (lateral movement) по мережі та ескалації привілеїв. Кінцевою метою зловмисників, як правило, є виконання довільного коду, приховане встановлення шкідливого програмного забезпечення, викрадення інтелектуальної власності або повна дестабілізація бізнес-

процесів. Нижче наведено детальний аналіз найбільш поширених векторів атак на інфраструктуру Active Directory.

Однією з найефективніших тактик, яку використовують зловмисники для первинного проникнення в периметр мережі, є атака типу «Password Spraying» або «розпилення паролів». На відміну від класичного брутфорсу (brute-force), де зловмисник намагається підібрати пароль до одного конкретного акаунту шляхом перебору тисяч варіантів, що швидко призводить до блокування облікового запису, техніка «розпилення» діє за інверсним принципом. Атакуючий використовує обмежений набір найпопулярніших паролів (наприклад, "Password123" або "QWERTY") і перевіряє їх на величезній кількості облікових записів одночасно.

Такий підхід дозволяє обходити стандартні політики безпеки, що блокують користувача після певної кількості невдалих спроб входу, оскільки для кожного окремого акаунту генерується лише одна-дві помилки. Успішна компрометація хоча б одного облікового запису надає зловмиснику легітимний доступ до внутрішніх ресурсів, що дозволяє розпочати розвідку та встановлення шкідливого ПЗ. Стратегія захисту від подібних загроз має базуватися на примусовому впровадженні складних парольних політик, використанні списків заборонених паролів та, що найважливіше, імплементації багатофакторної аутентифікації (MFA). Наявність другого фактора перевірки робить викрадення пароля недостатнім для успішної авторизації, створюючи надійний бар'єр навіть у випадку компрометації текстового секрету.

Атака «Pass-the-Hash» (PtH) є класичним прикладом техніки, що дозволяє обходити потребу у знанні відкритого пароля користувача. Механізм цієї атаки базується на особливостях протоколу аутентифікації NTLM, де для підтвердження особи використовується не сам пароль, а його криптографічний зліпок — хеш. Зловмисник, отримавши адміністративний доступ до однієї з робочих станцій (часто через попередні етапи атаки), витягує з оперативної

пам'яті (процес LSASS) збережені хеші паролів користувачів, які раніше входили в систему.

Використовуючи перехоплений хеш, хакер може безпосередньо автентифікуватися на інших серверах та робочих станціях мережі, видаючи себе за легітимного користувача. Це дозволяє здійснювати приховане переміщення по мережі доти, доки не буде знайдено обліковий запис із правами адміністратора домену. Для протидії PtH-атакам необхідно мінімізувати використання застарілого протоколу NTLM, переходячи на більш захищений Kerberos, а також впроваджувати архітектуру безпеки з ізоляцією рівнів (Tier Model), що забороняє адміністраторам домену авторизуватися на ненадійних робочих станціях.

Мережева інфраструктура Active Directory критично залежить від коректної роботи служби DNS, що робить її вразливою до атак типу DNS Spoofing (підробка DNS). Суть загрози полягає в тому, що зловмисник, перебуваючи всередині локальної мережі, втручається в процес розв'язання доменних імен, підміняючи IP-адреси легітимних серверів на адресу власного підконтрольного вузла.

У контексті AD це дозволяє перенаправити запити аутентифікації або трафік оновлень на фальшивий сервер. Як наслідок, зловмисник отримує можливість реалізувати атаку «людина посередині» (MitM), перехоплюючи облікові дані або підміняючи контент, що передається по мережі. Схематичне зображення цього процесу представлено на рис. 1.7.

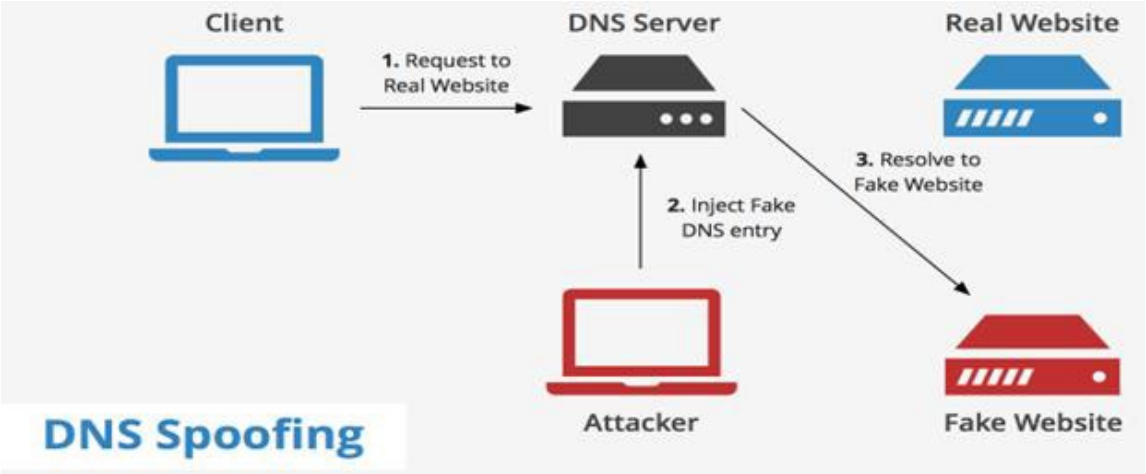


Рисунок 1.7 – Механізм реалізації атаки DNS-спуфінг

Для нівелювання цієї загрози рекомендується використання розширень безпеки DNSSEC, які забезпечують криптографічну перевірку автентичності джерела даних DNS, а також налаштування суворого моніторингу журналів DNS-серверів для виявлення аномальних змін у записах зон.

Об'єкти групової політики (GPO) є потужним інструментом адміністрування, який дозволяє централізовано керувати налаштуваннями тисяч комп'ютерів. Однак, у руках зловмисників GPO перетворюється на зброю масового ураження. Якщо атакуючий отримує права на редагування політик, він може використати цей механізм для миттєвого розповсюдження шкідливого коду (наприклад, програм-вимагачів) на всі комп'ютери домену або для створення прихованих облікових записів адміністраторів (бекдорів).

Небезпека полягає в тому, що дії, виконані через GPO, сприймаються системою як легітимні адміністративні команди. Наприклад, зловмисник може створити завдання планувальника через GPO, яке запускатиме шкідливий скрипт на всіх серверах. Щоб запобігти подібним сценаріям, організаціям необхідно суворо контролювати права доступу до редагування політик, регулярно проводити аудит змін у GPO та використовувати спеціалізовані рішення для моніторингу (наприклад, AGPM), які дозволяють відстежувати версійність політик та вимагають затвердження змін перед їх застосуванням.

Під терміном «мережеві атаки» слід розуміти комплекс навмисних деструктивних дій, метою яких є порушення тріади інформаційної безпеки: конфіденційності, цілісності або доступності даних. Об'єктами таких посягань стають як критичні державні системи та корпоративні мережі, так і персональні пристрої окремих користувачів. Методологія зловмисників постійно еволюціонує, проте базові вектори атак можна систематизувати за принципами їх реалізації та кінцевою метою [15].

Атаки, спрямовані на відмову в обслуговуванні, мають на меті виснаження системних ресурсів цільового вузла, що унеможливлює його використання легітимними користувачами. У класичному варіанті DoS-атаки (Denial of Service) зловмисник генерує надмірну кількість запитів з одного джерела, намагаючись переповнити пропускну здатність каналу або обчислювальні потужності сервера (процесорний час, оперативну пам'ять).

Більш небезпечною та складною для протидії є розподілена атака — DDoS (Distributed Denial of Service). Її ключова відмінність полягає у використанні не одного, а тисяч розподілених пристроїв, об'єднаних у так звані ботнети. Ці мережі складаються із заражених комп'ютерів або IoT-пристроїв («зомбі»), які за командою контрольного центру одночасно надсилають трафік на жертву. Ефект синергії дозволяє вивести з ладу навіть потужні промислові сервери, які не здатні обробити лавиноподібний потік даних. Схематичну різницю між цими підходами наведено на рис. 1.8.

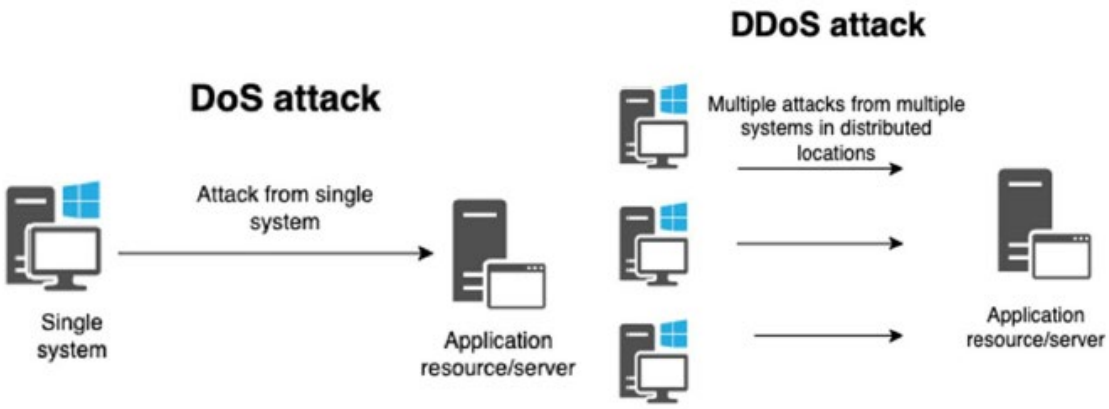


Рисунок 1.8 – Структурна схема реалізації атак на відмову в обслуговуванні: а) одиночний вектор (DoS); б) розподілений вектор (DDoS)

Фішинг є найпоширенішим вектором атак, що експлуатує людський фактор. Це методика соціальної інженерії, спрямована на виманювання автентифікаційних даних, фінансової інформації або персональних відомостей шляхом маскування під довірені джерела.

Найчастіше цей вид шахрайства реалізується через електронну пошту. Зловмисники розсилають листи, що візуально імітують офіційну кореспонденцію від банківських установ, платіжних систем або державних органів. Такі повідомлення містять заклики до термінових дій (наприклад, "підтвердіть вхід" або "оновіть дані") та посилання на шкідливі ресурси або вкладення з вірусним навантаженням. Приклад такої схеми показано на рис. 1.9.

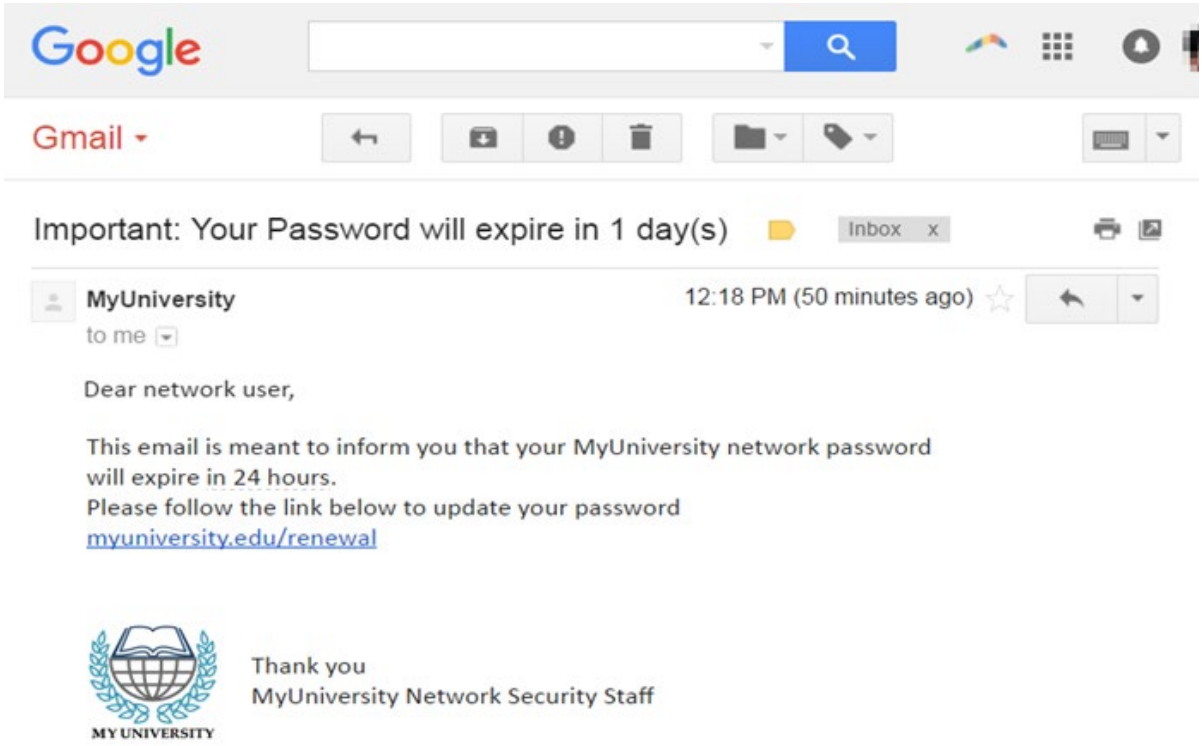


Рисунок 1.9 – Типовий сценарій фішингової атаки з використанням E-mail

Логічним продовженням поштових розсилок є створення сайтів-імітацій (спуфінг веб-ресурсів). Зловмисники розробляють точні візуальні копії сторінок входу популярних сервісів. Коли жертва вводить свої облікові дані на такому ресурсі, вони миттєво передаються хакеру, як це проілюстровано на рис. 1.10.

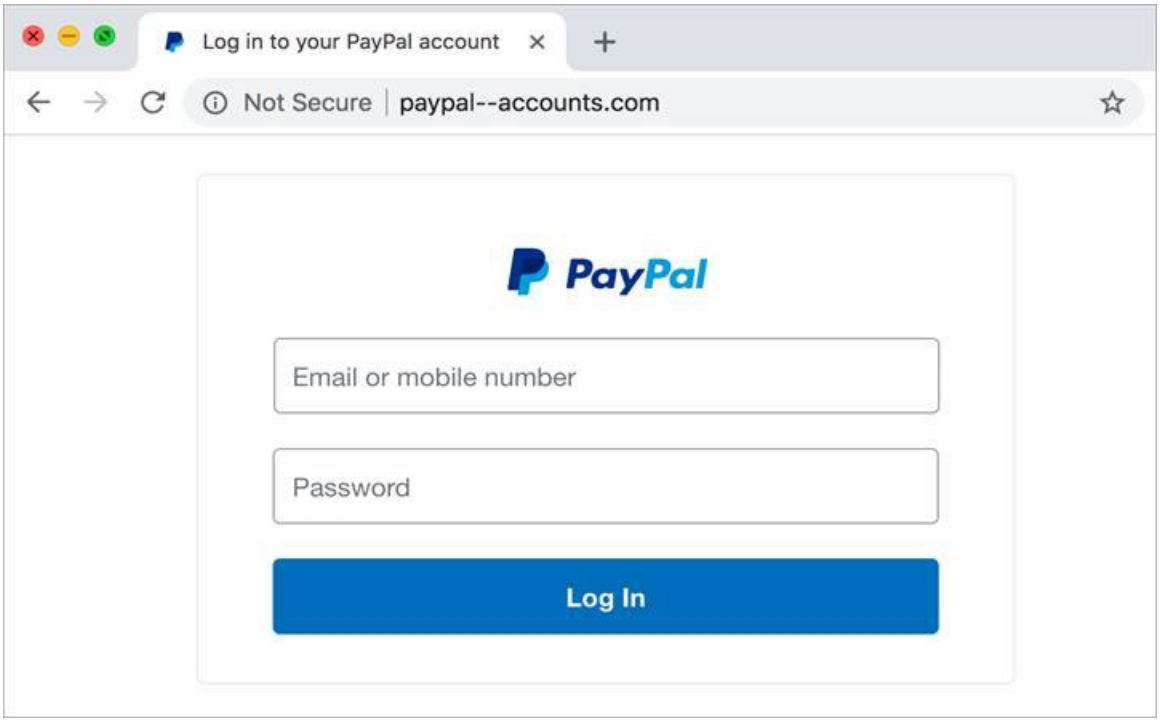


Рисунок 1.10 – Механізм перехоплення даних через підроблений веб-інтерфейс

Окрім класичних методів, популярності набуває фішинг у соціальних мережах, де через фейкові профілі або зламані акаунти друзів розповсюджуються шкідливі посилання під виглядом розіграшів чи опитувань (рис. 1.11). Окремим напрямком є вішинг (голосовий фішинг), коли зловмисники телефонують жертві, представляючись співробітниками служби безпеки банку, та психологічним тиском змушують розголосити конфіденційні дані.

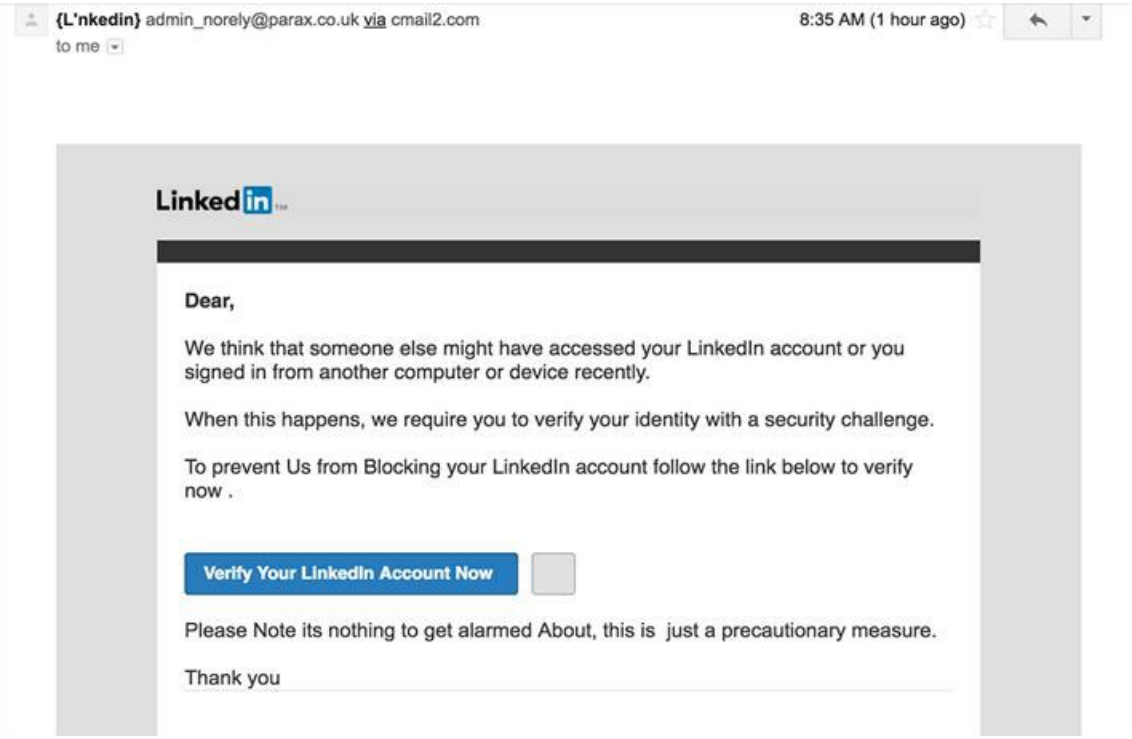


Рисунок 1.11 – Вектор фішингової атаки в середовищі соціальних мереж

Атака «Людина посередині» (Man-in-the-Middle, MITM) базується на прихованому втручанні в канал зв'язку між двома учасниками обміну даними. Зловмисник перехоплює трафік, маючи можливість читати його вміст або модифікувати його в реальному часі, причому легітимні учасники вважають, що спілкуються напряму.

Технічна реалізація MITM може включати сніфінг (аналіз пакетів), SSL Stripping (примусове пониження захищеного HTTPS з'єднання до незахищеного HTTP) або атаки на бездротові мережі (створення фальшивих точок доступу Wi-Fi). Це дозволяє викрадати сесійні ключі, змінювати реквізити в банківських транзакціях або впроваджувати шкідливий код у потік даних, що передаються [15].

Сканування портів та вразливостей є етапом технічної розвідки, який передує активній фазі злому. Процес розпочинається зі збору інформації: пасивного (аналіз відкритих джерел, WHOIS) та активного (зондування мережі). Далі зловмисники застосовують спеціалізоване ПЗ для сканування TCP та UDP портів з метою виявлення запущених служб.

Наступним кроком є співставлення версій виявленого ПЗ з базами відомих вразливостей (CVE). Це дозволяє ідентифікувати слабкі місця, які можна експлуатувати. Результати такої розвідки часто оформлюються у вигляді звітів для подальшого продажу в даркнеті або безпосереднього використання для проникнення.

Zero-Day атаки представляють найвищий рівень небезпеки, оскільки вони спрямовані на вразливості, про які ще не відомо розробникам програмного забезпечення. Термін "нульовий день" означає, що у вендора було нуль днів на випуск виправлення (патча) з моменту виявлення загрози.

Основними характеристиками таких атак є раптовість, висока швидкість поширення та низька ймовірність виявлення традиційними антивірусами, оскільки сигнатури для них ще не створені. Це дозволяє зловмисникам певний час безперешкодно компрометувати системи, завдаючи значної шкоди конфіденційності та цілісності даних [15].

Шкідливе програмне забезпечення (Malware) є широкою категорією, що охоплює будь-який код, створений для деструктивних дій. Серед основних типів виділяють віруси та троянські програми. Комп'ютерний вірус характеризується здатністю до самовідтворення шляхом інфікування інших файлів. Його дії можуть варіюватися від простого видалення даних до шифрування дисків.

Троянські програми (трояни) діють інакше: вони маскуються під легітимне ПЗ, вводячи користувача в оману. Після запуску троян може відкривати бекдори (приховані входи) для зловмисників, викрадати паролі або завантажувати інші шкідливі модулі. На відміну від вірусів, трояни зазвичай не розмножуються самостійно, а покладаються на методи соціальної інженерії для поширення.

Особливу категорію загроз становлять внутрішні атаки (Insider Threats), джерелом яких є співробітники організації. Небезпека полягає в тому, що інсайдери вже мають легітимний доступ до периметра мережі та знають її архітектуру.

Спектр таких дій включає зловживання правами адміністратора для несанкціонованого перегляду даних, ескалацію привілеїв (підвищення прав доступу через експлойти) та промислове шпигунство. Також можливі атаки, спрямовані на порушення цілісності інформації, наприклад, фальсифікація фінансової звітності адміністратором бази даних. Боротьба з внутрішніми загрозами вимагає впровадження суворих політик контролю доступу та поведінкового аналізу дій користувачів [15].

Забезпечення інформаційної безпеки — це безперервний процес, спрямований на гарантування тріади властивостей інформації: цілісності, конфіденційності та доступності. В умовах постійної еволюції методів кіберзлочинців, фокусування виключно на протидії відомим типам атак є недостатнім. Ефективна система захисту вимагає імплементації превентивних стратегій та загальних рекомендацій, що охоплюють усі рівні інфраструктури — від фізичного до адміністративного [15].

Ключовим елементом успішної інтеграції нових технологій та протоколів безпеки є підвищення кваліфікації персоналу. Користувачі часто розглядаються як найслабша ланка в системі безпеки, тому систематичне навчання є критично необхідним для формування так званого "людського фаєрволу". Освітні ініціативи повинні включати тренінги, вебінари та розробку методичних матеріалів, що допомагають співробітникам адаптуватися до вимог безпеки.

Програма підготовки має охоплювати ознайомлення з функціоналом корпоративних систем, методику безпечного виконання рутинних операцій, а також чіткі інструкції щодо поводження з паролями та конфіденційними даними. Важливим аспектом є інформування про доступні канали технічної підтримки та алгоритми дій у типових проблемних ситуаціях. Крім того, персонал повинен бути своєчасно повідомлений про оновлення програмного забезпечення та появу нових функцій. Завершальним етапом будь-якого навчання є оцінка його ефективності, яка дозволяє верифікувати рівень засвоєння знань та готовність персоналу дотримуватися правил кібергігієни.

Паралельно з навчанням реалізується стратегія обмеження прав доступу, що базується на принципах аутентифікації, авторизації та рольового управління (RBAC). Фундаментальним правилом тут є надання мінімально необхідних прав (Principle of Least Privilege). Це означає, що права доступу користувача повинні чітко відповідати його посадовим обов'язкам: адміністратори отримують розширені повноваження, тоді як пересічні користувачі — лише базовий набір функцій. Реалізація цієї стратегії передбачає сувору ідентифікацію суб'єктів доступу та безперервний моніторинг їхніх дій для виявлення аномалій або спроб несанкціонованого використання ресурсів, що значно знижує ризики внутрішніх витоків інформації.

Парольний захист залишається першою лінією оборони мережевого периметра. Надійність пароля прямо пропорційна його ентропії, яка залежить від довжини та різноманітності використаних символів. Рекомендований стандарт передбачає використання комбінацій довжиною не менше 12 символів, що включають літери верхнього та нижнього регістрів, цифри та спеціальні знаки.

Критично важливо уникати використання словникових слів, оскільки вони вразливі до атак перебору. Ефективною практикою є використання парольних фраз (passphrases), які легше запам'ятовуються користувачами, але є стійкими до злому. Організаційна політика повинна забороняти повторне використання паролів для різних сервісів та вимагати їх періодичної зміни. Для нівелювання ризиків, пов'язаних із компрометацією паролів, обов'язковим є впровадження двофакторної автентифікації (2FA/MFA), яка створює додатковий бар'єр безпеки навіть за умови викрадення основного секретного ключа [15].

Своєчасне оновлення програмного забезпечення (Patch Management) є критичним процесом для закриття відомих вразливостей (CVE). Найбільш ефективним підходом є налаштування автоматичного встановлення оновлень

для операційних систем та прикладного ПЗ, що мінімізує вплив людського фактора.

Організація повинна затвердити графік регулярних перевірок наявності патчів, використовуючи виключно офіційні репозиторії розробників для уникнення завантаження модифікованого шкідливого коду. Важливо пам'ятати, що оновленню підлягають не лише ОС, але й браузери, плагіни та сторонні додатки, які часто стають вектором атак. У корпоративному середовищі перед розгортанням критичних оновлень обов'язковим є їх попереднє тестування в ізольованому середовищі (пісочниці) та створення резервних копій систем, що дозволяє уникнути збоїв у робочому процесі через несумісність версій.

В умовах зростання активності шкідливого програмного забезпечення (Malware), використання надійних антивірусних рішень є обов'язковим стандартом. Вибір продукту має базуватися на репутації вендора та результатах незалежних тестувань. Сучасні антивіруси повинні забезпечувати не лише сигнатурний аналіз, який потребує регулярного оновлення баз, але й евристичний аналіз для виявлення нових, невідомих загроз.

Функціонал захисту має включати сканування в режимі реального часу, перевірку вкладень електронної пошти, веб-фільтрацію та модулі захисту від мережевих атак. Регулярне повне сканування системи дозволяє виявити приховані загрози, а моніторинг активності процесів допомагає ідентифікувати ознаки інфікування за непрямими показниками поведінки програм [15].

Для забезпечення прозорості процесів у мережі необхідно впроваджувати комплексні системи моніторингу та проводити регулярні аудити. Моніторинг передбачає безперервний збір та аналіз телеметрії мережі, журналів подій та трафіку для виявлення аномалій, що можуть свідчити про початок кібератаки, наприклад, DDoS або спроби експлойту. Це дозволяє команді безпеки оперативно реагувати на інциденти.

Аудит безпеки, у свою чергу, є періодичним процесом оцінки захищеності інфраструктури. Він включає аналіз відповідності політик безпеки міжнародним стандартам (GDPR, PCI DSS, ISO 27001) та проведення тестів на проникнення (Penetration Testing). Тестування дозволяє виявити реальні вектори вторгнення та слабкі місця в конфігурації систем до того, як ними скористаються зловмисники.

Фундаментом збереження інформаційних активів є стратегії резервного копіювання та шифрування. Резервне копіювання (Backup) гарантує можливість відновлення діяльності після інцидентів, таких як атаки програм-вимагачів або апаратні збої. Ефективна політика бекапування передбачає створення копій на різних рівнях (файловому, системному) та їх зберігання в географічно рознесених локаціях.

Шифрування даних забезпечує їх конфіденційність, роблячи інформацію недоступною для прочитання без ключа дешифрування. Криптографічний захист повинен застосовуватися як до даних у стані спокою (на жорстких дисках), так і до даних у процесі передачі. Це є обов'язковою вимогою багатьох регуляторних норм, зокрема у фінансовому та медичному секторах [15, 16].

Технології віртуальних приватних мереж (VPN) та міжмережевих екранів (фаєрволів) утворюють захищений периметр організації. VPN створює зашифрований тунель для передачі даних через публічні мережі, приховуючи реальну IP-адресу користувача та захищаючи трафік від перехоплення. Це особливо актуально для забезпечення безпечного віддаленого доступу співробітників та об'єднання розрізнених філій компанії.

Фаєрволи виконують функцію фільтрації вхідного та вихідного трафіку на основі заданих правил безпеки. Для ефективного захисту ці технології повинні працювати в тандемі. Налаштування брандмауера має дозволяти VPN-з'єднання лише з довірених джерел, використовувати сучасні протоколи (наприклад, OpenVPN, IPSec/IKEv2) та блокувати застарілі (PPTP). Крім того, важливо сегментувати доступ через VPN, надаючи користувачам права лише

на конкретні ресурси, а не на всю внутрішню мережу, та вести детальне журналювання всіх з'єднань для подальшого аналізу [16].

2 АРХІТЕКТУРНЕ ПРОЕКТУВАННЯ ЗАХИЩЕНОГО КОРПОРАТИВНОГО СЕРЕДОВИЩА

2.1 Обґрунтування вибору апаратного забезпечення для побудови комунікаційної архітектури

Процес побудови надійної мережевої інфраструктури розпочинається з ретельного підбору активного мережевого обладнання, яке має відповідати вимогам продуктивності, відмовостійкості та масштабованості. Для реалізації рівнів ядра мережі та рівня розподілу, після аналізу ринкових пропозицій, було прийнято рішення зупинити вибір на маршрутизаторах серії Cisco 7600.

Ця лінійка обладнання позиціонується як високопродуктивна платформа, що слугує фундаментом для стратегічного розвитку IT-інфраструктури підприємства. Маршрутизатори Cisco 7600 забезпечують виняткову надійність та ефективність обробки IP-протоколу, що робить їх стандартом де-факто для багатьох сучасних обчислювальних центрів та вузлів зв'язку. Архітектурні особливості серії дозволяють використовувати її як у масштабах великих корпорацій, так і для побудови розподілених мереж типу MAN (міські мережі) та WAN (глобальні мережі). Це досягається завдяки підтримці широкого спектру інтерфейсів та здатності адаптуватися до умов високого навантаження.

Функціональний набір Cisco 7600 є надзвичайно широким. Насамперед, платформа забезпечує повну підтримку всього спектру можливостей операційної системи Cisco IOS™, що гарантує сумісність та гнучкість налаштувань. Конструктивно шасі маршрутизатора (зокрема моделі 7609) відповідає суворим вимогам стандарту NEBS, що передбачає специфічну організацію системи охолодження з потоком повітря від передньої до задньої панелі, забезпечуючи стабільну роботу в серверних стійках.

Критично важливою характеристикою для ядра мережі є продуктивність маршрутизації. У даній серії реалізовано підтримку технології Distributed Cisco Express Forwarding (dCEF), яка дозволяє розподіляти навантаження з пересилання пакетів між модульними процесорами, значно підвищуючи загальну пропускну здатність (за винятком молодших моделей, таких як 7603). Висока доступність та безперервність сервісів забезпечується завдяки апаратному резервуванню критичних вузлів — блоків живлення та модулів управління, а також програмним механізмам Cisco IOS Global Resilience IP.

Окрім того, маршрутизатори цієї серії оснащені засобами апаратного прискорення мережевих сервісів на базі технології Cisco PXF, що дозволяє обробляти трафік без затримок навіть при застосуванні складних політик фільтрації. Важливим аспектом є підтримка технології MPLS, яка необхідна для побудови сучасних конвергентних мереж. З точки зору інвестиційної ефективності, Cisco 7600 демонструє високу універсальність завдяки сумісності з модулями розширення від комутаторів серії Catalyst 6500, а також підтримці інтерфейсних модулів від маршрутизаторів серій 7200, 7100, 7400 та 7500 через спеціалізований адаптер FlexWAN [19]. Зовнішній вигляд обраного пристрою наведено на рис. 2.1.



Рисунок 2.1 – Конструктивне виконання маршрутизатора ядра мережі Cisco 7600 Series

Для організації другого рівня моделі OSI (рівня доступу), де відбувається безпосереднє підключення кінцевих користувачів, було обрано комутатори Cisco Catalyst 2960. Цей вибір обумовлений здатністю пристроїв забезпечити побудову розвиненої, керованої та захищеної локальної мережі, що є актуальним як для головних офісів великих корпорацій, так і для віддалених філій.

Архітектура Cisco 2960 дозволяє організувати підключення робочих станцій на швидкостях 10, 100 та 1000 Мбіт/с, залежно від моделі, що повністю покриває потреби сучасного офісу. Технічні характеристики серії включають різноманітні конфігурації портів Fast Ethernet та Gigabit Ethernet (8, 24 або 48 портів), що дозволяє гнучко масштабувати мережу. Особливої уваги заслуговує підтримка технології Power over Ethernet (PoE) у моделях з 24 портами, що дозволяє передавати електроживлення пристроям (IP-телефони, камери

відеонагляду, точки доступу Wi-Fi) безпосередньо через мережевий кабель (кручену пару).

У контексті створення захищеної інфраструктури, комутатори Cisco 2960 пропонують покращені функції безпеки, включаючи можливість створення складних списків управління доступом (ACL) безпосередньо на рівні порту, що дозволяє фільтрувати небажаний трафік ще до потрапляння в ядро мережі. Також реалізовано широкий спектр механізмів QoS (Quality of Service) для пріоритезації критичного трафіку, такого як голос або відео.

Інтелектуальні сервіси на межі мережі дозволяють автоматизувати багато рутинних задач адміністрування. Додатковою перевагою є надання довічної гарантії на обладнання, що знижує операційні витрати. Для спрощення процесів налаштування та моніторингу, кожен пристрій комплектується програмним забезпеченням Cisco Network Assistant. Це централізована консоль управління, яка пропонує інтуїтивно зрозумілі майстри налаштування, дозволяючи навіть фахівцям середньої кваліфікації ефективно розгортати та обслуговувати мережеву інфраструктуру [20]. Візуалізація комутатора рівня доступу представлена на рис. 2.2.



Рисунок 2.2 – Зовнішній вигляд комутатора рівня доступу Cisco Catalyst 2960

2.2 Архітектурне планування та топологічна організація корпоративної мережі

При розробці проекту мережевої інфраструктури було застосовано класичну ієрархічну модель проектування, яка базується на трирівневій архітектурі. Такий підхід дозволяє створити масштабовану, надійну та економічно ефективну систему. Структура мережі логічно розділена на три функціональні площини: рівень ядра (Core Layer), рівень розподілу (Distribution Layer) та рівень доступу (Access Layer). Кожен з цих рівнів виконує специфічні завдання, що дозволяє оптимізувати обробку трафіку та спростити адміністрування.

Рівень ядра виступає високошвидкісним магістральним каналом, завданням якого є максимально швидка комутація пакетів. У розробленому проекті до цього рівня віднесено маршрутизатор провайдера, що забезпечує зовнішній канал зв'язку. Наступним ешелоном є рівень розподілу, який слугує сполучною ланкою між ядром та рівнем доступу. Тут розміщено два маршрутизатори, що відповідають за маршрутизацію між віртуальними локальними мережами (VLAN), фільтрацію трафіку та реалізацію політик доступу. Рівень доступу, який забезпечує безпосереднє підключення кінцевих пристроїв до мережі, сформовано з п'яти комутаторів. Вони обслуговують окремі логічні сегменти: мережу управління (Management), локальні сегменти користувачів (LAN A, LAN B, LAN C) та виділену северну ферму.

Узагальнена апаратна конфігурація проекту включає три маршрутизатори для організації логіки мережі, п'ять комутаторів для фізичного підключення, вісім робочих станцій, що імітують навантаження користувачів, та два сервери, на яких розгорнуто службу каталогів Active Directory. Схематичне зображення спроектованої архітектури наведено на рис. 2.3.

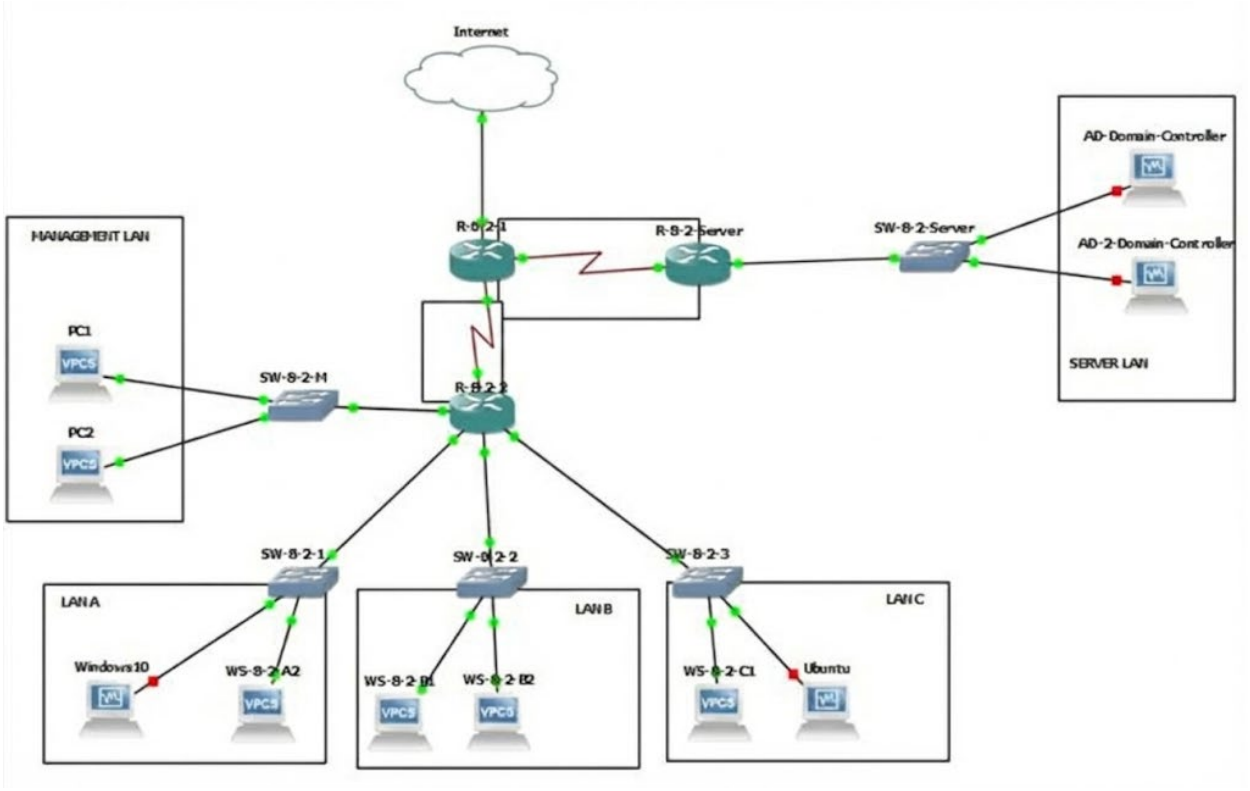


Рисунок 2.3 – Концептуальна схема ієрархічної побудови мережі

Організація каналів зв'язку між рівнями має свої особливості. Для з'єднання пристроїв рівня ядра та розподілу використано послідовні інтерфейси (serial connection), що часто застосовується для емуляції WAN-з'єднань або специфічних магістральних каналів. Натомість на рівні доступу, де критично важлива висока пропускна здатність для кінцевих користувачів, застосовано технологію Ethernet. Повна деталізована схема комутації та адресації представлена у відповідному додатку А.

Важливим етапом проектування є вибір топології, під якою розуміють фізичну або логічну конфігурацію взаємного з'єднання вузлів мережі. Значення топології у контексті розгортання Active Directory важко переоцінити, оскільки вона безпосередньо впливає на шляхи реплікації даних каталогів, швидкість авторизації користувачів, загальну відмовостійкість системи та її захищеність. Грамотно спроектована топологія дозволяє мінімізувати затримки передачі даних та забезпечити безперервність бізнес-процесів [18].

Для даного проекту було обрано гнучку гібридну топологію, яка поєднує переваги деревоподібної та зіркової структур. Деревоподібна складова (Tree Topology) формує магістральний каркас інфраструктури. У такій ієрархії вузли об'єднуються у групи, де кожен рівень підпорядковується вищому, нагадуючи розгалужене дерево. Це дозволяє ефективно сегментувати трафік, ізолювати проблеми окремих гілок та легко масштабувати мережу шляхом додавання нових відгалужень, не порушуючи роботу ядра. Крім того, така структура підвищує живучість системи, оскільки відсутність єдиного центрального концентратора для всієї мережі знижує ризик повного колапсу інфраструктури при відмові одного пристрою.

На рівні локальних підмереж реалізовано топологію «зірка» (Star Topology). Це означає, що всі кінцеві пристрої (комп'ютери, принтери) у межах одного сегменту підключаються до центрального пристрою — комутатора рівня доступу. Така організація забезпечує простоту управління та діагностики: вихід з ладу одного кабелю або робочої станції не впливає на роботу інших вузлів сегменту. Зіркова топологія є стандартом для сучасних локальних мереж завдяки своїй надійності, високій продуктивності та легкості модернізації.

2.3 Організація логічного адресного простору та реалізація протоколів маршрутизації

Для забезпечення коректного обміну пакетами даних між різними сегментами спроектованої інфраструктури було прийнято рішення про впровадження протоколу динамічної маршрутизації OSPF (Open Shortest Path First). Функціонування даного протоколу базується на алгоритмі відстеження стану каналів зв'язку (link-state) та використанні математичного алгоритму Дейкстри для обчислення найкоротшого маршруту до цільового вузла. Вибір

саме OSPF обумовлений специфічними вимогами інфраструктури, побудованої навколо служби каталогів Active Directory.

Ключовим фактором стала здатність протоколу до швидкої конвергенції — оперативного оновлення таблиць маршрутизації при змінах у топології. Це є критично важливим для забезпечення безперервної реплікації бази даних Active Directory між контролерами домену, оскільки будь-яка тривала затримка у відновленні з'єднання може призвести до розсинхронізації даних. Крім того, ієрархічна структура OSPF, що передбачає поділ мережі на зони, дозволяє оптимізувати навантаження на обладнання та ефективно масштабувати систему. Важливою перевагою є також підтримка багатошляхової маршрутизації, що підвищує загальну відмовостійкість системи, гарантуючи доступність сервісів навіть при виході з ладу окремих каналів.

Детальний план розподілу адресного простору та параметри конфігурації мережевих інтерфейсів представлено у таблиці 2.1. У схемі адресації використано приватний діапазон адрес класу A (10.20.x.x), що забезпечує гнучкість для майбутнього розширення, а порядок записів структуровано за функціональним призначенням: від користувацьких сегментів до ядра мережі.

Таблиця 2.1 – Зведений план IP-адресації та конфігурації інтерфейсів

Сегмент мережі / Пристрій	Інтерфейс підключення	IP-адреса	Маска підмережі	Префікс CIDR
КОРИСТУВАЦЬКИЙ СЕГМЕНТ LAN-A (10.20.10.0)				
Маршрутизатор R-Core-2	FastEthernet 1/0 (Шлюз)	10.20.10.1	255.255.255.192	/26
Комутатор SW-Access-A	Vlan 1	10.20.10.2	255.255.255.192	/26
Робоча станція WS-User-A1	Адаптер (DHCP)	Динамічна	255.255.255.192	/26

Робоча станція WS-User-A2	Адаптер (DHCP)	Динамічна	255.255.255.192	/26
КОРИСТУВАЦЬКИЙ СЕГМЕНТ LAN-B (10.20.10.64)				
Маршрутизатор R-Core-2	FastEthernet 1/1 (Шлюз)	10.20.10.65	255.255.255.192	/26
Комутатор SW-Access-B	Vlan 1	10.20.10.66	255.255.255.192	/26
Робоча станція WS-User-B1	Адаптер (DHCP)	Динамічна	255.255.255.192	/26
Робоча станція WS-User-B2	Адаптер (DHCP)	Динамічна	255.255.255.192	/26
КОРИСТУВАЦЬКИЙ СЕГМЕНТ LAN-C (10.20.10.128)				
Маршрутизатор R-Core-3	FastEthernet 2/0 (Шлюз)	10.20.10.129	255.255.255.192	/26
Комутатор SW-Access-C	Vlan 1	10.20.10.130	255.255.255.192	/26
Робоча станція WS-User-C1	Адаптер (DHCP)	Динамічна	255.255.255.192	/26
Робоча станція WS-User-C2	Адаптер (DHCP)	Динамічна	255.255.255.192	/26
МЕРЕЖА УПРАВЛІННЯ (MANAGEMENT LAN) (10.20.20.0)				
Маршрутизатор R-Core-2	FastEthernet 0/0 (Шлюз)	10.20.20.1	255.255.255.192	/26
Комутатор SW-Mgmt	Vlan 1	10.20.20.2	255.255.255.192	/26
Робоча станція WS-Admin-1	Адаптер (Static)	10.20.20.10	255.255.255.192	/26
Робоча станція WS-Admin-2	Адаптер (Static)	10.20.20.11	255.255.255.192	/26

СЕРВЕРНА ФЕРМА (SERVER LAN) (10.20.30.0)				
Маршрутизатор R-Server-GW	FastEthernet 0/0 (Шлюз)	10.20.30.1	255.255.255.192	/26
Комутатор SW-Server	Vlan 1	10.20.30.2	255.255.255.192	/26
Контролер домену DC-01	Адаптер (DNS Server)	10.20.30.5	255.255.255.192	/26
Контролер домену DC-02	Адаптер	10.20.30.6	255.255.255.192	/26
МАГІСТРАЛЬНИЙ КАНАЛ ЯДРА №1 (R1-R2 Link) (10.20.99.0)				
Маршрутизатор R-Core-1	Serial 6/0	10.20.99.1	255.255.255.252	/30
Маршрутизатор R-Core-2	Serial 6/0	10.20.99.2	255.255.255.252	/30
МАГІСТРАЛЬНИЙ КАНАЛ ЯДРА №2 (R1-Srv Link) (10.20.99.4)				
Маршрутизатор R-Core-1	Serial 6/1	10.20.99.5	255.255.255.252	/30
Маршрутизатор R-Server-GW	Serial 6/1	10.20.99.6	255.255.255.252	/30
ЗОВНІШНЯ МЕРЕЖА (INTERNET UPLINK) (192.168.100.0)				
Провайдер ISP	Ethernet (GW)	192.168.100.1	255.255.255.0	/24
Маршрутизатор R-Core-1	FastEthernet 0/0	192.168.100.2	255.255.255.0	/24

3 ПРАКТИЧНА ІМПЛЕМЕНТАЦІЯ ТА ВЕРИФІКАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

3.1 Конфігурація активного мережевого обладнання та базових сервісів

Етап практичної реалізації спроектованої архітектури розпочинається з безпосереднього налаштування програмно-апаратних комплексів. Забезпечення коректного функціонування комунікаційної інфраструктури вимагає послідовного внесення конфігураційних параметрів до всіх вузлів мережі: маршрутизаторів ядра, розподільчих шлюзів та комутаторів рівня доступу. Цей процес включає ініціалізацію фізичних та логічних інтерфейсів, організацію маршрутизації потоків даних та впровадження політик безпеки адміністративного доступу.

Першочерговим завданням є призначення логічних адрес мережевим інтерфейсам маршрутизаторів згідно з розробленим у попередньому розділі планом IP-адресації. Процедура виконується в режимі глобальної конфігурації терміналу, де для кожного фізичного порту (FastEthernet або Serial) задається унікальна IP-адреса та відповідна маска підмережі. Обов'язковим кроком є активація інтерфейсу, який за замовчуванням перебуває у вимкненому стані, а також додавання опису (description), що дозволяє адміністраторам швидко ідентифікувати призначення каналу при подальшій діагностиці. Фрагмент процесу присвоєння адрес наведено на рис. 3.1.

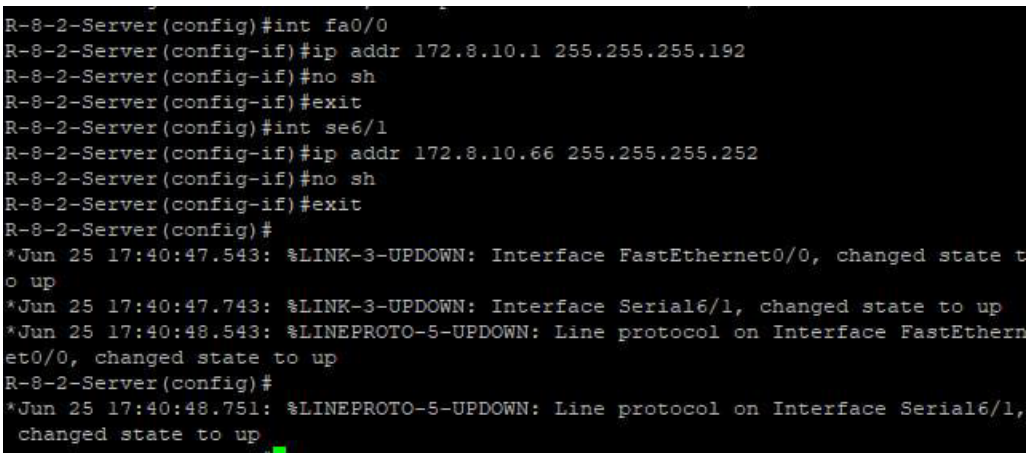


Рисунок 3.1 – Фрагмент конфігурації мережевих інтерфейсів маршрутизатора

Після забезпечення мережевої зв'язності на рівні інтерфейсів здійснюється налаштування логіки обміну даними між підмережами. Для цього активується процес динамічної маршрутизації OSPF. Конфігурація передбачає запуск процесу з певним ідентифікатором та оголошення мереж, які маршрутизатор транслюватиме сусідам. Особливістю налаштування OSPF є використання зворотних масок (wildcard masks) для визначення діапазону адрес, а також прив'язка мереж до конкретних зон (Areas). У рамках даного проекту всі критичні вузли віднесено до магістральної зони (Area 0) для забезпечення швидкої конвергенції та обміну маршрутною інформацією, що проілюстровано на рис. 3.2.

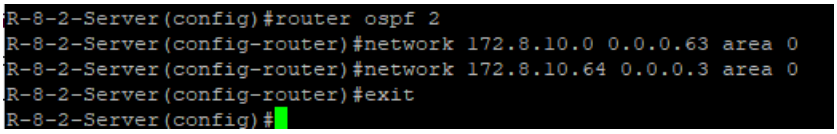


Рисунок 3.2 – Ініціалізація протоколу динамічної маршрутизації OSPF

Критично важливим етапом налаштування є захист самої площини управління (Control Plane) мережевих пристроїв. Базова конфігурація безпеки включає встановлення паролів на привілейований режим доступу (enable mode), причому рекомендується використовувати алгоритми хешування (enable secret) замість зберігання паролів у відкритому вигляді.

Далі створюється локальна база даних користувачів з розмежуванням прав доступу, що дозволяє відмовитися від загальних паролів на користь персоналізованої аутентифікації. Налаштування віртуальних ліній термінального доступу (VTY) та консольного порту передбачає активацію перевірки облікових даних через локальну базу, встановлення тайм-аутів сесій та налаштування шифрування всіх паролів у конфігураційному файлі. Приклад реалізації цих заходів безпеки показано на рис. 3.3.

```
R-8-2-1(config)#enable secret strongpass99
R-8-2-1(config)#service password-encryption
R-8-2-1(config)#no service password-recovery
Password recovery disable mode is not supported by the current ROMMON.
Please upgrade the ROMMON if you want to use this feature.

R-8-2-1(config)#username admin privilege 15 secret adminpass99
R-8-2-1(config)#username technic privilege 7 secret techpass88
R-8-2-1(config)#
R-8-2-1(config)#line console 0
R-8-2-1(config-line)#password conpass88
R-8-2-1(config-line)#login
R-8-2-1(config-line)#exit
R-8-2-1(config)#
R-8-2-1(config)#line vty 0 4
R-8-2-1(config-line)#password vtypass77
R-8-2-1(config-line)#login
R-8-2-1(config-line)#transport input ssh
R-8-2-1(config-line)#transport output ssh
R-8-2-1(config-line)#exec-timeout 60 0
R-8-2-1(config-line)#exit
R-8-2-1(config)#
```

Рисунок 3.3 – Забезпечення безпеки адміністративного доступу та налаштування аутентифікації

3.2 Розгортання та конфігурація архітектури служб каталогів

Наступним критичним етапом побудови захищеної інфраструктури є імплементація доменних служб Active Directory (AD DS). Цей крок трансформує мережу з набору розрізнених робочих груп у керовану ієрархічну систему. Впровадження AD дозволяє реалізувати концепцію єдиного простору ідентифікації, забезпечуючи централізовану аутентифікацію користувачів та авторизацію доступу до корпоративних ресурсів. Окрім посилення безпеки,

служба каталогів виступає фундаментом для автоматизації рутинних адміністративних процесів, таких як масове розгортання політик безпеки, оновлення програмного забезпечення та управління конфігураціями кінцевих точок, що суттєво підвищує загальну керованість IT-ландшафту.

Процес розгортання розпочинається з підготовки першого сервера, який виконуватиме роль первинного контролера домену (PDC). На цьому етапі через диспетчер серверів здійснюється інсталяція ролі AD DS та супутніх служб, зокрема DNS, який є невід'ємною частиною інфраструктури для розпізнавання імен у домені. Ініціалізація процесу встановлення ролей відображена на рис. 3.4.

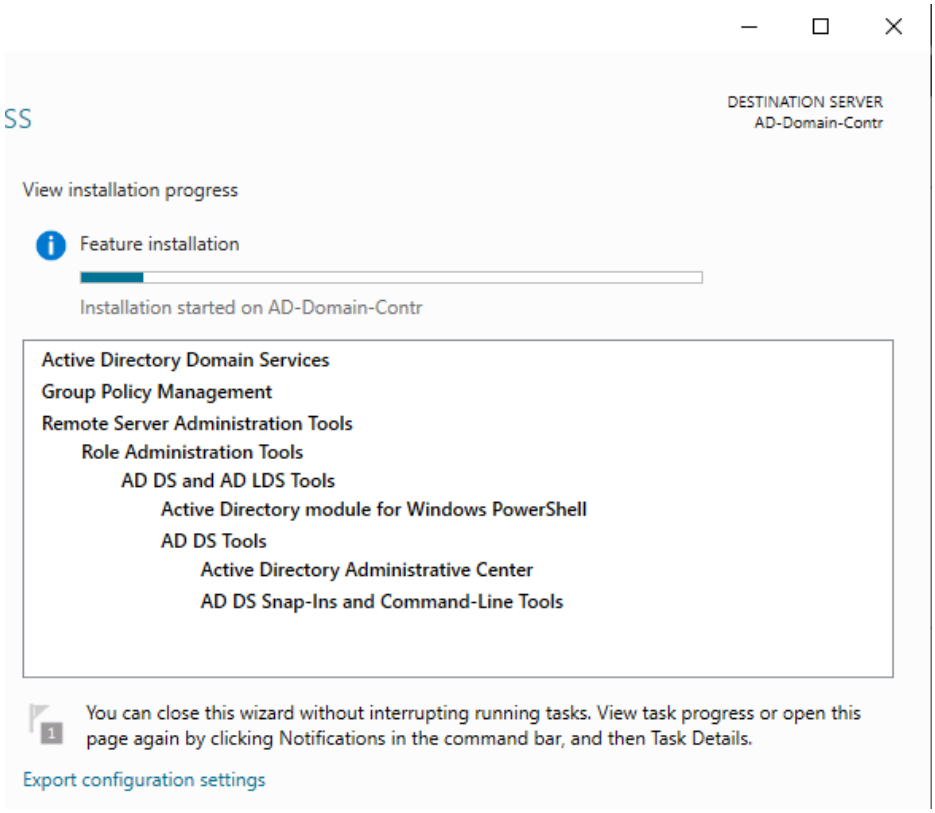


Рисунок 3.4 – Інсталяція рольових компонентів служби каталогів на первинному сервері

Після завершення інсталяції бінарних файлів необхідна процедура підвищення ролі сервера до рівня контролера домену (Promote to Domain

Controller). Оскільки це перший сервер у новій інфраструктурі, обирається опція створення нового лісу (Forest) та визначається кореневе доменне ім'я. На цьому ж етапі задається пароль для режиму відновлення служб каталогів (DSRM), що є важливим елементом стратегії аварійного відновлення. Процес конфігурації параметрів нового домену показано на рис. 3.5 - 3.6.

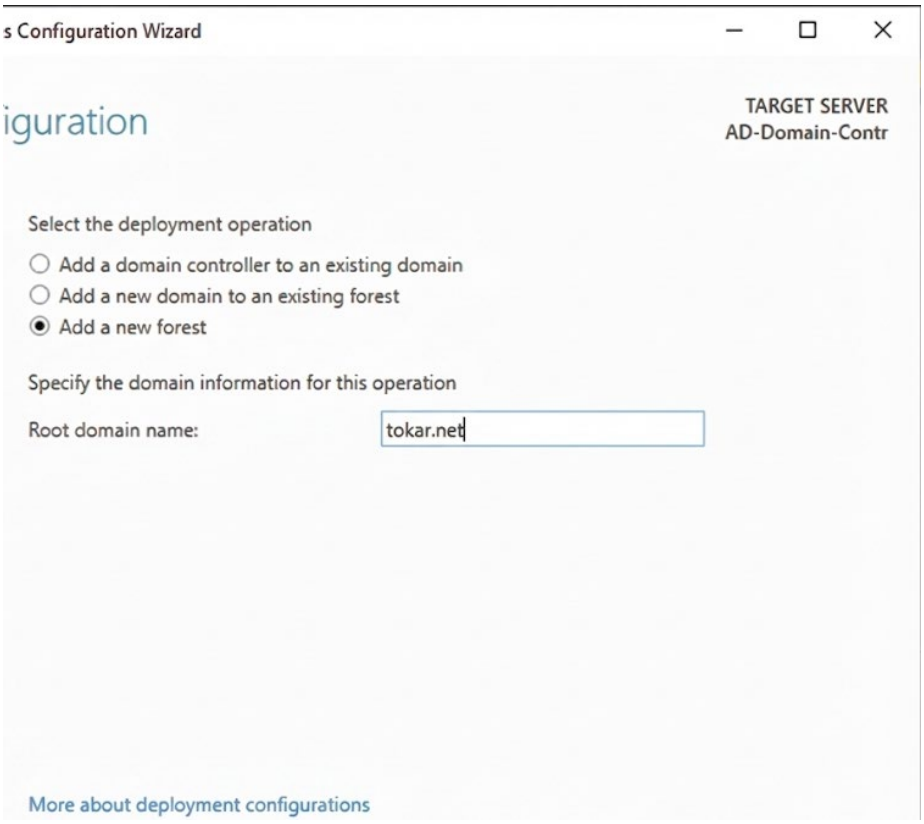


Рисунок 3.5 – Створення кореневого домену нового лісу Active Directory

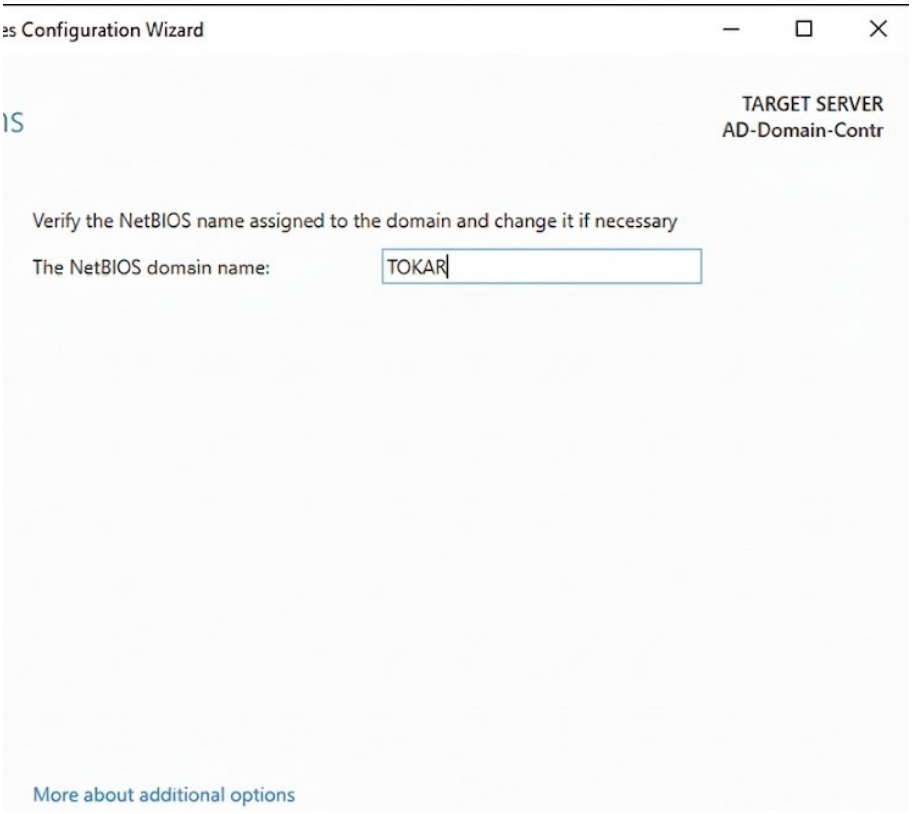


Рисунок 3.6 – Визначення функціонального рівня домену та параметрів DNS

Завершення майстра налаштування ініціює перезавантаження сервера, після чого він починає функціонувати як повноцінний контролер домену. Для підтвердження успішності операції проводиться перевірка статусу служб та доступності адміністративних оснасток, як це проілюстровано на рис. 3.7.

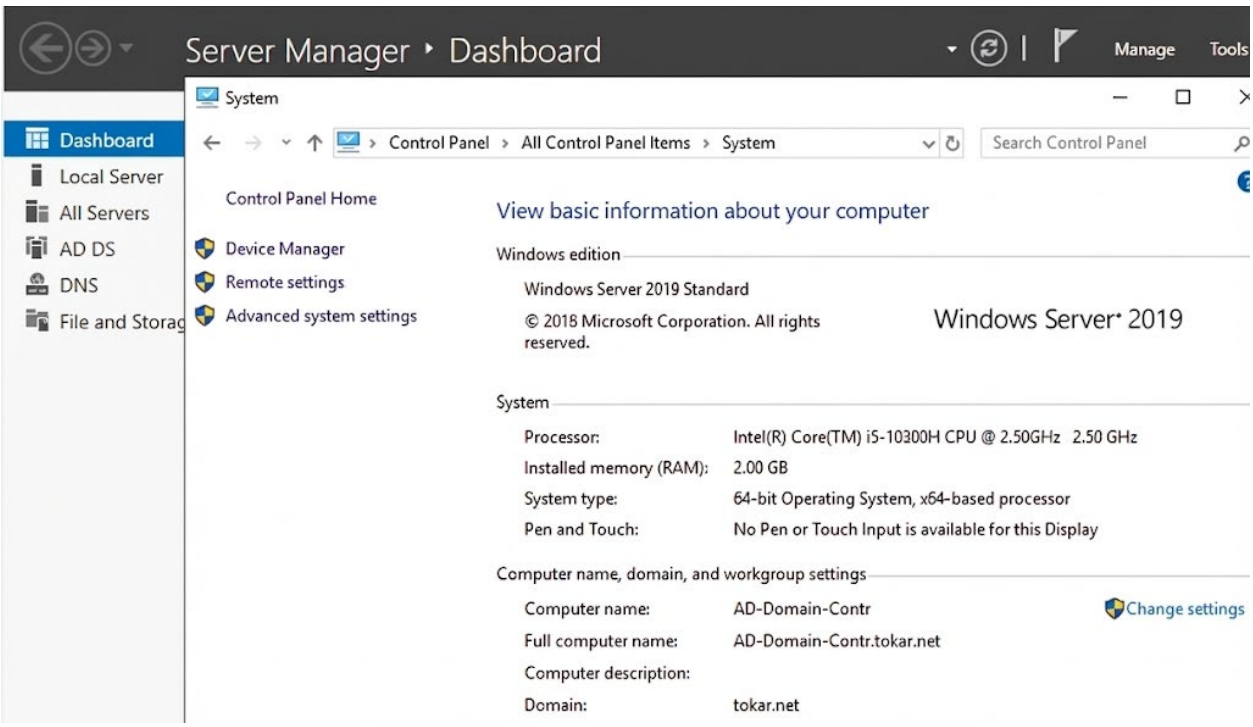


Рисунок 3.7 – Верифікація успішного розгортання первинного контролера

Для забезпечення відмовостійкості мережі (Fault Tolerance) архітектура проекту передбачає введення в експлуатацію другого контролера домену. Це гарантує доступність сервісів аутентифікації навіть у випадку фізичного виходу з ладу основного сервера. Процедура починається аналогічно до першого сервера — зі встановлення ролі AD DS на резервний вузол, рис. 3.8.

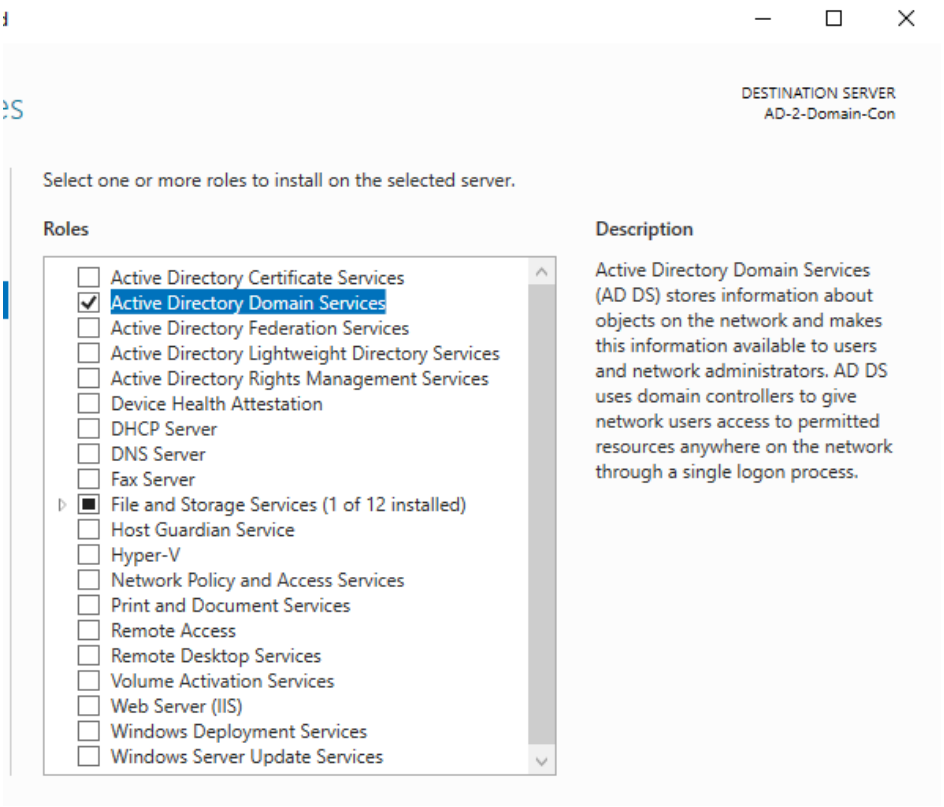


Рисунок 3.8 – Підготовка резервного сервера до розгортання ролі контролера

Ключова відмінність на етапі налаштування другого сервера полягає у виборі сценарію розгортання: замість створення нового лісу обирається опція додавання контролера до вже існуючого домену. Це ініціює процес реплікації, під час якого новий сервер завантажує актуальну базу даних Active Directory з первинного контролера. Налаштування параметрів приєднання та синхронізації відображено на рис. 3.9 та рис. 3.10.

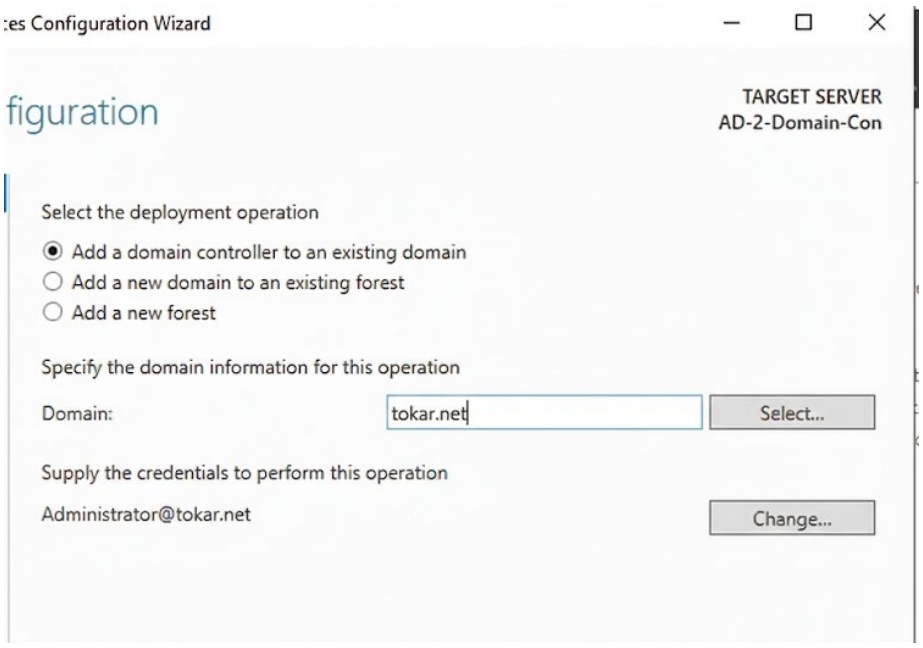


Рисунок 3.9 – Інтеграція резервного контролера в існуючу доменну структуру

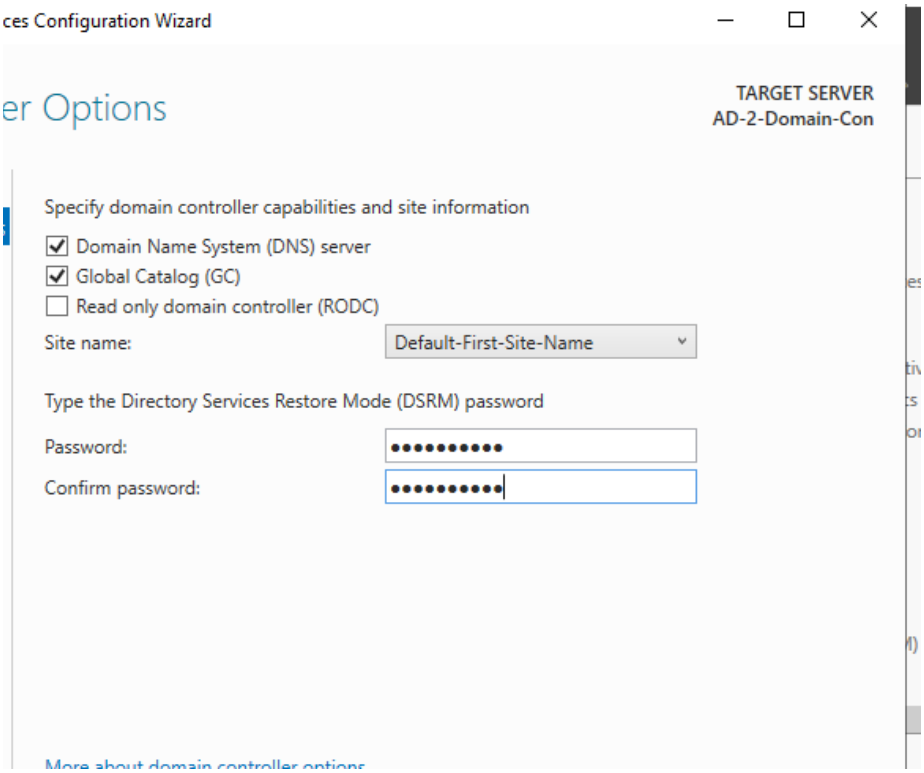


Рисунок 3.10 – Конфігурація параметрів реплікації бази даних каталогів

Після завершення налаштування другого контролера необхідно переконатися у коректності роботи механізмів реплікації та відсутності помилок у журналах подій, рис.3.11. Успішне створення кластера

відмовостійкості підтверджується наявністю обох серверів у контейнері "Domain Controllers" адміністративної консолі, що демонструє рис. 3.12.

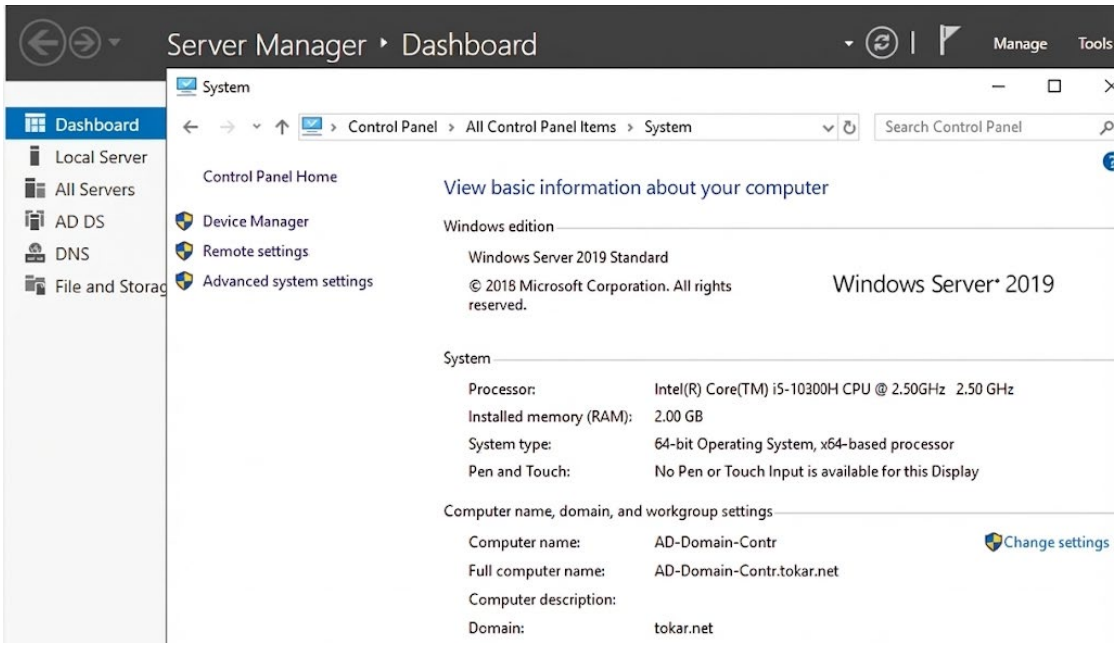


Рисунок 3.11 – Перевірка цілісності налаштувань резервного вузла

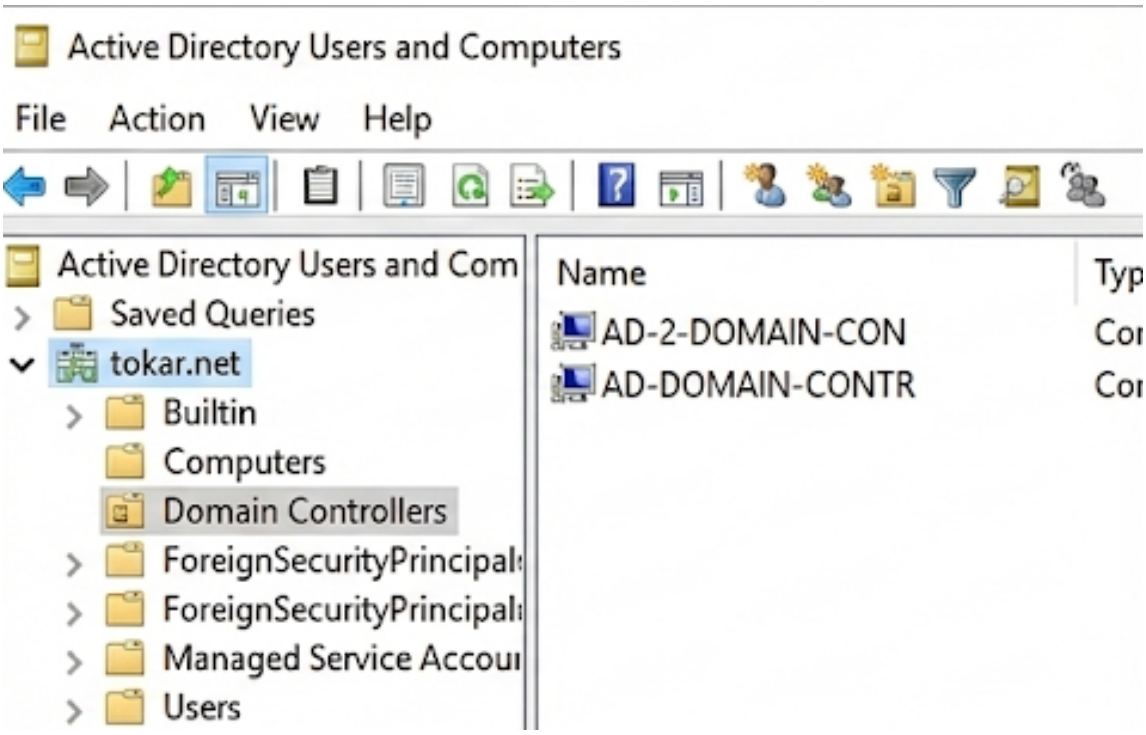


Рисунок 3.12 – Відображення списку активних контролерів в оснастці управління

Фінальним етапом побудови базової інфраструктури є підключення клієнтських робочих станцій до створеного домену. Ця процедура виконується на стороні клієнтської ОС шляхом зміни параметрів належності комп'ютера (перехід з робочої групи в домен) та введення облікових даних адміністратора домену для авторизації дії. Процес приєднання робочої станції показано на рис. 3.13.

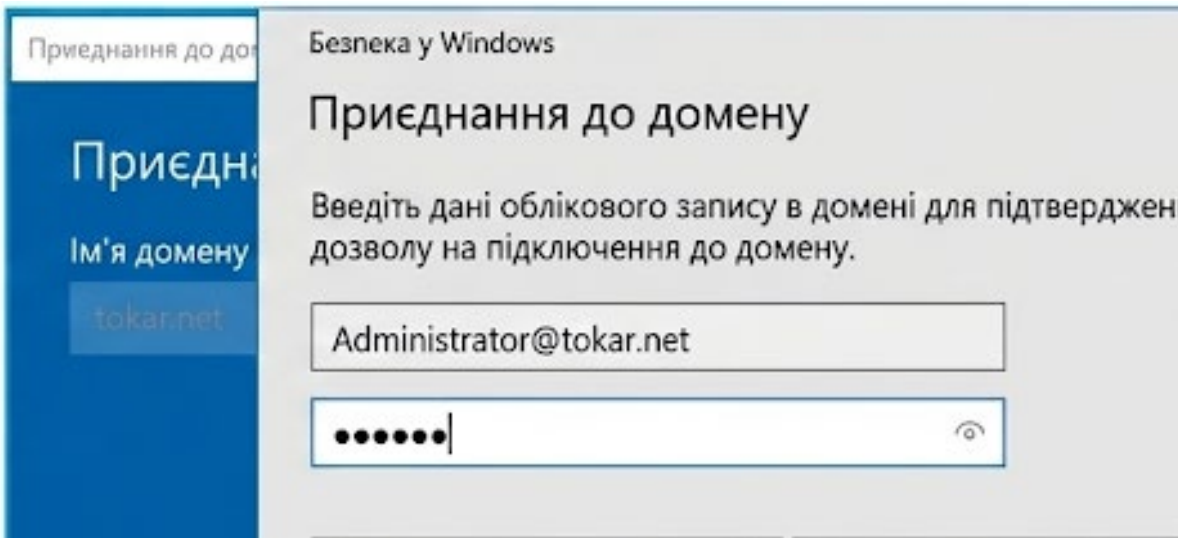


Рисунок 3.13 – Процедура введення клієнтської робочої станції до корпоративного домену

Після перезавантаження клієнтського комп'ютера його обліковий запис автоматично створюється в базі Active Directory, що можна перевірити через оснастку "Active Directory Users and Computers". Це підтверджує, що станція знаходиться під управлінням централізованих політик, рис. 3.14.

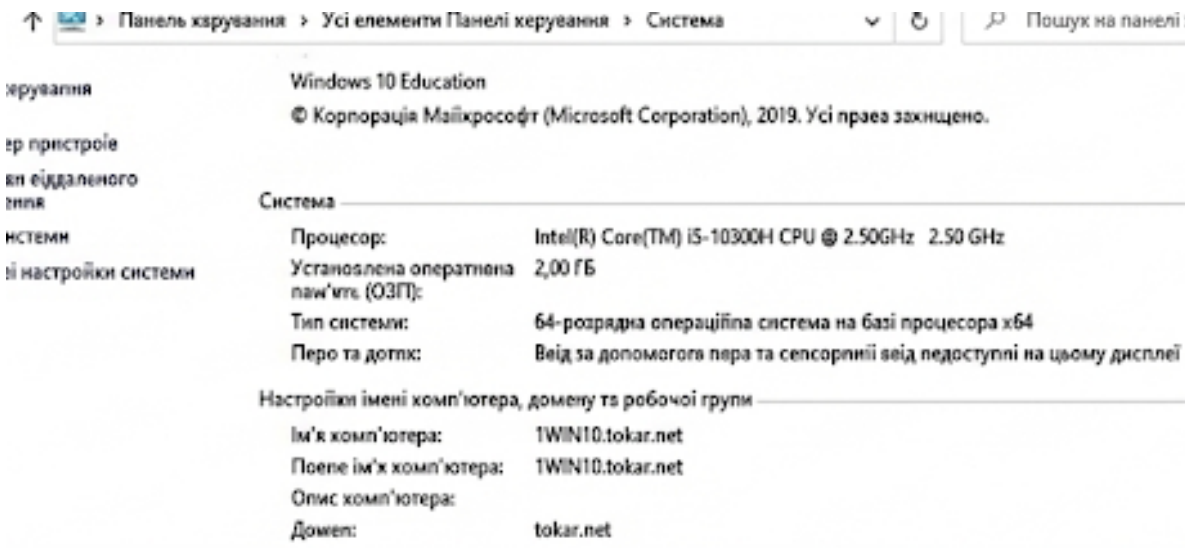


Рисунок 3.14 – Підтвердження реєстрації об’єкта комп’ютера в базі даних AD.

3.3 Верифікація функціональності та тестування логічної структури домену

Після успішного розгортання контролерів домену та приєднання клієнтських станцій, наступним кроком є побудова та тестування внутрішньої логічної архітектури каталогу. Цей етап передбачає створення ієрархії контейнерів, яка повинна відображати реальну організаційну структуру підприємства або адміністративну модель управління ресурсами.

Першочерговим завданням є створення організаційних одиниць (Organizational Units, OU), які слугують головними контейнерами для групування об'єктів. Це дозволяє делегувати адміністративні повноваження та застосовувати групові політики (GPO) до конкретних відділів, а не до всього домену одразу. Процес розпочинається зі створення кореневих OU, що відповідають великим департаментам або філіям компанії. В адміністративній оснастці ініціюється створення нового об'єкта типу "Organizational Unit", де задається його унікальне ім'я. Важливою опцією на цьому етапі є захист

контейнера від випадкового видалення, що є стандартною практикою безпеки. Візуалізацію створення кореневого підрозділу наведено на рис. 3.17.

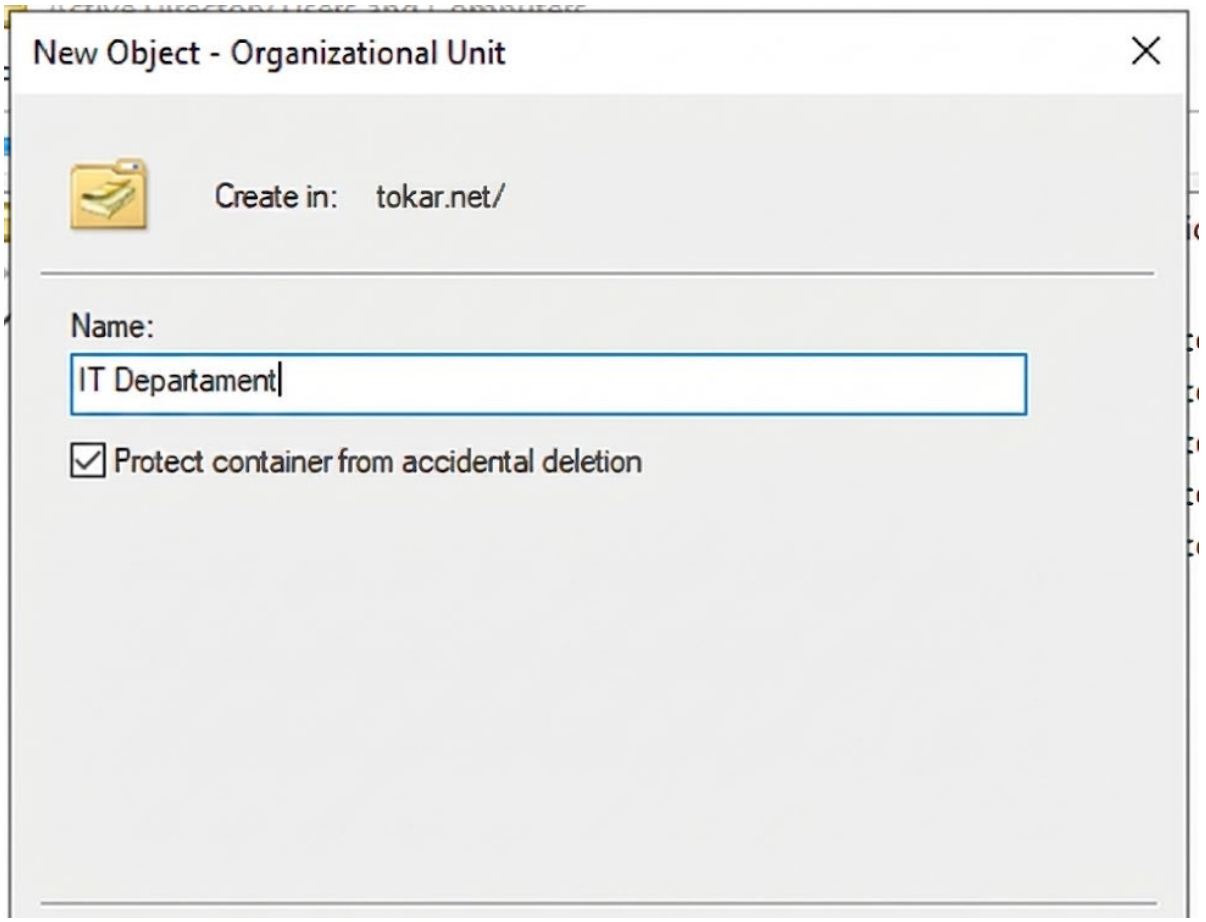


Рисунок 3.17 – Формування кореневого контейнера організаційної структури

Для забезпечення більшої гнучкості та деталізації управління, всередині кореневих підрозділів створюється вкладена ієрархія. Наприклад, у межах департаменту IT можуть бути створені окремі контейнери для відділу розробки, технічної підтримки та системного адміністрування. Така вкладеність дозволяє успадковувати загальні політики верхнього рівня та, при необхідності, перевизначати їх специфічними налаштуваннями для вузьких груп користувачів, що показано на рис. 3.18.

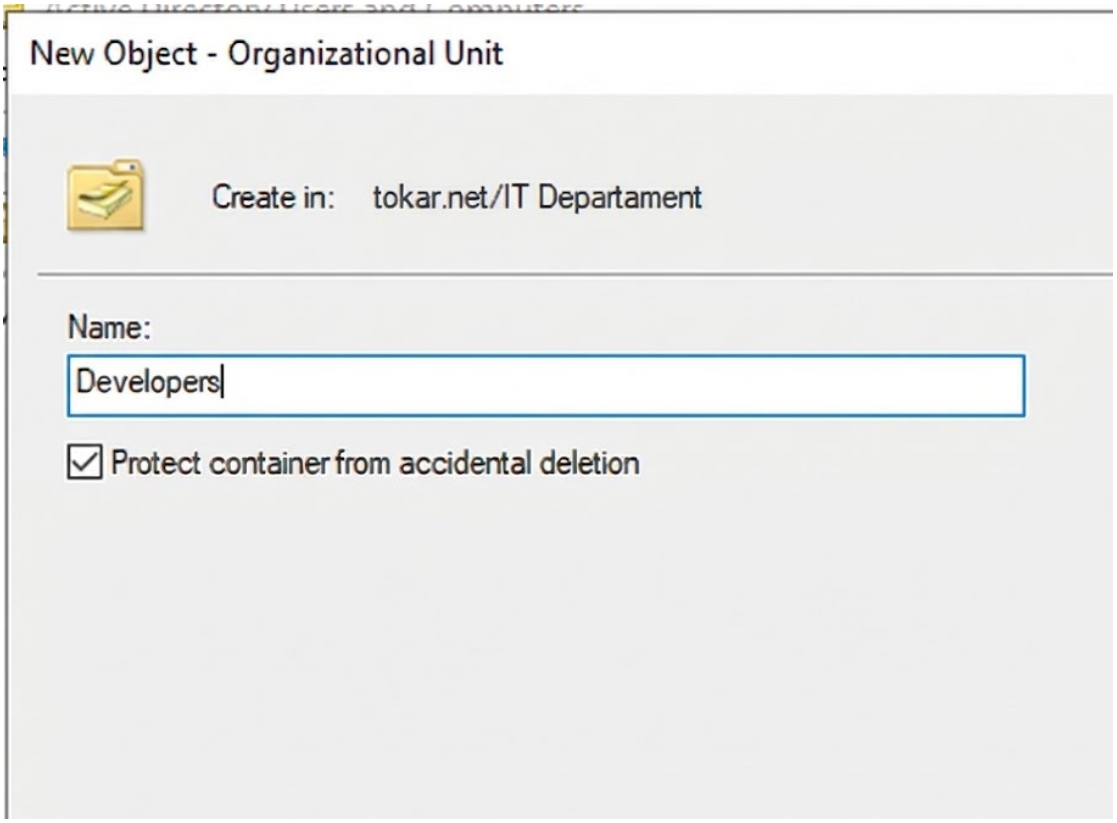


Рисунок 3.18 – Побудова багаторівневої ієрархії вкладених підрозділів

Після затвердження структури контейнерів здійснюється наповнення каталогу об'єктами користувачів. Процедура створення облікового запису включає введення персональних даних співробітника (ім'я, прізвище) та генерацію унікального імені входу (User Principal Name). Критичним аспектом є налаштування первинних параметрів безпеки: встановлення тимчасового пароля та активація вимоги його обов'язкової зміни при першому вході в систему. Це гарантує, що лише сам користувач знатиме свій постійний пароль. Інтерфейс створення користувача продемонстровано на рис. 3.19.

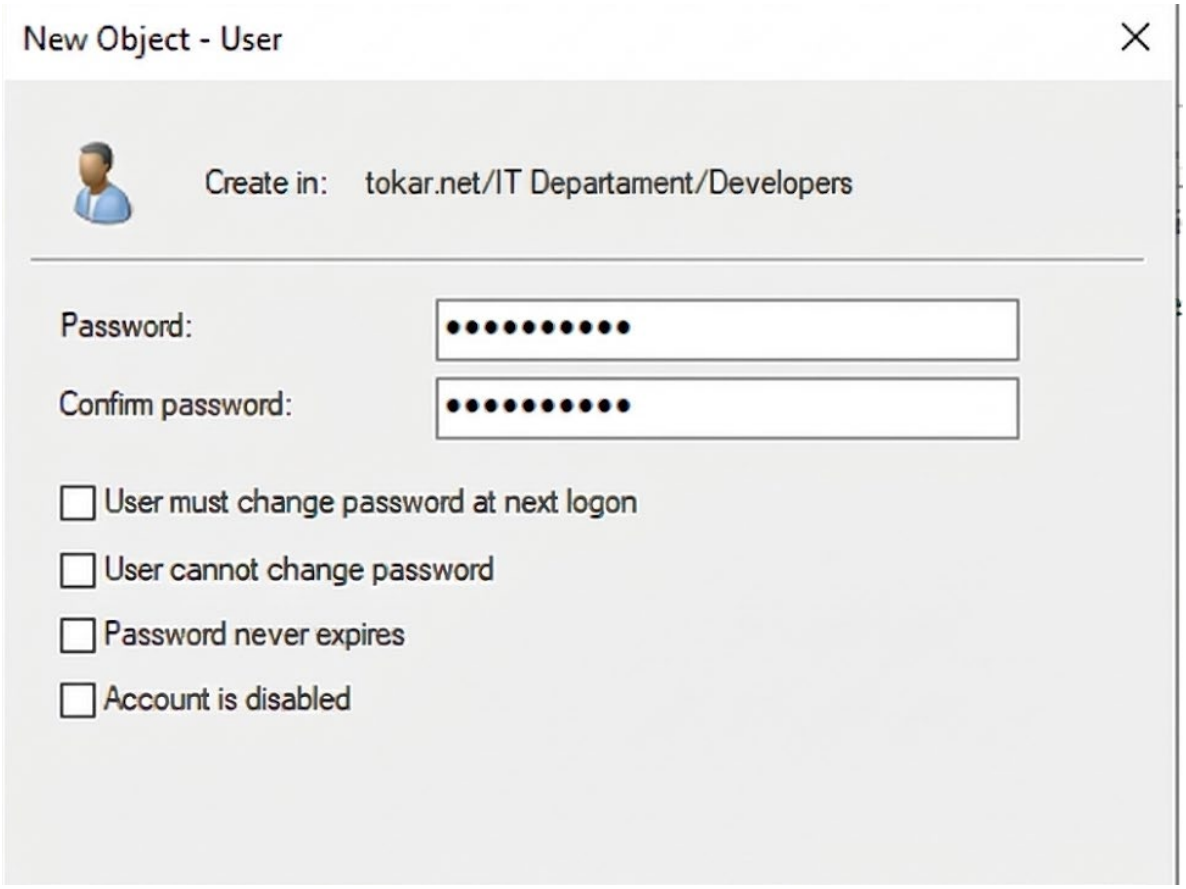


Рисунок 3.19 – Процес реєстрації нового облікового запису користувача в системі

Фінальним етапом тестування є перевірка можливості авторизації створених користувачів на клієнтських робочих місцях. Для цього на робочій станції, попередньо введеній у домен, виконується вихід із поточної сесії адміністратора та здійснюється спроба входу під новим обліковим записом. Успішна авторизація, завантаження профілю користувача та застосування відповідних прав доступу свідчать про коректне функціонування служби аутентифікації Kerberos та правильність налаштування DNS-записів, які забезпечують пошук контролера домену, рис. 3.20.

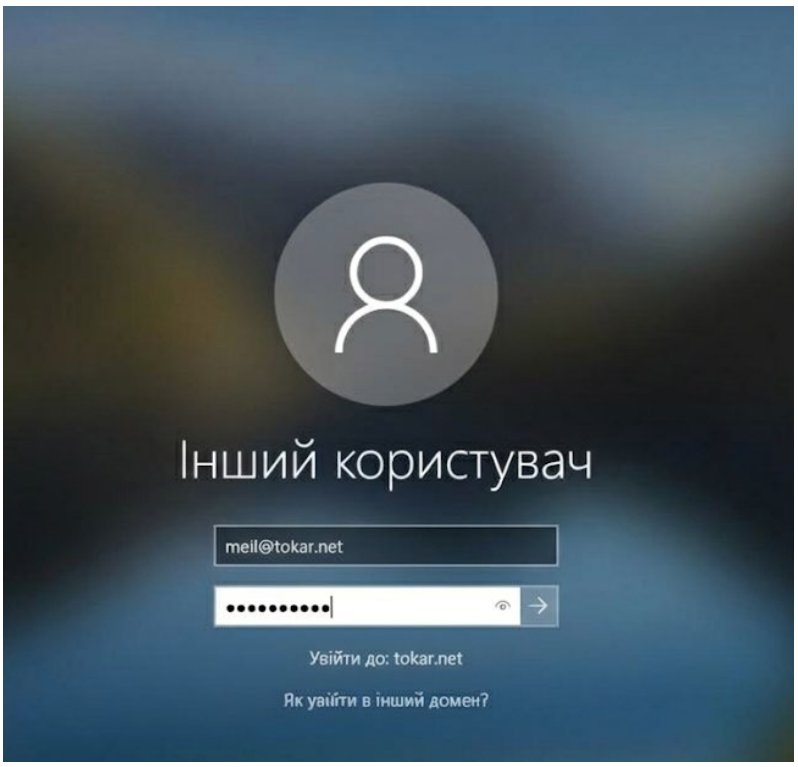


Рисунок 3.20 – Успішна авторизація користувача в доменному середовищі

ВИСНОВКИ

У магістерській кваліфікаційній роботі вирішено актуальне науково-прикладне завдання щодо проектування та імплементації захищеного інформаційного середовища підприємства, яке базується на централізованому управлінні та ешелонованому захисті.

Основні результати роботи полягають у наступному:

1. Систематизовано підходи до організації IT-інфраструктури. Визначено, що гібридні моделі, які поєднують локальні сервери та хмарні технології, забезпечують оптимальний баланс між безпекою та гнучкістю.

2. Проаналізовано роль Active Directory в системі кібербезпеки. Показано, що використання групових політик та багатофакторної автентифікації є критично необхідним для протидії атакам на ідентифікацію, таким як Password Spraying та Pass-the-Hash.

3. Досліджено вразливості стеку протоколів TCP/IP та DNS. Визначено методи протидії атакам типу Spoofing та Man-in-the-Middle шляхом сегментації мережі, шифрування каналів та моніторингу трафіку.

4. Обґрунтовано вибір апаратної платформи. Для рівня ядра обрано маршрутизатори Cisco 7600, що забезпечують високу продуктивність маршрутизації, а для рівня доступу — комутатори Cisco Catalyst 2960 з функціями безпеки на рівні портів.

5. Розроблено та реалізовано ієрархічну трирівневу топологію мережі. Впровадження протоколу OSPF забезпечило швидку конвергенцію мережі та надійність каналів зв'язку між підмережами.

6. Здійснено практичне розгортання відмовостійкої структури служби каталогів. Встановлено первинний та резервний контролери домену, налаштовано реплікацію бази даних Active Directory, створено організаційну структуру та облікові записи користувачів.

7. Проведено верифікацію системи захисту. Тестування підтвердило успішну авторизацію клієнтських станцій у домені, коректність застосування політик безпеки та стабільність роботи мережевої інфраструктури під управлінням розробленої системи.

Розроблена система створює надійну основу для функціонування сучасного підприємства, забезпечуючи конфіденційність, цілісність та доступність корпоративних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. W. Stallings. "Cryptography and Network Security: Principles and Practice." Pearson Education, 7th Edition (2017): 15-45. https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000003254.

2. P. Mell et al. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Special Publication 800-145 (2011): 1-7. https://doi.org/10.6028/NIST.SP.800-145.

3. J. F. Kurose et al. "Computer Networking: A Top-Down Approach." Pearson, 8th Edition (2021): 350-420. https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000003260.

4. M. Arregoces et al. "Data Center Fundamentals." Cisco Press (2003): 105-160. https://www.ciscopress.com/store/data-center-fundamentals-9781587050239.

5. T. Davenport. "Mission Critical: Realizing the Promise of Enterprise Systems." Harvard Business Review Press (2000): 23-56. https://store.hbr.org/product/mission-critical-realizing-the-promise-of-enterprise-systems/2596.

6. T. Erl et al. "Cloud Computing: Concepts, Technology & Architecture." Prentice Hall (2013): 89-124. https://www.pearson.com/en-us/subject-catalog/p/cloud-computing-concepts-technology--architecture/P200000003248.

7. J. Moy. "OSPF: Anatomy of an Internet Routing Protocol." Addison-Wesley Professional (1998): 45-98. https://www.informit.com/store/ospf-anatomy-of-an-internet-routing-protocol-9780201634723.

8. M. E. Whitman et al. "Principles of Information Security." Cengage Learning, 6th Edition (2018): 215-260. https://www.cengage.com/c/principles-of-information-security-7e-whitman/9780357506431/.

9. B. Desmond et al. "Active Directory." O'Reilly Media, 5th Edition (2013): 10-150. https://www.oreilly.com/library/view/active-directory-5th/9781449361213/.

10. P. Albitz et al. "DNS and BIND." O'Reilly Media, 5th Edition (2006): 15-60. https://www.oreilly.com/library/view/dns-and-bind/0596100574/.

11. S. Metcalf. "Active Directory Security: Attack Vectors and Defense Strategies." 2018 IEEE International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (2018): 1-8. https://doi.org/10.1109/CyberSec.2018.8482891.

12. M. Souppaya et al. "Guide to Enterprise Patch Management Technologies." National Institute of Standards and Technology, Special Publication 800-40r3 (2013): 1-15. https://doi.org/10.6028/NIST.SP.800-40r3.

13. J. Moskowitz. "Group Policy: Fundamentals, Security, and the Managed Desktop." Sybex, 3rd Edition (2015): 45-120. https://www.wiley.com/en-us/Group+Policy%3A+Fundamentals%2C+Security%2C+and+the+Managed+Desktop%2C+3rd+Edition-p-9781119035574.

14. W. C. Preston. "Backup & Recovery: Inexpensive Backup Solutions for Open Systems." O'Reilly Media (2007): 25-50. https://www.oreilly.com/library/view/backup-recovery/0596102461/.

15. J. Mirkovic et al. "Internet Denial of Service: Attack and Defense Mechanisms." Prentice Hall (2004): 10-45. https://www.pearson.com/en-us/subject-catalog/p/internet-denial-of-service-attack-and-defense-mechanisms/P200000003258.

16. E. O. Kizza. "Guide to Computer Network Security." Springer, 5th Edition (2020): 331-356. https://doi.org/10.1007/978-3-030-38141-7.

17. E. Rescorla. "SSL and TLS: Designing and Building Secure Systems." Addison-Wesley Professional (2000): 50-90. https://www.informit.com/store/ssl-and-tls-designing-and-building-secure-systems-9780201615982.

18. M. Gouda et al. "Formal Specification and Verification of the OSPF Protocol." IEEE/ACM Transactions on Networking, 29 (2021): 112-125. https://doi.org/10.1109/TNET.2021.3051234.

19. Cisco Systems. "Cisco 7600 Series Router Deployment Guide." Cisco White Paper (2019): 1-50. https://www.cisco.com/c/en/us/products/routers/7600-series-routers/index.html.R. Padilla et al. "A Survey on Performance Metrics for Object-Detection Algorithms." 2020 International Conference on Systems, Signals and Image Processing (IWSSIP) (2020): 237-242. https://doi.org/10.1109/iwssip48289.2020.9145130.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)